SNI

Standar Nasional Indonesia

SNI IEC/ISO 31010:2016

Manajemen risiko – Teknik penilaian risiko

Risk management – Risk assessment techniques

(IEC/ISO 31010:2009, IDT)

ICS 03.100.001

Badan Standardisasi Nasional

Daftar isi

Prakata

Standar Nasional Indonesia (SNI) IEC/ISO 31010:2016 dengan judul *Manajemen risiko – Teknik penilaian risiko*, merupakan adopsi identik dari IEC ISO 31010:2009, *Risk management – Risk assessment techniques,* dengan metode terjemahan dua bahasa (*bilingual*), untuk menggantikan SNI IEC/ISO 31010:2016 hasil adopsi dengan metode republikasi-*reprint*.

Standar ini disusun oleh Komite Teknis 03-10, *Manajemen Risiko*. Standar ini telah dibahas dan disetujui dalam rapat konsensus nasional di Jakarta pada tanggal 7 September 2017. Konsensus ini dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah.

Standar ini merupakan bagian dari seri SNI ISO 31000, *Manajemen risiko,* yang terdiri dari 4 standar yaitu:

- SNI ISO 31000:2011, *Manajemen risiko – Prinsip dan pedoman;*
- SNI ISO Guide 73:2016, *Manajemen risiko – Kosakata;*
- SNI ISO/TR 31004:2016, *Manajemen risiko – Panduan untuk implementasi SNI ISO 31000;* dan
- SNI IEC/ISO 31010:2016 *Manajemen risiko – Teknik penilaian risiko.*

Dalam Standar ini, istilah ”*this International Standard*” diganti menjadi ”*this Standard*” dan diterjemahkan menjadi ”Standar ini”.

Terdapat Standar ISO yang diacu di acuan normatif dalam Standar ini telah diadopsi menjadi Standar Nasional Indonesia (SNI), yaitu:

1) ISO Guide 73:2009, *Risk management - Vocabulary,* telah diadopsi secara identik menjadi SNI ISO Guide 73:2016, *Manajemen risiko - Kosakata.*

2) ISO 31000:2009, *Risk management — Principles and guidelines,* telah diadopsi secara identik menjadi SNI ISO 31000:2011, *Manajemen risiko — Prinsip dan pedoman.*

Standar ini telah melalui tahap jajak pendapat pada tanggal 25 September 2017 sampai dengan 25 Oktober 2017, dengan hasil akhir disetujui menjadi SNI.

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari dokumen standar ini dapat berupa hak paten. Badan Standardisasi Nasional tidak bertanggung jawab untuk pengidentifikasian salah satu atau seluruh hak paten yang ada.

Apabila pengguna menemukan keraguan dalam Standar ini, maka disarankan untuk melihat standar aslinya yaitu IEC/ISO 31010:2009 dan/atau dokumen terkait lain yang menyertai.

Pendahuluan

Semua jenis dan ukuran organisasi menghadapi berbagai risiko yang mempengaruhi pencapaian sasaran mereka.

Sasaran tersebut dapat terkait dengan berbagai kegiatan organisasi, dari inisiatif strategik hingga pada operasi, proses dan proyek, serta tercermin dalam hal terkait sosial, lingkungan, manfaat-keluaran keselamatan dan keamanan, ukuran komersial, finansial, dan ekonomi, dan juga dampak sosial, budaya, politik dan reputasi.

Semua kegiatan dari organisasi yang melibatkan risiko sebaiknya dikelola. Proses manajemen risiko membantu pembuatan keputusan dengan memperhitungkan ketidakpastian dan kemungkinan dari kejadian masa depan atau keadaan (disengaja maupun tidak) serta efek keputusan tersebut pada sasaran yang telah disepakati.

Manajemen risiko mencakupi penerapan metode logis dan sistematis untuk :
- pengomunikasian dan pengonsultasian di sepanjang proses ini;
- penetapan konteks untuk pengidentifikasian, penganalisisan, pengevaluasian, perlakuan risiko yang terkait dengan setiap aktivitas, proses, fungsi atau produk;
- pemantauan dan peninjauan risiko;
- pelaporan dan perekaman suatu hasil secara tepat.

Penilaian risiko adalah bagian dari manajemen risiko yang menyediakan suatu proses terstruktur yang mengidentifikasi bagaimana sasaran mungkin akan dipengaruhi, dan analisis risiko dalam hal konsekuensi dan probabilitasnya sebelum pengambilan keputusan apakah diperlukan perlakuan lebih lanjut.

Penilaian risiko berupaya untuk menjawab pertanyaan-pertanyaan mendasar berikut ini:
- apa yang dapat terjadi dan mengapa (berdasarkan identifikasi risiko)?
- apa konsekuensinya?
- apa probabilitas dari peristiwa tersebut di masa depan?
- apakah ada faktor yang memitigasikan konsekuensi risiko atau yang mengurangi probabilitas risiko?
-

Apakah tingkat risiko masih dapat ditolerir atau diterima dan apakah membutuhkan perlakuan lebih lanjut? Standar ini dimaksudkan untuk mencerminkan praktik yang baik saat ini dalam pemilihan dan pendayagunaan teknik penilaian risiko, dan tidak mengacu pada konsep baru atau yang terus berkembang yang belum mencapai suatu tingkat konsensus profesional yang memuaskan.

Standar ini bersifat umum, sehingga dapat memberikan panduan di banyak industri dan jenis sistem. Mungkin terdapat standar yang lebih spesifik keberadaannya di suatu industri yang menetapkan metodologi dan tingkat penilaian yang disukai untuk aplikasi tertentu. Jika standar tersebut selaras dengan standar ini, standar spesifik umumnya akan memadai.

Manajemen risiko – Teknik penilaian risiko

1 Ruang lingkup

Standar ini merupakan standar pendukung untuk SNI ISO 31000 dan menyediakan panduan pada pemilihan dan penerapan teknik sistematis untuk penilaian risiko.

Penilaian risiko yang dilakukan sesuai dengan standar ini memberikan kontribusi untuk kegiatan manajemen risiko lainnya.

Penerapan berbagai teknik diperkenalkan, dengan referensi spesifik pada standar internasional lain di mana konsep dan teknik penerapan dijelaskan secara lebih rinci.

Standar ini tidak dimaksudkan untuk sertifikasi, regulasi atau penggunaan untuk kontraktual.

Standar ini tidak menyediakan kriteria spesifik untuk pengidentifikasian kebutuhan analisis risiko, maupun menspesifikasikan jenis metode analisis risiko yang diperlukan untuk penerapan tertentu.

Standar ini tidak mengacu pada semua teknik, dan pengabaian suatu teknik dari standar ini bukan berarti tidak sah. Fakta bahwa suatu metode dapat diterapkan pada keadaan tertentu bukan berarti bahwa metode tersebut sebaiknya perlu diterapkan.

CATATAN Standar ini tidak secara khusus menangani keselamatan. Ini adalah suatu standar manajemen risiko generik dan setiap referensi untuk keselamatan adalah murni bersifat informatif. Panduan pada pengenalan aspek keselamatan ke dalam standar IEC ditetapkan dalam ISO/IEC Guide 51.

2 Acuan normatif

Dokumen yang menjadi acuan berikut ini sangat diperlukan untuk penerapan dokumen ini. Untuk acuan bertanggal, yang berlaku hanya edisi terkutip. Untuk acuan tidak bertanggal, yang berlaku edisi terakhir dari dokumen (termasuk amandemen).

ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*

ISO 31000, *Risk management – Principles and guidelines*

3 Istilah dan definisi

Untuk tujuan penggunaan dokumen ini, berlaku istilah dan definisi dari SNI ISO Guide 73.

4 Konsep penilaian risiko

4.1 Tujuan dan manfaat

Tujuan dari penilaian risiko adalah untuk menyediakan informasi berbasis bukti dan analisis untuk membuat keputusan berdasarkan informasi yang dianggap cukup tentang bagaimana memperlakukan risiko tertentu dan bagaimana memilih di antara opsi.

Beberapa manfaat utama pelaksanaan penilaian risiko meliputi:
- pemahaman risiko dan dampak potensialnya pada sasaran;
- penyediaan informasi bagi pengambil keputusan;
- memberikan kontribusi terhadap pemahaman risiko, dalam rangka untuk membantu dalam pemilihan opsi perlakuan;
- pengidentifikasian kontributor penting risiko dan tautan yang lemah dalam sistem dan organisasi;
- pembandingan risiko dalam sistem alternatif, teknologi atau pendekatan;
- pengomunikasian risiko dan ketidakpastian;
- membantu dengan penetapan prioritas;
- memberikan kontribusi terhadap pencegahan insiden berdasarkan investigasi paska insiden;
- pemilihan berbagai bentuk perlakuan resiko;
- pemenuhan persyaratan peraturan;
- penyediaan informasi yang akan membantu mengevaluasi apakah risiko sebaiknya diterima saat diperbandingkan dengan kriteria yang telah ditetapkan;
- penilaian risiko bagi limbah akhir.

4.2 Manajemen risiko dan kerangka kerja manajemen risiko

Standar ini mengasumsikan bahwa penilaian risiko dilakukan dalam kerangka kerja dan proses manajemen risiko yang dijelaskan dalam SNI ISO 31000.

Suatu kerangka kerja manajemen risiko menyediakan kebijakan, prosedur dan pengaturan organisasi yang akan melekatkan manajemen risiko di seluruh organisasi di semua tingkatan.

Sebagai bagian dari kerangka kerja ini, organisasi sebaiknya memiliki kebijakan atau strategi guna memutuskan kapan dan bagaimana risiko sebaiknya dinilai.

Secara khusus, mereka yang melaksanakan penilaian risiko sebaiknya paham tentang:
- konteks dan sasaran organisasi,
- tingkat dan jenis risiko yang ditoleransi, dan bagaimana risiko yang tidak dapat diterima harus diperlakukan,
- bagaimana penilaian risiko terintegrasi ke dalam proses organisasi,
- metode dan teknik yang akan digunakan untuk penilaian risiko, dan kontribusi mereka terhadap proses manajemen risiko,
- akuntabilitas, tanggung jawab dan wewenang untuk melakukan penilaian risiko,
- sumber daya yang tersedia untuk melaksanakan penilaian risiko,
- bagaimana penilaian risiko akan dilaporkan dan ditinjau.

4.3 Penilaian risiko dan proses manajemen risiko

4.3.1 Umum

Penilaian risiko terdiri dari elemen-elemen inti dari proses manajemen risiko yang didefinisikan dalam SNI ISO 31000 dan mengandung elemen-elemen berikut:
- komunikasi dan konsultasi;
- penetapan konteks;
- penilaian risiko (terdiri dari identifikasi risiko, analisis risiko and evaluasi risiko);
- perlakuan risiko;
- pemantauan dan tinjauan.

Penilaian risiko bukanlah kegiatan yang berdiri sendiri dan sebaiknya diintegrasikan sepenuhnya ke dalam komponen-komponen lain dalam proses manajemen risiko.

4.3.2 Komunikasi dan konsultasi

Penilaian risiko yang sukses tergantung pada komunikasi dan konsultasi dengan para pemangku kepentingan yang efektif.

Pelibatan para pemangku kepentingan dalam proses manajemen risiko akan membantu dalam:
- pengembangan suatu rencana komunikasi,
- pendefinisian konteks secara tepat,
- pemastian bahwa keinginan para pemangku kepentingan dipahami dan dipertimbangkan,
- membawa serta bersama berbagai bidang keahlian untuk pengidentifikasian dan penganalisaan risiko,
- pemastian bahwa pandangan yang berbeda-beda dipertimbangkan secara tepat dalam pengevaluasian risiko,
- pemastian bahwa risiko teridentifikasi secara cukup,
- pemastian pengesahan dan dukungan untuk rencana perlakuan.

Para pemangku kepentingan sebaiknya berkontribusi dalam penghubungan proses penilaian risiko dengan disiplin ilmu manajemen lainnya, termasuk manajemen perubahan, manajemen proyek dan program, dan juga manajemen keuangan.

4.3.3 Penetapan suatu konteks

Penetapan suatu konteks mendefinisikan parameter dasar untuk pengelolaan risiko dan mengatur ruang lingkup dan kriteria untuk proses yang tersisa. Penetapan konteks mencakup pertimbangan parameter internal dan eksternal yang relevan dengan organisasi secara keseluruhan, serta latar belakang risiko tertentu yang sedang dinilai.

Dalam penetapan suatu konteks, sasaran manajemen risiko, kriteria risiko, dan program penilaian risiko ditentukan dan disepakati.

Untuk suatu penilaian risiko spesifik, penetapan konteks sebaiknya mencakupi definisi dari konteks eksternal, internal dan manajemen risiko serta klasifikasi kriteria risiko:

a) Penetapan konteks eksternal melibatkan pengenalan dengan lingkungan di mana organisasi dan sistem beroperasi termasuk:
   - budaya, politik, hukum, peraturan, keuangan, ekonomi dan faktor lingkungan kompetitif, baik internasional, nasional, regional atau lokal;
   - pendorong utama dan tren memiliki dampak pada sasaran organisasi; dan
   - persepsi dan nilai-nilai dari para pemangku kepentingan eksternal.

b) Penetapan konteks internal melibatkan pemahaman
   - kemampuan organisasi dalam hal sumber daya dan pengetahuan,
   - arus informasi dan proses pengambilan keputusan,
   - para pemangku kepentingan internal,
   - sasaran dan strategi yang ada untuk dicapai,
   - persepsi, nilai dan budaya,
   - kebijakan dan proses,
   - standar dan model acuan yang diadopsi oleh organisasi, dan
   - struktur (misalnya tata kelola, peran dan akuntabilitas).

c) Penetapan konteks proses manajemen risiko meliputi:
- pendefinisian akuntabilitas dan tanggung jawab,
- pendefinisian sejauh mana kegiatan manajemen risiko yang akan dilakukan, termasuk spesifik yang dicantumkan dan yang dikecualikan,
- pendefinisian sejauh mana proyek, proses, fungsi atau kegiatan dalam hal waktu dan lokasi,
- pendefinisian hubungan antara suatu proyek atau kegiatan tertentu dengan proyek atau kegiatan organisasi lainnya,
- pendefinisian metodologi penilaian risiko,
- pendefinisian kriteria risiko,
- pendefinisian bagaimana kinerja manajemen risiko dievaluasi,
- pengidentifikasian dan penentuan keputusan dan tindakan yang harus dibuat, dan
- pengidentifikasian ruang lingkup atau penyusunan studi yang dibutuhkan, luasan, sasaran dan sumber daya yang diperlukan untuk studi tersebut.

d) Pendefinisian kriteria risiko melibatkan penentuan:
- sifat dan jenis konsekuensi yang harus dimasukkan dan bagaimana hal tersebut akan diukur,
- cara bagaimana probabilitas harus diungkapkan,
- bagaimana suatu tingkat risiko akan ditentukan,
- bagaimana kriteria akan diputuskan saat risiko membutuhkan perlakuan,
- kriteria penentuan kapan risiko dapat diterima dan/atau ditoleransi,
- apa dan bagaimana kombinasi dari risiko akan diperhitungkan. Kriteria dapat didasarkan pada sumber seperti
- sasaran proses yang disepakati,
- kriteria yang diidentifikasi dalam spesifikasi,
- sumber data umum,
- kriteria industri yang umumnya diterima seperti tingkat integritas keselamatan,
- selera risiko organisasi,
- hukum dan persyaratan lainnya untuk spesifik perangkat atau penerapan.

4.3.4 Penilaian risiko

Penilaian risiko adalah keseluruhan proses identifikasi risiko, analisis risiko dan evaluasi risiko.

Risiko dapat dinilai pada tingkatan organisasi, pada tingkatan departemen, untuk proyek-proyek, kegiatan individu atau risiko tertentu. Alat bantu dan teknik yang berbeda mungkin sesuai di konteks yang berbeda.

Penilaian risiko memberikan suatu pemahaman tentang risiko, penyebab risiko, konsekuensi dan probabilitas risiko. Ini memberikan masukan untuk keputusan tentang:
- apakah suatu kegiatan sebaiknya dilakukan;
- bagaimana memaksimalkan kesempatan;
- apakah perlakuan risiko diperlukan;
- memilih diantara pilihan dengan risiko yang berbeda;
- memprioritaskan pilihan perlakuan risiko;
- pemilihan strategi perlakuan risiko paling tepat yang akan membawa risiko tidak diharapkan ke tingkat yang ditoleransi.

4.3.5 Perlakuan risiko

Setelah suatu penilaian risiko diselesaikan, perlakuan risiko melibatkan pemilihan dan persetujuan satu atau lebih pilihan yang relevan guna pengubahan probabilitas kejadian, efek dari risiko, atau keduanya, dan penerapan opsi-opsi tersebut.

Hal ini diikuti dengan suatu proses siklus penilaian kembali tingkatan baru dari risiko, dengan maksud untuk penentuan tolerabilitasnya terhadap kriteria yang telah ditetapkan sebelumnya, dalam rangka untuk memutuskan apakah perlakuan lebih lanjut diperlukan.

4.3.6 Pemantauan dan tinjauan

Sebagai bagian dari proses manajemen risiko, risiko dan pengendalian sebaiknya dipantau serta ditinjau secara teratur untuk memverifikasi bahwa

- asumsi tentang risiko tetap berlaku;
- asumsi di mana penilaian risiko didasarkan, termasuk konteks eksternal dan internal, tetap berlaku;
- hasil yang diharapkan telah dicapai;
- hasil penilaian risiko sejalan dengan pengalaman aktual;
- teknik penilaian risiko sedang diterapkan secara tepat;
- perlakuan risiko adalah efektif.

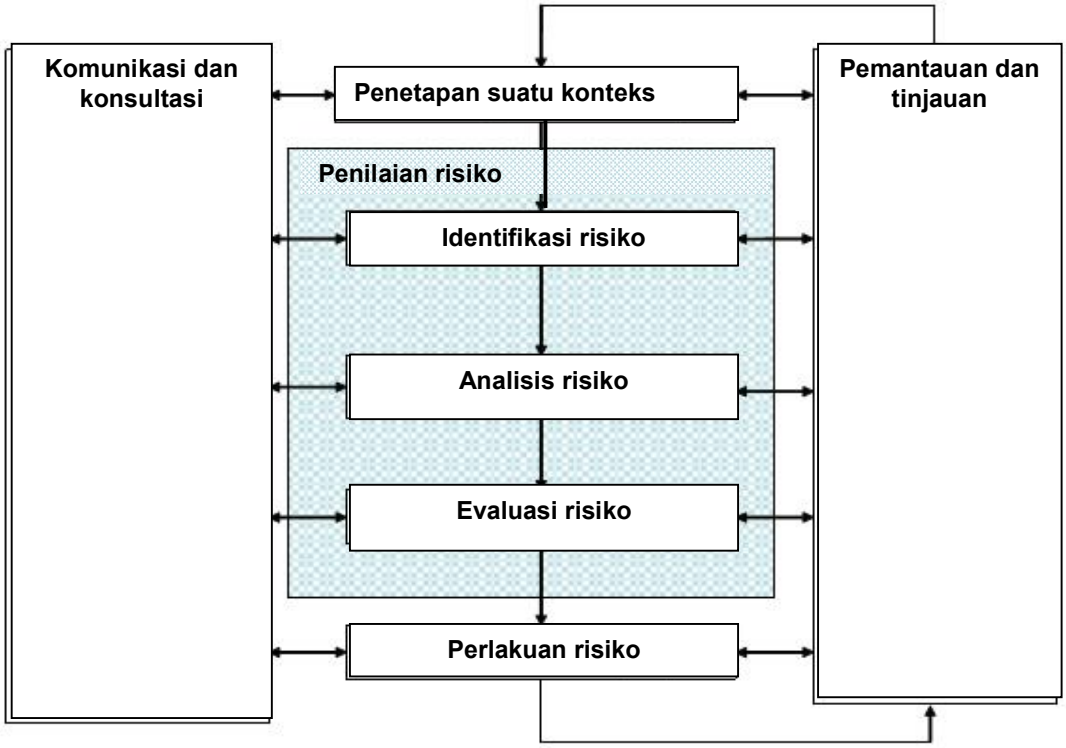
Akuntabilitas untuk pemantauan dan tinjauan kinerja sebaiknya ditetapkan.

5 Proses penilaian risiko

5.1 Tinjauan singkat

Penilaian risiko menyediakan para pengambil keputusan dan para pihak yang bertanggung jawab dengan suatu pemahaman risiko lebih baik yang dapat mempengaruhi pencapaian sasaran, dan kecukupan serta efektivitas pengendalian yang sudah ada. Hal ini menyediakan suatu dasar untuk keputusan tentang pendekatan yang paling tepat untuk digunakan memperlakukan risiko. Keluaran dari penilaian risiko merupakan masukan untuk proses pengambilan keputusan organisasi.

Penilaian risiko adalah proses keseluruhan identifikasi risiko, analisis risiko dan evaluasi risiko (lihat Gambar 1). Cara di mana proses ini diterapkan tergantung tidak hanya pada konteks proses manajemen risiko tetapi juga pada metode dan teknik yang digunakan untuk melakukan penilaian risiko.



Gambar 1 – Kontribusi penilaian risiko untuk proses manajemen risiko

Penilaian risiko mungkin memerlukan suatu pendekatan multidisiplin karena risiko dapat mencakup berbagai sebab dan konsekuensi.

5.2 Identifikasi risiko

Identifikasi risiko adalah proses penemuan, pengenalan dan perekaman risiko.

Tujuan dari identifikasi risiko adalah untuk mengidentifikasi apa yang mungkin terjadi atau situasi apa mungkin ada yang mungkin mempengaruhi pencapaian sasaran dari sistem atau organisasi. Setelah risiko diidentifikasi, organisasi sebaiknya mengidentifikasi setiap pengendalian yang ada seperti fitur rancangan, orang, proses dan sistem.

Proses identifikasi risiko mencakup pengidentifikasian penyebab dan sumber risiko (potensi bahaya dalam konteks kerusakan fisik), kejadian, situasi atau keadaan yang bisa memiliki dampak material pada sasaran dan sifat dampak itu.

Metode identifikasi risiko dapat mencakupi:
- metode berbasis bukti, contohnya daftar periksa dan tinjauan dari data historis;
- pendekatan tim yang sistematis di mana tim ahli mengikuti suatu proses sistematis untuk mengidentifikasi risiko dengan sarana suatu himpunan terstruktur dari gegasan atau pertanyaan;
- teknik penalaran induktif seperti HAZOP.

Berbagai teknik pendukung dapat digunakan untuk meningkatkan akurasi dan kelengkapan dalam identifikasi risiko, termasuk curah pendapat, dan metodologi Delphi.

Terlepas dari teknik yang sebenarnya dikerjakan, adalah penting bahwa pengakuan diberikan untuk faktor manusia dan organisasi ketika pengidentifikasian risiko. Oleh karena itu, penyimpangan dari yang diharapkan atas faktor manusia dan organisasi sebaiknya disertakan dalam proses identifikasi risiko begitu pula "perangkat keras" atau "perangkat lunak" kejadian.

5.3 Analisis risiko

5.3.1 Umum

Analisis risiko adalah tentang pengembangan suatu pemahaman tentang risiko. Hal ini memberikan masukan untuk penilaian risiko dan keputusan tentang apakah risiko perlu diberi perlakuan dan tentang strategi dan metode perlakuan yang paling tepat.

Analisis risiko terdiri dari penentuan konsekuensi dan probabilitasnya untuk mengidentifikasi kejadian risiko, dengan memperhitungkan keberadaan (atau ketidakberadaan) dan efektivitas dari setiap pengendalian yang ada. Konsekuensi dan probabilitas risiko tersebut kemudian dikombinasikan untuk menentukan tingkat risiko.

Analisis risiko melibatkan pertimbangan penyebab dan sumber risiko, konsekuensinya dan probabilitas risiko yang konsekuensinya dapat terjadi. Faktor-faktor yang mempengaruhi konsekuensi dan probabilitas sebaiknya diidentifikasi. Suatu kejadian dapat memiliki konsekuensi berganda dan dapat mempengaruhi beberapa sasaran. Pengendalian risiko yang ada dan efektivitas pengendalian tersebut harus diperhitungkan. Berbagai metode untuk analisis ini dijelaskan dalam Lampiran B. Lebih dari satu teknik mungkin diperlukan untuk aplikasi yang kompleks.

Analisis risiko biasanya mencakupi kisaran estimasi rentang konsekuensi potensial yang mungkin timbul dari suatu kejadian, situasi atau keadaan, dan probabilitas yang terkait, dalam rangka untuk mengukur tingkat risiko. Namun dalam beberapa hal, di mana konsekuensi cenderung tidak signifikan, atau probabilitas diharapkan menjadi sangat rendah, suatu perkiraan parameter tunggal mungkin cukup untuk sebuah keputusan yang akan dibuat.

Dalam beberapa keadaan, konsekuensi dapat terjadi sebagai akibat dari suatu kisaran kejadian atau kondisi yang berbeda, atau di mana kejadian tertentu tidak terdentifikasi. Dalam kasus ini, fokus dari penilaian risiko adalah pada penganalisaan kepentingan dan kerentanan komponen sistemnya dengan maksud untuk pendefinisian perlakuan yang berhubungan dengan tingkat strategi perlindungan atau pemulihan.

Metode yang digunakan dalam penganalisaan risiko dapat berupa kualitatif, semi-kuantitatif atau kuantitatif. Tingkat kerincian yang diperlukan akan tergantung pada aplikasi tertentu, ketersediaan data yang dapat dipercaya dan kebutuhan pengambilan keputusan organisasi. Beberapa metode dan tingkat kerincian dari analisis dapat dipersyaratkan oleh peraturan perundangan.

Penilaian kualitatif mendefinisikan konsekuensi, probabilitas dan tingkat risiko dengan tingkat signifikansi seperti "tinggi", "menengah" dan "rendah", dapat juga menggabungkan konsekuensi dan probabilitas, serta mengevaluasi tingkat risiko yang dihasilkan terhadap kriteria kualitatif.

Metode semi-kuantitatif menggunakan skala penilaian numerik untuk konsekuensi dan probabilitas serta menggabungkan hal tersebut untuk menghasilkan suatu tingkat risiko menggunakan suatu formula. Skala dapat linear atau logaritmik, atau memiliki beberapa hubungan lainnya; formula yang digunakan juga bisa bervariasi.

Analisis kuantitatif memperkirakan nilai praktis untuk konsekuensi dan probabilitasnya, serta menghasilkan nilai tingkat risiko dalam unit spesifik yang didefinisikan ketika pengembangan konteks. Analisis kuantitatif penuh mungkin tidak selalu memungkinkan atau diinginkan karena ketidakcukupan informasi tentang sistem atau kegiatan yang sedang dianalisis, kurangnya data, pengaruh faktor manusia, dll atau karena upaya analisis kuantitatif tidak dibenarkan atau tidak diperlukan. Dalam keadaan seperti itu, komparatif peringkat semi-kuantitatif atau kualitatif risiko oleh spesialis, yang berpengetahuan di bidang masing-masing, mungkin masih efektif.

Dalam kasus di mana analisis adalah kualitatif, sebaiknya ada suatu penjelasan tentang semua persyaratan yang digunakan dan dasar untuk semua kriteria harus direkam.

Bahkan di mana kuantifikasi penuh telah dilakukan, perlu dikenali bahwa tingkat risiko yang dihitung merupakan perkiraan. Perhatian sebaiknya diambil untuk memastikan bahwa kuantifikasi tidak dikaitkan suatu tingkat akurasi serta presisi tidak konsisten dengan akurasi data dan metode yang digunakan.

Tingkat risiko sebaiknya dinyatakan dalam istilah yang paling sesuai untuk jenis risiko dan dalam bentuk yang membantu evaluasi risiko. Dalam beberapa hal, besarnya suatu risiko dapat dinyatakan sebagai distribusi probabilitas atas suatu kisaran berbagai konsekuensi.

5.3.2 Pengendalian penilaian

Tingkat risiko akan tergantung pada kecukupan dan efektivitas pengendalian yang ada. Pertanyaan yang harus ditujukan meliputi:

- apa pengendalian yang ada untuk suatu risiko tertentu?
- apakah pengendalian tersebut mampu mencukupi dalam perlakuan risiko sehingga risiko terkendalikan ke tingkat yang ditoleransi?
- dalam prakteknya, apakah pengoperasian pengendalian sesuai dengan tata cara yang dimaksudkan dan pengendalian dapat didemonstrasikan secara efektif bila diperlukan?

Pertanyaan-pertanyaan ini hanya dapat dijawab dengan yakin jika ada dokumentasi dan jaminan proses yang tepat.

Tingkat efektivitas untuk pengendalian tertentu, atau kesesuaian pengendalian terkait, dapat dinyatakan secara kualitatif, semi-kuantitatif atau kuantitatif. Dalam kebanyakan kasus, tingkat akurasi yang tinggi tidak dibenarkan. Namun, mungkin berharga untuk mengekspresikan dan merekam ukuran efektivitas pengendalian risiko sehingga penilaian dapat dibuat pada apakah upaya terbaik dicurahkan dalam peningkatan pengendalian atau pemberian perlakuan risiko yang berbeda.

5.3.3 Analisis konsekuensi

Analisis konsekuensi menentukan sifat dan jenis dampak yang dapat terjadi dengan asumsi bahwa situasi kejadian tertentu atau keadaan telah terjadi. Sebuah kejadian mungkin memiliki kisaran besaran dampak yang berbeda, dan mempengaruhi berbagai sasaran yang berbeda serta pemangku kepentingan yang berbeda. Jenis konsekuensi yang akan dianalisis dan pemangku kepentingan yang dipengaruhi telah diputuskan ketika konteksnya ditetapkan.

Analisis konsekuensi dapat bervariasi dari deskripsi sederhana hasil keluaran hingga pemodelan kuantitatif rinci atau analisis kerentanan.

Dampak mungkin memiliki konsekuensi rendah tapi probabilitas tinggi, atau konsekuensi tinggi dan probabilitas rendah, atau hasil keluaran menengah. Dalam beberapa kasus, adalah tepat untuk fokus pada risiko dengan potensial manfaat-keluaran sangat besar, karena ini sering menjadi perhatian terbesar bagi manajer. Dalam kasus lain, mungkin penting untuk menganalisis baik risiko konsekuensi tinggi maupun rendah secara terpisah. Misalnya, masalah yang sering tetapi rendah-dampak (atau kronis) mungkin memiliki kumulatif besar atau efek jangka panjang. Selain itu, tindakan perlakuan untuk penanganan kedua jenis risiko yang khusus sering sangat berbeda, sehingga sangat berguna untuk menganalisa secara terpisah.

Analisis konsekuensi dapat meliputi:

- mempertimbangkan pengendalian yang ada untuk memperlakukan konsekuensi, bersama-sama dengan semua faktor penyebab relevan yang memiliki efek pada konsekuensi;
- mengaitkan konsekuensi risiko dengan sasaran orisinil;
- mempertimbangkan baik konsekuensi langsung dan yang mungkin timbul setelah waktu tertentu telah berlalu, jika ini adalah konsisten dengan ruang lingkup penilaian;
- mempertimbangkan konsekuensi sekunder, seperti yang berdampak pada sistem, kegiatan, peralatan atau organisasi terkait.

5.3.4 Analisis kemungkinan-kejadian dan memperkirakan probabilitas

Tiga pendekatan umum yang biasa digunakan untuk memperkirakan probabilitas; pendekatan tersebut mungkin dapat digunakan secara individu atau digabungkan:

a) Penggunaan data historis yang relevan untuk mengidentifikasi kejadian atau situasi yang telah terjadi di masa lalu dan karenanya dapat memperkirakan probabilitas terjadinya peristiwa di masa depan. Data yang digunakan sebaiknya relevan dengan jenis sistem, fasilitas, organisasi atau kegiatan sedang dipertimbangkan dan juga dengan standar operasional organisasi yang terlibat. Jika secara historis ada peristiwa dengan frekuensi sangat rendah, maka setiap perkiraan probabilitas akan sangat tidak pasti. Hal ini berlaku terutama untuk nol peristiwa, saat tidak dapat mengasumsikan kejadian, situasi atau keadaan tidak akan terjadi di masa depan.

b) Prakiraan probabilitas menggunakan teknik prediksi seperti analisis pohon kesalahan (*fault tree analysis*) dan analisis pohon kejadian (*event tree analysis*) (lihat Lampiran B). Ketika data historis tidak tersedia atau tidak mencukupi, adalah perlu untuk memperoleh probabilitas dengan menganalisis sistem, kegiatan, peralatan atau organisasi serta kondisi kegagalan atau keberhasilan yang terkait. Data numerik untuk peralatan, manusia, organisasi dan sistem dari pengalaman operasional, atau sumber data yang diterbitkan kemudian digabungkan untuk menghasilkan perkiraan probabilitas kejadian tertinggi. Ketika menggunakan teknik prediktif, adalah penting untuk memastikan bahwa kelonggaran yang wajar telah dibuat dalam analisis kemungkinan modus kegagalan umum yang melibatkan kegagalan insidental bersama dari sejumlah bagian yang berbeda atau komponen dalam sistem yang timbul dari penyebab yang sama. Teknik simulasi mungkin diperlukan untuk menghasilkan peralatan probabilitas dan kegagalan struktural karena proses penuaan dan degradasi lainnya, dengan memperhitungkan dampak dari ketidakpastian.

c) Pendapat ahli dapat digunakan dalam suatu proses yang sistematis dan terstruktur untuk memperkirakan probabilitas. Penilaian ahli sebaiknya menggambarkan semua informasi relevan yang tersedia termasuk sejarah, sistem-spesifik, spesifik-organisasional, eksperimental, rancangan, dll. Ada sejumlah metode formal untuk memunculkan penilaian ahli yang memberikan bantuan untuk perumusan pertanyaan yang tepat. Metode yang

tersedia meliputi pendekatan Delphi, pembandingan berpasangan, pemeringkatan kategori dan pertimbangan probabilitas mutlak.

5.3.5 Analisis pendahuluan

Risiko dapat disaring untuk mengidentifikasi risiko yang paling signifikan, atau untuk mengecualikan risiko kurang signifikan atau minor dari analisis lebih lanjut. Tujuannya adalah untuk memastikan bahwa sumber daya akan difokuskan pada risiko yang paling penting. Perhatian sebaiknya diambil untuk tidak menyaring risiko rendah yang sering terjadi dan memiliki suatu efek kumulatif yang signifikan.

Penyaringan sebaiknya didasarkan pada kriteria yang ditetapkan dalam konteks. Analisis pendahuluan menentukan satu atau lebih dari program tindakan berikut ini:
- memutuskan untuk memperlakukan risiko tanpa penilaian lebih lanjut;
- menyisihkan risiko tidak signifikan yang tidak akan menjustifikasi perlakuan;
- lakukan penilaian risiko yang lebih rinci.

Asumsi awal dan hasilnya sebaiknya didokumentasikan.

5.3.6 Ketidakpastian dan sensitivitas

Sering ada banyak ketidakpastian terkait dengan analisis risiko. Suatu pemahaman tentang ketidakpastian adalah perlu untuk menafsirkan dan mengkomunikasikan hasil analisis risiko secara efektif. Analisis ketidakpastian terkait dengan data, metode dan model yang digunakan untuk mengidentifikasi dan menganalisis risiko memainkan bagian penting dalam aplikasinya. Analisis ketidakpastian melibatkan penentuan variasi atau ketidaktepatan pada hasil, yang dihasilkan dari variasi kolektif dalam parameter dan asumsi yang digunakan untuk menentukan hasil. Area yang terkait erat dengan analisis ketidakpastian adalah analisis sensitivitas.

Analisis sensitivitas melibatkan penentuan ukuran dan signifikansi dari besarnya risiko untuk merubah di parameter masukan individu. Hal ini digunakan untuk mengidentifikasi data yang harus akurat tersebut, dan yang kurang sensitif serta karenanya memiliki pengaruh kurang pada akurasi keseluruhan.

Kelengkapan dan akurasi dari analisis risiko sebaiknya dinyatakan semaksimal mungkin. Sumber ketidakpastian sebaiknya diidentifikasi bila mungkin dan sebaiknya menangani baik data maupun model/metode ketidakpastian. Parameter pada analisa mana yang sensitif dan tingkat sensitivitas harus dinyatakan.

5.4 Evaluasi risiko

Evaluasi risiko melibatkan pembandingan tingkat estimasi risiko dengan kriteria risiko yang didefinisikan ketika konteks ditetapkan, dalam rangka untuk menentukan signifikansi tingkat dan jenis risiko.

Evaluasi risiko menggunakan pemahaman risiko yang diperoleh selama analisis risiko untuk membuat keputusan tentang tindakan masa depan. Pertimbangan etika, hukum, keuangan dan lainnya, termasuk persepsi risiko, juga masukan untuk keputusan.

Keputusan dapat meliputi:
- apakah risiko memerlukan perlakuan;
- prioritas untuk perlakuan;
- apakah suatu kegiatan sebaiknya dilakukan;

- sejumlah jalur yang mana sebaiknya diikuti.

Sifat keputusan yang perlu dibuat dan kriteria yang akan digunakan untuk membuat keputusan tersebut diputuskan saat penetapan konteks tetapi hal tersebut perlu ditinjau kembali secara lebih rinci pada tahap ini bahwa lebih banyak hal yang diketahui mengenai risiko -risiko tertentu yang telah teridentifikasi.

Kerangka kerja yang paling sederhana untuk penentuan kriteria risiko adalah sebuah tingkatan tunggal yang memisahkan risiko-risiko yang memerlukan perlakuan dengan yang tidak. Hal ini secara menarik memberikan hasil sederhana namun tidak mencerminkan hasil yang selengkapnya.

Ketidakpastian terlibat baik dalam memperkirakan risiko dan dalam pendefinisian batas risiko diantara hal tersebut yang membutuhkan perlakuan dan yang tidak.

Keputusan tentang apakah dan bagaimana memperlakukan risiko mungkin tergantung pada biaya dan manfaat dari pengambilan risiko serta biaya dan manfaat dari penerapan pengendalian yang ditingkatkan.

Pendekatan yang umum adalah dengan membagi risiko menjadi tiga kelompok:

a) kelompok atas di mana tingkat risiko dianggap tidak dapat ditoleransi apapun manfaat kegiatan dapat dibawa, dan perlakuan risiko adalah penting berapapun biayanya;

b) kelompok tengah (atau daerah 'abu-abu') di mana biaya dan manfaat, diperhitungkan serta kesempatan seimbang terhadap potensi konsekuensi;

c) kelompok yang lebih rendah di mana tingkat risiko dianggap sebagai diabaikan, atau lebih kecil yang tidak ada perlakuan risiko yang diperlukan.

Sistem kriteria ALARP (*as low as reasonably practicable* - serendah mungkin yang masuk akal untuk dapat diterapkan) yang digunakan dalam aplikasi keselamatan mengikuti pendekatan ini, di mana, di kelompok tengah, terdapat suatu skala bergeser untuk risiko rendah di mana biaya dan manfaat dapat langsung dibandingkan, sedangkan untuk risiko tinggi potensi kerusakan harus dikurangi, sampai biaya pengurangan lebih lanjut sepenuhnya tidak proporsional untuk manfaat keselamatan yang didapat.

5.5 Dokumentasi

Proses penilaian risiko sebaiknya didokumentasikan bersama-sama dengan hasil penilaian. Risiko sebaiknya diekspresikan dalam istilah yang dapat dimengerti, dan unit di mana tingkat risiko diekspresikan sebaiknya jelas.

Luasnya laporan akan tergantung pada sasaran dan ruang lingkup penilaian. Kecuali untuk penilaian yang sangat sederhana, dokumentasi dapat meliputi:

- sasaran dan ruang lingkup;
- deskripsi bagian relevan dari sistem dan fungsinya;
- suatu ringkasan konteks internal dan eksternal organisasi serta bagaimana kaitannya dengan situasi, sistem atau keadaan yang sedang dinilai;
- kriteria risiko yang diterapkan dan justifikasinya;
- keterbatasan, asumsi dan justifikasi hipotesis;
- metodologi penilaian;
- hasil identifikasi risiko;
- data, asumsi dan sumbernya serta validasi;
- hasil analisis risiko dan evaluasinya;

- analisis sensitivitas dan ketidakpastian;
- asumsi kritis dan faktor lain yang perlu dipantau;
- pembahasan hasil;
- kesimpulan dan rekomendasi;
- referensi.

Jika penilaian risiko mendukung suatu proses manajemen risiko yang terus-menerus, hal itu sebaiknya dilakukan dan didokumentasikan sedemikian rupa sehingga dapat dipertahankan sepanjang siklus hidup dari sistem, organisasi, peralatan atau kegiatan. Penilaian sebaiknya dilakukan pengkinian ketika terdapat informasi baru yang signifikan menjadi tersedia dan konteks berubah, sesuai dengan kebutuhan proses manajemen.

5.6 Pemantauan dan peninjauan penilaian risiko

Proses penilaian risiko akan menyoroti konteks dan faktor lain yang mungkin diharapkan bervariasi dari waktu ke waktu dan yang dapat mengubah atau membatalkan penilaian risiko. Faktor-faktor ini sebaiknya secara khusus diidentifikasi pemantauan dan tinjauan yang sedang berjalan, sehingga penilaian risiko dapat diperbarui bilamana diperlukan.

Data yang akan dipantau dalam rangka untuk memperbaiki penilaian risiko sebaiknya juga diidentifikasi dan dikumpulkan.

Efektivitas pengendalian juga sebaiknya dipantau dan didokumentasikan dalam rangka untuk menyediakan data untuk digunakan dalam analisis risiko. Akuntabilitas untuk penciptaan dan peninjauan bukti dan dokumentasi sebaiknya didefinisikan.

5.7 Penerapan penilaian risiko selama fase siklus hidup

Banyak kegiatan, proyek dan produk dapat dianggap memiliki siklus hidup mulai dari konsep dan definisi awal sepanjang realisasi sampai penyelesaian akhir yang mungkin termasuk penghentian dan pembuangan perangkat keras.

Penilaian risiko dapat diterapkan di semua tahapan siklus hidup dan biasanya diterapkan berkali-kali dengan berbagai tingkat rincian untuk membantu dalam pengambilan keputusan yang perlu dibuat pada setiap tahap.

Fase siklus hidup memiliki kebutuhan yang berbeda dan perlu teknik yang berbeda. Sebagai contoh, selama fase konsep dan definisi, ketika kesempatan diidentifikasi, penilaian risiko dapat digunakan untuk memutuskan apakah akan melanjutkan atau tidak.

Di mana beberapa pilihan tersedia, penilaian risiko dapat digunakan untuk mengevaluasi konsep alternatif untuk membantu memutuskan yang memberikan keseimbangan terbaik dari risiko positif dan negatif.

Selama fase rancangan dan pengembangan, penilaian risiko berkontribusi untuk
- pemastian bahwa risiko sistem dalam batas toleransi,
- proses penyempurnaan rancangan,
- studi efektivitas biaya,
- pengidentifikasian risiko yang berdampak pada fase siklus hidup berikutnya.

Sebagai hasil kegiatan, penilaian risiko dapat digunakan untuk memberikan informasi guna membantu dalam pengembangan prosedur untuk kondisi normal dan darurat.

6 Memilih teknik-teknik penilaian risiko

6.1 Umum

Pasal ini menjelaskan bagaimana teknik-teknik untuk penilaian risiko dapat dipilih. Daftar lampiran dan selanjutnya menjelaskan berbagai alat dan teknik yang dapat digunakan untuk melakukan penilaian risiko atau untuk membantu proses penilaian risiko. Kadang-kadang mungkin diperlukan untuk menerapkan lebih dari satu metode penilaian.

6.2 Memilih teknik-teknik

Penilaian risiko dapat dilakukan dalam berbagai tingkat kedalaman dan rincian serta menggunakan satu atau banyak metode mulai dari yang sederhana sampai yang kompleks. Bentuk penilaian dan keluarannya sebaiknya konsisten dengan kriteria risiko yang dikembangkan sebagai bagian dari penetapan konteks. Lampiran A mengilustrasikan hubungan konseptual antara kategori luas teknik penilaian risiko dan faktor yang ada dalam situasi risiko tertentu, serta memberikan contoh ilustrasi tentang bagaimana organisasi dapat memilih teknik penilaian risiko yang tepat untuk situasi tertentu.

Secara umum, teknik yang sesuai sebaiknya menunjukkan karakteristik sebagai berikut:

- teknik tersebut sebaiknya dapat dijustifikasi dan sesuai dengan situasi atau berdasarkan pertimbangan organisasi;
- teknik tersebut sebaiknya memberikan hasil dalam bentuk yang meningkatkan pemahaman tentang sifat dari risiko dan bagaimana hal itu dapat diperlakukan;
- teknik tersebut sebaiknya mampu digunakan dengan cara yang dapat ditelusuri, berulang dan dapat diverifikasi.

Alasan untuk teknik yang dipilih sebaiknya diberikan, sehubungan dengan relevansi dan kesesuaian. Ketika pengintegrasian hasil dari studi yang berbeda, teknik yang digunakan dan keluaran harus sebanding.

Begitu keputusan telah dibuat untuk melakukan penilaian risiko dan sasaran serta ruang lingkup telah didefinisikan, teknik sebaiknya dipilih berdasarkan faktor-faktor yang berlaku seperti:

- sasaran studi. Sasaran dari penilaian risiko akan memiliki pengaruh langsung pada teknik yang digunakan. Misalnya, jika studi banding antara pilihan yang berbeda sedang dilakukan, mungkin dapat diterima untuk menggunakan model konsekuensi kurang rinci untuk bagian dari sistem yang tidak terpengaruh oleh perbedaan;

- kebutuhan pengambil keputusan. Dalam beberapa kasus rincian tingkat tinggi dibutuhkan untuk membuat keputusan yang baik, dalamhal lain suatu pemahaman yang lebih umum sudah mencukupi;

- jenis dan berbagai risiko yang dianalisis;

- besarnya potensi konsekuensi. Keputusan dimana kedalaman penilaian risiko dilakukan sebaiknya mencerminkan konsekuensi persepsi awal (meskipun ini mungkin harus diubah setelah suatu evaluasi pendahuluan telah dilengkapi);

- tingkat keahlian, sumber daya manusia dan lainnya yang dibutuhkan. Suatu metode sederhana, dilakukan dengan baik, dapat memberikan hasil yang lebih baik daripada prosedur yang lebih canggih dilakukan dengan buruk, asalkan memenuhi sasaran dan ruang lingkup penilaian. Biasanya, upaya yang dimasukkan ke penilaian sebaiknya konsisten dengan tingkat potensi risiko yang dianalisis;

- ketersediaan informasi dan data. Beberapa teknik memerlukan informasi lebih lanjut dan data daripada yang lain;
- kebutuhan untuk modifikasi/pengkinian penilaian risiko. Penilaian mungkin perlu dimodifikasi/ dikinikan di masa mendatang dan beberapa teknik lebih bisa diperbaiki dari yang lain dalam hal ini;
- persyaratan peraturan dan kontrak.

Berbagai faktor yang mempengaruhi pemilihan pendekatan untuk penilaian risiko seperti ketersediaan sumber daya, sifat dan tingkat ketidakpastian dalam data dan informasi yang tersedia, serta kompleksitas penerapan (lihat Tabel A.2).

6.3 Ketersediaan sumber daya

Sumber daya dan kemampuan yang dapat mempengaruhi pilihan teknik penilaian risiko meliputi:
- keterampilan pengalaman kapasitas dan kemampuan dari tim penilaian risiko;
- kendala waktu dan sumber daya lainnya dalam organisasi;
- anggaran yang tersedia, jika sumber daya eksternal diperlukan.

6.4 Sifat dan tingkat ketidakpastian

Sifat dan tingkat ketidakpastian membutuhkan pemahaman tentang kualitas, kuantitas dan integritas informasi yang tersedia berkenaan dengan pertimbangan yang berdasarkan risiko. Ini termasuk sejauh mana tersedianya cukup informasi tentang risiko, sumber dan penyebabnya, serta konsekuensinya terhadap pencapaian sasaran. Ketidakpastian dapat berasal dari kualitas data yang buruk atau kurangnya data penting dan dapat diandalkan. Untuk menggambarkannya, metode pengumpulan data dapat berubah, cara organisasi menggunakan metode tersebut dapat berubah atau organisasi mungkin tidak memiliki metode pengumpulan yang efektif tersedia sama sekali, untuk pengumpulan data tentang risiko yang diidentifikasi.

Ketidakpastian juga dapat melekat dalam konteks eksternal dan internal organisasi. Data yang tersedia tidak selalu memberikan dasar yang dapat diandalkan untuk prediksi masa depan. Untuk jenis risiko yang unik, data historis mungkin tidak tersedia atau mungkin ada interpretasi yang berbeda atas data yang tersedia oleh berbagai pemangku kepentingan. Mereka yang melakukan penilaian risiko perlu memahami jenis dan sifat ketidakpastian serta menghargai implikasi untuk keandalan hasil penilaian risiko. Ini sebaiknya selalu dikomunikasikan kepada para pengambil keputusan.

6.5 Kompleksitas

Risiko dapat menjadi kompleks pada dasarnya, seperti, misalnya, dalam sistem yang kompleks yang risikonya perlu dinilai di seluruh sistem daripada perlakuan di setiap komponen secara terpisah dan mengabaikan interaksi. Dalam kasus lain, perlakuan risiko tunggal dapat memiliki implikasi di tempat lain dan bisa berdampak pada kegiatan lain. Dampak konsekuensi dan dependensi risiko perlu dipahami untuk memastikan bahwa dalam pengelolaan satu risiko, situasi yang tidak dapat ditolerir tidak tercipta di tempat lain. Pemahaman kompleksitas risiko tunggal atau portofolio risiko dari organisasi sangat penting untuk pemilihan metode atau teknik untuk penilaian risiko yang tepat.

6.6 Penerapan penilaian risiko selama fase siklus hidup

Banyak kegiatan, proyek dan produk dapat dianggap memiliki siklus hidup mulai dari konsep dan definisi awal sampai degan realisasi pada suatu penyelesaian akhir yang mungkin termasuk penghentian dan pembuangan perangkat keras.

Penilaian risiko dapat diterapkan di semua tahapan siklus hidup dan biasanya diterapkan berkali-kali dengan berbagai tingkat rincian untuk membantu dalam pengambilan keputusan yang perlu dibuat pada setiap tahap.

Fase siklus hidup memiliki kebutuhan yang berbeda dan memerlukan teknik yang berbeda. Sebagai contoh, selama fase konsep dan definisi, ketika kesempatan diidentifikasi, penilaian risiko mungkin digunakan untuk memutuskan apakah akan melanjutkan atau tidak.

Di mana beberapa pilihan tersedia, penilaian risiko dapat digunakan untuk mengevaluasi konsep alternatif untuk membantu memutuskan mana yang memberikan keseimbangan risiko.

Selama fase rancangan dan pengembangan, penilaian risiko berkontribusi untuk:
- pemastian bahwa risiko sistem dalam batas toleransi,
- proses penyempurnaan rancangan,
- studi efektivitas biaya,
- pengidentifikasian risiko yang berdampak pada fase siklus hidup berikutnya.

Sebagai hasil kegiatan, penilaian risiko dapat digunakan untuk memberikan informasi guna membantu dalam pengembangan prosedur untuk kondisi normal dan darurat.

6.7 Jenis-jenis teknik penilaian risiko

Teknik-teknik penilaian risiko dapat diklasifikasikan dalam berbagai cara untuk membantu pemahaman kekuatan dan kelemahan relatifnya. Tabel dalam Lampiran A mengkorelasikan beberapa teknik potensial dan kategorinya untuk tujuan ilustrasi.

Masing-masing teknik dielaborasi lebih lanjut dalam Lampiran B sesuai sifat dari penilaian yang diberikannya dan panduan penerapannya untuk situasi tertentu.

Lampiran A
(informatif)
Perbandingan teknik-teknik penilaian risiko

A.1 Jenis-jenis teknik

Klasifikasi pertama menunjukkan bagaimana teknik-teknik diterapkan untuk setiap langkah proses penilaian risiko sebagai berikut:
- identifikasi risiko;
- analisis risiko - analisis konsekuensi;
- analisis risiko - estimasi probabilitas kualitatif, semi-kuantitatif atau kuantitatif;
- analisis risiko - penilaian efektivitas dari setiap pengendalian yang ada;
- analisis risiko - estimasi tingkat risiko;
- evaluasi risiko.

Untuk setiap langkah dalam proses penilaian risiko, penerapan metode digambarkan sebagai sangat aplikatif, aplikatif atau tidak aplikatif (lihat Tabel A.1).

A.2 Faktor-faktor yang mempengaruhi pemilihan teknik-teknik penilaian risiko

Berikutnya atribut dari metode dijelaskan dalam hal:
- kompleksitas masalah dan metode yang diperlukan untuk menganalisis hal itu,
- sifat dan tingkat ketidakpastian dari penilaian risiko berdasarkan pada jumlah informasi yang tersedia dan apa yang diperlukan untuk memenuhi sasaran,
- tingkat sumber daya yang diperlukan dalam hal waktu dan tingkat keahlian, kebutuhan data atau biaya,
- apakah metode ini dapat memberikan keluaran kuantitatif.

Contoh jenis metode penilaian risiko yang tersedia tercantum pada Tabel A.2 di mana setiap metode diperingkatkan sebagai tinggi menengah atau rendah dalam hal atribut tersebut.

Tabel A.1 – Penerapan alat bantu yang digunakan untuk penilaian risiko

Alat bantu danTeknik	Proses Penilaian Risiko					Lihat Lampiran
	Identifikasi risiko	Analisis Risiko			Evaluasi Risiko	
		Konsekuensi	Probabilitas	Tingkat risiko		
Curah pendapat	SA[1)]	NA[2)]	NA	NA	NA	B 01
Wawancara terstruktur atau semi-terstruktur	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Daftar periksa	SA	NA	NA	NA	NA	B 04
Analisis pendahuluan potensi bahaya	SA	NA	NA	NA	NA	B 05
Studi potensi bahaya dan operabilitas (HAZOP)	SA	SA	A[3)]	A	A	B 06
Analisis potensi bahaya dan titik kendali kritis (HACCP)	SA	SA	NA	NA	SA	B 07
Penilaian risiko lingkungan	SA	SA	SA	SA	SA	B 08
Struktur “apa-jika” " (SWIFT)	SA	SA	SA	SA	SA	B 09
Analisis skenario	SA	SA	A	A	A	B 10
Analisis dampak bisnis	A	SA	A	A	A	B 11
Analisis akar penyebab	NA	SA	SA	SA	SA	B 12
Analisis modus kegagalan dan dampak	SA	SA	SA	SA	SA	B 13
Analisis pohon kesalahan	A	NA	SA	A	A	B 14
Analisis pohon kejadian	A	SA	A	A	NA	B 15
Analisis sebab dan konsekuensi	A	SA	SA	A	A	B 16
Analisis sebab-dan-akibat	SA	SA	NA	NA	NA	B 17
Analisis lapisan proteksi (LOPA)	A	SA	A	A	NA	B 18
Pohon keputusan	NA	SA	SA	A	A	B 19
Analisi keandalan manusia	SA	SA	SA	SA	A	B 20
Analisis dasi kupu-kupu	NA	A	SA	SA	A	B 21
Pemeliharaan yang terpusat pada keandalan	SA	SA	SA	SA	SA	B 22
Analisis rangkaian selinap	A	NA	NA	NA	NA	B 23
Analisis Markov	A	SA	NA	NA	NA	B 24
Simulasi Monte carlo	NA	NA	NA	NA	SA	B 25
Statistik Bayesian dan jaring Bayes	NA	SA	NA	NA	SA	B 26
Kurva FN	A	SA	SA	A	SA	B 27
Indeks risiko	A	SA	SA	A	SA	B 28
Matriks Konsekuensi/ probabilitas	SA	SA	SA	SA	A	B 29
Analisis biaya/manfaat	A	SA	A	A	A	B 30
Analisis keputusan multi-kriteria (MCDA)	A	SA	A	SA	A	B 31

1) SA = Sangat dapat diterapkan.

2) NA = Tidak dapat diterapkan

3) A = Dapat diterapkan

Tabel A.2 - Atribut-atribut dari suatu pemilihan alat bantu penilaian risiko

Jenis teknik penilaian risiko	Deskripsi	Relevansi dari faktor yang mempengaruhi			Dapat menyediakan keluaran kuantitatif
		Sumber daya dan kapabilitas	Sifat dan tingkat ketidakpastian	Kompleksitas	
METODE PENCARIAN					
Daftar periksa	Suatu bentuk sederhana dari identifikasi risiko. Suatu teknik yang menyediakan daftar ketidakpastian khas yang perlu dipertimbangkan. Pengguna mengacu pada daftar, kode atau standar yang disusun sebelumnya.	Rendah	Rendah	Rendah	Tidak
Analisis pendahuluan potensi bahaya	suatu metode analisis induktif sederhana yang sasarannya untuk mengidentifikasi potensi bahaya dan situasi serta kejadian berpotensi bahaya yang dapat menyebabkan kerugian untuk suatu kegiatan, fasilitas atau sistem.	Rendah	Tinggi	Sedang	Tidak
METODE PENDUKUNG					
Wawancara dan curah pendapat terstruktur	Suatu cara pengumpulan sekelompok besar ide dan evaluasi, pemeringkatan hal tersebut oleh suatu tim. Curah pendapat dapat distimulasi dengan cara diminta atau teknik wawancara satu dengan satu dan satu dengan banyak orang.	Rendah	Rendah	Rendah	Tidak
Teknik delphi	Suatu cara pengkombinasian pendapat ahli yang dapat mendukung identifikasi sumber dan pengaruh, estimasi probabilitas dan konsekuensi serta evaluasi risiko. Hal ini adalah suatu teknik kolaborasi untuk membangun konsensus di antara para ahli. Melibatkan analisis dan pemungutan suara independen oleh para ahli.	Sedang	Sedang	Sedang	Tidak
SWIFT "Apa-jika" terstruktur	Suatu sistem yang mendorong suatu tim untuk mengidentifikasi risiko. Normalnya digunakan dalam suatu workshop terfasilitasi. Normalnya terhubung pada suatu teknik analisis dan evaluasi risiko.	Sedang	Sedang	Apapun	Tidak
Analisis Keandalan Manusia (HRA)	Penilaian kehandalan manusia (HRA) berkaitan dengan dampak manusia pada kinerja sistem dan dapat digunakan untuk mengevaluasi pengaruh kesalahan manusia terhadap sistem.	Sedang	Sedang	Sedang	Ya
ANALISIS SKENARIO					
Analisis akar penyebab (Analisis kerugian tunggal)	Suatu kerugian tunggal yang telah terjadi dianalisis dalam rangka untuk memahami penyebab yang berkontribusi dan bagaimana sistem atau proses dapat ditingkatkan untuk menghindari kerugian semacam itu di masa mendatang. Analisis tersebut harus mempertimbangkan kendali apa yang ada pada waktu kerugian terjadi dan bagaimana kendali dapat di tingkatkan.	Sedang	Rendah	Sedang	Tidak

Tabel A.2 – Lanjutan

Jenis teknik penilaian risiko	Deskripsi	Relevansi dari faktor yang mempengaruhi			Dapat menyediakan keluaran kuantitatif
		Sumber daya dan kapabilitas	Sifat dan tingkat ketidakpastian	Kompleksitas	
Analisis skenario	Skenario masa depan yang mungkin diidentifikasikan melalui imajinasi atau ekstrapolasi dari risiko pada saat ini dan yang berbeda mempertimbangankan asumsi bahwa setiap skenario mungkin terjadi. Analisis ini dapat dikerjakan dengan formal atau informal secara kualitatif atau kuantitatif.	Sedang	Tinggi	Sedang	Tidak
Penilaian risiko terkait racun	Potensi bahaya diidentifikasi dan dianalisis serta jalur yang mungkin di mana target tertentu dapat terekspos pada potensi bahaya diidentifikasi. Informasi mengenai tingkat paparan dan sifat bahaya yang disebabkan oleh suatu tingkat paparan yang ada dikombinasikan untuk memberikan suatu ukuran probabilitas bahaya tertentu akan terjadi.	Tinggi	Tinggi	Sedang	Ya
Analisis dampak bisnis	Menyediakan suatu analisis tentang bagaimana risiko-risiko kunci yang mengganggu dapat mempengaruhi operasi sebuah organisasi dan mengidentifikasi serta mengkuantifikasi kemampuan yang dibutuhkan untuk mengelolanya.	Sedang	Sedang	Sedang	Tidak
Analisis pohon kesalahan	Suatu teknik yang dimulai dengan kejadian yang tidak diinginkan (kejadian puncak) dan menentukan seluruh jalan di mana kejadian tersebut dapat terjadi. Jalan tersebut ditampilkan berbentuk grafik dalam suatu diagram pohon logis. Ketika pohon kesalahan telah dibangun, pertimbangan sebaiknya diberikan pada cara untuk mengurangi dan mengeliminasi penyebab/sumber potensial	Tinggi	Tinggi	Sedang	Ya
Analisis pohon kejadian	Menggunakan pemikiran induktif untuk menterjemahkan probabilitas kejadian awal yang berbeda menjadi hasil keluaran yang mungkin.	Sedang	Sedang	Sedang	Ya
Analisis sebab/Konsekuensi	Suatu kombinasi analisis pohon kesalahan dan kejadian yang melibatkan keterlambatan waktu. Kedua sebab dan konsekuensi dari suatu kejadian awal dipertimbangkan.	Tinggi	Sedang	Tinggi	Ya

Tabel A.2 – Lanjutan

Jenis teknik penilaian risiko	Deskripsi	Relevansi dari faktor yang mempengaruhi			Dapat menyediakan keluaran kuantitatif
ANALISIS FUNGSI					
FMEA dan FMECA	FMEA (Analisis modus kegagalan dan efek) adalah suatu teknik yang mengidentifikasi modus dan mekanisme kegagalan, dan efeknya. Ada beberapa jenis dari FMEA: Rancangan (atau produk) FMEA yang digunakan untuk komponen dan produk, sistem FMEA yang digunakan untuk sistem, proses FMEA yang digunakan untuk manufaktur dan proses perakitan, layanan FMEA dan Perangkat lunak FMEA. FMEA dapat diikuti dengan suatu analisis kekritisan yang mendefinisikan signifikansi setiap modus kegagalan, secara kualitatif, semi-kuantitatif, atau kuantitatif (FMECA). Analisis kekritisan dapat didasarkan pada probabilitas di mana modus kegagalan akan menghasilkan kegagalan sistem, atau tingkat yang terasosiasikan dengan modus kegagalan, atau jumlah prioritas risiko.	Sedang	Sedang	Sedang	Ya
Pemeliharaan yang terpusat pada keandalan	Suatu metode untuk mengidentifikasi kebijakan yang harus dilaksanakan untuk mengelola kegagalan sehingga dapat dicapai efisien dan efektif yang memerlukan keselamatan, ketersediaan dan keekonomisan operasi untuk semua jenis peralatan.	Sedang	Sedang	Sedang	Ya
Analisis selinap (Analisis rangkaian selinap)	suatu metodologi untuk mengidentifikasi kesalahan rancangan. Kondisi selinap adalah kondisi laten perangkat keras, kondisi laten perangkat lunak atau kondisi laten terintegrasi yang dapat menyebabkan suatu kejadian yang tidak diinginkan terjadi atau dapat menghambat kejadian yang diinginkan dan tidak disebabkan oleh kegagalan komponen. Kondisi ini ditandai dengan sifat acak mereka dan kemampuan untuk menghindar pada saat deteksi paling ketat dari tes sistem terstandar. Kondisi selinap dapat menyebabkan operasi yang tidak benar, hilangnya ketersediaan sistem, keterlambatan program, atau bahkan kematian atau cedera untuk personel.	Sedang	Sedang	Sedang	Tidak
HAZOP Hazard and operability studies	Suatu proses umum dari identifikasi risiko untuk mendefinisikan deviasi yang mungkin dari kinerja yang diinginkan atau diupayakan .Hal ini menggunakan suatu sistem berbasis kata-kata panduan kekritisan deviasi dinilai.	Sedang	Tinggi	Tinggi	TIdak

HACCP Hazard analysis and critical control points	Suatu sistem yang sistematis proaktif dan preventif untuk memastikan kualitas produk, keandalan dan keselamatan proses dengan pengukuran dan pemantauan karakteristik spesifik yang dipersyaratkan untuk berada dalam batas yang ditentukan.	Sedang	Sedang	Sedang	Tidak

Tabel A.2 – Lanjutan

Jenis teknik penilaian risiko	Deskripsi	Relevansi dari faktor yang mempengaruhi			Dapat menyediakan keluaran kuantitatif
PENILAIAN KENDALI					
LOPA (Analisis lapisan proteksi)	(Mungkin juga disebut sebagai analisis hambatan). Analisis ini memungkinkan kendali dan efektifitasnya di evaluasi.	Sedang	Sedang	Sedang	Ya
Analisis dasi kupu-kupu	Suatu cara diagram sederhana yang menggambarkan dan menganalisis jalur risiko dari penyebab ke konsekuensi. Hal ini dapat dianggap sebagai kombinasi dari pemikiran analisis pohon kesalahan penyebab dari suatu kejadian (diwakili oleh simpul pada dasi kupu-kupu) dan konsekuensi analisis pohon kejadian	Medium	High	Medium	Yes
METODE STATISTIK					
Analisis Markov	Analisis Markov, terkadang disebut juga analisis ruang-keadaan, biasanya digunakan dalam analisis sistem kompleks yang dapat diperbaiki yang dapat muncul dalam berbagai keadaan, termasuk berbagai keadaan terdegradasi.	High	Low	High	Yes
Analisis Monte-Carlo	Simulasi monte carlo digunakan untuk menetapkan variasi agregat dalam suatu sistem yang dihasilkan dari berbagai variasi dalam sistem, untuk sejumlah masukan, di mana tiap masukan memiliki suatu distribusi yang terdefinisi dan masukan terkait dengan keluaran melalui hubungan yang terdefinisikan. Analisis tersebut dapat digunakan untuk suatu model spesifik di mana interaksi berbagai masukan secara matematis dapat di definisikan. Masukan tersebut dapat berdasarkan suatu variasi tipe distribusi menurut sifat ketidakpastian yang ingin ditampilkan. Untuk penilaian risiko, distribusi berbentuk segitiga atau distribusi beta umum digunakan.	High	Low	High	Yes
Analisis Bayesian	Suatu prosedur statistik yang menggunakan data distribusi awal untuk menilai probabilitas hasil tertentu. Analisis Bayesian bergantung pada akurasi distribusi awal untuk mendeduksi suatu hasil yang akurat. Jejaring keyakinan Bayesian memodelkan sebab-dan-efek dalam berbagai ranah dengan menangkap hubungan probabilistik dari masukan variabel untuk membuahkan suatu hasil	High	Low	High	Yes

Lampiran B
(informatif)
Teknik penilaian risiko

B.1 Curah pendapat *(Brainstorming)*

B.1.1 Tinjauan singkat

Curah pendapat melibatkan penstimulasian serta mendorong percakapan mengalir bebas di antara sekelompok orang yang berpengetahuan untuk mengidentifikasi potensial mode kegagalan dan potensi bahaya yang terkait, risiko, kriteria untuk keputusan dan/atau opsi untuk perlakuan. Istilah "curah pendapat" sering digunakan sangat longgar yang berarti setiap jenis diskusi kelompok. Namun curah pendapat yang benar melibatkan teknik tertentu untuk mencoba memastikan bahwa imajinasi orang dipicu oleh pikiran dan pernyataan dari orang lain dalam kelompok.

Fasilitasi yang efektif sangat penting dalam teknik ini dan termasuk stimulasi diskusi saat memulai, penggegasan berkala dari kelompok ke area lain yang relevan dan menangkap isu yang timbul dari diskusi (yang biasanya cukup hidup).

B.1.2 Penggunaan

Curah pendapat dapat digunakan bersama dengan metode penilaian risiko lain yang dijelaskan di bawah ini atau mungkin berdiri sendiri sebagai suatu teknik untuk mendorong pemikiran imajinatif pada setiap tahap proses manajemen risiko dan setiap tahap siklus hidup suatu sistem. Ini dapat digunakan untuk diskusi pada tingkat tinggi di mana masalah diidentifikasi, untuk tinjauan lebih rinci atau pada masalah tertentu dengan tingkat rinci.

Curah pendapat menempatkan suatu penekanan berat pada imajinasi. Oleh karena itu sangat berguna ketika mengidentifikasi risiko teknologi baru, di mana tidak ada data atau di mana solusi baru untuk masalah diperlukan.

B.1.3 Masukan

Suatu tim terdiri dari orang-orang dengan pengetahuan organisasi, sistem, proses atau penerapan yang sedang dinilai.

B.1.4 Proses

Curah pendapat dapat secara formal atau informal. Curah pendapat formal adalah lebih terstruktur dengan peserta dipersiapkan sebelumnya dan sesi tersebut memiliki tujuan serta manfaat-keluaran yang terdefinisikan dengan cara pengevaluasian ide-ide yang diajukan. Curah pendapat informal kurang terstruktur dan sering lebih ad-hoc.

Dalam proses formal:
- fasilitator mempersiapkan gegasan pemikiran dan memicu secara tepat pada konteks sebelum sesi;
- sasaran sesi didefinisikan dan aturan dijelaskan;
- fasilitator memulai serangkaian pemikiran dan semua orang mengeksplorasi pengidentifikasian ide-ide sebanyak mungkin isu. Tidak ada diskusi pada bagian ini tentang apakah hal yang sebaiknya atau tidak sebaiknya ada dalam suatu daftar atau apa

yang dimaksud dengan pernyataan tertentu karena ini cenderung menghambat pemikiran bebas mengalir. Semua masukan diterima dan tidak ada yang mengkritik serta kelompok bergerak dengan cepat untuk memperbolehkan ide-ide yang memicu pemikiran lateral;
- fasilitator dapat mengarahkan orang pergi pada sebuah jalur baru ketika satu arah pemikiran habis atau diskusi menyimpang terlalu jauh. Bagaimanapun idenya, adalah untuk mengumpulkan sebanyak mungkin ide yang beragam untuk analisis berikutnya.

B.1.5 Keluaran

Keluaran tergantung pada tahap proses manajemen risiko di mana hal tersebut diterapkan, misalnya pada tahap identifikasi, keluaran mungkin berupa daftar risiko dan pengendalian saat ini.

B.1.6 Kekuatan dan keterbatasan

Kekuatan curah pendapat meliputi:
- curah pendapat mendorong imajinasi yang membantu mengidentifikasi risiko baru dan solusi baru;
- curah pendapat melibatkan pemangku kepentingan kunci dan karenanya membantu komunikasi secara keseluruhan;
- curah pendapat relatif cepat dan mudah untuk disusun.

Keterbatasan meliputi:
- peserta mungkin tidak memiliki keterampilan dan pengetahuan untuk menjadi kontributor yang efektif;
- karena relatif tidak terstruktur, hal ini sulit untuk menunjukkan bahwa proses tersebut telah komprehensif, misalnya bahwa semua potensi risiko telah diidentifikasi;
- mungkin terdapat dinamika kelompok tertentu di mana beberapa orang dengan ide-ide yang berharga tetap diam sementara yang lain mendominasi diskusi. Hal ini dapat diatasi dengan curah pendapat menggunakan komputer, menggunakan forum obrolan atau teknik kelompok nominal. Curah pendapat menggunakan komputer dapat diatur untuk menjadi anonim, sehingga menghindari masalah-masalah pribadi dan politik yang dapat menghambat aliran bebas ide. Dalam kelompok nominal ide teknik disampaikan secara anonim pada moderator dan kemudian dibahas oleh kelompok.

B.2 Wawancara terstruktur atau semi-terstruktur

B.2.1 Tinjauan singkat

Dalam suatu wawancara terstruktur, individu yang diwawancara ditanya serangkaian pertanyaan dari suatu lembar gegas yang mendorong individu yang diwawancara untuk melihat suatu situasi dari perspektif yang berbeda dan dengan demikian mengidentifikasi risiko dari perspektif itu. Sebuah wawancara semi-terstruktur adalah serupa, namun memperbolehkan lebih banyak kebebasan untuk suatu percakapan untuk mengeksplorasi isu-isu yang timbul.

B.2.2 Penggunaan

Wawancara terstruktur dan semi-terstruktur berguna di saat sulit untuk mendapatkan orang-orang untuk sesi curah pendapat bersama-sama atau di saat diskusi bebas-mengalir dalam suatu kelompok yang dengan situasi atau orang yang terlibat tidak tepat. Wawancara tersebut paling sering digunakan untuk mengidentifikasi risiko atau untuk menilai efektivitas pengendalian yang sudah ada sebagai bagian dari analisis risiko. Wawancara tersebut dapat

diterapkan pada setiap tahap proyek atau proses. Wawancara tersebut dimaksudkan guna pemberian masukan pemangku kepentingan untuk penilaian risiko.

B.2.3 Masukan

Masukan meliputi:
- suatu definisi yang jelas tentang sasaran dari wawancara;
- suatu daftar orang yang diwawancarai dipilih dari pemangku kepentingan yang relevan;
- suatu set pertanyaan yang disiapkan.

B.2.4 Proses

Satu set pertanyaan yang relevan, dibuat untuk memandu pewawancara. Bilamana memungkinkan, pertanyaan sebaiknya bersifat terbuka, sederhana, dalam bahasa yang tepat bagi yang diwawancara dan mencakup satu isu saja. Pertanyaan lanjutan yang memungkinkan untuk mencari klarifikasi juga dipersiapkan.

Pertanyaan kemudian diajukan kepada orang yang diwawancarai. Dalam pencarian elaborasi, pertanyaan sebaiknya terbuka. Perlu menjadi perhatian sebaiknya tidak "mengarahkan" yang diwawancara.

Tanggapan sebaiknya dipertimbangkan dengan suatu tingkat fleksibilitas agar menyediakan kesempatan untuk pengeksplorasian area yang mungkin ingin dituju oleh yang diwawancara.

B.2.5 Keluaran

Keluaran adalah pandangan pemangku kepentingan pada isu-isu yang menjadi subjek wawancara.

B.2.6 Kekuatan dan keterbatasan

Kekuatan wawancara terstruktur adalah sebagai berikut:
- wawancara terstruktur memberikan orang waktu untuk mempertimbangkan pemikiran tentang masalah;
- komunikasi per individu bisa memungkinkan pertimbangan yang lebih mendalam pada isu;
- wawancara terstruktur memungkinkan keterlibatan sejumlah besar pemangku kepentingan dari pada curah pendapat yang menggunakan kelompok yang relatif kecil.

Keterbatasan adalah sebagai berikut:
- hal tersebut memakan waktu bagi fasilitator untuk mendapatkan opini beragam dengan cara ini;
- bias ditolerir dan tidak dipindahkan ke diskusi kelompok;
- memicu imajinasi dimana keistimewaan dari curah pendapat mungkin tidak akan tercapai.

B.3 Teknik Delphi

B.3.1 Tinjauan singkat

Teknik Delphi adalah prosedur untuk memperoleh opini konsensus yang andal dari sekelompok ahli. Meskipun istilah ini sekarang sering secara luas digunakan dengan peruntukan segala bentuk curah pendapat, suatu fitur penting dari teknik Delphi, seperti dirumuskan awalnya, bahwa ahli mengungkapkan pendapat mereka secara individu dan tanpa nama saat memiliki akses pada pandangan ahli lainnya selama proses berlangsung.

B.3.2 Penggunaan

Teknik Delphi dapat diterapkan pada setiap tahap proses manajemen risiko atau pada fase dari siklus hidup suatu sistem, di mana pun suatu konsensus pandangan para ahli dibutuhkan.

B.3.3 Masukan

Suatu set opsi dimana konsensus diperlukan.

B.3.4 Proses

Sekelompok ahli diberikan pertanyaan menggunakan kuesioner semi-terstruktur. Para ahli tidak bertemu sehingga pendapat mereka independen.

Prosedurnya adalah sebagai berikut:
- pembentukan tim untuk melakukan dan memantau proses Delphi;
- pemilihan sekelompok ahli (mungkin satu atau lebih panel ahli);
- pengembangan putaran 1 kuesioner;
- pengujian kuesioner;
- pengiriman kuesioner ke panelis secara individual;
- informasi dari tanggapan putaran pertama dianalisis dan dikombinasikan serta kembali beredar ke panelis;
- panelis merespon dan proses ini diulang sampai konsensus tercapai.

B.3.5 Keluaran

Konvergensi menuju konsensus tentang masalah terkendali.

B.3.6 Kekuatan dan keterbatasan

Kekuatan meliputi:
- sebagai pandangan tanpa nama, opini yang tidak populer lebih cenderung diungkapkan;
- semua pandangan memiliki bobot yang sama, yang menghindari masalah kepribadian yang mendominasi;
- mencapai kepemilikan atas manfaat-keluaran;
- orang tidak perlu dibawa bersama-sama di satu tempat pada satu waktu.

Keterbatasan meliputi:
- hal tersebut adalah padat karya dan memakan waktu;
- peserta harus mampu mengekspresikan diri dengan jelas secara tertulis.

B.4 Daftar periksa *(Check-lists)*

B.4.1 Tinjauan singkat

Daftar periksa adalah daftar dari potensi bahaya, risiko atau kegagalan pengendalian yang telah dikembangkan biasanya dari pengalaman, baik sebagai hasil dari penilaian risiko sebelumnya atau sebagai hasil dari kegagalan masa lalu.

B.4.2 Penggunaan

Sebuah daftar periksa dapat digunakan untuk mengidentifikasi potensi bahaya dan risiko atau untuk menilai efektivitas pengendalian. Hal tersebut dapat digunakan pada setiap tahap siklus hidup sebuah produk, proses atau sistem. Hal tersebut dapat digunakan sebagai bagian dari teknik penilaian risiko lain tetapi paling bermanfaat ketika diterapkan untuk memeriksa bahwa semuanya telah terpenuhi setelah suatu teknik yang lebih imajinatif yang mengidentifikasi masalah baru telah diterapkan.

B.4.3 Masukan

Informasi sebelumnya dan keahlian pada masalah ini, sehingga daftar periksa yang relevan dan sebaiknya divalidasi dapat dipilih atau dikembangkan.

B.4.4 Proses

Prosedurnya adalah sebagai berikut:

- ruang lingkup kegiatan didefinisikan;
- suatu daftar periksa dipilih yang melingkupi ruang lingkup secara memadai. Daftar periksa harus dipilih dengan cermat untuk tujuan tersebut. Misalnya suatu daftar periksa standar pengendalian tidak dapat digunakan untuk mengidentifikasi bahaya atau risiko baru;
- orang atau tim menggunakan langkah-langkah daftar periksa melalui setiap elemen dari proses atau sistem serta ulasan apakah hal pada daftar periksa ada.

B.4.5 Keluaran

Keluaran tergantung pada tahap proses manajemen risiko di mana hal tersebut diterapkan. Misalnya keluaran mungkin sebuah pengendalian yang tidak memadai atau sebuah daftar risiko.

B.4.6 Kekuatan dan keterbatasan

Kekuatan dari daftar periksa meliputi:
- daftar periksa dapat digunakan oleh non ahli;
- ketika dirancang dengan baik, hal tersebut menggabungkan keahlian luas menjadi sistem yang mudah untuk digunakan;
- daftar periksa dapat membantu memastikan masalah umum tidak dilupakan.

Keterbatasan meliputi:
- daftar periksa cenderung menghambat imajinasi dalam identifikasi risiko;
- daftar periksa mengatasi 'mengetahui yang diketahui', bukan 'mengetahui yang tidak diketahui' atau 'tidak mengetahui yang tidak diketahui'.
- daftar periksa mendorong perilaku jenis 'centang kotak';
- daftar periksa cenderung berdasarkan pengamatan, sehingga kehilangan masalah yang tidak mudah dilihat.

B.5 Analisis pendahuluan potensi bahaya *(Preliminary Hazard Analysis - PHA)*

B.5.1 Tinjauan singkat

PHA adalah suatu metode analisis induktif sederhana yang sasarannya untuk mengidentifikasi potensi bahaya dan situasi serta kejadian berpotensi bahaya yang dapat menyebabkan kerusakan untuk suatu kegiatan, fasilitas atau sistem.

B.5.2 Penggunaan

Hal ini paling sering dilakukan di awal pengembangan proyek ketika ada sedikit informasi tentang rincian rancangan atau prosedur operasi dan sering dapat menjadi pendahuluan untuk melanjutkan studi atau untuk memberikan informasi untuk spesifikasi rancangan sistem. Hal ini juga dapat berguna ketika menganalisis sistem yang ada untuk memprioritaskan potensi bahaya dan risiko untuk analisis lebih lanjut atau di mana keadaan mencegah teknik yang lebih luas digunakan.

B.5.3 Masukan

Masukan meliputi:
- informasi pada sistem yang akan dinilai;
- rincian dari rancangan sistem seperti yang tersedia dan relevan.

B.5.4 Proses

Sebuah daftar potensi bahaya dan situasi umum berpotensi bahaya serta risiko dirumuskan dengan mempertimbangkan karakteristik seperti:
- bahan yang digunakan atau diproduksi dan kereaktifannya;
- peralatan yang digunakan;
- lingkungan operasi;
- tata letak;
- hubungan di antara komponen sistem, dll.

Konsekuensi analisis kualitatif dari suatu kejadian yang tidak diinginkan dan probabilitas mereka dapat dilakukan untuk mengidentifikasi risiko guna penilaian lebih lanjut.

PHA sebaiknya dikinikan selama tahap rancangan, konstruksi dan pengujian guna mendeteksi bahaya baru serta melakukan koreksi, jika perlu. Hasil yang diperoleh dapat disajikan dalam berbagai cara seperti tabel dan diagram pohon.

B.5.5 Keluaran

Keluaran meliputi:
- sebuah daftar potensi bahaya dan risiko;
- rekomendasi dalam bentuk penerimaan, pengendalian yang direkomendasikan, spesifikasi rancangan atau permintaan untuk penilaian yang lebih rinci.

B.5.6 Kekuatan dan keterbatasan

Kekuatan meliputi:
- bahwa hal tersebut dapat digunakan bila ada informasi yang terbatas;

- hal tersebut memungkinkan risiko yang harus dipertimbangkan sangat awal dalam sistem siklus hidup.

Keterbatasan meliputi:
- PHA hanya menyediakan informasi pendahuluan; itu tidak komprehensif, juga tidak memberikan informasi rinci tentang risiko dan bagaimana mereka dapat dicegah dengan baik.

B.6 HAZOP

B.6.1 Tinjauan singkat

HAZOP adalah akronim untuk *HAZard and OPerability study* (studi potensi bahaya dan operabilitas) dan, adalah pengujian terstruktur dan sistematis dari sebuah rencana atau produk, poses, prosedur atau sistem yang sudah ada. Ini adalah teknik untuk mengidentifikasi risiko untuk orang, peralatan, lingkungan dan / atau sasaran organisasi. Tim peneliti juga diharapkan, bilamana mungkin, untuk memberikan solusi untuk perlakuan risiko.

Proses HAZOP adalah sebuah teknik kualitatif berdasarkan penggunaan kata-kata panduan yang mempertanyakan bagaimana maksud rancangan atau kondisi operasi mungkin tidak dicapai pada setiap langkah dalam rancangan, proses, prosedur atau sistem. Hal ini umumnya dilakukan oleh tim multi-disiplin selama serangkaian pertemuan.

HAZOP mirip dengan FMEA dalam hal mengidentifikasi mode kegagalan proses, sistem atau prosedur, penyebabnya dan konsekuensinya. Ini berbeda ketika tim menganggap hasil keluaran yang tidak diinginkan dan penyimpangan dari hasil keluaran serta kondisi dan pekerjaan kembali pada penyebab dan mode kegagalan yang mungkin, sedangkan FMEA dimulai dengan pengidentifikasian mode kegagalan.

B.6.2 Penggunaan

Teknik HAZOP awalnya dikembangkan untuk menganalisis sistem proses kimia, tetapi telah diperluas untuk jenis lain dari sistem dan operasi yang kompleks. Ini termasuk sistem mekanik dan elektronik, prosedur, serta sistem perangkat lunak, dan bahkan untuk mengorganisasikan perubahan dan untuk merancang serta meninjau kontrak hukum.

Proses HAZOP dapat menangani semua bentuk penyimpangan dari maksud rancangan yang dikarenakan kekurangan dalam rancangan, komponen, prosedur yang direncanakan sereta tindakan manusia.

Hal ini banyak digunakan untuk tinjauan rancangan perangkat lunak. Saat diterapkan untuk keselamatan pengendalian instrumen dan sistem komputer kritis mungkin dikenal sebagai CHAZOP (*Control HAzards and OPerability Analysis* - Analisis potensi bahaya dan operabilitas kendali atau analisis potensi bahaya dan operabilitas komputer).

Sebuah studi HAZOP biasanya dilakukan pada tahap rancangan rinci, ketika suatu diagram utuh dari proses yang dimaksud tersedia, tetapi sementara perubahan rancangan masih dipraktekkan. Hal tersebut bagaimanapun dimungkinkan, dilakukan dalam pendekatan bertahap dengan panduan berbeda untuk setiap tahap sebagai suatu pengembangan rancangan secara rinci. Suatu studi HAZOP juga dapat dilakukan selama operasi tetapi perubahan yang diperlukan memerlukan biaya yang mahal pada tahap tersebut.

B.6.3 Masukan

Masukan penting untuk studi HAZOP mencakup informasi terkini tentang sistem, proses atau prosedur yang harus ditinjau dan maksud serta kinerja spesifikasi rancangan. masukan dapat mencakup: gambar, lembar spesifikasi, lembar aliran, proses pengendalian dan diagram logika, gambar tata letak, prosedur operasi dan pemeliharaan, dan prosedur tanggap darurat. Untuk non-perangkat keras yang berhubungan HAZOP masukan dapat berupa dokumen yang menjelaskan fungsi dan elemen dari sistem atau prosedur yang diteliti. Sebagai contoh, masukan dapat berupa diagram organisasi dan deskripsi peran, draft kontrak atau bahkan prosedur rancangan.

B.6.4 Proses

HAZOP mengambil "rancangan" dan spesifikasi dari proses, prosedur atau sistem yang dipelajari dan tinjauan masing-masing bagian dari itu untuk menemukan apa penyimpangan dari kinerja yang dimaksudkan dapat terjadi, apa penyebab potensial serta apa kemungkinan konsekuensi penyimpangan. Hal ini dicapai dengan penelitian sistematis bagaimana setiap bagian dari sistem, proses atau prosedur akan merespon perubahan parameter kunci dengan menggunakan kata panduan yang cocok. Kata panduan dapat disesuaikan dengan sistem, proses atau prosedur tertentu atau kata-kata umum dapat digunakan yang mencakup semua jenis penyimpangan. Tabel B.1 memberikan contoh kata panduan umum yang digunakan untuk sistem teknis. Kata panduan serupa seperti 'terlalu dini', 'terlalu terlambat', 'terlalu banyak', 'terlalu sedikit', 'terlalu lama', 'terlalu pendek', 'salah arah', pada 'objek yang salah', 'tindakan yang salah' bisa digunakan untuk mengidentifikasi mode kesalahan manusia.

Langkah yang normal dalam studi HAZOP meliputi:

- pencalonan seseorang dengan tanggung jawab dan wewenang yang diperlukan untuk melakukan studi HAZOP dan untuk memastikan bahwa setiap tindakan yang timbul dari studi ini selesai;
- definisi sasaran dan ruang lingkup studi;
- menetapkan satu set kunci atau kata panduan untuk studi;
- pendefinisian suatu tim studi HAZOP; tim ini biasanya multidisiplin dan sebaiknya mencakup rancangan dan operasi personil dengan keahlian teknis yang tepat untuk mengevaluasi efek penyimpangan dari rancangan yang dimaksud atau saat ini. Direkomendasikan bahwa tim termasuk orang yang tidak terlibat langsung dalam rancangan atau sistem, proses atau prosedur dalam peninjauan;
- koleksi dokumentasi yang diperlukan.

Dalam suatu lokakarya yang difasilitasi tim studi:

- membelah sistem, proses atau prosedur menjadi elemen-elemen yang lebih kecil atau sub-sistem atau subroses atau sub-elemen untuk membuat tinjauan nyata;
- menyetujui maksud rancangan untuk setiap subsistem, sub-proses atau sub-elemen dan kemudian untuk setiap item dalam subsistem itu atau elemen penerapan kata panduan satu demi satu untuk mendalilkan kemungkinan penyimpangan yang akan memiliki hasil yang tidak diinginkan;
- di mana hasil yang tidak diinginkan diidentifikasi, persetujuan penyebab dan konsekuensi dalam setiap kasus serta menyarankan bagaimana hal tersebut mungkin diperlakukan untuk mencegah hasil yang tidak diinginkan terjadi atau memitigasi konsekuensi jika hal tersebut terjadi;
- pendokumentasian diskusi dan persetujuan tindakan spesifik untuk perlakuan risiko yang teridentifikasi.

Tabel B.1 – Contoh kata petunjuk HAZOP yang dimungkinkan

Istilah	Definisi
Tanpa atau Tidak	Tidak ada bagian dari hasil yang dimaksud tercapai atau syarat yang dimaksud tidak ada
Lebih (lebih Tinggi)	Kenaikan kuantitatif dalam keluaran atau dalam kondisi operasi
Kurang (lebih rendah)	Penurunan kuantitatif
Sebaik	Kenaikan kuantitatif (misalnya material tambahan)
Bagian dari	Penurunan kuantitatif (misalnya hanya satu atau dua komponen dalam satu campuran)
Kebalikan/lawan	Kebalikan (misalnya arus balik)
Selain	Tidak ada satu bagian pun dari maksud yang tercapai, sesuatu yang sama sekali berbeda terjadi (misalnya material aliran atau material yang salah)
Kompatibilitas	Material; lingkungan
Kata-kata panduan yang diaplikasikan pada parameter seperti	
	Sifat fisik dari suatu material atau proses
	Kondisi fisik seperti suhu, kecepatan
	Suatu maksud tertentu dari suatu unsur sistem atau rancangan (misalnya transfer informasi)
	Aspek operasional

B.6.5 Keluaran

Risalah rapat HAZOP yang direkam berisi setiap poin tinjauan. Ini sebaiknya mencakup: kata petunjuk yang digunakan, deviasi,penyebab yang mungkin, tindakan untuk mengatasi masalah teridentifikasi dan orang yang bertanggung jawab terhadap tindakan.

Untuk setiap penyimpangan yang tidak dapat diperbaiki, maka risiko untuk penyimpangan sebaiknya dinilai.

B.6.6 Kekuatan dan keterbatasan

Sebuah analisis HAZOP menawarkan keuntungan sebagai berikut:

- HAZOP analisis menyediakan sarana untuk secara sistematis dan seksama menguji sistem, proses atau prosedur;
- HAZOP analisis melibatkan suatu tim multidisiplin termasuk orang-orang dengan pengalaman operasional di kehidupan nyata dan mereka yang mungkin harus melakukan tindakan perlakuan;
- HAZOP analisis menghasilkan solusi dan tindakan perlakuan risiko;
- HAZOP analisis berlaku untuk berbagai sistem, proses dan prosedur;
- HAZOP analisis memungkinkan pertimbangan eksplisit dari penyebab dan konsekuensi dari kesalahan manusia;
- HAZOP analisis menciptakan rekaman tertulis dari proses yang dapat digunakan untuk menunjukkan uji kelayakan.

Keterbatasannya meliputi:

- suatu analisis rinci dapat sangat memakan waktu dan oleh karenanya menjadi mahal;

- suatu analisis rinci membutuhkan suatu dokumentasi atau sistem/proses dan spesifikasi prosedur tingkat tinggi;
- HAZOP analisis dapat fokus pada pencarian solusi rinci daripada menantang asumsi dasar (bagaimanapun, hal ini dapat diatasi dengan suatu pendekatan bertahap);
- diskusi dapat difokuskan pada isu-isu rinci dari rancangan, dan bukan pada isu-isu yang lebih luas atau eksternal;
- HAZOP analisi dibatasi oleh (draf) rancangan dan maksud rancangan, serta ruang lingkup dan sasran yang diberikan kepada tim;
- proses sangat bergantung pada keahlian dari para rancanganer yang mungkin merasa sulit untuk menjadi cukup obyektif dalam mencari masalah dalam rancangan mereka.

B.6.7 Dokumen Referensi

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

B.7 Analisis potensi bahaya dan titik kendali kritis (*Hazard analysis and critical control points* - HACCP)

B.7.1 Tinjauan singkat

Analisis potensi bahaya dan titik kendali kritis (HACCP) menyediakan struktur untuk pengidentifikasian potensi bahaya dan meletakkan kendali di tempat di semua bagian yang relevan dari suatu proses untuk melindungi terhadap potensi bahaya dan untuk menjaga kehandalan kualitas serta keamanan produk. HACCP bertujuan untuk memastikan bahwa risiko diminimalkan oleh pengendalian di seluruh proses daripada melalui inspeksi pada produk akhir.

B.7.2 Penggunaan

HACCP dikembangkan untuk memastikan kualitas makanan untuk program luar angkasa NASA. Hal ini sekarang digunakan oleh organisasi yang beroperasi di mana saja dalam rantai makanan untuk mengendalikan risiko dari fisik, kimia atau kontaminan biologis makanan. Ini juga telah diperluas untuk digunakan dalam pembuatan obat-obatan dan peralatan medis. Prinsip pengidentifikasian hal yang dapat mempengaruhi kualitas produk, dan titik yang menentukan dalam proses di mana parameter kritis dapat dipantau dan potensi bahaya dikendalikan, dapat digeneralisasi untuk sistem teknis lainnya.

B.7.3 Masukan

HACCP dimulai dari suatu diagram alir dasar atau diagram proses dan informasi tentang potensi bahaya yang mungkin mempengaruhi kualitas, keselamatan atau keandalan produk atau keluaran proses. Informasi tentang potensi bahaya dan risiko mereka serta cara di mana mereka dapat dikendalikan merupakan masukan untuk HACCP.

B.7.4 Proses

HACCP terdiri dari tujuh prinsip-prinsip berikut:
- mengidentifikasi bahaya dan langkah-langkah pencegahan terkait dengan bahaya tersebut;
- menentukan titik-titik dalam proses dimana bahaya dapat dikendalikan atau dihilangkan (titik kendali kritis atau CCP);
- menetapkan batas kritis yang diperlukan untuk mengontrol bahaya, yaitu masing-masing CCP harus beroperasi dalam parameter tertentu untuk memastikan bahaya dikendalikan;

- memonitor batas kritis untuk setiap CCP pada interval didefinisikan;
- menetapkan tindakan koreksi jika proses jatuh batas luar didirikan;
- menetapkan prosedur verifikasi;
- menerapkan pencatatan dan dokumentasi prosedur untuk setiap langkah.

B.7.5 Keluaran

Rekaman yang terdokumentasi termasuk suatu lembar kerja analisis potensi bahaya dan suatu rencana HACCP.

Daftar lembar kerja analisis potensi bahaya untuk setiap langkah dari proses:
- potensi bahaya yang bisa diperkenalkan, dikendalikan atau diperburuk pada langkah ini;
- apakah potensi bahaya saat ini menimbulkan suatu risiko yang signifikan (berdasarkan pertimbangan konsekuensi dan probabilitas dari kombinasi pengalaman, data dan literatur teknis);
- suatu justifikasi untuk signifikansi;
- langkah-langkah pencegahan yang mungkin untuk setiap potensi bahaya;
- apakah pemantauan atau pengendalian tindakan dapat diterapkan pada langkah ini (yaitu apakah itu CCP?).

Rencana HACCP melukiskan prosedur yang harus diikuti untuk menjamin pengendalian dari suatu rancangan, produk, proses atau prosedur tertentu. Rencana tersebut meliputi daftar semua CCP dan untuk setiap CCP:
- batasan kritis bagi langkah-langkah pencegahan;
- pemantauan dan kegiatan pengendalian terus-menerus (termasuk apa, bagaimana, dan kapan pemantauan akan dilakukan dan oleh siapa);
- tindakan perbaikan yang diperlukan jika penyimpangan dari batasan kritis terdeteksi;
- kegiatan verifikasi dan penyimpanan rekaman.

B.7.6 Kekuatan dan keterbatasan

Kekuatan meliputi:
- suatu proses terstruktur yang memberikan bukti terdokumentasi untuk pengendalian kualitas serta pengidentifikasian dan pengurangan risiko;
- suatu fokus pada kepraktisan bagaimana dan di mana, di dalam suatu proses, potensi bahaya bisa dicegah dan risiko dikendalikan;
- pengendalian risiko yang lebih baik selama proses daripada mengandalkan pada pemeriksaan produk akhir;
- suatu kemampuan untuk mengidentifikasi potensi bahaya diperkenalkan melalui tindakan manusia dan bagaimana hal tersebut dapat dikendalikan pada titik pengenalan atau selanjutnya.

Keterbatasan meliputi:
- HACCP mensyaratkan bahwa potensi bahaya diidentifikasi, risiko yang mereka mewakili didefinisikan, dan signifikansi mereka dipahami sebagai masukan untuk proses. Pengendalian yang tepat juga perlu didefinisikan. Hal Ini diperlukan untuk menentukan titik pengendalian kritis dan parameter pengendalian selama HACCP serta mungkin perlu dikombinasikan dengan alat-alat bantu lain untuk mencapai hal tersebut;
- Tindakan diambil ketika parameter pengendalian melebihi batas yang ditetapkan dapat melewati secara bertahap pada parameter pengendalian yang signifikan yang secara statistik dan karenanya sebaiknya ditindaklanjuti.

B.7.7 Dokumen Referensi

ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

B.8 Penilaian toksisitas

B.8.1 Tinjauan singkat

Penilaian risiko lingkungan digunakan di sini untuk mencakup proses yang diikuti dalam penilaian risiko terhadap tanaman, hewan dan manusia sebagai suatu akibat dari paparan berbagai potensi bahaya lingkungan. Manajemen risiko mengacu pada langkah-langkah pengambilan keputusan termasuk evaluasi risiko dan perlakuan risiko.

Metode ini melibatkan penganalisaan potensi bahaya atau sumber bahaya dan bagaimana hal tersebut mempengaruhi target populasi, dan jalur di mana potensi bahaya dapat mencapai suatu target populasi rentan. Informasi ini kemudian dikombinasikan untuk memberikan perkiraan kemungkinan tingkat dan sifat bahaya.

B.8.2 Penggunaan

Proses ini digunakan untuk menilai risiko terhadap tanaman, hewan dan manusia sebagai suatu akibat dari paparan potensi bahaya seperti bahan kimia, mikro-organisme atau spesies lainnya.

Aspek metodologi, seperti analisis jalur yang mengeksplorasi jalur yang berbeda di mana target mungkin terkena sumber risiko, dapat diadaptasi dan digunakan di seluruh rentang yang sangat luas dari daerah risiko yang berbeda, diluar kesehatan manusia dan lingkungannya, serta berguna dalam pengidentifikasian perlakuan untuk mengurangi risiko.

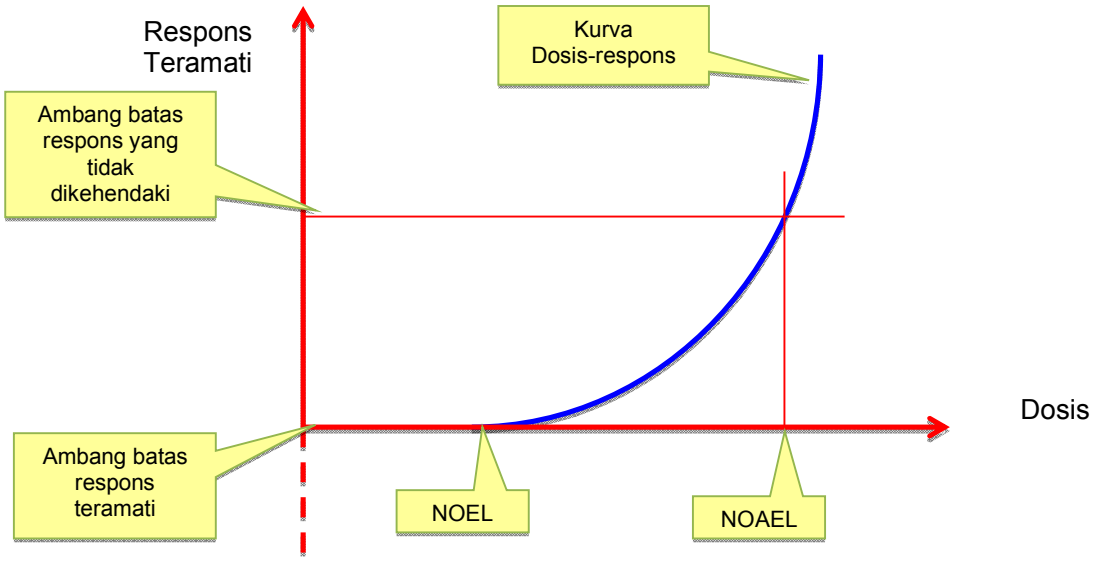
B.8.3 Masukan

Metode ini memerlukan data yang baik pada alam dan sifat dari potensi bahaya, kepekaan dari populasi target (atau populasi) dan cara di mana keduanya berinteraksi. Data ini biasanya didasarkan pada penelitian berbasis laboratorium atau epidemiologi.

B.8.4 Proses

Prosedurnya adalah sebagai berikut:

a) Perumusan masalah - ini termasuk pengaturan ruang lingkup penilaian dengan pendefinisian kisaran ketertarikan populasi target dan jenis potensi bahaya;
b) Identifikasi potensi bahaya - ini melibatkan pengidentifikasian semua sumber bahaya pada populasi target dari potensi bahaya dalam ruang lingkup studi. Identifikasi potensi bahaya biasanya bergantung pada pengetahuan ahli dan tinjauan literatur;
c) Analisis potensi bahaya - ini melibatkan memahami sifat bahaya dan bagaimana berinteraksi dengan target. Misalnya, dalam mempertimbangkan paparan efek kimia, bahaya mungkin termasuk toksisitas akut dan kronis, berpotensi merusak DNA, atau potensi untuk menyebabkan kanker atau cacat lahir. Untuk setiap efek yang berbahaya, besarnya efek (respon) dibandingkan dengan jumlah bahaya yang target terkena (dosis) dan, jika memungkinkan, mekanisme yang efek yang dihasilkan ditentukan. Tingkat di mana tidak ada efek yang dapat diamati (*No Observable Effect*-NOEL) dan tidak ada efek yang tidak dikehendaki yang dapat diamati (*no Observable Adverse Effect*-NOAEL) dicatat. Ini kadang-kadang digunakan sebagai kriteria untuk keberterimaan terhadap risiko.



Gambar B.1 - Kurva dosis-respon

Untuk paparan bahan kimia, hasil tes digunakan untuk memperoleh kurva dosis-respons seperti yang ditunjukkan secara skematis pada Gambar B.1. Ini biasanya berasal dari tes pada hewan atau dari sistem eksperimental seperti kultur jaringan atau sel.

Efek potensi bahaya lain seperti mikro-organisme atau spesies diperkenalkan dapat ditentukan dari data lapangan dan studi epidemiologi. Sifat interaksi penyakit atau hama dengan target yang sudah ditentukan dan probabilitas bahwa tingkat tertentu suatu bahaya dari suatu paparan tertentu untuk potensi bahaya sudah diperkirakan.

d) Analisis paparan - langkah ini meneliti bagaimana zat berbahaya atau residunya mungkin mencapai suatu target populasi rentan dan dalam jumlah berapa. Ini sering melibatkan suatu analisis jalur yang menganggap rute yang berbeda potensi bahaya mungkin ambil, hambatan yang mungkin mencegah dari mencapai target dan faktor-faktor yang mungkin mempengaruhi tingkat paparan. Misalnya, dalam pertimbangan risiko dari penyemprotan bahan kimia analisis paparan akan mempertimbangkan berapa banyak bahan kimia disemprotkan, dengan cara apa dan dalam kondisi apa, apakah ada paparan langsung pada manusia atau hewan, berapa banyak mungkin ditinggalkan sebagai residu pada tanaman hidup , nasib dari lingkungan dimana pestisida mencapai tanah, apakah itu dapat terakumulasi dalam hewan atau apakah itu memasuki air tanah. Dalam biosekuriti, analisis jalur mungkin mempertimbangkan bagaimana hama memasuki negara itu mungkin memasuki lingkungan, menjadi terpancang dan menyebar.

e) Karakterisasi risiko - dalam langkah ini, informasi dari analisis potensi bahaya dan analisis paparan dibawa bersama-sama untuk memperkirakan probabilitas dari konsekuensi tertentu ketika efek dari semua jalur digabungkan. Dimana ada sejumlah besar potensi bahaya atau jalur, suatu penyaringan awal dapat dilakukan dan potensi bahaya rinci serta analisis paparan dan karakterisasi risiko dilakukan pada skenario risiko yang lebih tinggi.

B.8.5 Keluaran

Keluaran biasanya merupakan indikasi tingkat risiko dari paparan atas suatu target tertentu pada potensi bahaya tertentu dalam konteks yang bersangkutan. Risiko dapat dinyatakan secara kuantitatif, semi kuantitatif atau kualitatif. Misalnya, risiko kanker sering dinyatakan secara kuantitatif sebagai suatu probabilitas, bahwa seseorang akan mengidap kanker selama periode tertentu diberi paparan tertentu untuk kontaminan. Semi-kuantitatif analisis dapat digunakan untuk menurunkan indeks risiko untuk kontaminan tertentu atau hama dan keluaran kualitatif mungkin suatu tingkat risiko (misalnya tinggi, sedang, rendah) atau deskripsi dengan data praktis dari dampak yang mungkin.

B.8.6 Kekuatan dan keterbatasan

Kekuatan analisis ini adalah bahwa analisi tersebut memberikan pemahaman yang sangat rinci tentang sifat masalah dan faktor-faktor yang meningkatkan risiko.

Analisis jalur adalah alat yang berguna, umumnya, untuk semua bidang risiko dan persetujuan identifikasi bagaimana dan di mana hal tersebut dimungkinkan untuk meningkatkan pengendalian atau memperkenalkan yang baru.

Memang, bagaimanapun, membutuhkan data yang baik yang sering tidak tersedia atau memiliki tingkat ketidakpastian yang tinggi terkait dengan itu. Misalnya, kurva dosis respon yang berasal dari mengekspos hewan pada potensi bahaya tingkat tinggi harus diekstrapolasi untuk memperkirakan efek dari tingkat yang sangat rendah dari kontaminan untuk manusia dan ada beberapa model dimana ini tercapai. Di mana target adalah lingkungan bukan manusia dan potensi bahaya bukan kimia, data yang langsung relevan dengan kondisi khusus penelitian mungkin terbatas.

B.9 Teknik "apa-jika" terstruktur (*Structured “What-if” Technique*- SWIFT)

B.9.1 Tinjauan singkat

SWIFT pada awalnya dikembangkan sebagai suatu alternatif sederhana untuk HAZOP. Ini adalah suatu studi sistematis, berdasarkan tim, memanfaatkan serangkaian kata-kata 'gegas' atau frase yang digunakan oleh fasilitator dalam lokakarya untuk menstimulasi peserta untuk mengidentifikasi risiko. Fasilitator dan tim menggunakan jenis frase standar 'apa-jika' dalam kombinasi dengan gegasan untuk menyelidiki bagaimana suatu sistem, barang pabrik, organisasi atau prosedur akan terpengaruh oleh penyimpangan dari operasi dan perilaku normal. SWIFT biasanya diterapkan pada banyak tingkatan sistem dengan tingkat yang rinci yang lebih rendah dari HAZOP.

B.9.2 Penggunaan

Sementara SWIFT awalnya dirancang untuk studi potensi bahaya kimia dan pabrik petrokimia, teknik ini saat ini sudah banyak diterapkan untuk sistem, hal terkait pabrik,

prosedur, organisasi umumnya. Secara khusus digunakan untuk meneliti konsekuensi dari perubahan dan risiko sehingga diubah atau dibuat.

B.9.3 Masukan

Sistem, prosedur, barang tanaman dan / atau perubahan harus didefinisikan secara hati-hati sebelum studi dapat dimulai. Kedua konteks eksternal dan internal ditetapkan melalui wawancara dan melalui studi dokumen, rencana dan gambar oleh fasilitator. Biasanya, bagian, situasi atau sistem untuk studi dibagi menjadi simpul atau elemen kunci untuk memudahkan proses analisis tapi ini jarang terjadi pada tingkat definisi yang diperlukan untuk HAZOP.

Masukan kunci lain adalah keahlian dan pengalaman saat ini dari tim studi yang harus dipilih secara hati-hati. Semua pemangku kepentingan sebaiknya diwakili jika mungkin bersama orang-orang dengan pengalaman bagian tersebut, sistem, perubahan atau situasi serupa.

B.9.4 Proses

Proses umum adalah sebagai berikut:

a) Sebelum studi dimulai, fasilitator mempersiapkan suatu daftar kata atau frasa gegas yang sesuai yang mungkin didasarkan pada satu set standar atau dibuat untuk memungkinkan tinjauan komprehensif dari potensi bahaya atau risiko.

b) Pada lokakarya konteks eksternal dan internal dari item, sistem, perubahan atau situasi dan ruang lingkup studi dibahas dan disepakati.

c) Fasilitator meminta peserta untuk menaikkan dan mendiskusikan:
   - risiko yang dikenal dan potensi bahaya;
   - pengalaman dan insiden sebelumnya;
   - pengendalian dan pengamanan yang dikenal dan ada;
   - persyaratan peraturan dan kendala.

d) Diskusi difasilitasi dengan membuat pertanyaan menggunakan sebuah frasa 'apa-jika' dan kata yang gegas atau subjek. Frasa 'apa-jika' yang akan digunakan adalah "bagaimana jika ...", "apa yang akan terjadi jika ...", "bisakah seseorang atau sesuatu ...", "pernahkah seseorang atau sesuatu ...." Tujuannya adalah untuk menstimulasi tim studi dalam pegeksplorasian skenario potensial, penyebab dan konsekuensi dan dampak.

e) Risiko dirangkum dan tim mempertimbangkan pengendalian yang ada.

f) Deskripsi risiko, penyebabnya, konsekuensi dan pengendalian yang diharapkan dikonfirmasi dengan tim dan direkam.

g) Tim mempertimbangkan apakah pengendalian memadai dan efektif serta sesuai denga suatu pernyataan efektivitas pengendalian risiko. Jika ini kurang memuaskan, tim lebih mempertimbangkan tugas perlakuan risiko dan pengendalian potensial didefinisikan.

h) Selama diskusi ini lebih lanjut pertanyaan 'apa-jika' diajukan untuk mengidentifikasi risiko lebih lanjut.

i) Fasilitator menggunakan daftar gegas untuk memantau diskusi dan untuk menyarankan masalah tambahan serta skenario untuk dibahas oleh tim.

j) Adalah normal untuk menggunakan metode penilaian risiko kualitatif atau semi-kuantitatif untuk menentukan peringkat tindakan dibuat dalam hal prioritas. Penilaian risiko ini

biasanya dilakukan dengan memperhitungkan pengendalian yang ada dan efektivitas mereka.

B.9.5 Keluaran

Keluaran termasuk suatu daftar risiko dengan peringkat tindakan atau tugas. Tugas-tugas ini kemudian dapat menjadi dasar untuk suatu rencana perlakuan.

B.9.6 Kekuatan dan keterbatasan

Kekuatan dari SWIFT:
- SWIFT diterapkan secara luas untuk semua bentuk fisik pabrik atau sistem, situasi atau keadaan, organisasi atau kegiatan;
- SWIFT memerlukan persiapan minimal dengan tim;
- SWIFT relatif cepat dan potensi bahaya besar dan risiko cepat menjadi jelas dalam sesi lokakarya;
- studi ini adalah 'berorientasi sistem' dan memungkinkan peserta untuk melihat pada respon sistem untuk penyimpangan bukan hanya pemeriksaan konsekuensi dari kegagalan komponen;
- dapat digunakan untuk mengidentifikasi kesempatan untuk perbaikan proses dan sistem serta umumnya dapat digunakan untuk mengidentifikasi tindakan yang menyebabkan dan meningkatkan probabilitas keberhasilan mereka;
- keterlibatan dalam lokakarya oleh mereka yang bertanggung jawab untuk pengendalian yang ada dan untuk tindakan perlakuan risiko lebih lanjut, memperkuat tanggung jawab mereka;
- SWIFT menciptakan suatu daftar risiko dan rencana perlakuan risiko dengan lebih sedikit usaha;
- sementara bentuk pemeringkatan risiko kualitatif atau semi-kuantitatif sering digunakan untuk penilaian risiko dan guna memprioritaskan perhatian pada tindakan yang menghasilkan, SW IFT dapat digunakan untuk mengidentifikasi risiko dan potensi bahaya yang dapat diambil ke depan ke dalam suatu studi kuantitatif.

Keterbatasan SWIFT:
- SWIFT perlu fasilitator yang berpengalaman dan mampu untuk menjadi efisien;
- persiapan hati-hati diperlukan agar waktu tim lokakarya tidak terbuang;
- jika tim lokakarya tidak memiliki basis pengalaman yang cukup lebar atau jika sistem gegas tidak komprehensif, beberapa risiko atau potensi bahaya tidak dapat diidentifikasi;
- teknik aplikasi tingkat tinggi mungkin tidak mengungkapkan penyebab kompleks, rinci atau berkorelasi.

B.10 Analisis skenario

B.10.1 Tinjauan singkat

Analisis skenario adalah sebuah nama yang diberikan untuk pengembangan model deskriptif tentang bagaimana masa depan mungkin berubah. Hal ini dapat digunakan untuk mengidentifikasi risiko dengan mempertimbangkan kemungkinan perkembangan masa depan dan menjelajahi implikasinya. Set skenario yang mencerminkan (misalnya) 'kasus terbaik', 'kasus terburuk' dan 'kasus yang diharapkan' dapat digunakan untuk menganalisis. Potensi konsekuensi dan probabilitas mereka untuk masing-masing skenario sebagai bentuk analisis sensitivitas ketika penganalisisan risiko.

Kekuatan analisis skenario diilustrasikan dengan mempertimbangkan pergeseran besar selama 50 tahun terakhir dalam teknologi, preferensi konsumen, sikap sosial, dll. Analisa skenario tidak dapat memprediksi probabilitas suatu perubahan tersebut tetapi dapat mempertimbangkan konsekuensi dan bantuan organisasi mengembangkan kekuatan dan ketangguhan yang diperlukan untuk beradaptasi dengan perubahan mendatang.

B.10.2 Penggunaan

Analisis skenario dapat digunakan untuk membantu dalam pembuatan keputusan kebijakan dan perencanaan strategi masa depan serta mempertimbangkan kegiatan yang ada saat ini. Hal ini dapat berperan dalam keseluruhan tiga komponen penilaian risiko. Untuk identifikasi dan analisis, set skenario yang mencerminkan (misalnya) kasus terbaik, kasus terburuk dan kasus 'yang diharapkan' dapat digunakan untuk mengidentifikasi apa yang mungkin terjadi dalam keadaan tertentu dan menganalisis potensi konsekuensi dan probabilitas mereka untuk setiap skenario.

Analisis skenario dapat digunakan untuk mengantisipasi bagaimana kedua ancaman dan kesempatan mungkin berkembang dan dapat digunakan untuk semua jenis risiko baik frame waktu jangka pendek maupun jangka panjang. Dengan frame waktu singkat dan data yang baik, skenario kemungkinan dapat diekstrapolasi dari sekarang. Untuk frame waktu yang lebih lama atau dengan data yang lemah, analisis skenario menjadi lebih imajinatif dan dapat disebut sebagai analisis berjangka.

Analisis skenario mungkin berguna di mana terdapat perbedaan distribusi yang kuat antara hasil keluaran yang positif dan hasil keluaran negatif dalam ruang, waktu dan kelompok di masyarakat atau seuatu organisasi.

B.10.3 Masukan

Prasyarat untuk suatu analisis skenario adalah tim dari orang-orang yang di antara mereka memiliki pemahaman tentang sifat perubahan yang relevan (misalnya kemungkinan kemajuan di teknologi) dan imajinasi untuk berpikir ke masa depan tanpa harus ekstrapolasi dari masa lalu. Akses ke literatur dan data tentang perubahan yang sudah terjadi juga berguna.

B.10.4 Proses

Struktur untuk analisis skenario dapat berupa formal atau informal.

Setelah menetapkan suatu tim dan saluran komunikasi yang relevan, serta didefinisikan konteks masalah dan isu-isu yang harus dipertimbangkan, langkah berikutnya adalah mengidentifikasi sifat perubahan yang mungkin terjadi. Ini akan membutuhkan penelitian tren utama dan waktu kemungkinan perubahan tren serta pemikiran imajinatif tentang masa depan.

Perubahan yang harus dipertimbangkan meliputi:
- perubahan eksternal (seperti perubahan teknologi);
- keputusan yang perlu dibuat dalam waktu dekat tetapi yang mungkin memiliki berbagai hasil keluaran;
- kebutuhan pemangku kepentingan dan bagaimana mereka bisa berubah;
- perubahan dalam lingkungan makro (peraturan, demografi, dll). Beberapa akan terelakkan dan beberapa akan pasti.

Kadang-kadang, suatu perubahan mungkin karena konsekuensi dari risiko lain. Misalnya, risiko perubahan iklim mengakibatkan perubahan permintaan konsumen yang berhubungan

dengan makanan. Hal ini akan mempengaruhi makanan mana yang dapat menguntungkan untuk diekspor serta makanan mana yang dapat tumbuh secara lokal.

Faktor-faktor lokal dan makro atau tren sekarang dapat didaftar dan diperingkat untuk (1) pentingnya (2) ketidakpastian. Perhatian khusus diberikan kepada faktor yang paling penting dan paling pasti. Faktor kunci atau tren yang dipetakan terhadap satu sama lain untuk menunjukkan daerah di mana skenario dapat dikembangkan.

Serangkaian skenario diusulkan dengan masing-masing berfokus pada perubahan yang masuk akal dalam parameter.

Sebuah "cerita" kemudian ditulis untuk setiap skenario yang memberitahu bagaimana Anda mungkin bergerak dari sini menuju skenario subjek. Cerita-cerita mungkin termasuk rincian yang masuk akal yang menambah nilai skenario.

Skenario kemudian dapat digunakan untuk menguji atau mengevaluasi pertanyaan awal. Tes memperhitungkan faktor-faktor yang signifikan namun dapat diprediksi (misalnya pola penggunaan), dan kemudian mengeksplorasi bagaimana 'kesuksesan' kebijakan (aktivitas) akan dalam skenario baru ini, dan hasil keluaran 'pra-tes' dengan menggunakan pertanyaan 'bagaimana jika' berdasarkan pada asumsi model.

Ketika pertanyaan atau proposal telah dievaluasi sehubungan dengan masing-masing skenario, hal tersebut mungkin jelas bahwa itu harus dimodifikasi untuk membuatnya lebih kuat atau kurang berisiko. Hal ini juga harus memungkinkan untuk mengidentifikasi beberapa indikator terkemuka yang menunjukkan ketika perubahan terjadi. Pemantauan dan menanggapi indikator utama dapat memberikan kesempatan untuk perubahan dalam strategi yang direncanakan.

Sejak skenario hanya didefinisikan 'irisan' kemungkinan masa depan, adalah penting untuk memastikan bahwa akun diambil dari probabilitas hasil tertentu (skenario) yang terjadi, yaitu untuk mengadopsi suatu kerangka kerja risiko. Misalnya, di mana skenario kasus terbaik, kasus terburuk dan kasus yang diharapkan digunakan, beberapa upaya sebaiknya dilakukan untuk memenuhi syarat, atau mengungkapkan probablilitas masing-masing skenario yang terjadi.

B.10.5 Keluaran

Mungkin tidak ada skenario terbaik dan pas tetapi sebaiknya diakhiri dengan persepsi yang lebih jelas dari berbagai opsi dan bagaimana memodifikasi tindakan yang dipilih sebagai indikator bergerak.

B.10.6 Kekuatan dan keterbatasan

Analisis skenario memperhitungkan berbagai kemungkinan masa depan yang mungkin lebih baik untuk pendekatan tradisional yang mengandalkan prakiraan tinggi-sedang-rendah yang diasumsikan, melalui penggunaan data historis, bahwa kejadian masa depan mungkin akan terus mengikuti tren masa lalu. Hal ini penting untuk situasi di mana ada sedikit pengetahuan saat ini yang menjadi dasar prediksi atau di mana risiko sedang dipertimbangkan dalam waktu jangka panjang.

Kekuatan ini bagaimanapun memiliki kelemahan terkait yang mana bahwa terdapat ketidakpastian yang tinggi pada beberapa skenario yang mungkin tidak realistis.

Kesulitan utama dalam menggunakan analisis skenario terkait dengan ketersediaan data, dan kemampuan para analis serta pengambil keputusan untuk dapat mengembangkan skenario realistis yang setuju untuk menggali hasil keluaran yang mungkin.

Bahaya penggunaan analisis skenario sebagai alat bantu pengambilan keputusan adalah bahwa skenario yang digunakan mungkin tidak memiliki landasan yang memadai; data tersebut mungkin spekulatif; dan bahwa hasil tidak realistis mungkin tidak diakui seperti itu.

B.11 Analisis dampak bisnis (*Business Impact Analysis* - BIA)

B.11.1 Tinjauan singkat

Analisis dampak bisnis, yang juga dikenal sebagai penilaian dampak bisnis, menganalisis bagaimana risiko-risiko kunci yang mengganggu dapat mempengaruhi operasi sebuah organisasi dan mengidentifikasi serta mengkuantifikasi kemampuan yang dibutuhkan untuk mengelolanya.Secara khusus, BIA menyediakan suatu pengertian yang sama atas:

- identifikasi dan kekritisan dari proses kunci bisnis, fungsi dan sumber-sumber terkait serta interdependensi kunci yang ada untuk suatu organisasi;
- bagaimana kejadian yang mengganggu akan mempengaruhi kapasitas dan kemampuan dalam pencapaian sasaran bisnis yang kritis;
- kapasitas dan kemampuan yang dibutuhkan untuk mengelola dampak dari suatu gangguan dan memulihkan organisasi pada tingkat operasi yang disetujui.

B.11.2 Penggunaan

BIA digunakan untuk menentukan kekritisan dan jangka waktu pemulihan dari proses dan sumber-sumber terkait (orang, peralatan, teknologi informasi) untuk memastikan pencapaian sasaran yang berkelanjutan. Sebagai tambahan, BIA membantu dalam penentuan interdependensi dan hubungan timbal-balik antar proses, pihak internal dan eksternal serta setiap hubungan rantai pasokan.

B.11.3 Masukan

Masukan mencakupi:

- sebuah tim yang melakukan analisis dan mengembangkan suatu rencana;
- informasi tentang sasaran, lingkungan, operasi dan interdependensi dari organisasi;
- rincian aktifitas dan operasi organisasi, termasuk proses, sumber pendukung, hubungan dengan organisasi lain, pengaturan alih daya, pemangku kepentingan;
- konsekuensi kerugian dari proses kritis finansial dan operasional;
- daftar pertanyaan yang disiapkan;
- daftar orang yang diwawancara dari area yang relevan dari organisasi dan/atau pemangku kepentingan yang akan dihubungi;

B.11.4 Proses

BIA dapat dilakukan dengan menggunakan daftar pertanyaan, wawancara, lokakarya terstruktur atau kombinasi dari ketiganya, untuk memperoleh suatu pengertian dari proses kritis, efek kerugian dari proses tersebut dan jangka waktu pemulihan yang diperlukan serta sumber-sumber pendukung.

Langkah-langkah kunci mencakupi:

- berdasarkan pada penilaian risiko dan kerentanan, konfirmasi terhadap proses kunci dan keluaran dari organisasi untuk menentukan kekritisan dari proses;
- penentuan konsekuensi dari suatu gangguan pada proses kritis yang teridentifikasi dalam istilah finansial dan/atau operasional, sepanjang periode yang ditetapkan;
- identifikasi terhadap interdependensi dengan pemangku kepentingan internal dan eksternal. Hal ini dapat mencakup pemetaan sifat dari interdependensi melalui rantai pasokan;
- penentuan sumber-sumber yang saat ini tersedia dan tingkatan penting dari sumber-sumber yang dibutuhkan untuk melanjutkan operasi pada tingkat minimum yang dapat diterima setelah terjadinya suatu gangguan;
- identifikasi solusi alternatif dan proses yang dipakai saat ini atau direncanakan untuk dikembangkan. Solusi alternatif dan proses mungkin butuh untuk dikembangkan dimana sumber-sumber atau kemampuan tidak dapat diakses atau tidak cukup selama terjadinya gangguan;
- penentuan waktu kegagalan maksimal yang dapat diterima (*Maximum Acceptable Outage Time* - MAO) untuk setiap proses berdasarkan pada konsekuensi yang teridentifikasi dan faktor-faktor kesuksesan yang kritis untuk fungsi tersebut. MAO merepresentasikan periode waktu maksimal organisasi dapat mentolerir hilangnya kapabilitas proses tersebut;
- Penentuan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) untuk setiap peralatan khusus atau teknologi informasi. RTO merepresentasikan waktu dimana organisasi bertujuan untuk memulihkan peralatan khusus atau kemampuan informasi teknologi;
- Konfirmasi dari tingkat kesiapan saat ini dari proses kritis untuk mengelola suatu gangguan. Hal ini dapat mencakupi evaluasi tingkat pengulangan dalam proses (seperti suku cadang peralatan) atau eksistensi pemasok yang berganti-ganti.

B.11.5 Keluaran

Keluarannya adalah sebagai berikut:
- daftar prioritas dari proses kritis dan saling ketergantungannya;
- dampak finansial dan operasional yang terdokumentasikan dari suatu proses kritis yang hilang;
- sumber daya pendukung yang dibutuhkan untuk proses kritis yang teridentifikasi;
- kerangka waktu penghentian sementara untuk proses kritis dan kerangka waktu pemulihan informasi teknologi yang terkait.

B.11.6 Kekuatan dan keterbatasan

Kekuataan dari BIA meliputi:
- suatu pengertian dari proses kritis yang mempersiapkan organisasi dengan kemampuan untuk melanjutkan pencapaian sasaran mereka;
- suatu pengertian dari sumber daya yang diperlukan;
- suatu kesempatan untuk mendefinisikan kembali proses operasional dari suatu organisasi untuk membantu ketangguhan organisasi.

Keterbatasan meliputi:
- kekurangan pengetahuan dari partisipan yang terlibat dalam melengkapi daftar pertanyaan, wawancara atau lokakarya;
- dinamika kelompok dapat mempengaruhi analisis yang lengkap dari proses kritis;
- ekspektasi yang menggampangkan atau terlalu optimis dari syarat pemulihan;
- kesulitan dalam mendapatkan tingkat pengertian yang cukup terhadap operasi dan aktifitas organisasi.

B.12 Analisis Akar Penyebab (*Root cause analysis* - RCA)

B.12.1 Tinjauan singkat

Analisis dari suatu kerugian besar untuk mencegah kejadian berulang secara umum disebut Analisis Akar Penyebab (RCA), Analisis Akar Penyebab Kegagalan (RCFA) atau analisis kerugian. RCA difokuskan pada kerugian aset yang disebabkan oleh jenis kegagalan yang bervariasi, sedangkan analisis kerugian utamanya terkonsentrasi dengan kerugian finansial atau ekonomi yang disebabkan oleh faktor eksternal atau malapetaka. Analisis ini mencoba untuk mengidentifikasi akar atau penyebab asal dan bukan hanya berurusan dengan gejala yang langsung tampak. Diakui bahwa tindakan perbaikan tidak selalu sepenuhnya efektif dan perbaikan secara berkelanjutan bisa saja diperlukan. RCA sering diaplikasikan pada evaluasi kerugian besar tetapi dapat juga digunakan untuk menganalisis kerugian yang lebih umum untuk menentukan dimana perbaikan dapat dibuat.

B.12.2 Penggunaan

RCA digunakan dalam beragam kontek dengan penggunaan di area yang luas sebagai berikut:

- RCA berbasis keselamatan digunakan untuk investigasi kecelakaan dan pekerjaan yang berhubungan dengan kesehatan dan keselamatan;
- Analisis kegagalan digunakan dalam sistem teknologi yang berhubungan dengan kehandalan dan perbaikan;
- RCA berbasis produksi digunakan di area pengendalian kualitas untuk industri manufaktur;
- RCA berbasis proses difokuskan dalam proses bisnis;
- RCA berbasis sistem telah dikembangkan sebagai kombinasi dari area-area sebelumnya untuk berurusan dengan sistem yang kompleks dengan aplikasi manajemen perubahan, manajemen risiko dan analisis sistem.

B.12.3 Masukan

Masukan dasar pada Analisis Akar Penyebab adalah semua bukti yang dikumpulkan dari kegagalan atau kerugian. Data dari kegagalan lainnya yang serupa dapat juga dipertimbangkan dalam analisis tersebut. Masukan lainnya dapat berupa hasil yang digunakan untuk menguji hipotesis tertentu.

B.12.4 Proses

Pada saat kebutuhan untuk Analisis Akar Penyebab diidentifikasi, sekelompok ahli ditunjuk untuk melalukan analisis dan membuat rekomendasi. Tipe ahli akan sangat tergantung pada keahlian tertentu yang dibutuhkan untuk menganalisa kegagalan tersebut.

Walaupun metode yang berbeda dapat digunakan untuk melakukan analisis, langkah dasar dalam mengeksekusi suatu Analisis Akar Penyebab adalah serupa dan:

- membentuk suatu tim;
- membuat cakupan dan sasaran dari RCA tersebut;
- mengumpulkan data dan bukti dari kegagalan atau kerugian;
- melakukan suatu analisis terstruktur untuk menentukan akar masalah;
- mengembangkan solusi dan membuat rekomendasi;
- menerapkan rekomendasi tersebut;
- memverifikasi kesuksesan dari rekomendasi yang diterapkan;
- teknik analisis terstruktur dapat satu dari hal-hal berikut:

- teknik "5 kenapa"; seperti mengulang pertanyaan "kenapa?" untuk mengupas lapisan-lapisan penyebab dan sub-penyebab.
- analisis modus kegagalan dan dampak;
- analisis pohon kesalahan;
- diagram tulang ikan atau Ishikawa;
- analisis Pareto;
- pemetaan akar masalah.

Evaluasi terhadap penyebab seringkali berlangsung mulai dari penyebab berbentuk bukti fisik, hingga ke penyebab yang berkaitan dengan manusia, dan akhirnya pada hal-hal pengelolaan yang mendasar atau penyebab yang fundamental. Faktor penyebab harus dapat dikendalikan atau dieliminasi oleh pihak-pihak yang terlibat agar tindakan perbaikan dapat efektif dan bermanfaat.

B.12.5 Keluaran

Keluaran dari suatu RCA meliputi:
- dokumentasi data dan bukti yang dikumpulkan;
- hipotesa yang dipertimbangkan;
- kesimpulan mengenai akar masalah yang paling mungkin terjadi untuk kegagalan atau kerugian;
- rekomendasi untuk tindakan perbaikan.

B.12.6 Kekuatan dan keterbatasan

Kekuatan meliputi
- keterlibatan dari ahli terkait yang bekerja dalam lingkungan tim;
- analisis terstruktur;
- pertimbangan dari semua hipotesa yang mungkin;
- dokumentasi hasil;
- kebutuhan untuk menghasilkan rekomendasi akhir.

Keterbatasan dari suatu RCA:
- ahli yang dibutuhkan bisa jadi tidak tersedia;
- bukti kritis dapat terhancurkan dalam suatu kegagalan atau terhapus saat pembersihan;
- tim bisa jadi tidak punya cukup waktu atau sumber daya untuk mengevaluasi situasi tersebut secara keseluruhan;
- bisa jadi tidak dimungkinan untuk menerapkan rekomendasi secara memadai.

B.13 Analisis modus kegagalan dan dampak (*Failure modes and effects analysis* - FMEA) dan analisis modus kegagalan dan dampak serta kekritisan (*Failure modes and effects and criticality analysis* - FMECA)

B.13.1 Tinjauan singkat

Analisis modus kegagalan dan dampak (*Failure modes and effects analysis* - FMEA) adalah suatu teknik yang digunakan untuk mengidentifikasi cara dimana komponen, sistem atau proses dapat gagal untuk memenuhi rancangan yang dimaksud.

FMEA mengidentifikasi:
- semua potensi modus kegagalan dari beragam bagian dari suatu sistem (suatu modus kegagalan adalah apa yang diamati untuk gagal atau bekerja tidak semestinya);
- akibat kegagalan yang bisa terdapat pada sistem tersebut;

- mekanisme kegagalan;
- bagaimana menghindari kegagalan, dan/atau memitigasi akibat dari kegagalan pada sistem tersebut.

FMECA memperpanjang suatu FMEA sehingga setiap modus kegagalan yang teridentifikasi diperingkat menurut tingkat kepentingan atau kekritisannya.

Analisis kekritisan biasanya bersifat kualitatif atau semi-kuantitatif tapi bisa dikuantifikasi dengan menggunakan tingkat kegagalan yang sebenarnya.

B.13.2 Penggunaan

Ada beberapa aplikasi dari FMEA: Rancangan (atau produk) FMEA yang digunakan untuk komponen dan produk, sistem FMEA yang digunakan untuk sistem, Proses FMEA yang digunakan untuk manufaktur dan proses perakitan, Layanan FMEA dan perangkat lunak FMEA.

FMEA / FMECA dapat diaplikasikan selama proses rancangan, pembuatan atau operasi dari suatu sistem fisik.

Untuk memperbaiki ketergantungan, namun, perubahan biasanya lebih muda diimplementasikan pada tahap rancangan. FMEA dan FMECA dapat juga diaplikasikan untuk proses dan prosedur. Sebagai contoh, FMEA dan FMECA digunakan untuk mengidentifikasi potensi untuk kesalahan medis pada sistem kesehatan dan kegagalan dalam prosedur perbaikan.

FMEA/FMECA dapat digunakan untuk:
- membantu dalam memilih alternatif rancangan dengan ketergantungan yang tinggi,
- memastikan semua modus kegagalan dari sistem dan proses, beserta akibatnya pada kesuksesan operasional telah dipertimbangkan,
- mengidentifikasi modus dan akibat kesalahan manusia,
- menyediakan suatu dasar untuk perencanaan pengujian dan perbaikan sistem fisik,
- memperbaiki rancangan proses dan prosedur,
- menyediakan informasi kualitatif atau kuantitatif untuk teknik analisis seperti analisis pohon kesalahan.

FMEA dan FMECA dapat menyediakan masukan untuk teknik analisis yang lain seperti analisis pohon kesalahan di salah satu tingkat kualitatif atau kuantitatif.

B.13.3 Masukan

FMEA dan FMECA membutuhkan informasi yang cukup rinci mengenai elemen-elemen dari sistem untuk melakukan analisis mendalam tentang bagaimana setiap elemen tersebut dapat gagal. Untuk suatu Rancangan FMEA yang rinci, elemen tersebut dapat berada pada tingkat komponen individu yang rinci, sedangkan untuk Sistem FMEA dengan tingkat yang lebih tinggi, elemen tersebut dapat didefinisikan pada suatu tingkatan yang lebih tinggi.

Informasi bisa mencakupi:
- gambar atau suatu diagram alir dari sistem yang dianalisis dan komponennya, atau langkah dari suatu proses;
- suatu pengertian dari fungsi setiap langkah suatu proses atau komponen dari suatu sistem;
- rincian dari lingkungan dan parameter lainnya, yang bisa mempengaruhi operasi;
- suatu pengertian terhadap hasil dari kegagalan tertentu;
- informasi historis atas kegagalan termasuk data tingkat kegagalan jika tersedia.

B.13.4 Proses

Proses FMEA adalah sebagai berikut:
a) menetapkan cakupan dan sasaran dari studi tersebut;
b) membentuk suatu tim;
c) memahami sistem / proses yang akan diarahkan pada FMECA;
d) memperinci sistem tersebut ke dalam komponen atau langkah-langkahnya;
e) menetapkan fungsi dari setiap langkah atau komponen;
f) identifikasi untuk setiap komponen atau langkah yang terdaftar:
   - bagaimana setiap bagian yang gagal dapat dipahami?
   - mekanisme apa yang dapat menghasilkan modus kegagalan tersebut?
   - apa dampak yang dapat timbul jika kegagalan terjadi?
   - apakah kegagalan tersebut tidak membahayakan atau merusak?
   - bagaimana kegagalan tersebut dideteksi?
g) mengidentifikasi ketentuan yang melekat dalam rancangan untuk mengkompensasi kegagalan tersebut.

Untuk FMECA, tim studi melanjutkan untuk mengklasifikasi setiap modus kegagalan yang teridentifikasi sesuai dengan kekritisannya.

Ada beberapa cara hal ini dapat dilakukan. Metode yang umum mencakupi:
- indeks modus kekritisan;
- tingkat risiko;
- angka prioritas risiko.

Kekritisan model adalah suatu ukuran probablilitas dimana modus yang dipertimbangkan akan menghasilkan kegagalan sistem secara keseluruhan; hal ini didefinisikan sebagai:

Probabilitas dampak kegagalan * modus tingkat kegagalan * Waktu Operasi dari sistem tersebut

Hal ini paling sering diterapkan pada kegagalan peralatan dimana setiap bagian dapat didefinisikan secara kuantitatif dan semua modus kegagalan memiliki konsekuensi yang sama.

Tingkat risiko diperoleh dengan menggabungkan konsekuensi dari suatu modus kegagalan yang sedang terjadi dengan kemungkinan kegagalan tersebut. Hal ini digunakan ketika konsekuensi dari beragam modus kegagalan yang berbeda dan dapat diterapkan pada sistem atau proses peralatan. Tingkat risiko dapat diekspresikan secara kualitatif, semi-kuantitatif atau kuantitatif.

Angka prioritas risiko (*Risk Priority Number*-RPN) adalah ukuran semi-kuantitatif dari kekritisan yang diperoleh dengan mengalikan angka dari skala peringkat (biasanya antara 1 dan 10) untuk konsekuensi kegagalan, kemungkinan-kejadian kegagalan dan kemampuan untuk mendeteksi masalah. (Suatu kegagalan diberikan suatu prioritas yang lebih tinggi jika kegagalan itu susah untuk dideteksi.) Metode ini sering kali digunakan dalam aplikasi penjaminan mutu.

Segera sesudah modus kegagalan dan mekanisme teridentifikasi, tindakan perbaikan dapat didefinisikan dan diimplementasikan untuk modus kegagalan yang lebih penting.

FMEA didokumentasikan dalam suatu laporan yang berisi:
- detil dari suatu sistem yang dianalisis;
- cara pelaksanaan dilakukan;

- asumsi yang dibuat dalam analisis tersebut;
- sumber data;
- hasil, termasuk lembar kerja yang lengkap;
- kekritisan (jika lengkap) dan metodologi yang digunakan untuk mendefinisikannya;
- setiap rekomendasi untuk analisis lebih lanjut, perubahan desain atau fitur yang digabungkan dalam rencana uji, dll.

Sistem tersebut dapat dinilai kembali oleh siklus lain dari FMEA setelah tindakan telah selesai dilakukan.

B.13.5 Keluaran

Keluaran utama dari FMEA adalah suatu daftar modus kegagalan, mekanisme kegagalan dan efek dari setiap komponen atau langkah dari suatu sistem atau proses (yang dapat mencakupi informasi kemungkinan-kejadian kegagalan). Informasi juga diberikan pada penyebab kegagalan dan konsekuensinya terhadap sistem secara keseluruhan. Keluaran dari FMECA mencakupi suatu peringkat kepentingan berdasarkan pada kemungkinan-kejadian sistem tersebut akan gagal, tingkat risiko akibat dari modus kegagalan atau suatu kombinasi dari tingkat risiko dan kemampuan mendeteksi modus kegagalan.

FMECA dapat memberikan suatu keluaran kuantitatif jika data tingkat kegagalan yang sesuai dan konsekuensi kuantitatif digunakan.

B.13.6 Kekuatan dan keterbatasan

Kekuatan dari FMEA/FMECA adalah sebagai:
- berlaku secara luas pada modus kegagalan manusia, peralatan dan sistem, dan pada perangkat keras, perangkat lunak dan prosedur;
- mengidentifikasi modus kegagalan komponen, penyebab dan pengaruhnya terhadap sistem, dan mempresentasikannya dalam format yang mudah dibaca;
- menghindari kebutuhan akan modifikasi peralatan yang mahal dalam pelayanan dengan mengidentifikasi masalah pada awal proses perancangan;
- mengidentifikasi modus kegagalan satu titik dan persyaratan untuk sistem redundansi atau keselamatan;
- memberikan masukan kepada program pemantauan pengembangan dengan menyoroti fitur utama yang harus dipantau.

Keterbatasan meliputi:
- FMEA/FMECA hanya dapat digunakan untuk mengidentifikasi modus kegagalan tunggal, bukan kombinasi modus kegagalan;
- kecuali dikendalikanl dan difokuskan secara memadai, penelitian dapat memakan waktu dan biaya;
- FMEA/FMECA bisa sulit dan membosankan untuk sistem multi-layer yang kompleks.

B.13.7 Dokumen Referensi

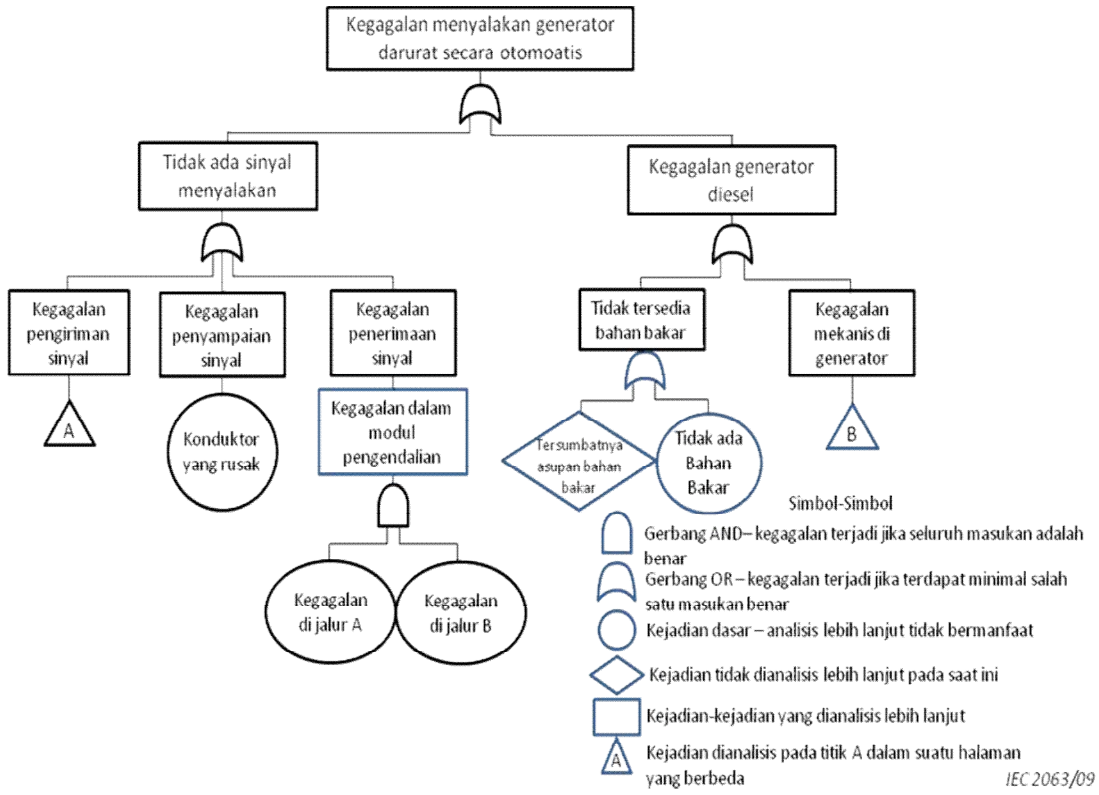
IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)*

B.14 Analisis Pohon Kesalahan (*Fault Tree Analysis*-FTA)

B.14.1 Tinjauan singkat

FTA adalah teknik untuk mengidentifikasi dan menganalisis faktor yang dapat berkontribusi pada kejadian yang tidak diinginkan (disebut "kejadian puncak"). Faktor penyebab diidentifikasi secara deduktif, disusun secara logis dan tergambar dalam bentuk diagram pohon yang menggambarkan faktor penyebab dan hubungan logis antara faktor penyebab tersebut dengan kejadian puncak.

Faktor-faktor yang diidentifikasi pada pohon tersebut dapat berupa kejadian yang terkait dengan kegagalan komponen perangkat keras, kesalahan manusia atau kejadian terkait lainnya yang menyebabkan kejadian yang tidak diinginkan.



Gambar B.2 - Contoh dari suatu FTA dari IEC 60300-3-9

B.14.2 Penggunaan

Suatu pohon kesalahan dapat digunakan secara kualitatif untuk mengidentifikasi penyebab potensial dan jalur menuju kegagalan (kejadian puncak) atau secara kuantitatif untuk menghitung probablilitas kejadian puncak, dengan mengetahui probabilitas dari sebab-akibat kejadian.

Pohon kesalahan dapat digunakan pada tahap perancangan sistem untuk mengidentifikasi penyebab kegagalan potensial dan karenanya dapat digunakan untuk memilih opsi dari beberapa rancangan yang berbeda. Pohon kesalahan dapat digunakan pada tahap operasi untuk mengidentifikasi kegagalan besar apa saja yang dapat terjadi dan tingkat relatif

kepentingannya dari jalur yang berbeda terhadap kejadian utama. Pohon kesalahan juga dapat digunakan untuk menganalisis suatu kegagalan yang terjadi untuk menampilkan secara diagram bagaimana kejadian yang berbeda bersamaan menyebabkan kegagalan.

B.14.3 Masukan

Untuk analisis kualitatif, diperlukan pemahaman tentang sistem dan penyebab kegagalan, serta pemahaman teknis bagaimana sistem dapat gagal. Diagram rinci berguna untuk membantu analisis.

Untuk analisis kuantitatif, data tentang tingkat kegagalan atau probabilitas untuk menjadi gagal diperlukan bagi semua kejadian dasar di dalam pohon kesalahan.

B.14.4 Proses

Langkah untuk pengembangan suatu pohon kesalahan adalah sebagai berikut:

- Kejadian puncak yang akan dianalisis didefinisikan. Ini mungkin sebuah kegagalan atau mungkin hasil yang lebih luas dari kegagalan itu. Dimana hasil keluarannya dianalisis, pohon tersebut mungkin berisi bagian yang berkaitan dengan mitigasi kegagalan sebenarnya.
- Dimulai dengan kejadian puncak, kemungkinan penyebab langsung atau modus kegagalan yang mengarah ke kejadian puncak diidentifikasi.
- Masing-masing sebab/modus kesalahan ini dianalisis untuk mengidentifikasi bagaimana kegagalannya dapat disebabkan.
- Identifikasi langkah demi langkah dari operasi sistem yang tidak diinginkan diikuti dengan tingkat sistem yang lebih rendah sampai analisis lebih lanjut menjadi tidak produktif. Dalam sistem perangkat keras, ini mungkin merupakan tingkat kegagalan komponen. Kejadian dan faktor penyebab pada tingkat sistem terendah yang dianalisis dikenal sebagai kejadian dasar.
- Dimana probabilitas dapat ditugaskan pada kejadian dasar, probabilitas kejadian puncak dapat dihitung. Agar kuantifikasi menjadi valid, maka harus dapat ditunjukkan bahwa, untuk setiap pintu masuk, semua masukan adalah perlu dan cukup untuk menghasilkan kejadian keluaran. Jika ini tidak terjadi, pohon kesalahan tidak valid untuk analisis kemungkinan tapi mungkin menjadi alat yang berguna untuk menampilkan hubungan sebab-akibat.

Sebagai bagian dari kuantifikasi pohon kesalahan mungkin perlu untuk disederhanakan dengan menggunakan aljabar Boolean untuk memperhitungkan modus kegagalan yang terduplikasi.

Sepanjang untuk penyediaan perkiraan probabilitas dari kejadian utama, kumpulan potongan minimal (minimal *cut sets*) dapat diidentifikasi dan pengaruhnya terhadap kejadian utama dapat dihitung. Dengan demikian maka jalur individu terpisah terarah ke kejadian utama tersebut dapat dibentuk.

Kecuali untuk pohon kesalahan sederhana, suatu paket perangkat lunak dibutuhkan untuk menangani perhitungan secara tepat ketika kejadian berulang ada di beberapa tempat di pohon kesalahan, serta untuk memerhitungkan kumpulan potongan minimal. Perangkat lunak membantu memastikan konsistensi, kebenaran, dan keterujian.

B.14.5 Keluaran

Keluaran dari analisis pohon kesalahan adalah sebagai berikut:

- suatu representasi bergambar tentang bagaimana kejadian puncak dapat terjadi yang menunjukkan jalur interaksi di mana dua atau lebih kejadian secara simultan pasti terjadi;
- suatu daftar kumpulan potongan minimal (jalur individu menuju kegagalan) dengan (dimana data tersedia).
- probabilitas bahwa setiap keluaran akan terjadi;
- probabilitas kejadian puncak.

B.14.6 Kekuatan dan keterbatasan

Kekuatan dari FTA:
- FTA memberikan pendekatan disiplin yang sangat sistematis, namun pada saat bersamaan cukup fleksibel untuk memungkinkan analisis dari berbagai faktor, termasuk interaksi manusia dan fenomena fisik.
- Penerapan pendekatan "atas-bawah", yang tersirat dalam teknik ini, memusatkan perhatian pada efek kegagalan yang terkait langsung dengan kejadian puncak.
- FTA sangat berguna untuk menganalisis sistem dengan banyak antarmuka dan interaksi.
- Representasi bergambar mengarah pada pemahaman yang mudah tentang perilaku sistem dan faktor-faktor yang termasuk di dalamnya, namun karena pohon tersebut seringkali besar, pemrosesan pohon kesalahan mungkin memerlukan sistem komputer. Fitur ini memungkinkan hubungan logis yang lebih kompleks untuk disertakan (misalnya NAND dan NOR) tetapi juga membuat verifikasi pohon kesalahan sulit dilakukan.
- Analisis logika pohon kesalahan dan identifikasi kumpulan potongan berguna untuk mengidentifikasi jalur kegagalan sederhana di dalam sistem yang sangat kompleks di mana kombinasi kejadian tertentu yang mengarah pada kejadian puncak dapat diabaikan.

Keterbatasan mencakupi:
- Ketidakpastian dalam probabilitas kejadian dasar dimasukkan dalam perhitungan probabilitas kejadian puncak. Hal ini dapat menyebabkan tingkat ketidakpastian yang tinggi di mana probabilitas kegagalan kejadian dasar tidak diketahui secara akurat; namun, tingkat kepercayaan yang tinggi dimungkinkan dalam sistem yang dipahami dengan baik.
- Dalam beberapa situasi, kejadian sebab akibat tidak terikat bersama dan sulit untuk memastikan apakah semua jalur penting menuju kejadian puncak disertakan. Misalnya, termasuk semua sumber pengapian dalam suatu analisis suatu kebakaran sebagai suatu kejadian puncak. Dalam situasi ini analisis probilitas tidak dimungkinkan.
- Pohon kesalahan adalah model statis; interdependensi waktu tidak dibahas.
- Pohon kesalahan hanya bisa berurusan dengan keadaan biner (gagal/tidak gagal) saja.
- Sementara modus kesalahan manusia dapat dimasukkan dalam suatu pohon kesalahan kualitatif, pada umumnya derajat kegagalan atau kualitas yang sering mencirikan kesalahan manusia tidak dapat dengan mudah disertakan;
- Suatu pohon kesalahan tidak memungkinkan efek domino atau kegagalan bersyarat untuk disertakan dengan mudah.

B.14.7 Dokumen acuan

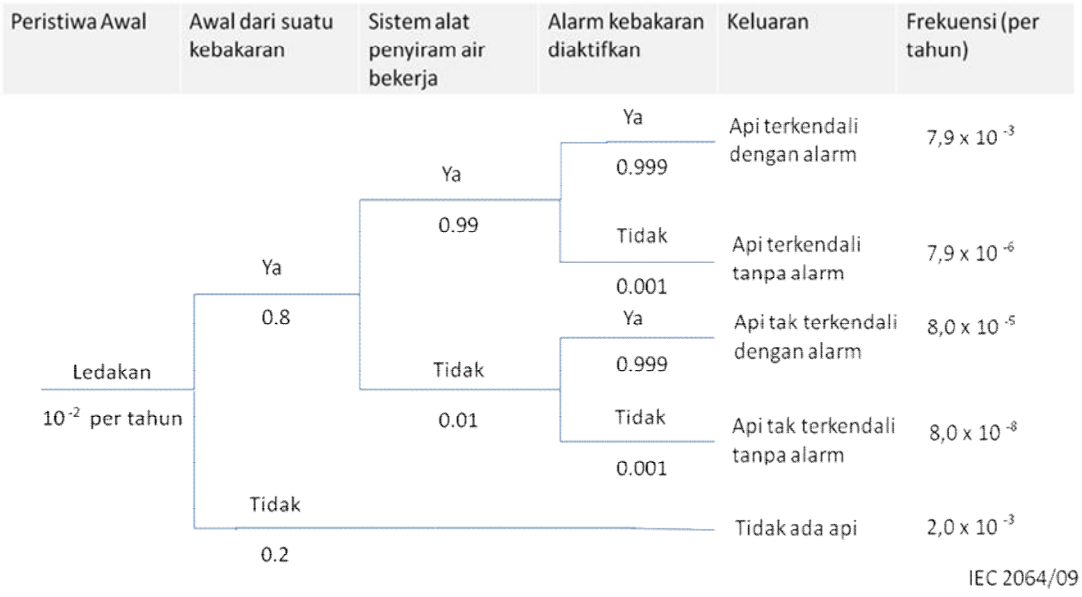
IEC 61025*, Fault tree analysis (FTA)*

IEC 60300-3-9, *Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems*

B.15 Analisis pohon kejadian (*Event tree analysis - ETA*)

B.15.1 Tinjauan singkat

ETA adalah teknik grafis untuk merepresentasikan urutan kejadian yang saling eksklusif mengikuti suatu kejadian inisiasi sesuai dengan berfungsinya/tidak berfungsinya berbagai sistem yang dirancang untuk memitigasi konsekuensinya (lihat Gambar B.3). Hal ini dapat diterapkan baik secara kualitatif maupun kuantitatif.



Gambar B.3 - Contoh dari suatu pohon kejadian

Gambar B.3 memperlihatkan perhitungan sederhana untuk suatu pohon kejadian, ketika cabang sepenuhnya independen.

Dengan bercabang-cabang seperti pohon, ETA mampu mewakili kejadian yang mengganggu atau memitigasi sebagai respon terhadap kejadian awal, dengan mempertimbangkan sistem tambahan, fungsi atau hambatan.

B.15.2 Penggunaan

ETA dapat digunakan untuk pemodelan, penghitungan dan pemeringkatan (dari sudut pandang suatu risiko) skenario kecelakaan yang berbeda mengikuti kejadian awal ETA yang dapat digunakan pada tahap apapun dalam siklus hidup suatu produk atau proses. Ini dapat digunakan secara kualitatif untuk membantu melakukan curah pikiran skenario potensial dan urutan kejadian mengikuti kejadian inisiasi dan bagaimana hasil keluaran dipengaruhi oleh berbagai perlakuan, hambatan atau pengendalian yang dimaksudkan untuk memitigasi hasil keluaran yang tidak diinginkan.

Analisis kuantitatif cocok untuk mempertimbangkan penerimaan pengendalian. Hal ini paling sering digunakan untuk memodelkan kegagalan di mana ada banyak perlindungan.

ETA dapat digunakan untuk memodelkan kejadian inisiasi yang mungkin membawa kerugian atau keuntungan. Akan tetapi, keadaan dimana jalur untuk mengoptimalkan keuntungan yang dicari lebih sering dimodelkan dengan menggunakan pohon keputusan.

B.15.3 Masukan

Masukan mencakupi:
- suatu daftar dari kejadian inisiasi yang tepat;
- informasi terhadap perlakuan, hambatan dan pengendalian, dan kemungkinan kegagalannya (untuk analisis kuantitatif);
- pemahaman proses dimana kegagalan awal meningkat.

B.15.4 Proses

Suatu pohon kejadian dimulai dengan memilih suatu kejadian initiasi. Hal ini mungkin berupa suatu insiden seperti ledakan debu atau suatu kejadian sebab akibat seperti kegagalan daya. Fungsi atau sistem yang ada untuk memitigasi hasil kemudian dicantumkan secara berurutan. Untuk setiap fungsi atau sistem, suatu kesimpulan ditarik untuk merepresentasikan keberhasilan atau kegagalannya. Kemungkinan kegagalan tertentu dapat diberikan untuk setiap baris, dengan kemungkinan bersyarat yang diperkirakan misalnya dengan penilaian ahli atau suatu analisis pohon kegagalan. Dengan cara ini, jalur yang berbeda dari kejadian inisiasi dimodelkan.

Perhatikan bahwa probabilitas pada pohon kejadian adalah probabilitas bersyarat, misalnya probabilitas dari alat penyiram air (*sprinkler*) berfungsi bukanlah probabilitas yang diperoleh dari pengujian dalam kondisi normal, melainkan probabilitas berfungsinya dalam kondisi kebakaran yang disebabkan oleh ledakan.

Setiap jalur yang melalui pohon tersebut merepresentasikan probabilitas bahwa semua kejadian di jalur tersebut akan terjadi. Oleh karena itu, frekuensi dari hasil keluaran direpresentasikan dengan pengalian kemungkinan kondisional individu dan frekuensi dari kejadian inisiasi tersebut, mengingat bahwa berbagai kejadian bersifat independen.

B.15.5 Keluaran

Keluaran dari ETA mencakupi berikut ini:
- deskripsi kualitatif tentang masalah potensial sebagai kombinasi kejadian yang menghasilkan berbagai jenis masalah (kisaran hasil) dari kejadian inisiasi;
- perkiraan kuantitatif dari frekuensi kejadian atau kemungkinan dan kepentingan relatif dari berbagai urutan kegagalan dan kejadian yang berkontribusi;
- daftar rekomendasi untuk mengurangi risiko;
- evaluasi kuantitatif terhadap efektivitas rekomendasi.

B.15.6 Kekuatan dan keterbatasan

Kekuatan dari ETA termasuk sebagai berikut:
- ETA menampilkan skenario potensial mengikuti kejadian inisiasi, dianalisis dan pengaruh keberhasilan atau kegagalan memitigasi sistem atau fungsi dalam suatu cara bagan yang jelas;
- ETA memperhitungkan efek waktu, ketergantungan dan efek domino yang tidak praktis untuk dimodelkan pada pohon kesalahan;
- ETA secara grafis merepresentasikan urutan kejadian yang tidak mungkin diwakili saat menggunakan pohon kesalahan.

Keterbatasan mencakupi:
- untuk menggunakan ETA sebagai bagian dari penilaian komprehensif, semua kejadian inisiasi potensial perlu diidentifikasi. Hal ini dapat dilakukan dengan menggunakan metode

analisis lainnya (misalnya HAZOP, PHA), akan tetapi, selalu ada potensi untuk kehilangan beberapa kejadian inisiasi yang penting;
- dengan pohon kejadian, hanya keadaan keberhasilan dan kegagalan dari suatu sistem yang ditangani, dan sulit untuk melibatkan kejadian keberhasilan yang tertunda atau pemulihan;
- jalur apapun mempersyaratkan kejadian yang terjadi pada titik cabang sebelumnya di sepanjang jalur tersebut. Oleh karena itu banyak kebergantungan di sepanjang jalur yang perlu ditangani. Akan tetapi, beberapa kebergantungan, seperti komponen umum, sistem dan operator utilitas, dapat terabaikan jika tidak ditangani dengan hati-hati, sehingga dapat menyebabkan perkiraan risiko yang optimis.

B.16 Analisis sebab-konsekuensi (*Cause-consequence analysis*)

B.16.1 Umum

Analisis sebab-konsekuensi pada awalnya dikembangkan sebagai alat kehandalan sistem kritis keselamatan untuk memberikan suatu pemahaman yang lebih lengkap tentang kegagalan sistem. Seperti analisis pohon kesalahan, analisis ini digunakan untuk merepresentasikan logika kegagalan yang mengarah kepada suatu kejadian kritis namun analisis ini menambahkan fungsionalitas suatu pohon kesalahan dengan menyebabkan kegagalan sekuensial waktu untuk dapat dianalisis. Metode ini juga memungkinkan penundaan waktu dimasukkan ke dalam analisis konsekuensi yang tidak mungkin dilakukan dengan pohon kejadian.

B.16.2 Penggunaan

Analisis sebab-konsekuensi pada awalnya dikembangkan sebagai alat kehandalan sistem kritis keselamatan untuk memberikan suatu pemahaman yang lebih lengkap tentang kegagalan sistem. Seperti analisis pohon kesalahan, analisis ini digunakan untuk merepresentasikan logika kegagalan yang mengarah kepada suatu kejadian kritis namun analisis ini menambahkan fungsionalitas suatu pohon kesalahan dengan menyebabkan kegagalan sekuensial waktu untuk dapat dianalisis. Metode ini juga memungkinkan penundaan waktu dimasukkan ke dalam analisis konsekuensi yang tidak mungkin dilakukan dengan pohon kejadian.

Metode ini digunakan untuk menganalisis berbagai jalur dari suatu sistem yang mengikuti kejadian kritis tertentu yang tergantung dari berbagai perilaku subsistem(contohnya sistem tanggap darurat). Jika dikuantifikasi, mereka akan memberikan estimasi probabilitas dari berbagai kemungkinan konsekuensi berbeda yang mengikuti suatu kejadian kritis.

Karena setiap urutan dalam suatu diagram sebab-konsekuensi adalah suatu kombinasi dari pohon sub-kesalahan, analisis sebab-konsekuensi dapat digunakan sebagai suatu alat untuk membangun pohon besar kesalahan.

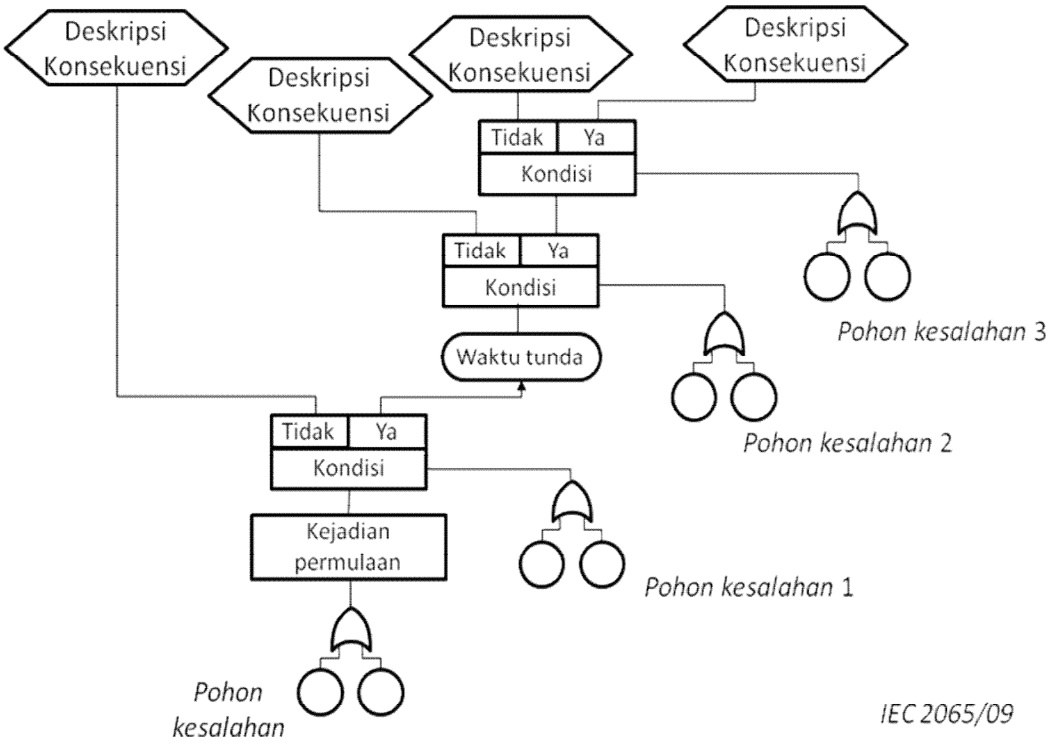
Diagram tersebut kompleks untuk dibuat dan digunakan, serta cenderung untuk digunakan ketika besaran potensi konsekuensi kegagalan membenarkan usaha yang intensif.

B.16.3 Masukan

Pemahaman tentang sistem dan modus kegagalannya serta skenario kegagalannya diperlukan.

B.16.4 Proses

Gambar B.4 menunjukkan diagram konseptual dari suatu analisis sebab-konsekuensi yang khas.



Gambar B.4 – Contoh dari analisis sebab-konsekuensi

Prosedur tersebut adalah sebagai berikut:

a) Identifikasi kejadian kritis (atau inisiasi) (setara dengan kejadian puncak dari suatu pohon kesalahan dan kejadian inisiasi dari suatu pohon kejadian).
b) Mengembangkan dan memvalidasi pohon kesalahan untuk penyebab dari kejadian inisiasi seperti yang dijelaskan dalam Klausul B.14. Simbol yang sama digunakan seperti dalam analisis pohon kesalahan konvensional.
c) Tentukan urutan dimana kondisi dipertimbangkan. Ini seharusnya menjadi suatu urutan logis seperti urutan waktu di mana mereka terjadi.
d) Bangun jalur untuk konsekuensi tergantung pada kondisi yang berbeda. Ini mirip dengan suatu pohon kejadian tetapi pembagian jalur dari pohon kejadian ditunjukkan sebagai suatu kotak berlabel dengan kondisi tertentu yang berlaku.
e) Apabila kegagalan untuk setiap kotak kondisi bersifat independen, probabilitas dari setiap konsekuensi dapat dihitung. Hal ini dicapai dengan pertama menetapkan probabilitas untuk setiap keluaran dari kotak kondisi (dengan menggunakan pohon kesalahan yang sesuai). Probabilitas dari urutan apa saja yang mengarah pada konsekuensi tertentu diperoleh dengan mengalikan probabilitas dari setiap urutan kondisi yang berakhir pada konsekuensi tersebut. Jika lebih dari satu urutan berakhir dengan konsekuensi yang sama, probabilitas dari setiap urutan ditambahkan. Jika ada ketergantungan antara kegagalan kondisi dalam suatu urutan (misalnya, suatu kegagalan daya dapat menyebabkan beberapa kondisi untuk gagal) maka dependensi harus ditangani terlebih dahulu sebelum perhitungan.

B.16.5 Keluaran

Keluaran dari analisis sebab-konsekuensi adalah suatu representasi diagram tentang bagaimana suatu sistem dapat gagal yang menunjukkan sebab dan konsekuensinya. Suatu estimasi kemungkinan dari kejadian setiap potensi konsekuensi berdasarkan pada analisis probabilitas peristiwa atas kondisi tertentu yang mengikuti kejadian kritis.

B.16.6 Kekuatan dan keterbatasan

Keuntungan dari analisis sebab-konsekuensi adalah sama dengan keuntungan yang dimiliki oleh pohon kejadian dan pohon kesalahan yang digabungkan. Sebagai tambahan, analisis ini juga mengatasi beberapa keterbatasan dari teknik pohon kejadian dan pohon kesalahan dengan dapat menganalisis kejadian yang berkembang dari waktu ke waktu. Analisis sebab-konsekuensi memberikan suatu pandangan menyeluruh tentang sistem tersebut.

Keterbatasannya adalah analisis ini lebih kompleks daripada analisis pohon kesalahan dan analisis pohon kejadian, baik untuk membangunnya maupun dalam hal berhadapan dengan dependensi selama proses kuantifikasi.

B.17 Analisis sebab-dan-akibat (*Cause-and-effect analysis*)

B.17.1 Tinjauan singkat

Analisis sebab-dan-akibat adalah metode terstruktur untuk mengidentifikasi kemungkinan penyebab dari suatu kejadian atau masalah yang tidak diinginkan. Analisis ini mengatur faktor kontribusi yang mungkin masuk ke dalam kategori yang luas sehingga semua kemungkinan hipotesis dapat dipertimbangkan. Akan tetapi, analisis ini tidak dengan sendirinya menunjuk pada penyebab sebenarnya, karena analisis ini hanya dapat ditentukan oleh bukti nyata dan pengujian hipotesis secara empiris. Informasi tersebut disusun baik dalam Diagram Tulang Ikan (juga disebut *Ishikawa*) atau kadang-kadang suatu diagram pohon (lihat B.17.4).

B.17.2 Penggunaan

Analisis sebab dan akibat memberikan suatu tampilan bergambar terstruktur dari suatu daftar penyebab efek tertentu. Efeknya mungkin positif (suatu sasaran) atau negatif (suatu masalah) tergantung konteksnya.

Analisis ini digunakan untuk memungkinkan pertimbangan semua skenario yang mungkin dan sebab yang dihasilkan oleh suatu tim ahli dan memperbolehkan konsensus untuk ditetapkan mengenai penyebab paling mungkin yang kemudian dapat diuji secara empiris atau dengan evaluasi dari data yang ada. Hal ini paling berharga pada awal suatu analisis untuk memperluas pemikiran tentang kemungkinan penyebab dan kemudian menetapkan hipotesis potensial yang dapat dianggap lebih formal.

Membangun suatu diagram sebab dan akibat dapat dilakukan bila ada kebutuhan untuk:

- mengidentifikasi kemungkinan akar masalah, alasan dasar, untuk suatu efek, masalah atau kondisi tertentu;
- memilah dan menghubungkan beberapa interaksi di antara faktor yang mempengaruhi suatu proses tertentu;
- menganalisis permasalahan yang ada sehingga tindakan korektif dapat dilakukan.

Manfaat dari membangun suatu diagram sebab dan akibat mencakupi:

- mengkonsentrasikan perhatian pada tinjauan anggota terhadap suatu masalah tertentu;

- untuk membantu menentukan akar suatu masalah dengan menggunakan suatu pendekatan terstruktur;
- mendorong partisipasi kelompok dan memanfaatkan pengetahuan kelompok untuk produk atau proses;
- menggunakan suatu format yang tersusun, mudah dibaca untuk menggambarkan hubungan sebab-dan-akibat dalam bentuk diagram;
- mengindikasikan variasi kemungkinan penyebab dalam suatu proses;
- mengidentifikasi area dimana data sebaiknya dikumpulkan untuk studi lebih lanjut.

Analisis sebab-dan-akibat dapat digunakan sebagai suatu metode dalam melakukan analisis akar masalah (lihat Klausul B.12).

B.17.3 Masukan

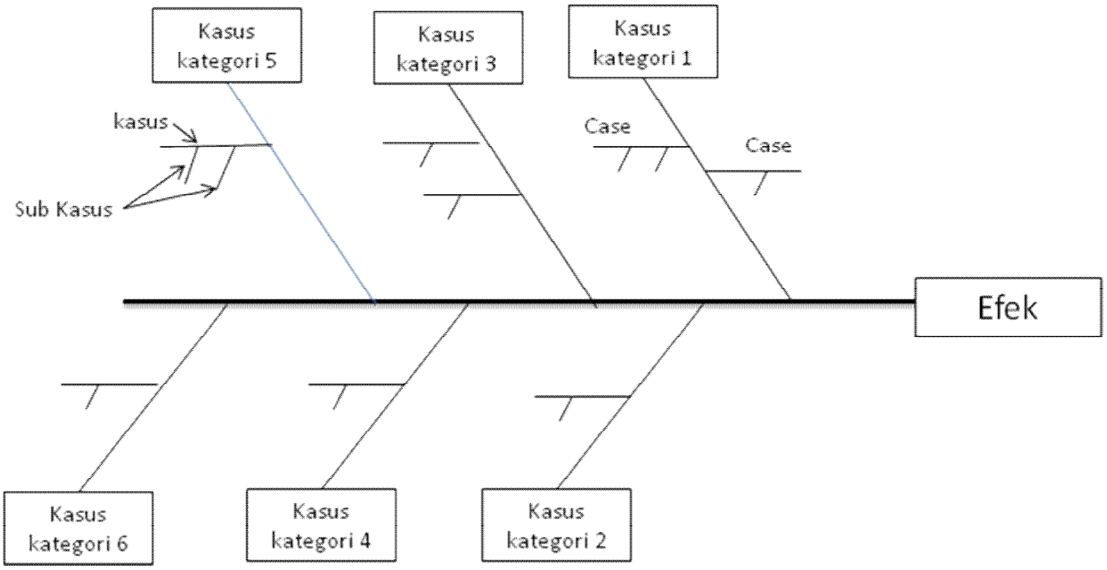
Masukan pada analisis sebab-akibat bisa berasal dari keahlian dan pengalaman dari peserta atau suatu model yang dikembangkan sebelumnya yang telah digunakan di masa lalu.

B.17.4 Proses

Analisis sebab dan akibat harus dilakukan oleh suatu tim ahli yang berpengetahuan dengan masalah yang membutuhkan resolusi.

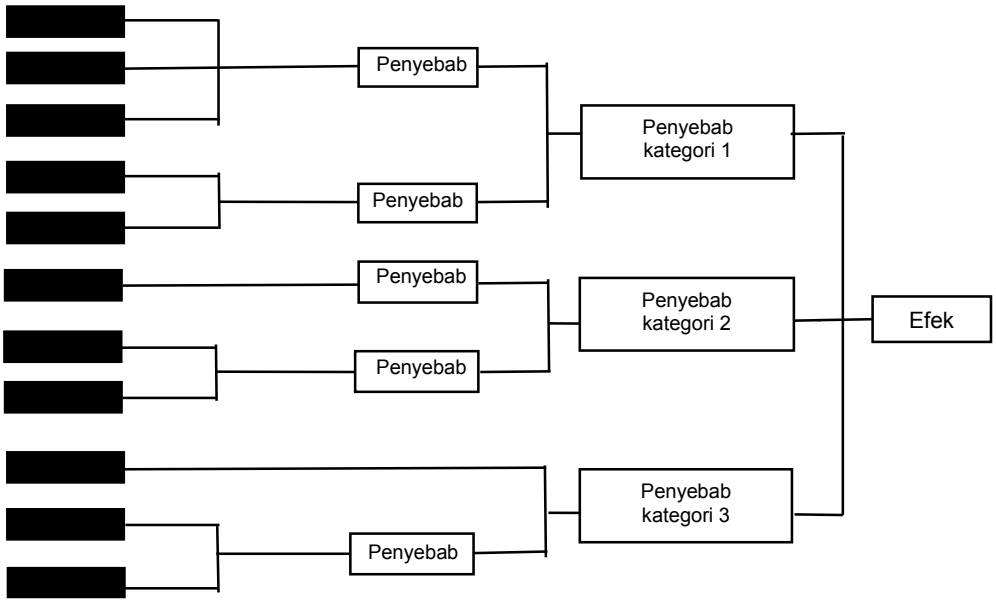
Langkah dasar dalam melakukan suatu analisis sebab dan akibat adalah sebagai berikut:
- tetapkan efek untuk dianalisis dan tempatkan dalam suatu kotak. Efeknya mungkin bisa positif (suatu sasaran) atau negatif (suatu masalah) tergantung pada keadaannya;
- tentukan kategori penyebab utama yang direpresentasikan oleh kotak dalam diagram tulang ikan (fishbone).
- khasnya, untuk suatu masalah sistem, kategori tersebut dapat berupa orang, peralatan, lingkungan, proses, dan lain-lain. Bagaimanapun, kategori tersebut dipilih sesuai dengan konteks terkait;
- isilah dengan kemungkinan penyebab untuk setiap kategori utama dengan cabang dan sub-cabang untuk menggambarkan hubungan di antara mereka;
- teruslah bertanya "mengapa?" atau "apa yang menyebabkan hal tersebut?" untuk menghubungkan dengan penyebabnya;
- tinjau semua cabang untuk memverifikasi konsistensi dan kelengkapan serta memastikan bahwa penyebabnya berkaitan dengan efek utamanya;
- identifikasi penyebab yang paling mungkin berdasarkan pendapat dari tim dan bukti yang ada tersebut.

Hasilnya biasa ditampilkan baik sebagai suatu diagram tulang ikan atau Ishikawa atau sebagai diagram pohon. Diagram tulang ikan disusun dengan memisahkan penyebab ke dalam kategori utama (ditunjukkan oleh garis dari tulang punggung ikan) dengan cabang dan sub-cabang yang menggambarkan penyebab yang lebih spesifik dalam kategori tersebut.



Gambar B.5 - Contoh diagram Ishikawa atau Tulang Ikan

Representasi berbentuk pohon ini mirip tampilannya dengan pohon kesalahan, meskipun sering ditampilkan dengan pohon yang berkembang dari kiri ke kanan daripada dari atas ke bawah. Bagaimanapun, hal ini tidak dapat dikuantifikasi untuk menghasilkan suatu probabilitas kejadian utama karena faktor penyumbang yang menyebabkan kejadian tersebut masih berupa suatu kemungkinan dibandingkan dengan suatu kegagalan yang memiliki probabilitas kejadian yang sudah diketahui.



Gambar B.6 - Contoh rumusan pohon dari analisis sebab-dan-akibat

Diagram sebab-dan-akibat biasanya digunakan secara kualitatif. Hal itu dimungkinkan untuk diasumsikan bahwa probabilitas masalahnya adalah 1 dan menetapkan probabilitas untuk penyebab umum, dan kemudian pada sub-penyebab, berdasarkan tingkat kepercayaan tentang relevansinya. Akan tetapi, faktor kontribusi sering berinteraksi dan berkontribusi pada efeknya dalam cara yang rumit yang membuat kuantifikasi menjadi tidak valid.

B.17.5 Keluaran

Keluaran dari suatu analisis sebab-dan-akibat adalah suatu diagram tulang ikan atau diagram pohon yang menampilkan penyebab yang mungkin dan lebih mungkin terjadi. Keluaran ini kemudian diverifikasi dan diuji secara empiris sebelum rekomendasi dibuat.

B.17.6 Kekuatan dan keterbatasan

Kekuatan mencakupi:
- keterlibatan dari ahli terapan yang bekerja dalam suatu lingkungan tim;
- analisis terstruktur;
- pertimbangan semua kemungkinan hipotesis;
- hasil berupa ilustrasi grafis yang mudah dibaca;
- area yang teridentifikasi untuk kebutuhan data lebih lanjut;
- dapat digunakan untuk mengidentifikasi efek faktor kontribusi baik yang diinginkan maupun yang tidak diinginkan. Mengambil suatu fokus positif pada suatu isu dapat mendorong rasa memiliki dan partisipasi yang lebih besar.

Keterbatasan mencakupi:
- tim mungkin tidak memiliki keahlian yang dibutuhkan;
- analisis ini bukan suatu proses yang lengkap dan perlu menjadi bagian dari suatu analisis akar masalah untuk menghasilkan rekomendasi;
- analisis ini adalah suatu teknik tampilan untuk curah pendapat daripada sekedar suatu teknik analisis yang terpisah;
- pemisahan faktor penyebab ke dalam kategori utama pada awal analisis berarti bahwa interaksi antar kategori mungkin tidak dipertimbangkan secara memadai, misalnya ketika kegagalan peralatan disebabkan oleh kesalahan manusia, atau masalah manusia disebabkan oleh rancangan yang buruk.

B.18 Analisis Lapisan Proteksi (*Layers of protection analysis - LOPA*)

B.18.1 Tinjauan singkat

LOPA adalah suatu metode semi-kuantitatif untuk memperkirakan risiko yang terkait dengan suatu kejadian atau skenario yang tidak diinginkan. LOPA menganalisis apakah ada tukuran yang memadai untuk mengendalikan atau memitigasi risiko tersebut.

Pasangan sebab-konsekuensi dipilih dan lapisan proteksi yang mencegah penyebab yang mengarah pada konsekuensi yang tidak diinginkan diidentifikasi. Suatu urutan besarnya perhitungan dilakukan untuk mengetahui apakah proteksi cukup memadai untuk mengurangi risiko pada suatu tingkat yang dapat ditolerir.

B.18.2 Penggunaan

LOPA dapat digunakan secara sederhana dalam bentuk kualitatif untuk meninjau lapisan proteksi antara suatu bahaya atau kejadian penyebab dan hasilnya. Biasanya suatu

pendekatan semi-kuantitatif diterapkan untuk menambah tingkat ketelitian pada proses penyaringan misalnya mengikuti teknik HAZOP atau PHA.

LOPA memberikan suatu dasar untuk spesifikasi lapisan proteksi yang mandiri (*independent protection layers - IPLs*) dan tingkat integritas keselamatan (tingkat *safety integrity level - SIL*) untuk sistem yang terinstrumentasi, seperti yang dijelaskan dalam seri IEC 61508 dan dalam IEC 61511, dalam penentuan persyaratan tingkat integritas keselamatan (SIL) untuk sistem instrumentasi keselamatan LOPA dapat digunakan untuk membantu mengalokasikan sumber daya pengurangan risiko secara efektif dengan menganalisis pengurangan risiko yang dihasilkan oleh setiap lapisan proteksi.

B.18.3 Masukan

Masukan ke LOPA mencakupi:
- informasi dasar tentang risiko termasuk bahaya, sebab dan konsekuensi seperti yang diberikan oleh suatu PHA;
- informasi tentang pengendalian terpasang atau usulan;
- frekuensi kejadian penyebab, dan kemungkinan kegagalan lapisan proteksi, ukuran konsekuensi dan suatu definisi risiko yang dapat ditolerir;
- menginisiasi frekuensi penyebab, kemungkinan kegagalan lapisan proteksi, ukuran konsekuensi dan suatu definisi risiko yang dapat ditolerir.

B.18.4 Proses

LOPA dilakukan dengan menggunakan suatu tim ahli yang menerapkan prosedur berikut:
- mengidentifikasi penyebab awal untuk suatu hasil yang tidak diinginkan dan mencari data tentang frekuensi dan konsekuensinya;
- memilih suatu pasangan sebab-konsekuensi tunggal;
- lapisan proteksi yang mencegah penyebab terjadinya konsekuensi yang tidak diinginkan diidentifikasi dan dianalisis untuk efektivitasnya;
- mengidentifikasi lapisan proteksi mandiri (IPLs) (tidak semua lapisan proteksi adalah IPLs);
- memperkirakan kemungkinan kegagalan dari setiap IPL;
- penyebab inisiasi frekuensi dikombinasikan dengan kemungkinan kegagalan dari setiap IPL dan kemungkinan dari setiap pengubah kondisi (suatu pengubah kondisi misalnya apakah seseorang yang hadir akan terkena dampaknya atau tidak) untuk menentukan frekuensi kejadian dari konsekuensi yang tidak diinginkan. Urutan besarnya digunakan untuk frekuensi dan kemungkinan;
- Tingkat risiko yang dihitung dibandingkan dengan tingkat toleransi risiko untuk menentukan apakah diperlukan proteksi lebih lanjut.

Suatu IPL adalah suatu sistem perangkat atau tindakan yang mampu mencegah suatu skenario yang akan berlanjut pada konsekuensi yang tidak diinginkan, terlepas dari kejadian penyebab atau setiap lapisan proteksi lainnya yang terkait dengan skenario tersebut.

IPLs mencakupi:
- fitur desain;
- perangkat perlindungan fisik;
- sistem yang bertautan dan mematikan (*shutdown*);
- alarm kritis dan intervensi manual;
- proteksi fisik pasca kejadian;
- sistem tanggap darurat (prosedur dan inspeksi bukan IPLs).

B.18.5 Keluaran

Rekomendasi untuk pengendalian lebih lanjut dan efektivitas dari pengendalian ini dalam mengurangi risiko sebaiknya diberikan.

LOPA adalah salah satu teknik yang digunakan untuk penilaian SIL pada saat berhadapan dengan sistem yang terkait/terinstrumentasi dengan keselamatan

B.18.6 Kekuatan dan keterbatasan

Kekuatan mencakupi:
- LOPA memerlukan sedikit waktu dan sumber daya dari pada suatu analisis pohon kesalahan atau penilaian risiko kuantitatif secara penuh namun lebih teliti dari pada penilaian subjektif kualitatif;
- LOPA membantu mengidentifikasi dan memfokuskan sumber daya pada lapisan proteksi yang paling kritis;
- LOPA mengidentifikasi operasi, sistem dan proses yang tidak dalam pengamanan yang memadai;
- LOPA memfokuskan pada konsekuensi yang paling serius.

Keterbatasan mencakupi:
- LOPA berfokus pada satu pasangan sebab-konsekuensi dan satu skenario pada suatu waktu. Interaksi kompleks antara risiko atau antar kendali tidak tercakupi;
- risiko yang dikuantifikasi mungkin tidak memperhitungkan kegagalan modus umum;
- LOPA tidak berlaku untuk skenario yang sangat kompleks dimana terdapat banyak pasangan sebab-konsekuensi atau di mana terdapat berbagai konsekuensi yang mempengaruhi pemangku kepentingan yang berbeda.

B.18.7 Dokumen Referensi

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

B.19 Analisis Pohon Keputusan (*Decision tree analysis*)

B.19.1 Tinjauan singkat

Suatu pohon keputusan merepresentasikan alternatif keputusan dan hasil dalam suatu urutan yang memperhitungkan hasil yang tidak pasti. Hal ini mirip dengan suatu pohon kejadian dimana dimulai dari suatu kejadian awal atau suatu keputusan awal dan memodelkan jalur dan hasil yang berbeda sebagai hasil dari kejadian yang mungkin terjadi dan keputusan yang berbeda yang mungkin dibuat.

B.19.2 Penggunaan

Suatu pohon keputusan digunakan dalam mengelola risiko projek dan dalam keadaan lain untuk membantu memilih tindakan terbaik di mana terdapat ketidakpastian. Tampilan grafis juga dapat membantu mengkomunikasikan alasan untuk keputusan.

B.19.3 Masukan

Suatu rencana proyek dengan beberapa titik keputusan. Informasi tentang hasil keputusan yang mungkin dan kejadian kebetulan yang mungkin mempengaruhi keputusan.

B.19.4 Proses

Suatu pohon keputusan dimulai dengan suatu keputusan awal, misalnya untuk melanjutkan dengan projek A daripada projek B. Ketika kedua projek hipotesis berlanjut, kejadian yang berbeda akan terjadi dan keputusan yang berbeda yang dapat diprediksi akan perlu untuk dibuat. Hal ini ditunjukkan dalam format pohon, mirip dengan suatu pohon kejadian. Probabilitas kejadian dapat diestimasi bersamaan dengan biaya atau utilitas dari hasil keluaran akhir jalur tersebut.

Informasi mengenai jalur keputusan terbaik secara logis adalah yang menghasilkan nilai harapan tertinggi yang dihitung sebagai produk dari semua kemungkinan bersyarat di sepanjang jalur dan nilai hasil tersebut.

B.19.5 Keluaran

Keluaran mencakupi:
- suatu analisis logis tentang risiko yang menampilkan pilihan berbeda yang mungkin diambil
- suatu perhitungan dari nilai yang diharapkan untuk setiap jalur yang mungkin

B.19.6 Kekuatan dan keterbatasan

Kekuatan mencakupi:
- analisis ini memberikan suatu gambaran grafis yang rinci tentang suatu masalah keputusan;
- analisis ini memungkinkan suatu perhitungan jalur terbaik melalui suatu situasi.

Keterbatasan antara lain:
- Pohon keputusan besar mungkin menjadi terlalu rumit untuk komunikasi yang mudah dengan orang lain;
- Mungkin ada suatu kecenderungan untuk terlalu menyederhanakan situasi sehingga mampu merepresentasikannya sebagai suatu diagram pohon.

B.20 Penilaian keandalan manusia (*Human reliability assessment- HRA*)

B.20.1 Tinjauan singkat

Penilaian kehandalan manusia (HRA) berkaitan dengan dampak manusia pada kinerja sistem dan dapat digunakan untuk mengevaluasi pengaruh kesalahan manusia terhadap sistem.

Banyak proses mengandung potensi kesalahan manusia, terutama ketika waktu yang tersedia bagi operator untuk membuat keputusan pendek. Probabilitas masalah akan cukup berkembang menjadi serius kecil. Namun terkadang, tindakan manusia akan menjadi satu-satunya pertahanan yang mencegah suatu kegagalan awal yang berkembang menuju suatu kecelakaan.

Pentingnya HRA telah diilustrasikan oleh berbagai kecelakaan di mana kesalahan manusia yang kritis berkontribusi pada serangkaian kejadian bencana. Kecelakaan semacam itu

adalah peringatan terhadap penilaian risiko yang hanya berfokus pada perangkat keras dan perangkat lunak dalam suatu sistem. Mereka menggambarkan bahaya dari mengabaikan kemungkinan kontribusi kesalahan manusia. Selain itu, HRA berguna dalam menyoroti kesalahan yang dapat menghambat produktivitas dan dalam mengungkapkan cara di mana kesalahan dan kegagalan lainnya (perangkat keras dan perangkat lunak) dapat "dipulihkan" oleh operator manusia dan personil pemeliharaan.

B.20.2 Penggunaan

HRA dapat digunakan secara kualitatif atau kuantitatif. Secara kualitatif, HRA digunakan untuk mengidentifikasi potensi dari kesalahan manusia dan penyebabnya sehingga kemungkinan kesalahan dapat dikurangi. HRA kuantitatif digunakan untuk menyediakan data tentang kegagalan manusia ke dalam FTA atau teknik lainnya.

B.20.3 Masukan

Masuk kepada HRA mencakupi:
- informasi untuk mendefinisikan tugas yang sebaiknya dilakukan orang;
- pengalaman dari jenis kesalahan yang terjadi dalam praktik dan potensi kesalahan;
- keahlian dalam kesalahan manusia dan kuantifikasinya.

B.20.4 Proses

Proses HRA adalah sebagai berikut:
- **Definisi masalah,** jenis keterlibatan manusia apa yang harus diselidiki / dinilai?
- **Analisis tugas**, bagaimana tugas dilakukan dan jenis alat bantu apa yang dibutuhkan untuk mendukung kinerja?
- **Analisis kesalahan manusia,** bagaimana kinerja tugas dapat gagal: kesalahan apa yang dapat terjadi dan bagaimana masalah itu dapat dipulihkan?
- **Representasi,** bagaimana kesalahan atau kegagalan kinerja tugas ini dapat diintegrasikan dengan perangkat keras, perangkat lunak, dan kejadian lingkungan lainnya untuk membuat probabilitas kegagalan sistem secara keseluruhan dapat dihitung?
- **Penyaringan,** apakah ada kesalahan atau tugas yang tidak memerlukan kuantifikasi yang terperinci?
- **Kuantifikasi,** seberapa sering terjadi kesalahan individu dan kegagalan tugas?
- **Penilaian dampak,** kesalahan atau tugas apa yang paling penting, yaitu mana yang memiliki kontribusi tertinggi terhadap kehandalan atau risiko?
- **Pengurangan kesalahan,** bagaimana kehandalan manusia yang lebih tinggi dapat dicapai?
- **Dokumentasi,** rincian HRA apa yang perlu untuk didokumentasikan?

Dalam praktiknya, proses HRA berjalan selangkah demi selangkah meski terkadang dengan bagian (misalnya analisis tugas dan identifikasi kesalahan) berjalan bersamaan satu sama lain.

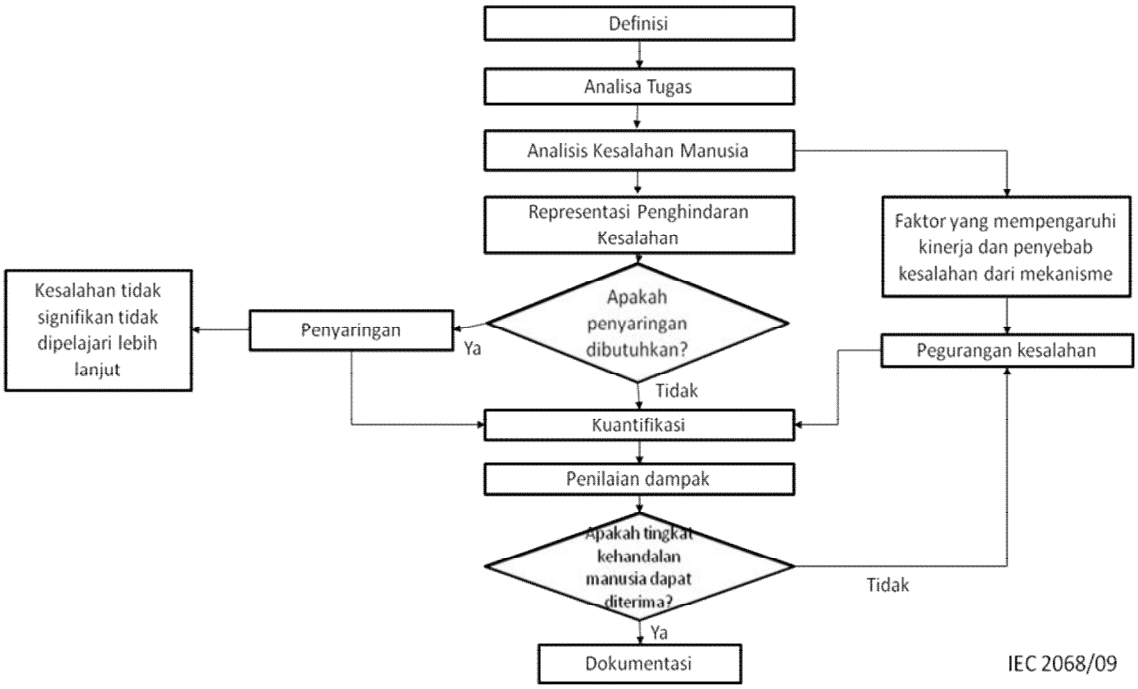
B.20.5 Keluaran

Keluaran mencakupi:
- suatu daftar kesalahan yang mungkin terjadi dan metode yang dengannya kesalahan tersebut dapat dikurangi - sebaiknya melalui perancangan ulang sistem tersebut;
- modus kesalahan, jenis kesalahan penyebab dan konsekuensi;
- suatu penilaian kualitatif atau kuantitatif terhadap risiko yang ditimbulkan oleh kesalahan tersebut.

B.20.6 Kekuatan dan keterbatasan

Kekuatan dari HRA mencakupi:
- HRA menyediakan suatu mekanisme formal untuk mencakupi kesalahan manusia dengan pertimbangan risiko yang terkait dengan sistem di mana manusia sering memainkan suatu peran penting;
- pertimbangan formal dari modus dan mekanisme kesalahan manusia dapat membantu mengurangi kemungkinan kegagalan akibat kesalahan.

Keterbatasan mencakupi:
- kompleksitas dan keberagaman manusia, yang membuat penentuan modus dan kemungkinan kesalahan yang sederhana menjadi sulit;
- banyak aktivitas manusia tidak memiliki modus lolos / gagal yang sederhana. HRA memiliki kesulitan berhadapan dengan kegagalan parsial atau kegagalan dalam kualitas atau pengambilan keputusan yang buruk.



Gambar B.7 - Contoh dari penilaian kehandalan manusia

B.21 Analisis dasi kupu-kupu (*Bow tie analysis*)

B.21.1 Tinjauan singkat

Analisis dasi kupu-kupu adalah cara diagram sederhana yang menggambarkan dan menganalisis jalur risiko dari penyebab ke konsekuensi. Hal ini dapat dianggap sebagai kombinasi dari pemikiran analisis pohon kesalahan penyebab dari suatu kejadian (diwakili oleh simpul pada dasi kupu-kupu) dan konsekuensi analisis pohon kejadian.Namun fokus dari dasi kupu-kupu adalah pada hambatan antara penyebab dan risiko, dan risiko dan konsekuensi. Diagram dasi kupu-kupu dapat dibangun mulai dari pohon kesalahan dan kejadian, tetapi lebih sering diambil langsung dari sesi curah pendapat (pengumpulan gagasan secara spontan).

B.21.2 Penggunaan

Analisis dasi kupu-kupu digunakan untuk memvisualisasikan risiko yang menunjukkan sebuah rentang kemungkinan penyebab dan konsekuensi. Analisis ini digunakan ketika situasi tidak menjamin kompleksitas suatu analisis pohon kesalahan secara utuh atau ketika fokus lebih pada memastikan bahwa ada penghalang atau pengendalian untuk setiap jalur kegagalan. Analisis ini berguna ketika terdapat jalur mandiri yang jelas mengarah pada kegagalan.

Analisis dasi kupu-kupu sering lebih mudah dipahami dari pada analisis pohon kejadian dan pohon kesalahan, dan oleh karenanya dapat menjadi alat komunikasi yang berguna di mana analisis dicapai dengan menggunakan teknik yang lebih kompleks.

B.21.3 Masukan

Pemahaman memerlukan informasi tentang penyebab dan konsekuensi dari risiko dan hambatan dan pengendalian yang dapat mencegah, mengurangi atau menstimulasi hal itu.

B.21.4 Proses

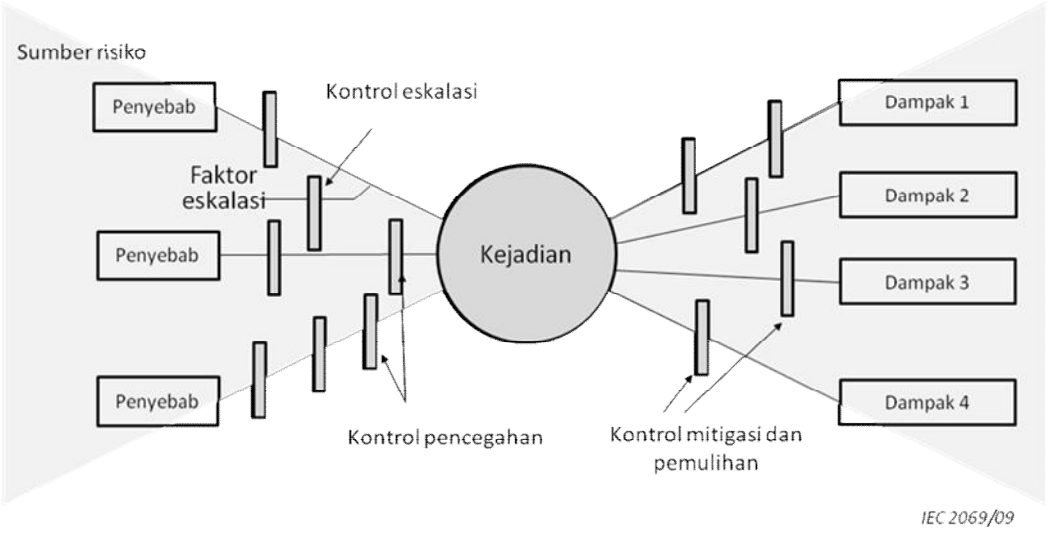
Analisis dasi kupu-kupu dapat digambar seperti berikut:

a) risiko tertentu diidentifikasi untuk dianalisa dan ditafsirkan sebagai simpul pusat dasi kupu-kupu.
b) Penyebab kejadian didaftar dengan mempertimbangkan sumber risiko (atau potensi bahaya dalam konteks keselamatan).
c) Mekanisme yang mengarahkan sumber risiko pada suatu kejadian kritis diidentifikasikan.
d) Garis ditarik antara tiap penyebab dan kejadian yang membentuk sisi kiri dasi kupu-kupu. Faktor-faktor yang mungkin mengarah pada eskalasi dapat diidentifikasi dan dimasukkan ke dalam diagram.
e) Hambatan yang sebaiknya mencegah setiap penyebab yang mengarah ke konsekuensi yang tidak diinginkan dapat ditampilkan sebagai bar vertikal di sepanjang garis tersebut. Apabila faktor yang mungkin menyebabkan eskalasi, hambatan untuk eskalasi dapat juga ditampilkan. Pendekatan ini dapat digunakan untuk konsekuensi positif di mana batang mencerminkan 'kendali' yang menstimulasi pembangkitan suatu kejadian.
f) Berbagai konsekuensi potensial dari risiko pada sisi kanan dasi kupu-kupu diidentifikasikan dan garis ditarik memancar keluar dari kejadian risiko ke setiap konsekuensi potensial tersebut.
g) Hambatan konsekuensinya digambarkan sebagai batang di sepanjang garis radial. Pendekatan ini dapat digunakan untuk konsekuensi positif di mana batang mencerminkan 'kendali' yang mendukung pembangkitan konsekuensi.
h) Fungsi manajemen yang mendukung kendali (seperti pelatihan dan inspeksi) dapat ditampilkan pada dasi kupu-kupu dan terkait dengan kendali masing-masing.

Tingkat kuantifikasi tertentu pada diagram dasi kupu-kupu dapat dimungkinkan ketika jalur-jalur tersebut mandiri, probabilitas dari suatu konsekuensi atau hasil keluaran dikenali, dan angka dapat diperkirakan untuk efektivitas suatu kendali.
Namun, dalam banyak situasi, jalur dan hambatan tidak mandiri serta kendali mungkin prosedural dan oleh karenanya efektivitas tidak jelas. Kuantifikasi sering lebih tepat dilakukan dengan menggunakan FTA dan ETA.

B.21.5 Keluaran

Keluaran adalah diagram sederhana yang menunjukkan jalur risiko utama dan hambatan ada untuk mencegah atau mengurangi konsekuensi yang tidak diinginkan atau menstimulasi dan mempromosikan konsekuensi yang diinginkan.



Gambar B.8 - Contoh diagram dasi kupu-kupu untuk konsekuensi yang tidak diinginkan

B.21.6 kekuatan dan keterbatasan

Kekuatan analisis dasi kupu-kupu:
- mudah untuk dipahami dan memberikan representasi gambaran masalah dengan jelas;
- memfokuskan perhatian pada kendali yang seharusnya berada di tempatnya untuk pencegahan dan mitigasi dan efektivitas mereka;
- dapat digunakan untuk konsekuensi yang diinginkan;
- tidak membutuhkan keahlian tingkat tinggi untuk menggunakannya.

Keterbatasan meliputi:
- tidak dapat menggambarkan ketika beberapa penyebab terjadi secara bersamaan yang menyebabkan suatu konsekuensi
  (contohnya ketika terdapat gerbang DAN pada suatu analisis pohon kesalahan yang menggambarkan sisi kiri dari dasi kupu-kupu);
- mungkin menyederhanakan secara berlebihan situasi yang kompleks, terutama ketika mencoba melakukan kuantifikasi.

B.22 Pemeliharaan yang terpusat pada keandalan (*Reliability centred maintenance-RCM*)

B.22.1 Tinjauan singkat

Pemeliharaan yang terpusat pada keandalan (RCM) adalah metode untuk mengidentifikasi kebijakan yang harus dilaksanakan untuk mengelola kegagalan sehingga dapat dicapai efisien dan efektif yang memerlukan keselamatan, ketersediaan dan keekonomisan operasi untuk semua jenis peralatan.

RCM sekarang ini adalah metodologi yang telah terbukti dan diterima untuk digunakan dalam berbagai industri.

RCM menyediakan suatu proses keputusan untuk mengidentifikasi persyaratan pemeliharaan pencegahan yang efektif dan dapat diterapkan untuk peralatan yang sesuai dengan konsekuensi keselamatan, operasional dan ekonomis dari kegagalan yang dapat diidentifikasi, dan mekanisme degradasi yang bertanggung jawab atas kegagalan tersebut. Hasil akhir kerja di seluruh proses tersebut adalah penilaian mengenai kebutuhan melakukan tugas pemeliharaan atau tindakan lain seperti perubahan operasional. Rincian mengenai penggunaan dan penerapan RCM disediakan dalam IEC 60300-3-11.

B.22.2 Penggunaan

Semua tugas didasarkan pada keselamatan terkait dengan personil dan lingkungan, dan perhatian operasional atau ekonomis. Namun, perlu dicatat bahwa kriteria yang dipertimbangkan akan bergantung pada sifat produk dan aplikasinya. Misalnya, proses produksi harus dapat berjalan terus secara ekonomis, dan mungkin sensitif terhadap pertimbangan lingkungan yang ketat, sedangkan suatu alat pertahanan harus tetap bisa beroperasi, tetapi mungkin memiliki kelonggaran dalam hal kriteria keselamatan, ekonomis dan lingkungan. Manfaat terbesar dapat dicapai melalui penetapan sasaran analisis pada kegagalan yang akan berakibat pada keselamatan, lingkungan, efek ekonomi atau operasional yang serius.

RCM digunakan untuk memastikan bahwa pelaksanaan dan pemeliharaan efektif dilakukan dan pada umumnya dilakukan selama fase perancangan dan pengembangan dan kemudian dijalankan selama beroperasi dan perawatan.

B.22.3 Masukan

keberhasilan penerapan RCM membutuhkan pemahaman yang baik tentang peralatan dan strukturnya, lingkungan operasional dan terkait sistem, subsistem dan butir peralatan, bersama-sama dengan kegagalan yang mungkin, dan dampak dari kegagalan-kegagalan tersebut.

B.22.4 Proses

Langkah-langkah dasar dari program RCM adalah sebagai berikut:
- inisiasi dan perencanaan;
- analisis kegagalan fungsional;
- pemilihan tugas;
- pelaksanaan;
- perbaikan terus-menerus.

RCM adalah berbasis risiko karena RCM mengikuti langkah-langkah dasar dalam penilaian risiko. Jenis penilaian risiko adalah suatu analisis modus kegagalan dan dampak serta kekritisan (FMECA) tetapi membutuhkan pendekatan khusus untuk menganalisis ketika digunakan dalam konteks ini.

Identifikasi risiko berfokus pada situasi di mana potensi kegagalan dapat dihilangkan atau dikurangi frekuensinya dan/atau konsekuensi dengan melakukan tugas-tugas pemeliharaan. Hal ini dilakukan dengan mengidentifikasi fungsi yang diperlukan dan kinerja standar dan gagalnya peralatan dan komponen yang dapat mengganggu fungsi-fungsi tersebut.

Risiko analisis meliputi memperkirakan frekuensi setiap kegagalan tanpa dilakukan perawatan. Konsekuensi ditetapkan dengan mendefinisikan efek kegagalan. Sebuah matriks risiko yang menggabungkan frekuensi kegagalan dan konsekuensi memungkinkan kategori untuk tingkat risiko yang akan ditetapkan.

Evaluasi risiko selanjutnya dilakukan dengan memilih kebijakan pengelolaan kegagalan yang tepat untuk setiap mode kegagalan.

Seluruh proses RCM didokumentasikan secara luas untuk referensi dan tinjauan masa depan. Pengumpulan kegagalan dan data terkait pemeliharaan memungkinkan pemantauan hasil dan pelaksanaan.

B.22.5 Keluaran

RCM memberikan sebuah definisi pada tugas pemeliharaan seperti pemantauan kondisi, restorasi terjadwal, penggantian terjadwal, temuan-kegagalan atau pemeliharaan non-preventif. Tindakan lain yang mungkin dihasilkan dari analisis dapat termasuk rancangan ulang, perubahan operasi atau prosedur pemeliharaan atau pelatihan tambahan. Tugas interval dan dan sumber daya yang dibutuhkan kemudian diidentifikasikan.

B.22.6 Dokumen Referensi

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.23 Analisis Selinap (*sneak analysis-SA*) dan analisis rangkaian Selinap (*sneak circuit analysis-SCA*)

B.23.1 Tinjauan singkat

Analisis selinap (SA) adalah suatu metodologi untuk mengidentifikasi kesalahan rancangan. Kondisi selinap adalah kondisi laten perangkat keras, kondisi laten perangkat lunak atau kondisi laten terintegrasi yang dapat menyebabkan suatu kejadian yang tidak diinginkan terjadi atau dapat menghambat kejadian yang diinginkan dan tidak disebabkan oleh kegagalan komponen. Kondisi ini ditandai dengan sifat acak mereka dan kemampuan untuk menghindar pada saat deteksi paling ketat dari tes sistem terstandar. Kondisi selinap dapat menyebabkan operasi yang tidak benar, hilangnya ketersediaan sistem, keterlambatan program, atau bahkan kematian atau cedera untuk personel.

B.23.2 Penggunaan

analisis rangkaian selinap (SCA) dikembangkan pada akhir 1960-an untuk NASA untuk memeriksa keutuhan dan fungsi dari rancangan mereka. Ini berfungsi sebagai alat yang berguna untuk menemukan ketidaksengajaan pembetukan jalur rangkaian listrik, dan membantu dalam merancang solusi untuk mengisolasi fungsi masing-masing. Namun, sebagai teknologi canggih, alat untuk analisis rangkaian selinap juga harus maju. analisis selinap termasuk dan jauh melebihi cakupan analisis rangkaian selinap. Analisis ini dapat menemukan masalah di perangkat kerasdan perangkat lunak dengan teknologi apapun. Alat analisis selinap dapat mengintegrasikan beberapa analisis seperti pohon kesalahan, Analisa modus kegagalan dan Dampak (FMEA), perkiraan keandalan, dll menjadi analisis tunggal hemat waktu dan biaya proyek.

B.23.3 Masukan

Analisis selinap adalah unik mulai dari proses rancangan karena dia menggunakan berbagai alat (jejaring pohon, jejaring hutan, dan jejaring petunjuk atau pertanyaan untuk membantu analis mengidentifikasi suatu kondisi selinap) untuk menemukan jenis tertentu dari masalah. Jejaring pohon dan jejaring hutan tersebut adalah pengelompokan secara topologis dari sistem yang sebenarnya. Setiap jejaring pohon mewakili sub-fungsi dan menunjukkan semua masukan yang dapat mempengaruhi keluaran sub-fungsi. sejumlah jejaring dibangun dengan menggabungkan jejaring pohon yang berkontribusi terhadap keluaran sistem tertentu. sejumlah jejaring yang tepat menunjukkan sistem keluaran dalam hal semua masukan terkaitnya. Ini, bersama dengan yang lainnya, menjadi masukan untuk analisis.

B.23.4 Proses

Langkah dasar dalam melakukan analisis Sneak terdiri dari:
- persiapan data;
- pembangunan jejaring pohon;
- evaluasi jalur jejaring;
- rekomendasi final dan laporan.

B.23.5 Keluaran

Rangkaian selinap adalah jalur tak terduga atau aliran logika dalam sistem yang, dalam kondisi tertentu, dapat memulai fungsi yang tidak diinginkan atau menghambat fungsi yang diinginkan. Jalur ini mungkin terdiri dari perangkat keras, perangkat lunak, tindakan operator, atau kombinasi elemen-elemen ini. Rangkaian selinap bukan hasil dari kegagalan perangkat keras namun kondisi laten, yang secara tidak sengaja masuk ke dalam rancangan sistem, dikodekan ke dalam program perangkat lunak, atau dipicu oleh kesalahan manusia. Ada empat kategori rangkaian selinap:

a) jalan selinap: jalur tak terduga sepanjang aliran arus, energi, atau logika yang mengalir dalam arah yang tidak disengaja;
b) waktu selinap: kejadian yang terjadi dalam urutan yang tidak terduga atau bertentangan;
c) indikasi selinap: tampilan kondisi sistem operasi yang tidak jelas atau membingungkan yang dapat menyebabkan sistem atau operator melakukan tindakan yang tidak diinginkan;
d) label selinap: pelabelan yang salah atau tidak tepat pada sistem fungsi , misalnya sistem masukan, pengendalian, tampilan bus yang dapat menyebabkan operator menerapkan stimulasi yang salah pada sistem.

B.23.6 Kekuatan dan keterbatasan

Kekuatan meliputi:
- Analisis selinap bagus untuk mengidentifikasi kesalahan desain;
- bekerja paling baik bila diterapkan bersamaan dengan HAZOP;
- sangat baik untuk menangani sistem yang memiliki banyak keadaan seperti pabrik batch dan semi-batch.

Keterbatasan dapat mencakup:
- Prosesnya bisa berbeda-beda tergantung pada apakah itu diterapkan pada rangkaian listrik, proses pabrik, peralatan mekanis atau perangkat lunak;
- Metode ini bergantung pada pembentukan jejaring pohon yang benar.

B.24 Analisis Markov

B.24.1 Tinjauan singkat

Analisis Markov digunakan di mana keadaan masa depan suatu sistem hanya bergantung pada keadaan saat ini. Hal ini biasa digunakan untuk analisis sistem yang dapat diperbaiki yang dapat ada di banyak kondisi dan penggunaan analisis keandalan blok tidak sesuai untuk menganalisis sistem secara memadai. Metode ini dapat diperluas ke sistem yang lebih kompleks dengan menggunakan proses Markov tingkat tinggi dan hanya dibatasi oleh model, perhitungan matematis dan asumsi.

Proses analisis Markov adalah suatu teknik kuantitatif dan dapat berupa diskrit (menggunakan probabilitas perubahan antar keadaan) atau terus menerus (menggunakan tingkat perubahan di seluruh keadaan).

Sementara analisis Markov dapat dilakukan dengan tangan, sifat dasar dari tekniknya cocok untuk penggunaan program komputer, banyak yang ada di pasaran.

B.24.2 Penggunaan

Teknik analisis Markov dapat digunakan pada berbagai struktur sistem, dengan atau tanpa perbaikan, termasuk:
- komponen independen secara paralel;
- komponen independen secara seri;
- sistem pembagian beban;
- sistem siaga, termasuk kasus dimana kegagalan perubahan dapat terjadi;
- sistem yang terdegradasi.

Teknik analisis Markov juga dapat digunakan untuk menghitung ketersediaan, termasuk memperhitungkan komponen suku cadang untuk perbaikan.

B.24.3 Masukan

Masukan yang penting untuk analisis Markov adalah sebagai berikut:
- daftar berbagai keadaan bahwa sistem, sub-sistem atau komponen dapat berada di dalam (misalnya operasional penuh, operasi parsial (contohnya keadaan terdegradasi), keadaan gagal, dll);
- pemahaman yang jelas tentang transisi yang mungkin yang perlu dimodelkan. Misalnya, kegagalan suatu ban mobil perlu mempertimbangkan keadaan roda cadangan dan termasuk frekuensi pemeriksaan;
- tingkat perubahan dari satu keadaan ke keadaan lainnya, biasanya direpresentasikan baik oleh probabilitas perubahan antara keadaan untuk kejadian diskrit, maupun tingkat kegagalan (λ) dan / atau tingkat perbaikan (μ) untuk kejadian berkelanjutan.

B.24.4 Proses

Teknik analisis Markov berpusat di seputar konsep "keadaan", misalnya. "tersedia" dan "gagal", dan transisi antara kedua keadaan ini dari waktu ke waktu berdasarkan suatu probabilitas perubahan yang konstan. Matriks probabilitas transisi stokastik digunakan untuk menggambarkan transisi antara masing-masing keadaan untuk memungkinkan perhitungan berbagai keluaran.

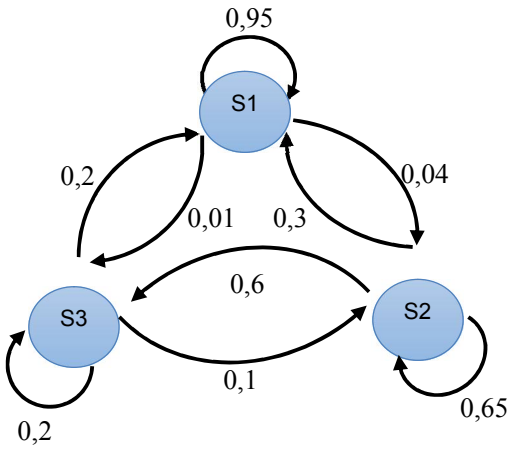
Untuk mengilustrasikan teknik analisis Markov, pertimbangkan sistem yang kompleks yang hanya ada di tiga Keadaan; Berfungsi, terdegradasi dan gagal, didefinisikan sebagai keadaan S1, S2, S3 masing-masing. Setiap hari, sistem itu ada di salah satu dari tiga

keadaan ini. Tabel B.3 menunjukkan probabilitas bahwa besok, sistem berada di keadaan Si dimana i bisa 1, 2 atau 3.

Table B.2 – Matriks Markov

		Keadaan hari ini		
		S1	S2	S3
Keadaan esok	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Rangkaian probabilitas ini disebut matriks Markov, atau matriks transisi. Perhatikan bahwa jumlah untuk masing-masing kolom adalah 1 karena jumlahnya adalah jumlah dari semua hasil yang mungkin terjadi dalam setiap kasus. Sistem ini, juga dapat ditunjukkan oleh diagram Markov di mana lingkaran mewakili keadaan, dan panah mewakili transisi, bersama dengan probabilitas yang menyertainya.



Gambar B.9 - Contoh diagram sistem Markov

Panah dari keadaan itu sendiri biasanya tidak diperlihatkan, namun ditunjukkan dalam contoh ini untuk kelengkapan.

Misalkan Pi mewakili probabilitas untuk menemukan sistem dalam keadaan i untuk i = 1, 2, 3, maka persamaan simultan yang harus dipecahkan adalah:

$$P1 = 0,95\ P1 + 0,30\ P2 + 0,20\ P3 \quad \text{(B.1)}$$

$$P2 = 0,04\ P1 + 0,65\ P2 + 0,60\ P3 \quad \text{(B.2)}$$

$$P3 = 0,01\ P1 + 0,05\ P2 + 0,20\ P3 \quad \text{(B.3)}$$

Ketiga persamaan ini tidak independen dan tidak akan menyelesaikan tiga keadaan yang tidak diketahui. Persamaan berikut sebaiknya digunakan dan salah satu persamaan di atas tidak digunakan.

$$1 = P1 + P2 + P3 \quad \text{(B.4)}$$

Solusinya adalah 0,85, 0,13, dan 0,02 untuk masing-masing keadaan 1, 2, 3. Sistem ini berfungsi penuh 85 % dari waktu, dalam keadaan terdegradasi sebesar 13 % dari waktu dan gagal untuk 2 % dari waktu.

Pertimbangkan dua butir yang beroperasi secara paralel dengan yang dibutuhkan untuk bisa beroperasi agar sistem dapat berfungsi. Butir dapat beroperasi atau gagal dan ketersediaan sistem bergantung pada kondisi butir.

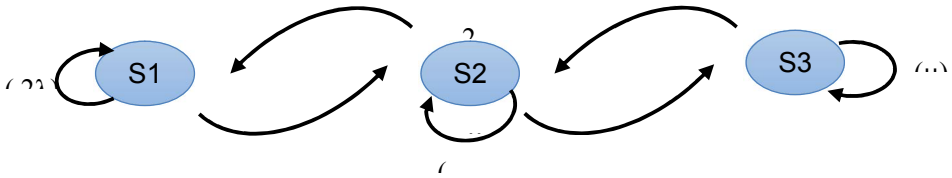
Keadaan dapat dipertimbangkan sebagai:

Keadaan 1 Kedua hal berfungsi dengan benar;

Keadaan 2 Satu barang telah gagal dan sedang diperbaiki, yang lain berfungsi;

Keadaan 3 Kedua barang telah gagal dan satu sedang mengalami perbaikan.

Jika tingkat kegagalan terus menerus untuk setiap butir diasumsikan λ dan tingkat perbaikannya adalah μ, maka diagram keadaan transisi adalah:



Gambar B.10 - Contoh diagram keadaan transisi

Perhatikan bahwa transisi dari keadaan 1 ke keadaan 2 adalah 2λ karena kegagalan salah satu dari dua hal akan membawa sistem ke keadaan 2.

Biarkan P*i(t)* menjadi probabilitas berada dalam keadaan awal *i* pada waktu *t*; dan

Biarkan P*i*(*t* + *δt*) menjadi probabilitas berada dalam keadaan akhir pada waktu *t* + *δt*

Matriks probabilitas transisi menjadi:

Tabel B.3 - matriks Markov final

		Keadaan awal		
		P1(t)	P2(t)	P3(t)
	P1($t + \delta t$)	-2λ	μ	0
Final state	P2($t + \delta t$)	2λ	$-(\lambda + \mu)$	μ
	P3($t + \delta t$)	0	λ	$-\mu$

Perlu dicatat bahwa nilai nol terjadi karena tidak mungkin bergerak dari keadaan 1 ke keadaan 3 atau dari keadaan 3 ke keadaan 1. Juga, jumlah kolom akan menjadi nol bila harga spesifik.

Persamaan simultan menjadi:

$$dP1/dt = -2\lambda\, P1(t) + \mu\, P2(t) \quad \text{(B.5)}$$

$$dP2/dt = 2\lambda\, P1(t) + (\lambda + \mu)\, P2(t) + \mu\, P3(t) \quad \text{(B.6)}$$

$$dP3/dt = \lambda\, P2(t) + \mu\, P3(t) \quad \text{(B.7)}$$

Untuk kesederhanaan, diasumsikan bahwa ketersediaan yang dibutuhkan adalah ketersediaan keadaan yang mapan.

Jika δt cenderung menjadi tidak terbatas, dPi / dt akan cenderung nol dan persamaan menjadi lebih mudah untuk dipecahkan. Persamaan tambahan seperti yang ditunjukkan pada Persamaan (B.4) di atas juga harus digunakan:

Sekarang persamaan A (t) = P1 (t) + P2 (t) dapat dinyatakan sebagai:

$A = P1 + P2$

Oleh karena itu $A = (\mu 2 + 2\,\lambda\,\mu) / (\mu 2 + 2\,\lambda\,\mu + \lambda 2)$ "

B.24.5 Keluaran

Keluaran dari analisis Markov adalah bermacam probabilitas berada di berbagai keadaan, dan oleh karena itu perkiraan probabilitas kegagalan dan / atau ketersediaan, salah satu komponen penting dari sebuah sistem.

B.24.6 Kekuatan dan keterbatasan

Kekuatan analisis Markov meliputi:
- kemampuan untuk menghitung probabilitas untuk sistem dengan kemampuan perbaikan dan beberapa keadaan terdegradasi.

Keterbatasan analisis Markov meliputi:
- asumsi probabilitas konstan pada perubahan keadaan; baik kegagalan atau perbaikan;
- semua kejadian secara statistik bersifat independen karena keadaan masa depan independen dari semua keadaan sebelumnya, kecuali keadaan dadakan yang mendahului;
- dibutuhkan pengetahuan tentang semua kemungkinan perubahan keadaan;

- pengetahuan tentang operasi matriks;
- hasil sulit untuk dikomunikasikan dengan personil non-teknis.

B.24.7 Perbandingan

Analisis Markov mirip dengan analisis Petri-Net dengan dapat memantau dan mengamati keadaan sistem, walaupun berbeda karena Petri-Net dapat ada di banyak keadaan pada saat bersamaan.

B.24.8 Dokumen referensi

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

B.25 Simulasi Monte Carlo

B.25.1 Tinjauan singkat

Efek ketidakpastian pada banyak sistem terlalu kompleks untuk dimodelkan dengan menggunakan teknik analisis, tetapi mereka dapat dievaluasi dengan mempertimbangkan masukan sebagai variabel acak dan menjalankan perhitungan sejumlah N (yang disebut simulasi) dengan mengambil sampel masukan agara supaya mendapatkan hasil keluaran sejumlah N yang mungkin bagi hasil yang diinginkan.

Metode ini dapat mengatasi situasi kompleks yang akan sangat sulit dipahami dan dipecahkan dengan metode analisis. Sistem dapat dikembangkan dengan menggunakan spreadsheet dan alat konvensional lainnya, namun alat yang lebih canggih tersedia untuk membantu persyaratan yang lebih kompleks, yang kebanyakan harganya relatif murah. Ketika teknik ini pertama kali dikembangkan, jumlah pengulangan yang diperlukan untuk simulasi Monte Carlo membuat prosesnya lamban dan memakan waktu, namun kemajuan dalam komputer dan perkembangan teoritis, seperti pengambilan sampel *Latin-hypercube*, telah membuat waktu pemrosesan hampir tidak signifikan untuk banyak aplikasi.

B.25.2 Penggunaan

Simulasi Monte Carlo menyediakan sarana untuk mengevaluasi efek ketidakpastian pada sistem dalam rentang situasi yang lebar. Hal ini khususnya digunakan untuk mengevaluasi kisaran kemungkinan hasil keluaran dan frekuensi relatif dari nilai dalam rentang tersebut untuk ukuran kuantitatif dari sistem seperti biaya, durasi, laluan (*throughput*), permintaan dan tindakan serupa. Simulasi Monte Carlo dapat digunakan untuk dua tujuan berbeda:

- propagasi ketidakpastian pada model analisis konvensional;
- perhitungan probabilitas ketika teknik analisis tidak dapat bekerja.

B.25.3 Masukan

Masukan untuk simulasi Monte Carlo adalah model yang baik mengenai sistem dan informasi tentang jenis masukan, sumber ketidakpastian yang akan dijabarkan dan keluaran yang dibutuhkan. masukan data dengan ketidakpastian direpresentasikan sebagai variabel acak dengan distribusi yang sedikit banyak menyebar sesuai dengan tingkat ketidakpastian. Distribusi seragam, segitiga, normal dan distribusi log normal sering digunakan untuk tujuan ini.

B.25.4 Proses

Prosesnya sebagai berikut:

a) Suatu model atau algoritma didefinisikan yang menampilkan semaksimal mungkin perilaku sistem yang sedang dipelajari.
b) Model ini dijalankan beberapa kali dengan menggunakan bilangan acak untuk menghasilkan model keluaran (simulasi dari sistem); Dimana aplikasinya adalah memodelkan efek ketidakpastian model tersebut dalam bentuk persamaan yang memberikan hubungan antara parameter masukan dan keluaran. Nilai yang dipilih untuk masukan diambil dari distribusi probabilitas yang sesuai yang mewakili sifat ketidakpastian parameter ini.
c) Dalam kasus manapun, komputer menjalankan model beberapa kali (seringkali sampai 10.000 kali) dengan masukan yang berbeda dan menghasilkan banyak keluaran. Ini bisa diolah menggunakan statistik konvensional untuk memberikan informasi seperti nilai rata-rata, standar deviasi, interval kepercayaan.

Contoh simulasi diberikan di bawah ini.

Perhatikan dua butir yang beroperasi secara paralel dan hanya satu yang diperlukan agar sistem berfungsi. Butir pertama memiliki reliabilitas 0,9 dan 0,8.

Dapat dimungkinkan untuk membuat halaman besar berisi tabel (*spreadsheet*) dengan kolom berikut:

Tabel B.4 - Contoh simulasi Monte Carlo

	Bagian 1		Bagian 2		
Nomor simulasi	Nomor acak	Fungsi?	Nomor acak	Fungsi?	Sistem
1	0,577243	YA	0,059355	YA	1
2	0,746909	YA	0,311324	YA	1
3	0,541728	YA	0,919765	TIDAK	1
4	0,423274	YA	0,643514	YA	1
5	0,917776	TIDAK	0,539349	YA	1
6	0,994043	TIDAK	0,972506	TIDAK	0
7	0,082574	YA	0,950241	TIDAK	1
8	0,661418	YA	0,919868	TIDAK	1
9	0,213376	YA	0,367555	YA	1
10	0,565657	YA	0,119215	YA	1

Generator acak menciptakan suatu angka antara 0 dan 1 yang digunakan untuk membandingkan dengan probabilitas masing-masing hal untuk menentukan apakah sistem beroperasi. Dengan hanya 10 putaran, hasil 0,9 tidak dapat diharapkan menjadi hasil yang akurat. Pendekatan yang biasa adalah dengan membuat suatu kalkulasi guna membandingkan hasil total sepanjang simulasi berlangsung untuk mencapai tingkat akurasi yang dibutuhkan. Dalam contoh ini, hasil 0,9799 dicapai setelah 20.000 pengulangan..

Model di atas dapat diperluas dengan berbagai cara. Sebagai contoh:
- dengan memperluas model itu sendiri (seperti mempertimbangkan butir kedua segera beroperasi hanya ketika butir pertama gagal);
- dengan mengubah probabilitas tetap menjadi variabel (contoh yang bagus adalah distribusi segitiga) bila probabilitas tidak dapat didefinisikan secara akurat;
- menggunakan tingkat kegagalan dikombinasikan dengan randomizer untuk mendapatkan waktu kegagalan (eksponensial, Weibull, atau distribusi lain yang sesuai) dan membangun pada waktu perbaikan.

Aplikasi meliputi, antara lain, penilaian ketidakpastian dalam prakiraan keuangan, kinerja investasi, perkiraan biaya proyek dan jadwal, gangguan proses bisnis dan persyaratan kepegawaian.

Teknik analitik tidak mampu untuk memberikan hasil yang relevan atau ketika terdapat ketidakpastian pada data masukan dan juga keluarannya.

B.25.5 Keluaran

Keluaran dapat berupa nilai tunggal, seperti yang ditentukan pada contoh di atas, bisa jadi hasil dinyatakan sebagai distribusi probabilitas atau frekuensi atau bisa juga identifikasi fungsi utama dalam model yang memiliki dampak terbesar pada keluaran.

Secara umum, simulasi Monte Carlo akan digunakan untuk menilai keseluruhan distribusi hasil yang dapat timbul atau ukuran kunci dari distribusi seperti:
- probabilitas yang timbul dari hasil keluaran yang ditetapkan;
- nilai hasil di mana pemilik masalah memiliki tingkat keyakinan tertentu bahwa hal itu tidak akan terlampaui atau dikalahkan, biaya yang kurang dari 10 % kemungkinan melebihi atau durasi yang 80 % pasti akan terlampaui.

Suatu analisis tentang hubungan antara masukan dan keluaran dapat menjelaskan signifikansi relatif faktor yang bekerja dan mengidentifikasi target yang berguna untuk upaya mempengaruhi ketidakpastian hasil keluaran.

B.25.6 Kekuatan dan keterbatasan

Kekuatan analisis Monte Carlo meliputi:
- metode ini pada prinsipnya dapat mengakomodasi distribusi apapun dalam variabel masukan, termasuk distribusi empiris yang berasal dari pengamatan sistem terkait;
- model relatif mudah dikembangkan dan dapat diperluas seiring dengan kebutuhan yang timbul;
- setiap pengaruh atau hubungan yang timbul dalam kenyataan dapat diwakili, termasuk efek yang tidak kentara seperti kebergantugan bersyarat;
- analisis sensitivitas dapat diterapkan untuk mengidentifikasi pengaruh yang kuat dan lemah;
- model dapat dengan mudah dipahami karena hubungan antara masukan dan keluaran transparan;
- model perilaku yang efisien seperti Petri-Nets (IEC 62551) tersedia yang terbukti sangat efisien untuk keperluan simulasi Monte Carlo;
- menyediakan ukuran keakuratan hasil;
- perangkat lunak sudah tersedia dan relatif murah.

Keterbatasan adalah sebagai berikut:

- keakuratan solusi bergantung pada jumlah simulasi yang dapat dilakukan (keterbatasan ini menjadi kurang penting dengan peningkatan kecepatan komputer);

- ini bergantung pada kemampuan untuk mewakili ketidakpastian parameter dengan distribusi yang valid;
- model besar dan kompleks mungkin menantang bagi pemodel dan mempersulit pemangku kepentingan untuk terlibat dengan proses tersebut;
- teknik ini mungkin tidak cukup mempertimbangkan kejadian dengan konsekuensi tinggi/ probabilitas rendah dan karena itu tidak membuat selera risiko organisasi tercermin dalam analisis ini.

B.25.7 Dokumen referensi

IEC 61649, *Weibull analysis*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*

ISO/IEC Guide 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)*

B.26 Statistik Bayesian dan Jaring Bayes

B.26.1 Tinjauan singkat

Statistik Bayesian dikaitkan dengan Pendeta Thomas Bayes. Dasar pemikirannya adalah bahwa setiap informasi yang sudah diketahui (yang sebelumnya-*the Prior*) dapat dikombinasikan dengan pengukuran berikutnya (yang sesudahnya-*the Posterior*) untuk menetapkan probabilitas keseluruhan. Ekspresi umum dari teorema Bayes dapat dinyatakan sebagai:

$$P(A \mid B) = \{P(A)\, P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

Dimana

probabilitas X dilambangkan dengan P (X);
probabilitas X pada kondisi yang Y telah terjadi dilambangkan dengan P (X | Y); dan Ei adalah kejadian ke-i.

Dalam bentuknya yang paling sederhana, ini mengurangi $P(A|B) = \{P(A)P(B|A)\} / P(B)$.

Statistik Bayesian berbeda dengan statistik klasik yang tidak berasumsi bahwa semua parameter distribusi tetap, namun parameternya adalah variabel yang acak. Probabilitas Bayesian dapat lebih mudah dipahami jika dianggap sebagai tingkat keyakinan seseorang dalam kejadian tertentu dibandingkan dengan cara klasik yang didasarkan pada bukti fisik. Karena pendekatan Bayesian didasarkan pada interpretasi probabilitas subyektif, ia menyediakan dasar siap untuk pemikiran keputusan dan pengembangan jaring Bayesian (atau jaringan kepercayaan, jejaring kepercayaan atau jejaring Bayesian).

Jaring Bayes menggunakan model grafis untuk mewakili satu set variabel dan hubungan probabilitas mereka. Jejaring terdiri dari simpul yang mewakili variabel acak dan panah yang menghubungkan simpul induk ke simpul anak, (di mana simpul induk adalah variabel yang secara langsung mempengaruhi variabel lain (anak)).

B.26.2 Penggunaan

Dalam beberapa tahun terakhir, penggunaan teori dan jaring Bays telah menyebar sebagian karena daya tarik intuitifnya dan juga karena ketersediaan alat bantu komputasi perangkat

lunak. Jaring Bayes telah digunakan pada berbagai topik: diagnosis medis, pemodelan citra, genetika, pengenalan ucapan, ekonomi, eksplorasi ruang angkasa dan mesin pencari web yang hebat yang digunakan saat ini. Mereka dapat berharga di berbagai area di mana terdapat persyaratan untuk mencari tahu tentang variabel yang tidak diketahui melalui penggunaan hubungan struktural dan data. Jaring Bayes dapat digunakan untuk mempelajari hubungan sebab-akibat untuk memberi pemahaman tentang wilayah permasalahan dan untuk memprediksi konsekuensi dari intervensi.

B.26.3 Masukan

Masukannya mirip dengan masukan untuk model Monte Carlo. Untuk jaring Bayes, contoh langkah-langkah yang harus diambil meliputi:

- menentukan variabel sistem;
- menentukan hubungan sebab-akibat antar variabel;
- menspesifikasikan probabilitas bersyarat dan yang sebelumnya;
- menambahkan bukti ke jaring;
- menampilkan pembaharuan kepercayaan;
- melakukan ekstraksi keyakinan yang sesudahnya.

B.26.4 Proses

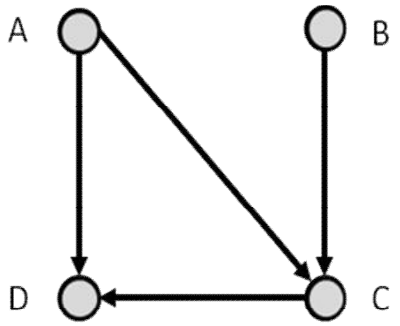
Teori Bayes dapat diterapkan dalam berbagai cara. Contoh ini akan mempertimbangkan pembuatan tabel Bayes dimana tes medis digunakan untuk menentukan apakah pasien memiliki penyakit. Keyakinan sebelum mengambil tes adalah bahwa 99 % populasi tidak memiliki penyakit ini dan 1 % memiliki penyakit ini, yaitu informasi sebelumnya. Keakuratan tes telah menunjukkan bahwa jika orang tersebut memiliki penyakit, hasil tesnya positif 98 % dari waktu. Ada juga kemungkinan bahwa jika Anda tidak memiliki penyakit ini, hasil tesnya positif 10 % dari waktu. Tabel Bayes menyediakan informasi berikut:

Table B.5 – Tabel data Bayes'

	AWAL	PROBABILITAS	PRODUK	AKHIR
Ada penyakit	0,01	0,98	0,009 8	0,090 1
Tidak ada penyakit	0,99	0,10	0,099 0	0,909 9
Jumlah	1		0,108 8	1

Dengan menggunakan aturan Bayes, produk ditentukan dengan menggabungkan data yang sebelumnya dan probabilitasnya. Bagian yang sesudahnya ditemukan dengan membagi nilai produk dengan total produk. Keluaran menunjukkan bahwa hasil tes positif mengindikasikan bahwa data-sebelumnya telah meningkat dari 1 % menjadi 9 %. Yang lebih penting lagi, terdapat suatu kemungkinan yang kuat bahwa walaupun dengan tes positif, kecil kemungkinan memiliki penyakit. Memeriksa persamaan (0,01 × 0,98) / ((0,01 × 0,98) + (0,99 × 0,1)) menunjukkan bahwa nilai 'hasil positif - tidak berpenyakit' memainkan peran utama dalam nilai yang sesudahnya.

Perhatikan jaring Bayes berikut ini:



IEC 2072/09

Gambar B.11 - Sampel jaring Bayes

Dengan probabilitas bersyarat dari data yang sebelumnya yang ditentukan dalam tabel berikut dan menggunakan notasi bahwa Y menunjukkan positif dan N menunjukkan negatif, positif dapat berarti "memiliki penyakit" seperti di atas, atau bisa tinggi dan N bisa rendah.

Tabel B.6 - Probabilitas Data-sebelumnya/*prior* untuk simpul A dan B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Tabel B.7 - Probabilitas bersyarat untuk simpul C dengan simpul A dan simpul B didefinisikan

A	*B*	P(*C* = *Y*)	P(*C* = *N*)
Y	*Y*	0,5	0,5
Y	*N*	0,9	0,1
N	*Y*	0,2	0,8
N	*N*	0,7	0,3

Tabel B.8 - Probabilitas bersyarat untuk simpul D dengan simpul A dan simpul C

A	C	P (D = Y)	P (D = N)
Y	Y	0,6	0,4
Y	N	1,0	0,0
N	Y	0,2	0,8
N	N	0,6	0,4

Untuk menentukan probabilitas yang sesudahnya P (A | D = N, C = Y), perlu dihitung terlebih dahulu P (A, B | D = N, C = Y).

Dengan menggunakan aturan Bayes, nilai P (D | A, C) P (C | A, B) P (A) P (B) ditentukan seperti yang ditunjukkan di bawah ini dan kolom terakhir menunjukkan probabilitas normal yang berjumlah 1 sebagai yang diturunkan Pada contoh sebelumnya (hasil dibulatkan).

Tabel B.9 - Probabilitas yang sesudahnya untuk simpul A dan B dengan simpul D dan simpul C didefinisikan

A	B	P(D|A,C)P(C|A,B)P(A)P(B)	P(A|D=N,C=Y)
Y	Y	0,4 x 0,5 x 0,9 x 0,6 = 0,110	0,4
Y	N	0,4 x 0,9 x 0,9 x 0,4 = 0,130	0,48
N	Y	0,8 x 0,2 x 0,1 x 0,6 = 0,110	0,04
N	N	0,8 x 0,7 x 0,1 x 0,4 = 0,022	0,08

Tabel B.10 - Probabilitas yang sesudahnya untuk simpul A dengan simpul D dan simpul C ditentukan

P(A=Y|D=N,C=Y)	P(A=N|D=N,C=Y)
0,88	0,12

Ini menunjukkan bahwa data yang sebelumnya untuk P (A = N) telah meningkat dari 0,1 ke posterior 0,12 yang hanya merupakan perubahan kecil. Di sisi lain, P (B = N | D = N, C = Y) telah berubah dari 0,4 menjadi 0,56 yang merupakan perubahan yang lebih signifikan.

B.26.5 Keluaran

Pendekatan Bayesian dapat diterapkan pada tingkat yang sama seperti statistik klasik dengan rentang keluaran yang luas, misalnya. analisis data untuk mendapatkan titik estimator dan interval keyakinan. Dewasa ini popularitasnya terkait dengan jaring Bayes untuk mendapatkan distribusi data yang sesudahnya. Keluaran grafis memberikan model yang mudah dipahami dan data yang dapat segera dimodifikasi untuk mempertimbangkan korelasi dan sensitivitas dari parameter.

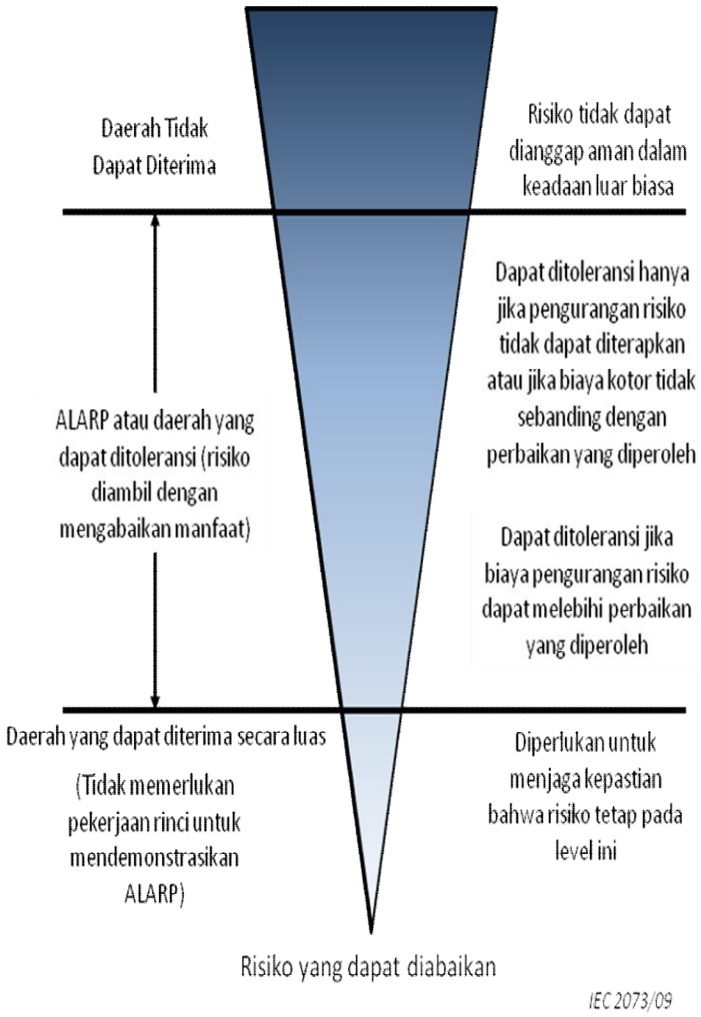
B.26.6 Kekuatan dan keterbatasan

Kekuatan:
- semua yang dibutuhkan adalah pengetahuan tentang data yang sebelumnya;
- pernyataan simpulan yang mudah dimengerti;
- semua yang dibutuhkan adalah aturan Bayes;
- aturan ini menyediakan mekanisme untuk menggunakan keyakinan subyektif dalam suatu masalah.

Keterbatasan:
- Mendefinisikan semua interaksi di jaring Bayes untuk sistem yang kompleks adalah masalah;
- Pendekatan Bayesian membutuhkan pengetahuan tentang banyak probabilitas kondisional yang umumnya diberikan oleh penilaian ahli. Peralatan perangkat lunak hanya bisa memberikan jawaban berdasarkan asumsi ini.

B.27 Kurva FN

B.27.1 Tinjauan singkat



Gambar B.12 - Konsep ALARP

Kurva FN adalah representasi grafis dari probabilitas kejadian yang menyebabkan tingkat kerusakan tertentu pada populasi tertentu. Paling sering mereka mengacu pada frekuensi sejumlah korban yang terjadi.

Kurva FN menunjukkan frekuensi kumulatif (F) di mana N atau lebih anggota populasi yang akan terpengaruh. Nilai N yang tinggi yang mungkin terjadi dengan suatu frekuensi F yang tinggi perlu perhatian khusus karena keduanya mungkin tidak dapat diterima secara sosial dan politik.

B.27.2 Penggunaan

Kurva FN adalah cara untuk menunjukan keluaran analisis risiko. Banyak kejadian memiliki probabilitas tinggi hasil dari konsekuensi rendah dan probabilitas rendah hasil dari konsekuensi tinggi. Kurva FN memberikan menunjukan tingkat risiko yang merupakan garis

yang menggambarkan kisaran ini daripada satu titik yang mewakili pasangan probabilitas konsekuensi.

Kurva FN dapat digunakan untuk membandingkan risiko, misalnya untuk membandingkan risiko yang sudah diprediksi dengan kriteria yang didefinisikan sebagai kurva FN, atau untuk membandingkan perkiraan risiko dengan data dari sejarah kejadian, atau dengan kriteria keputusan (juga dinyatakan sebagai kurva F / N).

Kurva FN dapat digunakan baik untuk perancangan sistem atau proses, atau untuk pengelolaan sistem yang ada.

B.27.3 Masukan

Masukannya diantaranya adalah:
- set pasangan konsekuensi probabilitas selama periode waktu tertentu;
- keluaran data dari analisis risiko kuantitatif yang memberikan perkiraan probabilitas untuk jumlah korban tertentu;
- data dari catatan sejarah dan analisis risiko kuantitatif.

B.27.4 Proses

Data yang tersedia diplotkan ke sebuah grafik dengan jumlah korban (ke tingkat bahaya tertentu, yaitu kematian) yang membentuk absis dengan probabilitas N atau lebih banyak korban membentuk ordinat. Karena banyaknya jajaran nilai, kedua sumbu biasanya berada pada skala logaritmik.

Kurva FN dapat dibangun secara statistik dengan menggunakan bilangan "nyata" dari kerugian masa lalu atau dapat dihitung berdasarkan estimasi model simulasi. Data yang digunakan dan asumsi yang dibuat dapat berarti bahwa kedua jenis kurva FN memberikan informasi yang berbeda dan harus digunakan secara terpisah dan untuk tujuan yang berbeda. Secara umum, teori kurva FN sangat berguna untuk perancangan sistem, dan secara statistik kurva FN paling berguna untuk pengelolaan sistem yang ada.

Kedua pendekatan turunan dapat sangat memakan waktu sehingga lazim menggunakan campuran keduanya. Data empiris kemudian akan membentuk titik-titik tetap dari korban yang diketahui dengan tepat yang terjadi dalam kecelakaan/insiden yang diketahui dalam periode waktu tertentu dan analisis risiko kuantitatif memberikan poin lain melalui ekstrapolasi atau interpolasi.

Kebutuhan untuk mempertimbangkan kecelakaan dengan frekuensi rendah, konsekuensi tinggi mungkin memerlukan pertimbangan waktu yang lama untuk mengumpulkan data yang cukup bagi analisis yang tepat. Hal ini pada gilirannya dapat membuat data yang tersedia menjadi dugaan jika kejadian yang mengawalinya kebetulan berubah sepanjang waktu.

B.27.5 Keluaran

Garis yang menggambarkan risiko di sepanjang rentang nilai konsekuensi yang dapat dibandingkan dengan kriteria yang sesuai untuk populasi yang sedang diteliti dan ditentukan tingkat kerusakannya.

B.27.6 Kekuatan dan keterbatasan

Kurva FN adalah suatu cara yang berguna untuk menyajikan informasi risiko yang dapat digunakan oleh pengelola dan perancang sistem untuk membantu membuat keputusan

mengenai tingkat risiko dan keselamatan. Kurva FN adalah suatu cara yang berguna untuk menyajikan informasi frekuensi dan konsekuensi dalam format yang mudah diakses.

Kurva FN sesuai untuk membandingan risiko dari situasi serupa dimana tersedia data yang memadai. Mereka sebaiknya tidak digunakan untuk membandingkan berbagai jenis risiko dengan berbagai karakteristik dalam situasi di mana kuantitas dan kualitas data bervariasi.

Keterbatasan kurva FN adalah kurva tersebut tidak menginformasikan apapun mengenai rentang efek atau hasil keluaran dari insiden selain dari jumlah orang yang terkena dampak, dan tidak ada cara untuk mengidentifikasi cara yang berbeda di mana tingkat bahaya mungkin sudah terjadi. Kurva itu memetakan jenis konsekuensi tertentu, biasanya membahayakan orang. Kurva FN bukanlah metode penilaian risiko, namun salah satu cara menyajikan hasil penilaian risiko.

Mereka adalah metode yang mapan untuk menyajikan hasil penilaian risiko namun memerlukan persiapan oleh analis yang terampil dan seringkali sulit dilakukan oleh spesialis non untuk menafsirkan dan mengevaluasi.

B.28 Indeks risiko

B.28.1 Tinjauan singkat

Indeks risiko adalah ukuran risiko semi kuantitatif yang merupakan estimasi yang diturunkan dari penggunaan pendekatan penilaian dengan skor menggunakan skala ordinal. Indeks risiko dapat digunakan untuk memeringkat serangkaian risiko dengan menggunakan kriteria serupa sehingga dapat dibandingkan. Angka skor diterapkan pada setiap komponen risiko, misalnya karakteristik kontaminan (sumber), rentang jalur paparan yang mungkin dan dampaknya terhadap penerima.

Indeks risiko pada dasarnya adalah pendekatan kualitatif untuk menentukan peringkat dan membandingkan risiko. Beberapa nomor digunakan, ini hanya untuk membolehan adanya manipulasi. Dalam banyak kasus di mana model atau sistem yang mendasarinya tidak diketahui atau tidak dapat dilukiskan, akan lebih baik menggunakan pendekatan kualitatif yang lebih terang-terangan.

B.28.2 Penggunaan

Indeks dapat digunakan untuk mengklasifikasikan berbagai risiko yang terkait dengan kegiatan jika sistem telah dipahami dengan baik. Mereka mengizinkan integrasi berbagai faktor yang berdampak pada tingkat risiko menjadi suatu skor numerikal tunggal untuk tingkat risiko

Indeks digunakan untuk berbagai jenis risiko biasanya sebagai alat pelingkupan untuk mengklasifikasi risiko sesuai dengan tingkat risiko. Ini dapat digunakan untuk menentukan risiko mana yang memerlukan penilaian lebih mendalam dan mungkin kuantitatif.

B.28.3 Masukan

Masukan berasal dari analisis sistem, atau deskripsi konteks yang luas. Ini memerlukan pemahaman yang baik tentang semua sumber risiko, jalur yang mungkin dan apa yang mungkin terpengaruh. Alat seperti analisis pohon kesalahan, analisis pohon kejadian dan analisis keputusan umum dapat digunakan untuk mendukung pengembangan indeks risiko.

Oleh karena pilihan skala ordinal, sampai batas tertentu, dapat dilakukan sesukanya, maka data yang cukup diperlukan untuk memvalidasi indeks.

B.28.4 Proses

Langkah pertama adalah memahami dan menggambarkan sistem. Setelah sistem didefinisikan, skor dikembangkan untuk masing-masing komponen sedemikian rupa sehingga dapat dikombinasikan untuk menyediakan indeks komposit. Misalnya, dalam konteks lingkungan, sumber, jalur dan penerima akan diberi skor, mencatat bahwa dalam beberapa kasus mungkin ada banyak jalur dan penerima untuk masing-masing sumber. Nilai individu digabungkan sesuai dengan skema yang memperhitungkan realitas fisik sistem. Adalah penting agar skor untuk setiap bagian sistem (sumber, jalur dan penerima) konsisten secara internal dan mempertahankan hubungan mereka yang benar. Skor dapat diberikan untuk komponen risiko (misalnya probabilitas, paparan, konsekuensi) atau faktor-faktor yang meningkatkan risiko.

Skor dapat ditambahkan, dikurangkan, dikalikan dan / atau dibagi sesuai dengan model tingkat tinggi ini. Efek kumulatif dapat diperhitungkan dengan menambahkan skor (misalnya, menambahkan skor untuk jalur yang berbeda). Hal ini benar-benar tidak berlaku untuk menerapkan rumus matematika ke skala ordinal. Oleh karena itu, sekali sistem penilaian telah dikembangkan, model harus divalidasi dengan menerapkannya pada sistem yang telah dikenal. Mengembangkan indeks adalah pendekatan yang berulang-ulang dan beberapa sistem yang berbeda untuk menggabungkan skor dapat dicoba sebelum analis merasa nyaman dengan validasi.

Ketidakpastian dapat diatasi dengan analisis sensitivitas dan berbagai skor untuk mengetahui parameter mana yang paling sensitif.

B.28.5 Keluaran

Keluarannya adalah serangkaian angka (indeks komposit) yang berhubungan dengan sumber tertentu dan yang dapat dibandingkan dengan indeks yang dikembangkan untuk sumber lain dalam sistem yang sama atau yang dapat dimodelkan dengan cara yang sama.

B.28.6 Kekuatan dan keterbatasan

Kekuatan:
- indeks dapat menyediakan alat yang baik untuk menentukan peringkat berbagai risiko;
- mereka memungkinkan beberapa faktor yang mempengaruhi tingkat risiko dimasukkan ke dalam satu skor/angka numerik untuk tingkat risiko.

Keterbatasan:
- jika proses (model) dan hasilnya tidak divalidasi dengan baik, hasilnya mungkin tidak ada artinya. Faktanya bahwa keluaran adalah nilai numerik untuk risiko dapat disalahartikan dan disalahgunakan, misalnya dalam analisis biaya / manfaat berikutnya;
- dalam banyak situasi di mana indeks digunakan, tidak ada model fundamental untuk menentukan apakah skala individual untuk faktor risiko bersifat linier, logaritmik atau dari bentuk lain, dan tidak ada model untuk menentukan bagaimana faktor sebaiknya digabungkan. Dalam situasi ini, pemeringkatan secara inheren tidak dapat diandalkan dan validasi terhadap data riil adalah penting secara khusus.

B.29 Matriks konsekuensi/probabilitas

B.29.1 Tinjauan singkat

Matriks konsekuensi/probabilitas adalah sarana untuk menggabungkan penilaian konsekuensi kualitatif atau semi kuantitatif dan probabilitas untuk menghasilkan tingkat risiko atau peringkat risiko.

Format matriks dan definisi yang diterapkan padanya bergantung pada konteks penggunaannya dan kepentinganya agar desain digunakan yang tepat untuk situasi tersebut.

B.29.2 Penggunaan

Matriks konsekuensi / probabilitas digunakan untuk menentukan peringkat risiko, sumber risiko atau perlakuan risiko berdasarkan tingkat risiko. Hal ini biasa digunakan sebagai alat penyaringan bila banyak risiko telah diidentifikasi, misalnya untuk menentukan risiko mana yang memerlukan analisis lebih lanjut atau lebih rinci, risiko mana yang memerlukan perlakuan terlebih dahulu, atau yang perlu dirujuk ke tingkat manajemen yang lebih tinggi. Ini juga dapat digunakan untuk memilih risiko yang tidak memerlukan dipertimbangkan lebih jauh saat ini. Matriks risiko semacam ini juga banyak digunakan untuk menentukan apakah risiko yang diberikan dapat diterima secara luas, atau tidak dapat diterima (lihat 5.4) sesuai dengan daerah di mana ia berada pada matriks.

Matriks konsekuensi/kemungkinan juga dapat digunakan untuk membantu mengkomunikasikan pemahaman bersama mengenai tingkat risiko kualitatif di seluruh organisasi. Cara tingkat risiko yang ditetapkan dan aturan keputusan yang diberikan kepada risiko-risiko sebaiknya diselaraskan dengan selera risiko organisasi.

Suatu bentuk matriks konsekuensi/probabilitas digunakan untuk analisis kritis di FMECA atau untuk menetapkan prioritas berdasarkan HAZOP. Ini juga dapat digunakan pada situasi di mana tidak cukupnya data untuk dianalisa terperinci atau situasinya tidak menjamin waktu dan usaha untuk analisa yang lebih kuantitatif.

B.29.3 Masukan

Masukan ke proses adalah skala yang disesuaikan untuk konsekuensi dan probabilitas serta suatu matriks yang menggabungkan keduanya.

Skala konsekuensi (atau skala) sebaiknya mencakup rentang berbagai jenis konsekuensi untuk dipertimbangkan (misalnya: kerugian finansial, keselamatan, lingkungan atau parameter lainnya, tergantung pada konteksnya) dan sebaiknya diperluas mulai dari konsekuensi maksimum yang dapat dipercaya hingga pada konsekuensi yang terendah yang menjadi perhatian. Sebagian contoh ditunjukkan pada Gambar B.6.

Skala mungkin memiliki sejumlah titik. Skala titik 3, 4 atau 5 adalah yang paling umum.

Skala probabilitas mungkin juga memiliki sejumlah titik. Definisi untuk probabilitas perlu dipilih agar semaksimal mungkin menjadi jelas. Jika panduan numerik digunakan untuk menentukan probabilitas yang berbeda, maka satuan sebaiknya diberikan. Skala probabilitas perlu merentang kisaran yang relevan bagi studi yang dikerjakan, mengingat bahwa probabilitas terendah harus dapat diterima untuk konsekuensi tertinggi yang didefinisikan, jika tidak semua kegiatan dengan konsekuensi tertinggi didefinisikan sebagai tidak dapat ditoleransi. Sebagian contoh ditunjukkan pada Gambar B.7.

Matriks digambar dengan konsekuensi pada satu sumbu dan probabilitas di sumbu yang lain. Gambar B.8 menunjukkan bagian dari matriks contoh dengan 6 titik konsekuensi dan 5 titik skala probabilitas .

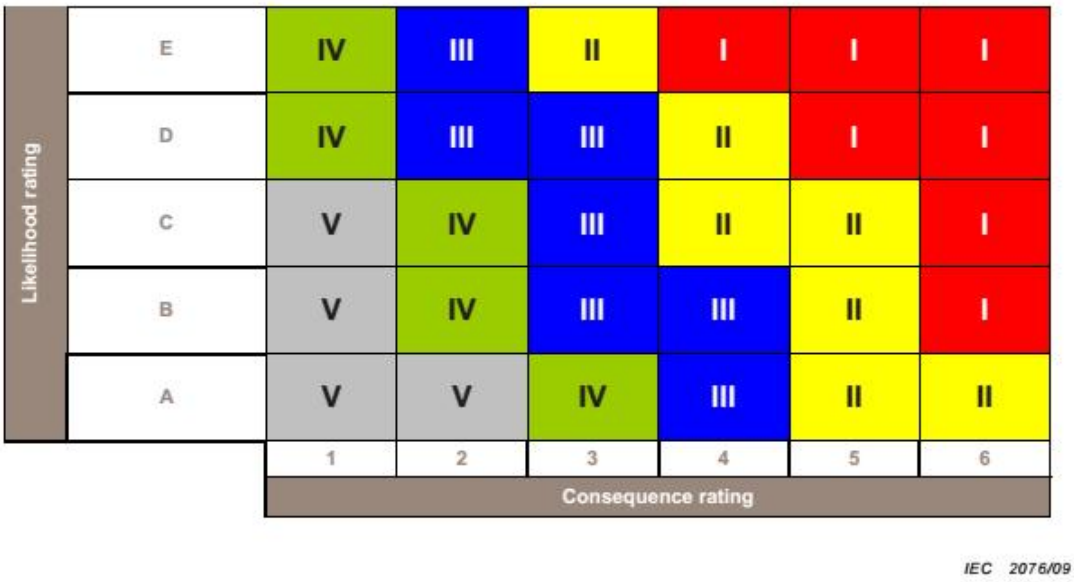
Tingkat risiko yang ditetapkan pada sel akan bergantung pada definisi skala probabilitas / konsekuensinya. Matriks dapat diatur untuk memberi bobot ekstra pada konsekuensi (seperti yang ditunjukkan) atau pada probabilitas, atau mungkin simetris, tergantung pada aplikasinya. Tingkat risiko dapat dikaitkan dengan aturan keputusan seperti tingkat perhatian manajemen atau skala waktu di mana respon diperlukan.

Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	Rugi atau untung lebih dari $100 juta	Rugi atau untung lebih dari $300 juta	• Banyak kematian, atau • Efek tak-terpulihkan (iresversibel) yang signifikan terhadap 10 orang	• Kerusakan pada lingkungan jangka panjang yang tidak dapat diperbaiki • Kemarahan masyarakat- potensi tindakan berskala besar	• Pelaporan pers internasional selama beberapa hari • Total kerugian dari pemegang saham yang berakibat pada tindakan divestasi • Direktur utama menyimpang dan dewan direstrukturisasi	• Litigasi atau penuntutan yang besar dengan kerugian lebih dari $50 juta ditambah biaya yang signifikan • Custodial sentence for company executive • Penutupan operasional yang berkepanjangan oleh pihak berwenang
5	Rugi atau untung $10 juta - $99 juta	Rugi atau untung $30 juta - $299 juta	• Satu korban jiwa dan/atau • cacat parah yang tidak dapat disembuhkan pada satu atau lebih orang	• Dampak pada lingkungan yang berkepanjangan • Perhatian masyarakat kelas atas meningkat – memerlukan tindakan remediasi yang signifikan	• Laporan pers nasional selama beberapa hari • Dampak berkelanjutan terhadap reputasi pemegang saham • Hilangnya pemegang saham mendukung ... pertumbuhan	• Biaya litigasi yang besar seharga $10 juta • Investigasi oleh badan regulasi yang mengakibatkan gangguan jangka panjang ....
4	Rugi atau untung $1 juta - $9 juta	Rugi atau untung $3m juta – $29 juta				
3	Rugi atau untung $100 ribu – 900k ribu					
2						
1						

Gambar B.13 - Contoh bagian tabel kriteria konsekuensi

Rating	Criteria
Sangat mungkin	Akan terjadi, atau Dapat terjadi dalam waktu "minggu ke bulan"
Mungkin	Mungkin terjadi segera tapi berbeda Dapat terjadi dalam ...
Tidak mungkin	Mungkin terjadi tetapi tidak ... Dapat terjadi dalam
Jarang	Kejadian Istimewa Hanya terjadi ...
Remote	

Gambar B.14 - Contoh bagian matriks peringkat risiko



Gambar B.15 - Contoh bagian matriks kriteria probabilitas

Skala penilaian dan matriks dapat diatur dengan skala kuantitatif. Misalnya, dalam konteks keandalan, skala probabilitas dapat mewakili tingkat indikasi kegagalan dan skala dampak dollar biaya kegagalan.

Penggunaan alat ini membutuhkan orang (idealnya sebuah tim) dengan keahlian dan data yang relevan tersedia untuk membantu dalam penilaian konsekuensi dan probabilitas.

B.29.4 Proses

Untuk memeringkat risiko, pengguna pertama-tama menemukan gambaran konsekuensi yang paling sesuai dengan situasinya kemudian menentukan probabilitas konsekuensi tersebut akan terjadi. Tingkat risiko kemudian terbaca dari matriks.

Banyak kejadian berisiko mungkin memiliki serangkaian rentangan hasil dengan berbagai probabilitas terkait. Biasanya, masalah kecil lebih sering terjadi daripada malapetaka. Oleh karena itu ada pilihan untuk menentukan urutan hasil paling umum atau kombinasi paling serius atau kombinasi lainnya. Dalam banyak kasus, tepat untuk berfokus pada hasil yang paling serius yang dapat dipercaya karena ini merupakan ancaman terbesar dan seringkali menjadi perhatian utama. Dalam beberapa kasus, mungkin tepat untuk menentukan peringkat umum dan malapetaka yang mungkin terjadi sebagai risiko yang terpisah. Penting bahwa probabilitas yang relevan dengan konsekuensi yang dipilih digunakan dan bukan probabilitas secara keseluruhan kejadian.

Tingkat risiko yang didefinisikan oleh matriks dapat juga dikaitkan dengan aturan keputusan seperti untuk memperlakukan atau tidak memperlakukan risiko.

B.29.5 Keluaran

Keluaranya adalah peringkat untuk setiap risiko atau peringkat daftar risiko dengan tingkat signifikansi yang telah ditentukan.

B.29.6 Kekuatan dan keterbatasan

Kekuatan:
- relatif mudah digunakan;
- dengan cepat enyediakan peringkat risiko ke dalam tingkat kepentingan yang berbeda.

Keterbatasan:
- suatu matriks sebaiknya dirancang sesuai dengan keadaan-keadaan tertentu karenanya sulit untuk memiliki sistem yang umum untuk penerapan diseluruh rentang kondisi yang relevan bagi suatu organisasi;
- sulit untuk menentukan skala yang tidak ambigu;
- penggunaan sangat subjektif dan cenderung ada variasi yang signifikan antara penilai;
- risiko tidak dapat digabungkan (yaitu kita tidak dapat menentukan bahwa sejumlah risiko rendah atau risiko rendah yang teridentifikasi dalam beberapa waktu tertentu adalah setara dengan suatu risiko menengah);
- sulit untuk menggabungkan atau membandingkan tingkat risiko untuk berbagai kategori konsekuensi.

Hasil akan tergantung dari tingkat kerincian suatu analisis, yaitu semakin rinci suatu analisis, semakin tinggi jumlah skenario, sehingga masing-masing memiliki probabilitas yang lebih rendah. Ini akan meremehkan tingkat risiko yang sebenarnya. Cara bagaimana skenario dikelompokkan bersama dalam menggambarkan risiko, sebaiknya konsisten dan didefinisikan pada saat awal penelitian.

B.30 Analisis biaya/manfaat (*Cost/benefit analysis - CBA*)

B.30.1 Tinjauan singkat

Analisis biaya/manfaat dapat digunakan untuk evaluasi risiko di mana total biaya yang diharapkan ditimbang terhadap total manfaat yang diharapkan untuk memilih opsi terbaik atau yang paling menguntungkan. Hal tersebut adalah suatu bagian yang implisit dari banyak sistem evaluasi risiko. Hal tersebut dapat bersifat kualitatif atau kuantitatif atau melibatkan suatu kombinasi unsur kuantitatif dan kualitatif. Kuantitatif CBA mengumpulkan nilai moneter dari semua biaya dan semua manfaat untuk semua pemangku kepentingan yang termasuk dalam ruang lingkup serta disesuaikan dengan periode waktu yang berbeda di mana biaya dan manfaatnya meningkat. Nilai bersih sekarang (*net present value-NPV*) yang dihasilkan menjadi masukan bagi keputusan tentang risiko. NPV positif terkait dengan suatu tindakan yang biasanya berarti bahwa tindakan tersebut sebaiknya terjadi. Namun, untuk beberapa risiko negatif, terutama yang melibatkan risiko terhadap kehidupan manusia atau kerusakan lingkungan, prinsip ALARP dapat diterapkan. Hal ini membagi risiko menjadi tiga tingkatan: tingkat di atas di mana risiko negatif tidak dapat ditolerir dan tidak boleh dilakukan kecuali pada keadaan luar biasa; Tingkat bawah di mana risiko diabaikan dan hanya perlu dipantau untuk memastikan mereka tetap rendah; Dan pita ditengah di mana risiko dibuat serendah mungkin (ALARP). Menjelang berakhirnya risiko lebih rendah di wilayah ini, analisis biaya yang ketat mungkin diberlakukan namun jika risiko hampir tidak dapat ditolerir, harapan dari prinsip ALARP adalah bahwa perlakuan risiko akan dilakukan kecuali jika biaya perlakuan sangat tidak proporsional dengan keuntungan yang didapat.

B.30.2 Penggunaan

Analisis biaya / manfaat dapat digunakan untuk menentukan antar opsi risiko terkait.

Sebagai contoh
- sebagai masukan terhadap keputusan tentang apakah suatu risiko harus diperlakukan,

- untuk membedakan antara dan memutuskan bentuk terbaik dari perlakuan risiko,
- untuk memutuskan diantara berbagai tindakan yang berbeda.

B.30.3 Masukan

Masukan mencakup informasi mengenai biaya dan manfaat bagi pemangku kepentingan terkait dan ketidakpastian biaya dan manfaat tersebut. Biaya dan manfaat yang berwujud dan tidak berwujud harus dipertimbangkan. Biaya mencakup sumber daya yang dikeluarkan dan hasil yang negatif, manfaat mencakup hasil yang positif, hasil yang negatif dihindari dan sumber daya disimpan.

B.30.4 Proses

Para pemangku kepentingan yang mungkin memiliki pengalaman biaya atau menerima manfaat diidentifikasi. Dalam suatu analisis manfaat biaya secara lengkap semua pemangku kepentingan disertakan.

Manfaat dan biaya langsung serta tidak langsung kepada semua pemangku kepentingan yang relevan dari opsi yang sedang dipertimbangkan telah diidentifikasi. Manfaat langsung adalah semua yang mengalir langsung dari tindakan yang diambil, namun manfaat tidak langsung atau tambahan adalah hal yang kebetulan terjadi tetapi masih mungkin berkontribusi signifikan terhadap keputusan tersebut. Contoh manfaat tidak langsung meliputi perbaikan reputasi, kepuasan staf dan "ketenangan pikiran". (Hal ini sering diberikan bobot yang berat dalam pengambilan keputusan).

Biaya langsung adalah biaya yang berhubungan langsung dengan tindakan. Biaya tidak langsung adalah semua penambahan, biaya tambahan dan hilang, seperti kehilangan utilitas, gangguan pengelolaan waktu atau pengalihan modal dari investasi potensial lainnya. Saat menerapkan analisis manfaat biaya untuk memutuskan apakah akan memperlakukan risiko, biaya dan manfaat yang terkait dengan penanganan risiko, dan dengan mengambil risiko, harus menyertakan.

Dalam analisis biaya / manfaat kuantitatif, bila semua biaya dan manfaat berwujud dan tidak berwujud telah diidentifikasi, nilai moneter diberikan untuk semua biaya dan manfaat (termasuk biaya dan manfaat tak berwujud). Ada sejumlah cara standar untuk melakukan ini termasuk pendekatan 'kemauan membayar' dan menggunakan pengganti. Jika, seperti yang sering terjadi, biaya dikeluarkan dalam waktu singkat (misalnya setahun) dan manfaatnya mengalir untuk waktu yang lama setelahnya, biasanya perlu untuk mengurangi manfaat yang akan dibawa ke "nilai uang saat ini" sehingga Perbandingan yang valid bisa didapat. Semua biaya dan manfaat dinyatakan sebagai nilai sekarang. Nilai sekarang dari semua biaya dan semua keuntungan bagi semua pemangku kepentingan dapat digabungkan untuk menghasilkan nilai bersih sekarang. NPV positif menyiratkan bahwa tindakan tersebut bermanfaat. Rasio biaya manfaat juga digunakan lihat B.30.5

Jika ada ketidakpastian mengenai tingkat biaya atau manfaat, salah satu atau kedua syarat tersebut dapat dibobot sesuai dengan probabilitasnya.

Dalam analisis manfaat biaya kualitatif tidak ada upaya yang dilakukan untuk menentukan nilai moneter untuk biaya dan manfaat tak berwujud dan, daripada memberikan satu angka yang merangkum biaya dan manfaat, hubungan dan pertukaran antara biaya dan tunjangan yang berbeda dianggap secara kualitatif.

Teknik yang terkait adalah analisis efektivitas biaya. Ini diasumsikan bahwa suatu keuntungan atau hasil tertentu diinginkan, dan ada beberapa cara alternatif untuk mencapainya. Analisis ini hanya melihat biaya dan cara termurah untuk meraih keuntungan.

B.30.5 Keluaran

Keluaran dari suatu analisis biaya / manfaat adalah informasi mengenai biaya dan manfaat yang terkait dari berbagai opsi atau tindakan. Hal ini dapat dinyatakan secara kuantitatif sebagai suatu nilai bersih saat ini (NPV) suatu tingkat pengembalian internal (*internal rate of return-IRR*) atau sebagai rasio dari nilai manfaat saat ini terhadap nilai saat ini dari biaya. Keluaran secara kualitatif biasanya merupakan tabel yang membandingkan biaya dan manfaat dari berbagai jenis biaya dan manfaat, yang menarik perhatian untuk pertukaran.

B.30.6 Kekuatan dan keterbatasan

Kekuatan analisis biaya manfaat:
- memungkinkan biaya dan manfaat dibandingkan menggunakan satu metrik (uang);
- memberikan transparansi pada pengambilan keputusan;
- memerlukan informasi terperinci untuk dikumpulkan pada semua aspek keputusan yang mungkin. Ini bisa sangat berharga dalam mengungkapkan ketidaktahuan dan juga mengkomunikasikan pengetahuan.

Keterbatasan:
- CBA kuantitatif dapat memberikan hasil angka yang sangat berbeda, tergantung pada metode yang digunakan untuk menetapkan nilai ekonomi terhadap manfaat non-ekonomi;
- Dalam beberapa aplikasi, sulit untuk menentukan tingkat diskonto yang valid untuk biaya dan manfaat masa depan;
- manfaat yang diperoleh pada populasi besar sulit diperkirakan, terutama yang berkaitan dengan barang publik yang tidak dipertukarkan di pasar;
- praktik diskonto berarti bahwa keuntungan yang didapat di masa depan memiliki pengaruh yang dapat diabaikan terhadap keputusan yang tergantung pada tingkat diskonto yang dipilih. Metode ini menjadi tidak sesuai dalam mempertimbangkan risiko yang mempengaruhi generasi mendatang kecuali tingkat diskontonya yang sangat rendah atau ditetapkan nol.

B.31 Analisis keputusan multi kriteria (*Multi-criteria decision analysis* - MCDA)

B.31.1 Tinjauan singkat

Sasarannya adalah untuk menggunakan rentang kriteria dalam menilai secara obyektif, transparan serta kelayakan menyeluruh dari seperangkat pilihan. Secara umum, tujuan keseluruhan adalah untuk menghasilkan preferensi susunan antara pilihan yang tersedia. Analisis ini melibatkan pengembangan matriks pilihan dan kriteria yang diurutkan dan digabungkan untuk memberikan skor keseluruhan pada setiap pilihan.

B.31.2 Penggunaan

MCDA bisa digunakan untuk
- membandingkan beberapa opsi untuk analisis tahap pertama yang diterima untuk menentukan opsi yang diutamakan dan opsi potensial serta opsi yang tidak tepat,
- membandingkan opsi dilakukan apabila terdapat banyak kriteria dan terkadang kriteria tersebut bertentangan,
- mencapai konsensus mengenai suatu keputusan dari pemangku kepentingan berbeda yang memiliki sasaran atau nilai yang bertentangan.

B.31.3 Masukan

Suatu kumpulan pilihan untuk analisis. Kriteria, berdasarkan pada tujuan yang bisa digunakan di semua pilihan untuk membedakan diantaranya.

B.31.4 Proses

Secara umum, sekelompok pemangku kepentingan yang berpengetahuan luas melakukan proses berikut:

a) mendefinisikan sasaran;
b) menentukan kelengkapan (kriteria atau ukuran kinerja) yang berhubungan dengan setiap sasaran;
c) menyusun kelengkapan menjadi suatu hierarki;
d) mengembangkan opsi untuk dievaluasi mengacu pada kriteria;
e) menentukan pentingnya kriteria dan menetapkan bobot yang sesuai dengan mereka;
f) mengevaluasi alternatif berkenaan dengan kriteria. Ini dapat digambarkan sebagai matriks skor.
g) mengkombinasikan banyak skor kelengkapan tunggal menjadi suatu nilai tunggal gabungan skor multi kelengkapan;
h) mengevaluasi hasilnya.

Ada beberapa metode yang berbeda dimana pembobotan untuk setiap kriteria dapat diperoleh dan cara yang berbeda untuk menggabungkan nilai kriteria untuk setiap opsi menjadi suatu nilai tunggal multi kelengkapan. Misalnya, skor dapat digabungkan sebagai jumlah tertimbang atau produk tertimbang atau menggunakan proses analisis hierarki, suatu teknik elisitasi *(elicitation technique)* untuk pembobotan dan penilaian berdasarkan pembandingan berpasangan *(pairwise comparisons)*. Semua metode ini mengasumsikan bahwa preferensi untuk setiap kriteria tidak bergantung pada nilai kriteria lainnya. jika asumsi ini tidak valid, model yang berbeda digunakan.

Karena skor adalah subyektif, analisis sensitivitas berguna untuk menguji sejauh mana bobot dan skor mempengaruhi seluruh preferensi diantara opsi.

B.31.5 Keluaran

Urutan penyajian dari beberapa opsi dimulai dari yang paling diutamakan hingga yang kurang diutamakan. Jika proses menghasilkan matriks dimana sumbu matriks adalah kriteria bobot dan kriteria skor untuk setiap opsi, maka opsi yang gagal memenuhi kriteria tertimbang juga dapat dieliminasi.

B.31.6 Kekuatan dan keterbatasan

Kekuatan:
- menyediakan suatu struktur yang sederhana untuk pengambilan keputusan yang efisien dan penyajian asumsi dan kesimpulan;
- dapat membuat keputusan untuk masalah yang kompleks, yang tidak sesuai dengan analisis biaya / manfaat, menjadi lebih mudah dikelola;
- dapat membantu mempertimbangkan masalah secara rasional di mana pengorbanan perlu dilakukan;
- dapat membantu mencapai kesepakatan ketika para pemangku kepentingan memiliki tujuan dan kriteria yang berbeda.

Keterbatasan:
- dapat dipengaruhi oleh pemilihan kriteria keputusan yang bias dan buruk;

- sebagian besar masalah MCDA tidak memiliki suatu solusi yang meyakinkan atau unik;
- algoritma gabungan yang menghitung bobot kriteria dari preferensi yang disebutkan atau gabungan dari pendapat yang berbeda dapat menyamarkan dasar keputusan yang sebenarnya.

Risk management – Risk assessment techniques

(ISO/IEC 31010:2009, IDT)

Introduction

Organizations of all types and sizes face a range of risks that may affect the achievement of their objectives.

These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that should be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management includes the application of logical and systematic methods for

- communicating and consulting throughout this process;
- establishing the context for identifying, analysing, evaluating, treating risk associated with any activity, process, function or product;
- monitoring and reviewing risks;
- reporting and recording the results appropriately.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

- what can happen and why (by risk identification)?
- what are the consequences?
- what is the probability of their future occurrence?
- are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Is the level of risk tolerable or acceptable and does it require further treatment? This standard is intended to reflect current good practices in selection and utilization of risk assessment techniques, and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus.

This standard is general in nature, so that it may give guidance across many industries and types of system. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of assessment for particular applications. If these standards are in harmony with this standard, the specific standards will generally be sufficient.

Risk management – Risk assessment techniques

1 Scope

This International Standard is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.

Risk assessment carried out in accordance with this standard contributes to other risk management activities.

The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail.

This standard is not intended for certification, regulatory or contractual use.

This standard does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application.

This standard does not refer to all techniques, and omission of a technique from this standard does not mean it is not valid. The fact that a method is applicable to a particular circumstance does not mean that the method should necessarily be applied.

NOTE: This standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*

ISO 31000, *Risk management – Principles and guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions of ISO/IEC Guide 73 apply

4 Risk assessment concepts

4.1 Purpose and benefits

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options.

Some of the principal benefits of performing risk assessment include:

- understanding the risk and its potential impact upon objectives;
- providing information for decision makers;
- contributing to the understanding of risks, in order to assist in selection of treatment options;
- identifying the important contributors to risks and weak links in systems and organizations;
- comparing of risks in alternative systems, technologies or approaches;
- communicating risks and uncertainties;
- assisting with establishing priorities;
- contributing towards incident prevention based upon post-incident investigation;
- selecting different forms of risk treatment;
- meeting regulatory requirements;
- providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria;
- assessing risks for end-of-life disposal.

4.2 Risk assessment and the risk management framework

This standard assumes that the risk assessment is performed within the framework and process of risk management described in ISO 31000.

A risk management framework provides the policies, procedures and organizational arrangements that will embed risk management throughout the organization at all levels.

As part of this framework, the organization should have a policy or strategy for deciding when and how risks should be assessed.

In particular, those carrying out risk assessments should be clear about
- the context and objectives of the organization,
- the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,
- how risk assessment integrates into organizational processes,
- methods and techniques to be used for risk assessment, and their contribution to the risk management process,
- accountability, responsibility and authority for performing risk assessment,
- resources available to carry out risk assessment,
- how the risk assessment will be reported and reviewed.

4.3 Risk assessment and the risk management process

4.3.1 General

Risk assessment comprises the core elements of the risk management process which are defined in ISO 31000 and contain the following elements:

- communication and consultation;
- establishing the context;
- risk assessment (comprising risk identification, risk analysis and risk evaluation);
- risk treatment;
- monitoring and review.

Risk assessment is not a stand-alone activity and should be fully integrated into the other components in the risk management process.

4.3.2 Communication and consultation

Successful risk assessment is dependent on effective communication and consultation with stakeholders.

Involving stakeholders in the risk management process will assist in
- developing a communication plan,
- defining the context appropriately,
- ensuring that the interests of stakeholders are understood and considered,
- bringing together different areas of expertise for identifying and analysing risk,
- ensuring that different views are appropriately considered in evaluating risks,
- ensuring that risks are adequately identified,
- securing endorsement and support for a treatment plan.

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and programme management, and also financial management.

4.3.3 Establishing the context

Establishing the context defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Establishing the context includes considering internal and external parameters relevant to the organization as a whole, as well as the background to the particular risks being assessed.

In establishing the context, the risk assessment objectives, risk criteria, and risk assessment programme are determined and agreed.

For a specific risk assessment, establishing the context should include the definition of the external, internal and risk management context and classification of risk criteria:

a) Establishing the external context involves familiarization with the environment in which the organization and the system operates including :
   - cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local;
   - key drivers and trends having impact on the objectives of the organization; and
   - perceptions and values of external stakeholders.

b) Establishing the internal context involves understanding
   - capabilities of the organization in terms of resources and knowledge,
   - information flows and decision-making processes,
   - internal stakeholders,
   - objectives and the strategies that are in place to achieve them,
   - perceptions, values and culture,
   - policies and processes,
   - standards and reference models adopted by the organization, and
   - structures (e.g. governance, roles and accountabilities).

c) Establishing the context of the risk management process includes
   - defining accountabilities and responsibilities,
   - defining the extent of the risk management activities to be carried out, including specific inclusions and exclusions,
   - defining the extent of the project, process, function or activity in terms of time and location,

- defining the relationships between a particular project or activity and other projects or activities of the organization,
- defining the risk assessment methodologies,
- defining the risk criteria,
- defining how risk management performance is evaluated,
- identifying and specifying the decisions and actions that have to be made, and
- identifying scoping or framing studies needed, their extent, objectives and the resources required for such studies.

d) Defining risk criteria involves deciding
- the nature and types of consequences to be included and how they will be measured,
- the way in which probabilities are to be expressed,
- how a level of risk will be determined,
- the criteria by which it will be decided when a risk needs treatment,
- the criteria for deciding when a risk is acceptable and/or tolerable,
- whether and how combinations of risks will be taken into account. Criteria can be based on sources such as
- agreed process objectives,
- criteria identified in specifications,
- general data sources,
- generally accepted industry criteria such as safety integrity levels,
- organizational risk appetite,
- legal and other requirements for specific equipment or applications.

4.3.4 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risks can e assessed at an organizational level, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:
- whether an activity should be undertaken;
- how to maximize opportunities;
- whether risks need to be treated;
- choosing between options with different risks;
- prioritizing risk treatment options;
- the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

4.3.5 Risk treatment

Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and implementing these options.

This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required.

4.3.6 Monitoring and review

As part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that

- assumptions about risks remain valid;
- assumptions on which the risk assessment is based, including the external and internal context, remain valid;
- expected results are being achieved;
- results of risk assessment are in line with actual experience;
- risk assessment techniques are being properly applied;
- risk treatments are effective.

Accountability for monitoring and performing reviews should be established.

5 Risk assessment process

5.1 Overview

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (see Figure 1). The manner in which this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.

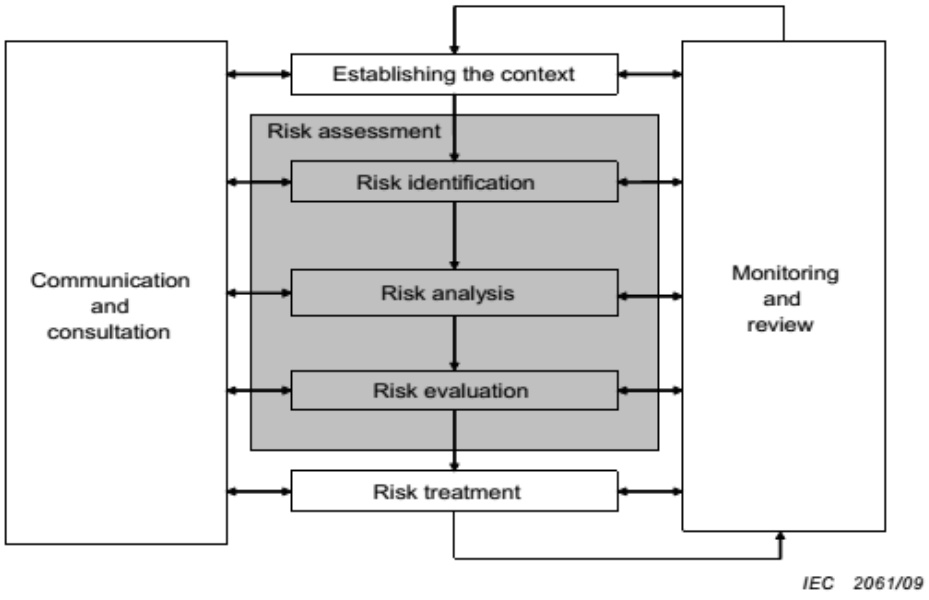


Figure 1 – Contribution of risk assessment to the risk management process

Risk assessment may require a multidisciplinary approach since risks may cover a wide range of causes and consequences.

5.2 Risk identification

Risk identification is the process of finding, recognizing and recording risks.

The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.

The risk identification process includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact.

Risk identification methods can include:
- evidence based methods, examples of which are check-lists and reviews of historical data;
- systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions;
- inductive reasoning techniques such as HAZOP.

Various supporting techniques can be used to improve accuracy and completeness in risk identification, including brainstorming, and Delphi methodology.

Irrespective of the actual techniques employed, it is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" or "software" events.

5.3 Risk analysis

5.3.1 General

Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account. Various methods for these analyses are described in Annex B. More than one technique may be required for complex applications.

Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made.

In some circumstances, a consequence can occur as a result of a range of different events or conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analysing the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies.

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs of the organization. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Even where full quantification has been carried out, it needs to be recognized that the levels of risk calculated are estimates. Care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of a risk can be expressed as a probability distribution over a range of consequences.

5.3.2 Controls assessment

The level of risk will depend on the adequacy and effectiveness of existing controls. Questions to be addressed include:

- what are the existing controls for a particular risk?
- are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- in practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

These questions can only be answered with confidence if there are proper documentation and assurance processes in place.

The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of

risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment.

5.3.3 Consequence analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. An event may have a range of impacts of different magnitudes, and affect a range of different objectives and different stakeholders. The types of consequence to be analysed and the stakeholders affected will have been decided when the context was established.

Consequence analysis can vary from a simple description of outcomes to detailed quantitative modelling or vulnerability analysis.

Impacts may have a low consequence but high probability, or a high consequence and low probability, or some intermediate outcome. In some cases, it is appropriate to focus on risks with potentially very large outcomes, as these are often of greatest concern to managers. In other cases, it may be important to analyse both high and low consequence risks separately. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is useful to analyse them separately.

Consequence analysis can involve:
- taking into consideration existing controls to treat the consequences, together with all relevant contributory factors that have an effect on the consequences;
- relating the consequences of the risk to the original objectives;
- considering both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the assessment;
- considering secondary consequences, such as those impacting upon associated systems, activities, equipment or organizations.

5.3.4 Likelihood analysis and probability estimation

Three general approaches are commonly employed to estimate probability; they may be used individually or jointly:

a) The use of relevant historical data to identify events or situations which have occurred in the past and hence be able to extrapolate the probability of their occurrence in the future. The data used should be relevant to the type of system, facility, organization or activity being considered and also to the operational standards of the organization involved. If historically there is a very low frequency of occurrence, then any estimate of probability will be very uncertain. This applies especially for zero occurrences, when one cannot assume the event, situation or circumstance will not occur in the future.

b) Probability forecasts using predictive techniques such as fault tree analysis and event tree analysis (see Annex B). When historical data are unavailable or inadequate, it is necessary to derive probability by analysis of the system, activity, equipment or organization and its associated failure or success states. Numerical data for equipment, humans, organizations and systems from operational experience, or published data sources are then combined to produce an estimate of the probability of the top event. When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the co-incidental failure of a number of different parts or components within the system arising from the same cause. Simulation techniques may be required to generate probability of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties.

c) Expert opinion can be used in a systematic and structured process to estimate probability. Expert judgements should draw upon all relevant available information including historical, system-specific, organizational-specific, experimental, design, etc. There are a number of formal methods for eliciting expert judgement which provide an aid to the formulation of appropriate questions. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgement.

5.3.5 Preliminary analysis

Risks may be screened in order to identify the most significant risks, or to exclude less significant or minor risks from further analysis. The purpose is to ensure that resources will be focussed on the most important risks. Care should be taken not to screen out low risks which occur frequently and have a significant cumulative effect

Screening should be based on criteria defined in the context. The preliminary analysis determines one or more of the following courses of action:

- decide to treat risks without further assessment;
- set aside insignificant risks which would not justify treatment;
- proceed with more detailed risk assessment.

The initial assumptions and results should be documented.

5.3.6 Uncertainties and sensitivities

There are often considerable uncertainties associated with the analysis of risk. An understanding of uncertainties is necessary to interpret and communicate risk analysis results effectively. The analysis of uncertainties associated with data, methods and models used to identify and analyse risk plays an important part in their application. Uncertainty analysis involves the determination of the variation or imprecision in the results, resulting from the collective variation in the parameters and assumptions used to define the results. An area closely related to uncertainty analysis is sensitivity analysis.

Sensitivity analysis involves the determination of the size and significance of the magnitude of risk to changes in individual input parameters. It is used to identify those data which need to be accurate, and those which are less sensitive and hence have less effect upon overall accuracy.

The completeness and accuracy of the risk analysis should be stated as fully as possible. Sources of uncertainty should be identified where possible and should address both data and model/method uncertainties. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated.

5.4 Risk evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk.

Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs to the decision.

Decisions may include:

- whether a risk needs treatment;
- priorities for treatment;
- whether an activity should be undertaken;

- which of a number of paths should be followed.

The nature of the decisions that need to be made and the criteria which will be used to make those decisions were decided when establishing the context but they need to be revisited in more detail at this stage now that more is known about the particular risks identified.

The simplest framework for defining risk criteria is a single level which divides risks that need treatment from those which do not. This gives attractively simple results but does not reflect

The uncertainties involved both in estimating risks and in defining the boundary between those that need treatment and those that do not.

The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls.

A common approach is to divide risks into three bands:
a) an upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;
b) a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;
c) a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

The 'as low as reasonably practicable' or ALARP criteria system used in safety applications follows this approach, where, in the middle band, there is a sliding scale for low risks where costs and benefits can be directly compared, whereas for high risks the potential for harm must be reduced, until the cost of further reduction is entirely disproportionate to the safety benefit gained.

5.5 Documentation

The risk assessment process should be documented together with the results of the assessment. Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear.

The extent of the report will depend on the objectives and scope of the assessment. Except for very simple assessments, the documentation can include:
- objectives and scope;
- description of relevant parts of the system and their functions;
- a summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed;
- risk criteria applied and their justification;
- limitations, assumptions and justification of hypotheses;
- assessment methodology;
- risk identification results;
- data, assumptions and their sources and validation;
- risk analysis results and their evaluation;
- sensitivity and uncertainty analysis;
- critical assumptions and other factors which need to be monitored;
- discussion of results;
- conclusions and recommendations;
- references.

If the risk assessment supports a continuing risk management process, it should be performed and documented in such a way that it can be maintained throughout the life cycle of the system, organization, equipment or activity. The assessment should be updated as significant new information becomes available and the context changes, in accordance with the needs of the management process.

5.6 Monitoring and reviewing risk assessment

The risk assessment process will highlight context and other factors that might be expected to vary over time and which could change or invalidate the risk assessment. These factors should be specifically identified for on-going monitoring and review, so that the risk assessment can be updated when necessary.

Data to be monitored in order to refine the risk assessment should also be identified and collected.

The effectiveness of controls should also be monitored and documented in order to provide data for use in risk analysis. Accountabilities for creation and reviewing the evidence and documentation should be defined.

5.7 Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycles phases have different requirements and need different techniques For example, during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of positive and negative risks.

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable,
- the design refinement process,
- cost effectiveness studies,
- identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

6 Selection of risk assessment techniques

6.1 General

This clause describes how techniques for risk assessment may be selected. The annexes list and further explain a range of tools and techniques that can be used to perform a risk assessment or to assist with the risk assessment process. It may sometimes be necessary to employ more than one method of assessment.

6.2 Selection of techniques

Risk assessment may be undertaken in varying degrees of depth and detail and using one or many methods ranging from simple to complex. The form of assessment and its output should be consistent with the risk criteria developed as part of establishing the context. Annex A illustrates the conceptual relationship between the broad categories of risk assessment techniques and the factors present in a given risk situation, and provides illustrative examples of how organizations can select the appropriate risk assessment techniques for a particular situation.

In general terms, suitable techniques should exhibit the following characteristics:

- it should be justifiable and appropriate to the situation or organization under consideration;
- it should provide results in a form which enhances understanding of the nature of the risk and how it can be treated;
- it should be capable of use in a manner that is traceable, repeatable and verifiable.

The reasons for the choice of techniques should be given, with regard to relevance and suitability. When integrating the results from different studies, the techniques used and outputs should be comparable.

Once the decision has been made to perform a risk assessment and the objectives and scope have been defined, the techniques should be selected, based on applicable factors such as:

- the objectives of the study. The objectives of the risk assessment will have a direct bearing on the techniques used. For example, if a comparative study between different options is being undertaken, it may be acceptable to use less detailed consequence models for parts of the system not affected by the difference;
- the needs of decision-makers. In some cases a high level of detail is needed to make a good decision, in others a more general understanding is sufficient;
- the type and range of risks being analysed;
- the potential magnitude of the consequences. The decision on the depth to which risk assessment is carried out should reflect the initial perception of consequences (although this may have to be modified once a preliminary evaluation has been completed);
- the degree of expertise, human and other resources needed. A simple method, well done, may provide better results than a more sophisticated procedure poorly done, so long as it meets the objectives and scope of the assessment. Ordinarily, the effort put into the assessment should be consistent with the potential level of risk being analysed;
- the availability of information and data. Some techniques require more information and data than others;
- the need for modification/updating of the risk assessment. The assessment may need to be modified/updated in future and some techniques are more amendable than others in this regard;
- any regulatory and contractual requirements.

Various factors influence the selection of an approach to risk assessment such as the availability of resources, the nature and degree of uncertainty in the data and information available, and the complexity of the application (see Table A.2).

6.3 Availability of resources

Resources and capabilities which may affect the choice of risk assessment techniques include:

- the skills experience capacity and capability of the risk assessment team;
- constraints on time and other resources within the organization;
- the budget available if external resources are required.

6.4 The nature and degree of uncertainty

The nature and degree of uncertainty requires an understanding of the quality, quantity and integrity of information available concerning the risk under consideration. This includes the extent to which sufficient information about the risk, its sources and causes, and its consequences to the achievement of objectives is available. Uncertainty can stem from poor data quality or the lack of essential and reliable data. To illustrate, data collection methods may change, the way organizations use such methods may change or the organization may not have an effective collection method in place at all, for collecting data about the identified risk.

Uncertainty can also be inherent in the external and internal context of the organization. Available data do not always provide a reliable basis for the prediction of the future. For unique types of risks, historical data may not be available or there may be different interpretations of available data by different stakeholders. Those undertaking risk assessment need to understand the type and nature of the uncertainty and appreciate the implications for the reliability of the risk assessment results. These should always be communicated to decision-makers.

6.5 Complexity

Risks can be complex in themselves, as, for example, in complex systems which need to have their risks assessed across the system rather than treating each component separately and ignoring interactions. In other cases, treating a single risk can have implications elsewhere and can impact on other activities. Consequential impacts and risk dependencies need to be understood to ensure that in managing one risk, an intolerable situation is not created elsewhere. Understanding the complexity of a single risk or of a portfolio of risks of an organization is crucial for the selection of the appropriate method or techniques for risk assessment.

6.6 Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycle phases have different needs and require different techniques For example during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available, risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of risks.

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable,
- the design refinement process,
- cost effectiveness studies,

- identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

6.7 Types of risk assessment techniques

Risk assessment techniques can be classified in various ways to assist with understanding their relative strengths and weaknesses. The tables in Annex A correlate some potential techniques and their categories for illustrative purposes.

Each of the techniques is further elaborated upon in Annex B as to the nature of the assessment they provide and guidance to their applicability for certain situations.

Annex A
(informative)
Comparison of risk assessment techniques

A.1 Types of technique

The first classification shows how the techniques apply to each step of the risk assessment process as follows:
- risk identification;
- risk analysis – consequence analysis;
- risk analysis – qualitative, semi-quantitative or quantitative probability estimation;
- risk analysis – assessing the effectiveness of any existing controls;
- risk analysis – estimation the level of risk;
- risk evaluation.

For each step in the risk assessment process, the application of the method is described as being either strongly applicable, applicable or not applicable (see Table A.1).

A.2 Factors influencing selection of risk assessment techniques

Next the attributes of the methods are described in terms of
- complexity of the problem and the methods needed to analyse it,
- the nature and degree of uncertainty of the risk assessment based on the amount of information available and what is required to satisfy objectives,
- the extent of resources required in terms of time and level of expertise, data needs or cost,
- whether the method can provide a quantitative output.

Examples of types of risk assessment methods available are listed in Table A.2 where each method is rated as high medium or low in terms of these attributes.

Table A.1 – Applicability of tools used for risk assessment

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SW IFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

1) Strongly applicable.

2) Not applicable.

3) Applicable.

Table A.2 – Attributes of a selection of risk assessment tools

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
LOOK-UP METHODS					
Check-lists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards	Low	Low	Low	No
Preliminary hazard analysis	A simple inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system	Low	High	Medium	No
SUPPORTING METHODS					
Structured Interview and brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them by a team. Brainstorming may be stimulated by prompts or by one-on-one and one-on-many	Low	Low	Low	No
Delphi technique	A means of combining expert opinions that may support the source and influence identification, probability and consequence estimation and risk evaluation. It is a collaborative technique for building consensus among experts. Involving independent analysis and voting by experts	Medium	Medium	Medium	No
SWIFT					
Structured “what-if”)	A system for prompting a team to identify risks. Normally used within a facilitated workshop. Normally linked to a risk analysis and evaluation technique	Medium	Medium	Any	No
Human reliability analysis (HRA)	Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system	Medium	Medium	Medium	Yes
SCENARIO ANALYSIS					
Root cause analysis (single loss analysis)	A single loss that has occurred is analysed in order to understand contributory causes and how the system or process can be improved to avoid such future losses. The analysis shall consider what controls were in place at the time the loss occurred and how controls might be improved	Medium	Low	Medium	No

Table A.2 – Contd.

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
Scenario analysis	Possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur. This can be done formally or informally qualitatively or quantitatively	Medium	High	Medium	No
Toxicological risk assessment	Hazards are identified and analysed and possible pathways by which a specified target might be exposed to the hazard are identified. Information on the level of exposure and the nature of harm caused by a given level of exposure are combined to give a measure of the probability that the specified harm will occur	High	High	Medium	Yes
Business impact analysis	Provides an analysis of how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be required to manage it	Medium	Medium	Medium	No
Fault tree analysis	A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources	High	High	Medium	Yes
Event tree analysis	Using inductive reasoning to translate probabilities of different initiating events into possible outcomes	Medium	Medium	Medium	Yes
Cause/ consequence analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered	High	Medium	High	Yes

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
FUNCTION ANALYSIS					
FMEA and FMECA	FMEA (Failure Mode and Effect Analysis) is a technique which identifies failure modes and mechanisms, and their effects. There are several types of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA. FMEA may be followed by a criticality analysis which defines the significance of each failure mode, qualitatively, semi-qualitatively, or quantitatively (FMECA). The criticality analysis may be based on the probability that the failure mode will result in system failure, or the level of risk associated with the failure mode, or a risk priority number	Medium	Medium	Medium	Yes
Reliability-centred maintenance	A method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment	Medium	Medium	Medium	Yes
Sneak analysis (Sneak circuit analysis)	A methodology for identifying design errors. A sneak condition is a latent hardware, software, or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel	Medium	Medium	Medium	No
HAZOP Hazard and operability studies	A general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system. The criticalities of the deviations are assessed	Medium	High	High	No
HACCP Hazard analysis and critical control points	A systematic, proactive, and preventive system for assuring product quality, reliability and safety of processes by measuring and monitoring specific characteristics which are required to be within defined limits	Medium	Medium	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
CONTROLS ASSESSMENT					
LOPA (Layers of protection analysis)	(May also be called barrier analysis). It allows controls and their effectiveness to be evaluated	Medium	Medium	Medium	Yes
Bow tie analysis	A simple diagrammatic way of describing and analysing the pathways of a risk from hazards to outcomes and reviewing controls. It can be considered to be a combination of the logic of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an event tree analysing the consequences	Medium	High	Medium	Yes
STATISTICAL METHODS					
Markov analysis	Markov analysis, sometimes called State-space analysis, is commonly used in the analysis of repairable complex systems that can exist in multiple states, including various degraded states	High	Low	High	Yes
Monte-Carlo analysis	Monte Carlo simulation is used to establish the aggregate variation in a system resulting from variations in the system, for a number of inputs, where each input has a defined distribution and the inputs are related to the output via defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be mathematically defined. The inputs can be based upon a variety of distribution types according to the nature of the uncertainty they are intended to represent. For risk assessment, triangular distributions or beta distributions are commonly used	High	Low	High	Yes
Bayesian analysis	A statistical procedure which utilizes prior distribution data to assess the probability of the result. Bayesian analysis depends upon the accuracy of the prior distribution to deduce an accurate result. Bayesian belief networks model cause-and-effect in a variety of domains by capturing probabilistic relationships of variable inputs to derive a result	High	Low	High	Yes

Annex B
(informative)
Risk assessment techniques

B.1 Brainstorming

B.1.1 Overview

Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify potential failure modes and associated hazards, risks, criteria for decisions and/or options for treatment. The term “brainstorming” is often used very loosely to mean any type of group discussion. However true brainstorming involves particular techniques to try to ensure that people's imagination is triggered by the thoughts and statements of others in the group.

Effective facilitation is very important in this technique and includes stimulation of the discussion at kick-off, periodic prompting of the group into other relevant areas and capture of the issues arising from the discussion (which is usually quite lively).

B.1.2 Use

Brainstorming can be used in conjunction with other risk assessment methods described below or may stand alone as a technique to encourage imaginative thinking at any stage of the risk management process and any stage of the life cycle of a system. It may be used for high-level discussions where issues are identified, for more detailed review or at a detailed level for particular problems.

Brainstorming places a heavy emphasis on imagination. It is therefore particularly useful when identifying risks of new technology, where there is no data or where novel solutions to problems are needed.

B.1.3 Inputs

A team of people with knowledge of the organization, system, process or application being assessed.

B.1.4 Process

Brainstorming may be formal or informal. Formal brainstorming is more structured with participants prepared in advance and the session has a defined purpose and outcome with a means of evaluating ideas put forward. Informal brainstorming is less structured and often more ad-hoc.

In a formal process:
- the facilitator prepares thinking prompts and triggers appropriate to the context prior to the session;
- objectives of the session are defined and rules explained;
- the facilitator starts off a train of thought and everyone explores ideas identifying as man y issues as possible There is no discussion at this point about whether things should or should not be in a list or what is meant by particular statements because this tends to inhibit free-flowing thought. All input is accepted and none is criticized and the group moves on quickly to allow ideas to trigger lateral thinking;

- the facilitator may set people off on a new track when one direction of thought is exhausted or discussion deviates too far. The idea however, is to collect as many diverse ideas as possible for later analysis.

B.1.5 Outputs

Outputs depend on the stage of the risk management process at which it is applied, for example at the identification stage, outputs might be a list of risks and current controls.

B.1.6 Strengths and limitations

Strengths of brainstorming include:
- it encourages imagination which helps identify new risks and novel solutions;
- it involves key stakeholders and hence aids communication overall;
- it is relatively quick and easy to set up.

Limitations include:
- participants may lack the skill and knowledge to be effective contributors;
- since it is relatively unstructured, it is difficult to demonstrate that the process has been comprehensive, e.g. that all potential risks have been identified;
- there may be particular group dynamics where some people with valuable ideas stay quiet while others dominate the discussion. This can be overcome by computer brainstorming, using a chat forum or nominal group technique. Computer brainstorming can be set up to be anonymous, thus avoiding personal and political issues which may impede free flow of ideas. In nominal group technique ideas are submitted anonymously to a moderator and are then discussed by the group.

B.2 Structured or semi-structured interviews

B.2.1 Overview

In a structured interview, individual interviewees are asked a set of prepared questions from a prompting sheet which encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective. A semi-structured interview is similar, but allows more freedom for a conversation to explore issues which arise.

B.2.2 Use

Structured and semi-structured interviews are useful where it is difficult to get people together for a brainstorming session or where free-flowing discussion in a group is not appropriate for the situation or people involved. They are most often used to identify risks or to assess effectiveness of existing controls as part of risk analysis. They may be applied at any stage of a project or process. They are a means of providing stakeholder input to risk assessment.

B.2.3 Inputs

Inputs include:
- a clear definition of the objectives of the interviews;
- a list of interviewees selected from relevant stakeholders;
- a prepared set of questions.

B.2.4 Process

A relevant question set, is created to guide the interviewer. Questions should be open-ended where possible, should be simple, in appropriate language for the interviewee and cover one issue only. Possible follow-up questions to seek clarification are also prepared.

Questions are then posed to the person being interviewed. When seeking elaboration, questions should be open-ended. Care should be taken not to “lead” the interviewee.

Responses should be considered with a degree of flexibility in order to provide the opportunity of exploring areas into which the interviewee may wish to go.

B.2.5 Outputs

The outputs are the stakeholder’s views on the issues which are the subject of the interviews.

B.2.6 Strengths and limitations

The strengths of structured interviews are as follows :
- structured interviews allow people time for considered thought about an issue;
- one-to-one communication may allow more in-depth consideration of issues;
- structured interviews enable involvement of a larger number of stakeholders than brainstorming which uses a relatively small group.

Limitations are as follows:
- it is time-consuming for the facilitator to obtain multiple opinions in this way;
- bias is tolerated and not removed through group discussion;
- the triggering of imagination which is a feature of brainstorming may not be achieved.

B.3 Delphi technique

B.3.1 Overview

The Delphi technique is a procedure to obtain a reliable consensus of opinion from a group of experts. Although the term is often now broadly used to mean any form of brainstorming, an essential feature of the Delphi technique, as originally formulated, was that experts expressed their opinions individually and anonym ously while having access to the other expert’s views as the process progresses.

B.3.2 Use

The Delphi technique can be applied at any stage of the risk management process or at any phase of a system life cycle, wherever a consensus of views of experts is needed.

B.3.3 Inputs

A set of options for which consensus is needed.

B.3.4 Process

A group of experts are questioned using a semi-structured questionnaire. The experts do not meet so their opinions are independent.

The procedure is as follows:
- formation of a team to undertake and monitor the Delphi process;
- selection of a group of experts (may be one or more panels of experts);
- development of round 1 questionnaire;

- testing the questionnaire;
- sending the questionnaire to panellists individually;
- information from the first round of responses is analysed and combined and re-circulated to panellists;
- panellists respond and the process is repeated until consensus is reached.

B.3.5 Outputs

Convergence toward consensus on the matter in hand.

B.3.6 Strengths and limitations

Strengths include:
- as views are anonymous, unpopular opinions are more likely to be expressed;
- all views have equal weight, which avoids the problem of dominating personalities;
- achieves ownership of outcomes;
- people do not need to be brought together in one place at one time.

Limitations include:
- it is labour intensive and time consuming;
- participants need to be able to express themselves clearly in writing.

B.4 Check-lists

B.4.1 Overview

Check-lists are lists of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures.

B.4.2 Use

A check-list can be used to identify hazards and risks or to assess the effectiveness of controls. They can be used at any stage of the life cycle of a product, process or system. They may be used as part of other risk assessment techniques but are most useful when applied to check that everything has been covered after a more imaginative technique that identifies new problems has been applied.

B.4.3 Inputs

Prior information and expertise on the issue, such that a relevant and preferably validated check-list can be selected or developed.

B.4.4 Process

The procedure is as follows:
- the scope of the activity is defined;
- a check-list is selected which adequately covers the scope. Check-lists need to be carefully selected for the purpose. For example a check-list of standard controls cannot be used to identify new hazards or risks;
- the person or team using the check-list steps through each element of the process or system and reviews whether items on the check-list are present.

B.4.5 Outputs

Outputs depend on the stage of the risk management process at which they are applied. For example output may be a list of controls which are inadequate or a list of risks.

B.4.6 Strengths and limitations

Strengths of check-lists include:
- they may be used by non experts;
- when well designed, they combine wide ranging expertise into an easy to use system;

they can help ensure common problems are not forgotten.

Limitations include:
- they tend to inhibit imagination in the identification of risks;
- they address the ‘known known’s’, not the ‘known unknown’s or the ‘unknown unknowns’.
- they encourage ‘tick the box’ type behaviour;
- they tend to be observation based, so miss problems that are not readily seen.

B.5 Preliminary hazard analysis (PHA)

B.5.1 Overview

PHA is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system.

B.5.2 Use

It is most commonly carried out early in the development of a project when there is little information on design details or operating procedures and can often be a precursor to further studies or to provide information for specification of the design of a system. It can also be useful when analysing existing systems for prioritizing hazards and risks for further analysis or where circumstances prevent a more extensive technique from being used.

B.5.3 Inputs

Inputs include:
- information on the system to be assessed;
- such details of the design of the system as are available and relevant.

B.5.4 Process

A list of hazards and generic hazardous situations and risks is formulated by considering characteristics such as:
- materials used or produced and their reactivity;
- equipment employed;
- operating environment;
- layout;
- interfaces among system components, etc.

Qualitative analysis of consequences of an unwanted event and their probabilities may be carried out to identify risks for further assessment.

PHA should be updated during the phases of design, construction and testing in order to detect any new hazards and make corrections, if necessary. The results obtained may be presented in different ways such as tables and trees.

B.5.5 Outputs

Outputs include:
- a list of hazards and risks;
- recommendations in the form of acceptance, recommended controls, design specification or requests for more detailed assessment.

B.5.6 Strengths and limitations

Strengths include:
- that it is able to be used when there is limited information;
- it allows risks to be considered very early in the system lifecycle.

Limitations include:
- a PHA provides only preliminary information; it is not comprehensive, neither does it provide detailed information on risks and how they can best be prevented.

B.6 HAZOP

B.6.1 Overview

HAZOP is the acronym for **HAZ**ard and **OP**erability study and, is a structured and systematic examination of a planned or existing product, process, procedure or system. It is a technique to identify risks to people, equipment, environment and/or organizational objectives. The study team is also expected, where possible, to provide a solution for treating the risk.

The HAZOP process is a qualitative technique based on use of guide words which question how the design intention or operating conditions might not be achieved at each step in the design, process, procedure or system. It is generally carried out by a multi-disciplinary team during a set of meetings.

HAZOP is similar to FMEA in that it identifies failure modes of a process, system or procedure their causes and consequences. It differs in that the team considers unwanted outcomes and deviations from intended outcomes and conditions and works back to possible causes and failure modes, whereas FMEA starts by identifying failure modes.

B.6.2 Use

The HAZOP technique was initially developed to analyse chemical process systems, but has been extended to other types of systems and complex operations. These include mechanical and electronic systems, procedures, and software systems, and even to organizational changes and to legal contract design and review.

The HAZOP process can deal with all forms of deviation from design intent due to deficiencies in the design, component(s), planned procedures and human actions.

It is widely used for software design review. When applied to safety critical instrument control and computer systems it may be known as CHAZOP (**C**ontrol **HA**zards and **OP**erability Analysis or computer hazard and operability analysis).

A HAZOP study is usually undertaken at the detail design stage, when a full diagram of the intended process is available, but while design changes are still practicable. It may however, be carried out in a phased approach with different guidewords for each stage as a design develops in detail. A HAZOP study may also be carried out during operation but required changes can be costly at that stage.

B.6.3 Inputs

Essential inputs to a HAZOP study include current information about the system, the process or procedure to be reviewed and the intention and performance specifications of the design. The inputs may include: drawings, specification sheets, flow sheets, process control and logic diagrams, layout drawings, operating and maintenance procedures, and emergency response procedures. For non-hardware related HAZOP the inputs can be any document that describes functions and elements of the system or procedure under study. For example, inputs can be organizational diagrams and role descriptions, a draft contract or even a draft procedure.

B.6.4 Process

HAZOP takes the “design” and specification of the process, procedure or system being studied and reviews each part of it to discover what deviations from the intended performance can occur, what are the potential causes and what are the likely consequences of a deviation. This is achieved by systematically examining how each part of the system, process or procedure will respond to changes in key parameters by using suitable guidewords. Guidewords can be customized to a particular system, process or procedure or generic words can be used that encompass all types of deviation. Table B.1 provides examples of commonly used guidewords for technical systems. Similar guidewords such as ‘too early’, ‘too late’, ‘too much’, ‘too little’, ‘too long’, ‘too short’, ‘wrong direction’, on ‘wrong object’, ‘wrong action’ can be used to identify human error modes.

The normal steps in a HAZOP study include:

- nomination of a person with the necessary responsibility and authority to conduct the
- HAZOP study and to ensure that any actions arising from the study are completed;
- definition of the objectives and scope of the study;
- establishing a set of key or guidewords for the study;
- defining a HAZOP study team; this team is usually m ultidisciplinary and should include design and operations personnel with appropriate technical expertise to evaluate the effects of deviations from intended or current design. It is recommended that the team include persons not directly involved in the design or the system, process or procedure under review;
- collection of the required documentation.

Within a facilitated workshop with the study team:

- splitting the system, process or procedure into smaller elements or sub-systems or sub-processes or sub-elements to make the review tangible;
- agreeing the design intent for each subsystem, sub-process or sub-element and then for each item in that subsystem or element applying the guidewords one after the other to postulate possible deviations which will have undesirable outcomes;
- where an undesirable outcome is identified, agreeing the cause and consequences in each case and suggesting how they might be treated to prevent them occurring or mitigate the consequences if they do;
- documenting the discussion and agreeing specific actions to treat the risks identified.

Table B.1 – Example of possible HAZOP guidewords

Terms	Definitions
No or not	No part of the intended result is achieved or the intended condition is absent
More (higher)	Quantitative increase in output or in the operating condition
Less(lower)	Quantitative decrease
As well as	Quantitative increase (e.g. additional material)
Part of	Quantitative decrease (e.g. only one or two components in a mixture)
Reverse /opposite	Opposite (e.g. backflow)
Other than	No part of the intention is achieved, something completely different happens (e.g. flow or wrong material)
Compatibility	Material; environment
Guide words are applied to parameters such as	
	Physical properties of a material or process Physical conditions such as temperature, speed A specified intention of a component of a system or design (e.g. information transfer) Operational aspects

B.6.5 Outputs

Minutes of the HAZOP meeting(s) with items for each review point recorded. This should include: the guide word used, the deviation(s), possible causes, actions to address the identified problems and person responsible for the action.

For any deviation that cannot be corrected, then the risk for the deviation should be assessed.

B.6.6 Strengths and limitations

A HAZOP analysis offers the following advantages:

- it provides the means to systematically and thoroughly examine a system, process or procedure;
- it involves a multidisciplinary team including those with real-life operational experience and those who may have to carry out treatment actions;
- it generates solutions and risk treatment actions;
- it is applicable to a wide range of systems, processes and procedures;
- it allows explicit consideration of the causes and consequences of human error;
- it creates a written record of the process which can be used to demonstrate due diligence.

The limitations include:

- a detailed analysis can be very time-consuming and therefore expensive;
- a detailed analysis requires a high level of documentation or system/process and procedure specification;

- it can focus on finding detailed solutions rather than on challenging fundamental assumptions (however, this can be mitigated by a phased approach);
- the discussion can be focused on detail issues of design, and not on wider or external issues;
- it is constrained by the (draft) design and design intent, and the scope and objectives given to the team;
- the process relies heavily on the expertise of the designers who may find it difficult to be sufficiently objective to seek problems in their designs.

B.6.7 Reference document

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

B.7 Hazard analysis and critical control points (HACCP)

B.7.1 Overview

Hazard analysis and critical control point (HACCP) provides a structure for identifying hazards and putting controls in place at all relevant parts of a process to protect against the hazards and to maintain the quality reliability and safety of a product. HACCP aims to ensure that risks are minimized by controls throughout the process rather than through inspection of the end product.

B.7.2 Use

HACCP was developed to ensure food quality for the NASA space program. It is now used by organizations operating anywhere within the food chain to control risks from physical, chemical or biological contaminants of food. It has also been extended for use in manufacture of pharmaceuticals and to medical devices. The principle of identifying things which can influence product quality, and defining points in a process where critical parameters can be monitored and hazards controlled, can be generalized to other technical systems.

B.7.3 Inputs

HACCP starts from a basic flow diagram or process diagram and information on hazards which might affect the quality, safety or reliability of the product or process output. Information on the hazards and their risks and ways in which they can be controlled is an input to HACCP.

B.7.4 Process

HACCP consists of the following seven principles:

- identifies hazards and preventive measures related to such hazards;
- determines the points in the process where the hazards can be controlled or eliminated (the critical control points or CCPs);
- establishes critical limits needed to control the hazards, i.e. each CCP should operate within specific parameters to ensure the hazard is controlled;
- monitors the critical limits for each CCP at defined intervals;
- establishes corrective actions if the process falls outside established limits;
- establishes verification procedures;
- implements record keeping and documentation procedures for each step.

B.7.5 Outputs

Documented records including a hazard analysis worksheet and a HACCP **plan.**

The hazard analysis worksheet lists for each step of the process:
- hazards which could be introduced, controlled or exacerbated at this step;
- whether the hazards present a significant risk (based on consideration of consequence and probability from a combination of experience, data and technical literature);
- a justification for the significance;
- possible preventative measures for each hazard;
- whether monitoring or control measures can be applied at this step (i.e. is it a CCP?).

The HACCP plan delineates the procedures to be followed to assure the control of a specific design, product, process or procedure. The plan includes a list of all CCPs and for each CCP:

- the critical limits for preventative measures;
- monitoring and continuing control activities (including what, how, and when monitoring will be carried out and by whom);
- corrective actions required if deviations from critical limits are detected;
- verification and record-keeping activities.

B.7.6 Strengths and limitations

Strengths include:

- a structured process that provides documented evidence for quality control as well as identifying and reducing risks;
- a focus on the practicalities of how and where, in a process, hazards can be prevented and risks controlled;
- better risk control throughout the process rather than relying on final product inspection;
- an ability to identify hazards introduced through human actions and how these can be controlled at the point of introduction or subsequently.

Limitations include:

- HACCP requires that hazards are identified, the risks they represent defined, and their significance understood as inputs to the process. Appropriate controls also need to be defined. These are required in order to specify critical control points and control parameters during HACCP and may need to be combined with other tools to achieve this;
- taking action when control parameters exceed defined limits may miss gradual changes in control parameters which are statistically significant and hence should be actioned.

B.7.7 Reference document

ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

B.8 Toxicity assessment

B.8.1 Overview

Environmental risk assessment is used here to cover the process followed in assessing risks to plants, animals and humans as a result of exposure to a range of environmental hazards.

Risk management refers to decision-making steps including risk evaluation and risk treatment.

The method involves analysing the hazard or source of harm and how it affects the target population, and the pathways by which the hazard can reach a susceptible target population. This information is then combined to give an estimate of the likely extent and nature of harm.

B.8.2 Use

The process is used to assess risks to plants, animals and humans as a result of exposure to hazards such as chemicals, micro-organisms or other species.

Aspects of the methodology, such as pathway analysis which explore different routes by which a target might be exposed to a source of risk, can be adapted and used across a very wide range of different risk areas, outside human health and the environment, and is useful in identifying treatments to reduce risk.

B.8.3 Inputs

The method requires good data on the nature and properties of hazards, the susceptibilities of the target population (or populations) and the way in which the two interact. This data is normally based on research which may be laboratory based or epidemiological.

B.8.4 Process

The procedure is as follows:

a) Problem formulation – this includes setting the scope of the assessment by defining the range of target populations and hazard types of interest;
b) Hazard identification – this involves identifying all possible sources of harm to the target population from hazards within the scope of the study. Hazard identification normally relies on expert knowledge and a review of literature;
c) Hazard analysis – this involves understanding the nature of the hazard and how it interacts with the target. For example, in considering human exposure to chemical effects, the hazard might include acute and chronic toxicity, the potential to damage DNA, or the potential to cause cancer or birth defects. For each hazardous effect, the magnitude of the effect (the response) is compared to the amount of hazard to which the target is exposed (the dose) and, wherever possible, the mechanism by which the effect is produced is determined. The levels at which there is No Observable Effect (NOEL) and no Observable Adverse Effect (NOAEL) are noted. These are sometimes used as criteria for acceptability of the risk.

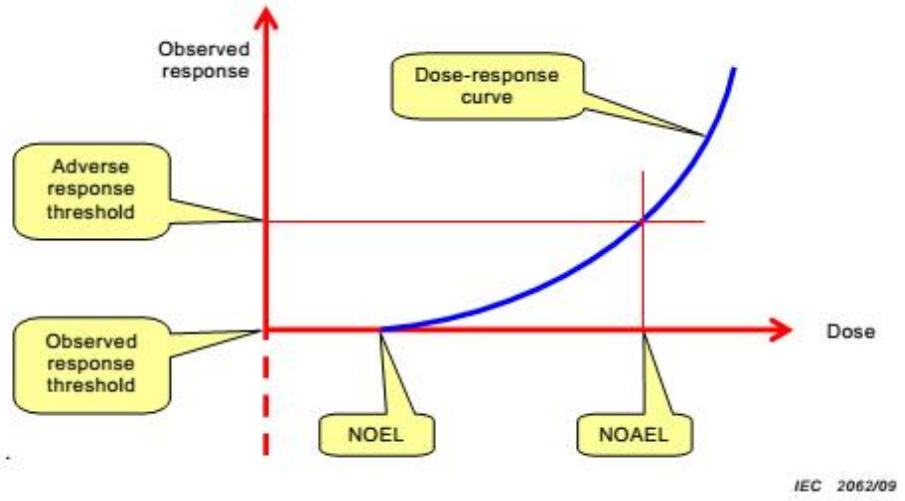


Figure B.1 – Dose-response curve

For chemical exposure, test results are used to derive dose-response curves such as that shown schematically in Figure B.1. These are usually derived from tests on animals or from experimental systems such as cultured tissues or cells.

Effects of other hazards such as micro-organisms or introduced species may be determined from field data and epidemiological studies. The nature of the interaction of diseases or pests with the target is determined and the probability that a particular level of harm from a particular exposure to the hazard is estimated.

a) Exposure analysis – this step examines how a hazardous substance or its residues might reach a susceptible target population and in what amount. It often involves a pathway analysis which considers the different routes the hazard might take, the barriers which might prevent it from reaching the target and the factors that might influence the level of exposure. For example, in considering the risk from chemical spraying the exposure analysis would consider how much chemical was sprayed, in what way and under what conditions, whether there was any direct exposure of humans or animals, how much might be left as residue on plant life, the environmental fate of pesticides reaching the ground, whether it can accumulate in animals or whether it enters groundwater. In bio security, the pathway analysis might consider how any pests entering the country might enter the environment, become established and spread.
b) Risk characterization – in this step, the information from the hazard analysis and the exposure analysis are brought together to estimate the probabilities of particular consequences when effects from all pathways are combined. Where there are large numbers of hazards or pathways, an initial screening may be carried out and the detailed hazard and exposure analysis and risk characterization carried out on the higher risk scenarios.

B.8.5 Outputs

The output is normally an indication of the level of risk from exposure of a particular target to a particular hazard in the context concerned. The risk may be expressed quantitatively semi-quantitatively or qualitatively. For example, the risk of cancer is often expressed quantitatively as the probability, that a person will develop cancer over a specified period given a specified exposure to a contaminant. Semi-quantitative analysis may be used to derive a risk index for

a particular contaminant or pest and qualitative output may be a level of risk (e.g. high, medium, low) or a description with practical data of likely effects.

B.8.6 Strengths and limitations

The strength of this analysis is that it provides a very detailed understanding of the nature of the problem and the factors which increase risk.

Pathway analysis is a useful tool, generally, for all areas of risk and permits the identification of how and where it may be possible to improve controls or introduce new ones.

It does, however, need good data which is often not available or has a high level of uncertainty associated with it. For example, dose response curves derived from exposing animals to high levels of a hazard should be extrapolated to estimate the effects of very low levels of the contaminants to humans and there are multiple models by which this is achieved. Where the target is the environment rather than humans and the hazard is not chemical, data which is directly relevant to the particular conditions of the study may be limited.

B.9 Structured “What-if” Technique (SWIFT)

B.9.1 Overview

SWIFT was originally developed as a simpler alternative to HAZOP. It is a systematic, team-based study, utilizing a set of ‘prompt’ words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks. The facilitator and team use standard ‘what-if’ type phrases in combination with the prompts to investigate how a system, plant item, organization or procedure will be affected by deviations from normal operations and behaviour. SWIFT is normally applied at more of a systems level with a lower level of detail than HAZOP.

B.9.2 Use

While SWIFT was originally designed for chemical and petrochemical plant hazard study, the technique is now widely applied to systems, plant items, procedures, organizations generally. In particular it is used to examine the consequences of changes and the risks thereby altered or created.

B.9.3 Inputs

The system, procedure, plant item and/or change has to be carefully defined before the study can commence. Both the external and internal contexts are established through interviews and through the study of documents, plans and drawings by the facilitator. Normally, the item, situation or system for study is split into nodes or key elements to facilitate the analysis process but this rarely occurs at the level of definition required for HAZOP.

Another key input is the expertise and experience present in the study team which should be carefully selected. All stakeholders should be represented if possible together with those with experience of similar items, systems, changes or situations.

B.9.4 Process

The general process is as follows:

a) Before the study commences, the facilitator prepares a suitable prompt list of words or phrases that may be based on a standard set or be created to enable a comprehensive review of hazards or risks.
b) At the workshop the external and internal context of the item, system, change or situation and the scope of the study are discussed and agreed.
c) The facilitator asks the participants to raise and discuss:
   - known risks and hazards;
   - previous experience and incidents;
   - known and existing controls and safeguards;
   - regulatory requirements and constraints.
d) Discussion is facilitated by creating a question using a 'what-if' phrase and a prompt word or subject. The 'what-if' phrases to be used are "what if…", "what would happen if…", "could someone or something…", "has anyone or anything ever…." The intent is to stimulate the study team into exploring potential scenarios, their causes and consequences and impacts.
e) Risks are summarized and the team considers controls in place.
f) The description of the risk, its causes, consequences and expected controls are confirmed with the team and recorded.
g) The team considers whether the controls are adequate and effective and agree a statement of risk control effectiveness. If this is less than satisfactory, the team further considers risk treatment tasks and potential controls are defined.
h) During this discussion further 'what-if' questions are posed to identify further risks.
i) The facilitator uses the prompt list to monitor the discussion and to suggest additional issues and scenarios for the team to discuss.
j) It is normal to use a qualitative or semi-quantitative risk assessment method to rank the actions created in terms of priority. This risk assessment is normally conducted by taking into account the existing controls and their effectiveness.

B.9.5 Outputs

Outputs include a risk register with risk-ranked actions or tasks. These tasks can then become the basis for a treatment plan.

B.9.6 Strengths and limitations

Strengths of SWIFT:

- it is widely applicable to all forms of physical plant or system, situation or circumstance, organization or activity;
- it needs minimal preparation by the team;
- it is relatively rapid and the major hazards and risks quickly become apparent within the workshop session;
- the study is 'systems orientated' and allows participants to look at the system response to deviations rather than just examining the consequences of component failure;
- it can be used to identify opportunities for improvement of processes and systems and generally can be used to identify actions that lead to and enhance their probabilities of success;
- involvement in the workshop by those who are accountable for existing controls and for further risk treatment actions, reinforces their responsibility;
- it creates a risk register and risk treatment plan with little more effort;
- while often a qualitative or semi-quantitative form of risk rating is used for risk assessment and to prioritize attention on the resulting actions, SW IFT can be used to identify risks and hazards that can be taken forward into a quantitative study.

Limitations of SWIFT:
- it needs an experienced and capable facilitator to be efficient;
- careful preparation is needed so that the workshop team's time is not wasted;
- if the workshop team does not have a wide enough experience base or if the prompt system is not comprehensive, some risks or hazards may not be identified;
- the high-level application of the technique may not reveal complex, detailed or correlated causes.

B.10 Scenario analysis

B.10.1 Overview

Scenario analysis is a name given to the development of descriptive models of how the future might turn out. It can be used to identify risks by considering possible future developments and exploring their implications. Sets of scenarios reflecting (for example) 'best case', 'worst case' and 'expected case' may be used to analyse. potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analysing risk.

The power of scenario analysis is illustrated by considering major shifts over the past 50 years in technology, consumer preferences, social attitudes, etc. Scenario analysis cannot predict the probabilities of such changes but can consider consequences and help organizations develop strengths and the resilience needed to adapt to foreseeable changes.

B.10.2 Use

Scenario analysis can be used to assist in making policy decisions and planning future strategies as well as to consider existing activities. It can play a part in all three components of risk assessment. For identification and analysis, sets of scenarios reflecting (for example) best case, worst case and 'expected' case may be used to identify what might happen under particular circumstances and analyse potential consequences and their probabilities for each scenario.

Scenario analysis may be used to anticipate how both threats and opportunities might develop and may be used for all types of risk with both short and long term time frames. With short time frames and good data, likely scenarios may be extrapolated from the present. For longer time frames or with weak data, scenario analysis becomes more imaginative and may be referred to as futures analysis.

Scenario analysis may be useful where there are strong distributional differences between positive outcomes and negative outcomes in space, time and groups in the community or an organization.

B.10.3 Inputs

The prerequisite for a scenario analysis is a team of people who between them have an understanding of the nature of relevant changes (for example possible advances in technology) and imagination to think into the future without necessarily extrapolating from the past. Access to literature and data about changes already occurring is also useful.

B.10.4 Process

The structure for scenario analysis may be informal or formal.

Having established a team and relevant communication channels, and defined the context of the problem and issues to be considered, the next step is to identify the nature of changes that might occur. This will need research into the major trends and the probable timing of changes in trends as well as imaginative thinking about the future.

Changes to be considered may include:

- external changes (such as technological changes);
- decisions that need to be made in the near future but which may have a variety of outcomes;
- stakeholder needs and how they might change;
- changes in the macro environment (regulatory, demographics, etc). Some will be inevitable and some will be uncertain.

Sometimes, a change may be due to the consequences of another risk. For example, the risk of climate change is resulting in changes in consumer demand related to food miles. This will influence which foods can be profitably exported as well as which foods can be grown locally. The local and macro factors or trends can now be listed and ranked for (1) importance (2) uncertainty. Special attention is paid to the factors that are most important and most uncertain. Key factors or trends are mapped against each other to show areas where scenarios can be developed.

A series of scenarios is proposed with each one focussing on a plausible change in parameters.

A “story” is then written for each scenario that tells how you might move from here towards the subject scenario. The stories may include plausible details that add value to the scenarios.

The scenarios can then be used to test or evaluate the original question. The test takes into account any significant but predictable factors (e.g. use patterns), and then explores how ‘successful’ the policy (activity) would be in this new scenario, and ‘pre-tests’ outcomes by using ‘what if’ questions based on model assumptions.

When the question or proposal has been evaluated with respect to each scenario, it may be obvious that it needs to be modified to make it more robust or less risky. It should also be possible to identify some leading indicators that show when change is occurring. Monitoring and responding to leading indicators can provide opportunity for change in planned strategies.

Since scenarios are only defined ‘slices’ of possible futures, it is important to make sure that account is taken of the probability of a particular outcome (scenario) occurring, i.e. to adopt a risk framework. For example, where best case, worst case and expected case scenarios are used, some attempt should be made to qualify, or express the probability of each scenario occurring.

B.10.5 Outputs

There may be no best-fit scenario but one should end with a clearer perception of the range of options and how to modify the chosen course of action as indicators move.

B.10.6 Strengths and limitations

Scenario analysis takes account of a range of possible futures which may be preferable to the traditional approach of relying on high-medium-low forecasts that assume, through the use of historical data, that future events will probably continue to follow past trends. This is important for situations where there is little current knowledge on which to base predictions or where risks are being considered in the longer term future.

This strength however has an associated weakness which is that where there is high uncertainty some of the scenarios may be unrealistic.

The main difficulties in using scenario analysis are associated with the availability of data, and the ability of the analysts and decision makers to be able to develop realistic scenarios that are amenable to probing of possible outcomes.

The dangers of using scenario analysis as a decision-making tool are that the scenarios used may not have an adequate foundation; that data may be speculative; and that unrealistic results may not be recognized as such.

B.11 Business impact analysis (BIA)

B.11.1 Overview

Business impact analysis, also known as business impact assessment, analyses how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of:

the identification and criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organization;

how disruptive events will affect the capacity and capability of achieving critical business objectives;

the capacity and capability needed to manage the impact of a disruption and recover the organization to agreed levels of operation.

B.11.2 Use

BIA is used to determine the criticality and recovery timeframes of processes and associated resources (people, equipment, information technology) to ensure the continued achievement of objectives. Additionally, the BIA assists in determining interdependencies and interrelationships between processes, internal and external parties and any supply chain linkages.

B.11.3 Inputs

Inputs include:

- a team to undertake the analysis and develop a plan;
- information concerning the objectives, environment, operations and interdependencies of the organization;
- details on the activities and operations of the organization, including processes, supporting resources, relationships with other organizations, outsourced arrangements, stakeholders;
- financial and operational consequences of loss of critical processes;

- prepared questionnaire;
- list of interviewees from relevant areas of the organization and/or stakeholders that will be contacted.

B.11.4 Process

A BIA can be undertaken using questionnaires, interviews, structured workshops or combinations of all three, to obtain an understanding of the critical processes, the effects of the loss of those processes and the required recovery timeframes and supporting resources.

The key steps include:
- based on the risk and vulnerability assessment, confirmation of the key processes and outputs of the organization to determine the criticality of the processes;
- determination of the consequences of a disruption on the identified critical processes in financial and/or operational terms, over defined periods;
- identification of the interdependencies with key internal and external stakeholders. This could include mapping the nature of the interdependencies through the supply chain;
- determination of the current available resources and the essential level of resources needed to continue to operate at a minimum acceptable level following a disruption;
- identification of alternate workarounds and processes currently in use or planned to be developed. Alternate workarounds and processes may need to be developed where resources or capability are inaccessible or insufficient during the disruption;
- determination of the maximum acceptable outage time (MAO) for each process based on the identified consequences and the critical success factors for the
- function. The MAO represents the maximum period of time the organization can tolerate the loss of capability;
- determination of the recovery time objective(s) (RTO) for any specialized equipment or information technology. The RTO represents the time within which the organization aims to recover the specialized equipment or information technology capability;
- confirmation of the current level of preparedness of the critical processes to manage a disruption. This may include evaluating the level of redundancy within the process (e.g. spare equipment) or the existence of alternate suppliers.

B.11.5 Outputs

The outputs are as follows:

- a priority list of critical processes and associated interdependencies;

- documented financial and operational impacts from a loss of the critical processes;

- supporting resources needed for the identified critical processes;

- outage time frames for the critical process and the associated information technology recovery time frames.

B.11.6 Strengths and limitations

Strengths of the BIA include:

- an understanding of the critical processes that provide the organization with the ability to continue to achieve their stated objectives;
- an understanding of the required resources;

- an opportunity to redefine the operational process of an organization to assist in the resilience of the organization.

Limitations include:

- lack of knowledge by the participants involved in completing questionnaires, undertaking interviews or workshops;
- group dynamics may affect the complete analysis of a critical process;
- simplistic or over-optimistic expectations of recovery requirements;
- difficulty in obtaining an adequate level of understanding of the organization's operations and activities.

B.12 Root cause analysis (RCA)

B.12.1 Overview

The analysis of a major loss to prevent its reoccurrence is commonly referred to as Root Cause Analysis (RCA), Root Cause Failure Analysis (RCFA) or loss analysis. RCA is focused on asset losses due to various types of failures while loss analysis is mainly concerned with financial or economic losses due to external factors or catastrophes. It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. It is recognized that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyse losses on a more global basis to determine where improvements can be made.

B.12.2 Use

RCA is applied in various contexts with the following broad areas of usage:

- safety-based RCA is used for accident investigations and occupational health and safety;
- failure analysis is used in technological systems related to reliability and maintenance;
- production-based RCA is applied in the field of quality control for industrial manufacturing;
- process-based RCA is focused on business processes;
- system-based RCA has developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

B.12.3 Inputs

The basic input to an RCA is all of the evidence gathered from the failure or loss. Data from other similar failures may also be considered in the analysis. Other inputs may be results that are carried out to test specific hypotheses.

B.12.4 Process

When the need for an RCA is identified, a group of experts is appointed to carry out the analysis and make recommendations. The type of expert will mostly be dependent on the specific expertise needed to analyse the failure.

Even though different methods can be used to perform the analysis, the basic steps in executing an RCA are similar and include:

- forming the team;
- establishing the scope and objectives of the RCA;

- gathering data and evidence from the failure or loss;
- performing a structured analysis to determine the root cause;
- developing solutions and make recommendations;
- implementing the recommendations;
- verifying the success of the implemented recommendations.

Structured analysis techniques may consist of one of the following:
- “5 whys” technique, i.e. repeatedly asking ‘why?’ to peel away layers of cause and sub cause);
- failure mode and effects analysis;
- fault tree analysis;
- Fishbone or Ishikawa diagrams;
- Pareto analysis;
- root cause mapping.

The evaluation of causes often progresses from initially evident physical causes to human-related causes and finally to underlying management or fundamental causes. Causal factors have to be able to be controlled or eliminated by involved parties in order for corrective action to be effective and worthwhile.

B.12.5 Outputs

The outputs from an RCA include:
- documentation of data and evidence gathered;
- hypotheses considered;
- conclusion about the most likely root causes for the failure or loss;
- recommendations for corrective action.

B.12.6 Strengths and limitations

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- documentation of results;
- need to produce final recommendations.

Limitations of an RCA:
- required experts may not be available;
- critical evidence may be destroyed in the failure or removed during clean-up;
- the team may not be allowed enough time or resources to fully evaluate the situation;
- it may not be possible to adequately implement recommendations.

B.13 Failure modes and effects analysis (FMEA) and failure modes and effects and criticality analysis (FMECA)

B.13.1 Overview

Failure modes and effects analysis (FMEA) is a technique used to identify the ways in which components, systems or processes can fail to fulfil their design intent.

FMEA identifies:

- all potential failure modes of the various parts of a system (a failure mode is what is observed to fail or to perform incorrectly);
- the effects these failures may have on the system;
- the mechanisms of failure;
- how to avoid the failures, and/or mitigate the effects of the failures on the system.

FMECA extends an FMEA so that each fault mode identified is ranked according to its importance or criticality.

This criticality analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.

B.13.2 Use

There are several applications of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA.

FMEA/FMECA may be applied during the design, manufacture or operation of a physical system.

To improve dependability, however, changes are usually more easily implemented at the design stage. FMEA AND FMECA may also be applied to processes and procedures. For example, it is used to identify potential for medical error in healthcare systems and failures in maintenance procedures.

FMEA/FMECA can be used to

- assist in selecting design alternatives with high dependability,
- ensure that all failure modes of systems and processes, and their effects on operational success have been considered,
- identify human error modes and effects,
- provide a basis for planning testing and maintenance of physical systems,
- improve the design of procedures and processes,
- provide qualitative or quantitative information for analysis techniques such as fault tree analysis.

FMEA and FMECA can provide input to other analyses techniques such as fault tree analysis at either a qualitative or quantitative level.

B.13.3 Inputs

FMEA and FMECA need information about the elements of the system in sufficient detail for meaningful analysis of the ways in which each element can fail. For a detailed Design FMEA the element may be at the detailed individual component level, while for higher level Systems FMEA, elements may be defined at a higher level.

Information may include:

- drawings or a flow chart of the system being analysed and its components, or the steps of a process;
- an understanding of the function of each step of a process or component of a system;
- details of environmental and other parameters, which may affect operation;
- an understanding of the results of particular failures;
- historical information on failures including failure rate data where available.

B.13.4 Process

The FMEA process is as follows:

a) define the scope and objectives of the study;
b) assemble the team;
c) understand the system/process to be subjected to the FMECA;
d) breakdown of the system into its components or steps;
e) define the function of each step or component;
f) for every component or step listed identify:
   - how can each part conceivably fail?
   - what mechanisms might produce these modes of failure?
   - what could the effects be if the failures did occur?
   - is the failure harmless or damaging?
   - how is the failure detected?
g) identify inherent provisions in the design to compensate for the failure.

For FMECA, the study team goes on to classify each of the identified failure modes according to its criticality

There are several ways this may be done. Common methods include

- the mode criticality index,
- the level of risk,
- the risk priority number.

The model criticality is a measure of the probability that the mode being considered will result in failure of the system as a whole; it is defined as:

Failure effect probability * Mode failure rate * Operating time of the system

It is most often applied to equipment failures where each of these terms can be defined quantitatively and failure modes all have the same consequence.

The risk level is obtained by combining the consequences of a failure mode occurring with the probability of failure. It is used when consequences of different failure modes differ and can be applied to equipment systems or processes. Risk level can be expressed qualitatively, semi-quantitatively or quantitatively.

The risk priority number (RPN) is a semi-quantitative measure of criticality obtained by multiplying numbers from rating scales (usually between 1 and 10) for consequence of failure, likelihood of failure and ability to detect the problem. (A failure is given a higher priority if it is difficult to detect.) This method is used most often in quality assurance applications.

Once failure modes and mechanisms are identified, corrective actions can be defined and implemented for the more significant failure modes.

FMEA is documented in a report that contains:

- details of the system that was analysed;
- the way the exercise was carried out;
- assumptions made in the analysis;
- sources of data;

- the results, including the completed worksheets;
- the criticality (if completed) and the methodology used to define it;
- any recommendations for further analyses, design changes or features to be incorporated in test plans, etc.

The system may be reassessed by another cycle of FMEA after the actions have been completed.

B.13.5 Outputs

The primary output of FMEA is a list of failure modes, the failure mechanisms and effects for each component or step of a system or process (which may include information on the likelihood of failure). Information is also given on the causes of failure and the consequences to the system as a whole. The output from FMECA includes a rating of importance based on the likelihood that the system will fail, the level of risk resulting from the failure mode or a combination of the level of risk and the 'detectability' of the failure mode.

FMECA can give a quantitative output if suitable failure rate data and quantitative consequences are used.

B.13.6 Strengths and limitations

The strengths of FMEA/FMECA are as follows:

- widely applicable to human, equipment and system failure modes and to hardware, software and procedures;
- identify component failure modes, their causes and their effects on the system, and present them in an easily readable format;
- avoid the need for costly equipment modifications in service by identifying problems early in the design process;
- identify single point failure modes and requirements for redundancy or safety systems;
- provide input to the development monitoring programmes by highlighting key features to be monitored.

Limitations include:

- they can only be used to identify single failure modes, not combinations of failure modes;
- unless adequately controlled and focussed, the studies can be time consuming and costly;
- they can be difficult and tedious for complex multi-layered systems.

B.13.7 Reference document

IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)*

B.14 Fault tree analysis (FTA)

B.14.1 Overview

FTA is a technique for identifying and analysing factors that can contribute to a specified undesired event (called the "top event"). Causal factors are deductively identified, organized in a logical manner and represented pictorially in a tree diagram which depicts causal factors and their logical relationship to the top event.

The factors identified in the tree can be events that are associated with component hardware failures, human errors or any other pertinent events which lead to the undesired event.

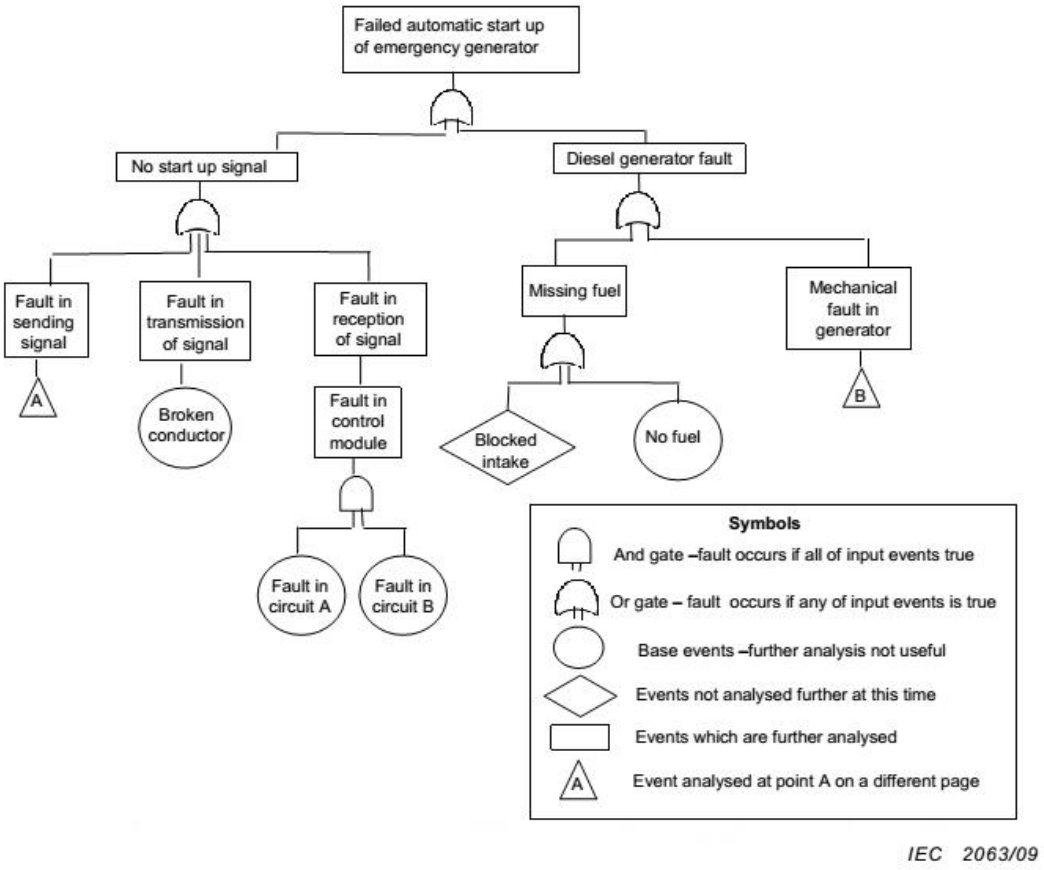


Figure B.2 – Example of an FTA from IEC 60300-3-9

B.14.2 Use

A fault tree may be used qualitatively to identify potential causes and pathways to a failure (the top event) or quantitatively to calculate the probability of the top event, given knowledge of the probabilities of causal events.

It may be used at the design stage of a system to identify potential causes of failure and hence to select between different design options. It may be used at the operating phase to identify how major failures can occur and the relative importance of different pathways to the head event. A fault tree may also be used to analyse a failure which has occurred to display diagrammatically how different events came together to cause the failure.

B.14.3 Inputs

For qualitative analysis, an understanding of the system and the causes of failure is required, as well as a technical understanding of how the system can fail. Detailed diagrams are useful to aid the analysis.

For quantitative analysis, data on failure rates or the probability of being in a failed state for all basic events in the fault tree are required.

B.14.4 Process

The steps for developing a fault tree are as follows:

- The top event to be analysed is defined. This may be a failure or maybe a broader outcome of that failure. Where the outcome is analysed, the tree may contain a section relating to mitigation of the actual failure.
- Starting with the top event, the possible immediate causes or failure modes leading to the top event are identified.
- Each of these causes/fault modes is analysed to identify how their failure could be caused.
- Stepwise identification of undesirable system operation is followed to successively lower system levels until further analysis becomes unproductive. In a hardware system this may be the component failure level. Events and causal factors at the lowest system level analysed are known as base events.
- Where probabilities can be assigned to base events the probability of the top event may be calculated. For quantification to be valid it must be able to be shown that, for each gate, all inputs are both necessary and sufficient to produce the output event. If this is not the case, the fault tree is not valid for probability analysis but may be a useful tool for displaying causal relationships.

As part of quantification the fault tree may need to be simplified using Boolean algebra to account for duplicate failure modes.

As well as providing an estimate of the probability of the head event, minimal cut sets, which form individual separate pathways to the head event, can be identified and their influence on the top event calculated.

Except for simple fault trees, a software package is needed to properly handle the calculations when repeated events are present at several places in the fault tree, and to calculate minimal cut sets. Software tools help ensure consistency, correctness and verifiability.

B.14.5 Outputs

The outputs from fault tree analysis are as follows:
- a pictorial representation of how the top event can occur which shows interacting pathways where two or more simultaneous events must occur;
- a list of minimal cut sets (individual pathways to failure) with (where data is available)
- the probability that each will occur;
- the probability of the top event.

B.14.6 Strengths and limitations

Strengths of FTA:
- It affords a disciplined approach which is highly systematic, but at the same time sufficiently flexible to allow analysis of a variety of factors, including human interactions and physical phenomena.
- The application of the "top-down" approach, implicit in the technique, focuses attention on those effects of failure which are directly related to the top event.
- FTA is especially useful for analysing systems with many interfaces and interactions.
- The pictorial representation leads to an easy understanding of the system behaviour and the factors included, but as the trees are often large, processing of fault trees may require

computer systems. This feature enables more complex logical relationships to be included (e.g. NAND and NOR) but also makes the verification of the fault tree difficult.
- Logic analysis of the fault trees and the identification of cut sets is useful in identifying simple failure pathways in a very complex system where particular combinations of events which lead to the top event could be overlooked.

Limitations include:
- Uncertainties in the probabilities of base events are included in calculations of the probability of the top event. This can result in high levels of uncertainty where base event failure probabilities are not known accurately; however, a high degree of confidence is possible in a well understood system.
- In some situations, causal events are not bound together and it can be difficult to ascertain whether all important pathways to the top event are included. For example, including all ignition sources in an analysis of a fire as a top event. In this situation probability analysis is not possible.
- Fault tree is a static model; time interdependencies are not addressed.
- Fault trees can only deal with binary states (failed/not failed) only.
- While human error modes can be included in a qualitative fault tree, in general failures of degree or quality which often characterize human error cannot easily be included;
- A fault tree does not enable domino effects or conditional failures to be included easily.

B.14.7 Reference document

IEC 61025*, Fault tree analysis (FTA)*

IEC 60300-3-9, *Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems*

B.15 Event tree analysis (ETA)

B.15.1 Overview

ETA is a graphical technique for representing the mutually exclusive sequences of events following an initiating event according to the functioning/not functioning of the various systems designed to mitigate its consequences (see Figure B.3). It can be applied both qualitatively and quantitatively.

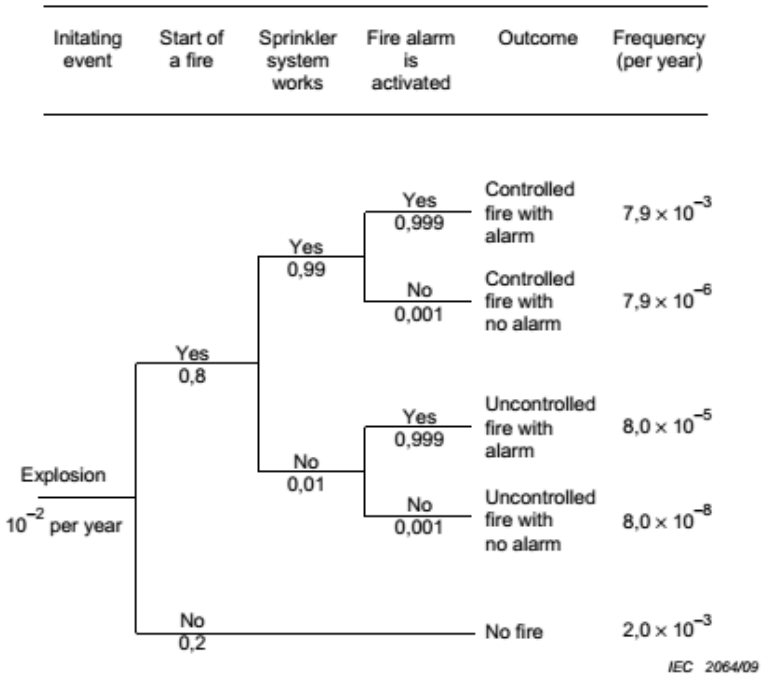


Figure B.3 – Example of an event tree

Figure B.3 shows simple calculations for a sample event tree, when branches are fully independent.

By fanning out like a tree, ETA is able to represent the aggravating or mitigating events in response to the initiating event, taking into account additional systems, functions or barriers.

B.15.2 Use

ETA can be used for modelling, calculating and ranking (from a risk point of view) different accident scenarios following the initiating event ETA can be used at any stage in the life cycle of a product or process. It may be used qualitatively to help brainstorm potential scenarios and sequences of events following an initiating event and how outcomes are affected by various treatments, barriers or controls intended to mitigate unwanted outcomes.

The quantitative analysis lends itself to consider the acceptability of controls. It is most often used to model failures where there are multiple safeguards.

ETA can be used to model initiating events which might bring loss or gain. However, circumstances where pathways to optimize gain are sought are more often modelled using a decision tree.

B.15.3 Inputs

Inputs include:
- a list of appropriate initiating events;
- information on treatments, barriers and controls, and their failure probabilities (for quantitative analyses);
- understanding of the processes whereby an initial failure escalates.

B.15.4 Process

An event tree starts by selecting an initiating event. This may be an incident such as a dust explosion or a causal event such as a power failure. Functions or systems which are in place to mitigate outcomes are then listed in sequence. For each function or system, a line is drawn to represent their success or failure. A particular probability of failure can be assigned to each line, with this conditional probability estimated e.g. by expert judgement or a fault tree analysis. In this way, different pathways from the initiating event are modelled.

Note that the probabilities on the event tree are conditional probabilities, for example the probability of a sprinkler functioning is not the probability obtained from tests under normal conditions, but the probability of functioning under conditions of fire caused by an explosion.

Each path through the tree represents the probability that all of the events in that path will occur. Therefore, the frequency of the outcome is represented by the product. of the individual conditional probabilities and the frequency of the initiation event, given that the various events are independent.

B.15.5 Outputs

Outputs from ETA include the following:
- qualitative descriptions of potential problems as combinations of events producing various types of problems (range of outcomes) from initiating events;
- quantitative estimates of event frequencies or probabilities and relative importance of various failure sequences and contributing events;
- lists of recommendations for reducing risks;
- quantitative evaluations of recommendation effectiveness.

B.15.6 Strengths and limitations

Strengths of ETA include the following:
- ETA displays potential scenarios following an initiating event, are analysed and the influence of the success or failure of mitigating systems or functions in a clear diagrammatic way;
- it accounts for timing, dependence and domino effects that are cumbersome to model in fault trees;
- it graphically represent sequences of events which are not possible to represent when using fault trees.

Limitations include:
- in order to use ETA as part of a comprehensive assessment, all potential initiating events need to be identified. This may be done by using another analysis method (e.g. HAZOP, PHA), however, there is always a potential for missing some important initiating events;
- with event trees, only success and failure states of a system are dealt with, and it is difficult to incorporate delayed success or recovery events;
- any path is conditional on the events that occurred at previous branch points along the path. Many dependencies along the possible paths are therefore addressed. However, some dependencies, such as common components, utility systems and operators, may be overlooked if not handled carefully, may lead to optimistic estimations of risk.

B.16 Cause-consequence analysis

B.16.1 General

Cause-consequence analysis is a combination of fault tree and event tree analysis. It starts from a critical event and analyses consequences by means of a combination of YES/NO logic gates which represent conditions that may occur or failures of systems designed to mitigate the consequences of the initiating event. The causes of the conditions or failures are analysed by means of fault trees (see Clause B.15)

B.16.2 Use

Cause-consequence analysis was originally developed as a reliability tool for safety critical systems to give a more complete understanding of system failures. Like fault tree analysis, it is used to represent the failure logic leading to a critical event but it adds to the functionality of a fault tree by allowing time sequential failures to be analysed. The method also allows time delays to be incorporated into the consequence analysis which is not possible with event trees.

The method is used to analyse the various paths a system could take following a critical event and depending on the behaviour of particular subsystems (such as emergency response systems). If quantified they will give an estimate of the probability of different possible consequences following a critical event.

As each sequence in a cause-consequence diagram is a combination of sub-fault trees, the cause-consequence analysis can be used as a tool to build big fault trees.

Diagrams are complex to produce and use and tend to be used when the magnitude of the potential consequence of failure justifies intensive effort.

B.16.3 Inputs

An understanding of the system and its failure modes and failure scenarios is required.

B.16.4 Process

Figure B.4 shows a conceptual diagram of a typical cause-consequence analysis.

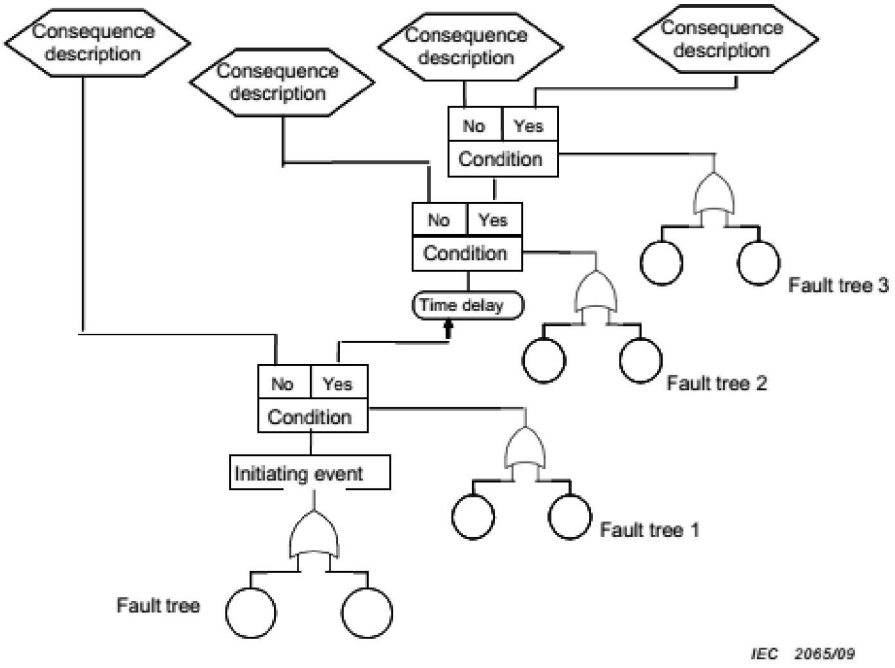


Figure B.4 – Example of cause-consequence analysis

The procedure is as follows:

a) Identify the critical (or initiating) event (equivalent to the top event of a fault tree and the initiating event of an event tree).
b) Develop and validate the fault tree for causes of the initiating event as described in clause B.14. The same symbols are used as in conventional fault tree analysis.
c) Decide the order in which conditions are to be considered. This should be a logical sequence such as the time sequence in which they occur.
d) Construct the pathways for consequences depending on the different conditions. This is similar to an event tree but the split in pathways of the event tree is shown as a box labelled with the particular condition that applies.
e) Provided the failures for each condition box are independent, the probability of each consequence can be calculated. This is achieved by first assigning probabilities to each output of the condition box (using the relevant fault trees as appropriate) The probability of any one sequence leading to a particular consequence is obtained by multiplying the probabilities of each sequence of conditions which terminates in that particular consequence. If more than one sequence ends up with the same consequence, the probabilities from each sequence are added. If there are dependencies between failures of conditions in a sequence (for example a power failure may cause several conditions to fail) then the dependencies should be dealt with prior to calculation.

B.16.5 Output

The output of cause-consequence analysis is a diagrammatic representation of how a system may fail showing both causes and consequences. An estimation of the probability of occurrence of each potential consequence based on analysis of probabilities of occurrence of particular conditions following the critical event.

B.16.6 Strengths and limitations

The advantages of cause-consequence analysis are the same as those of event trees and fault trees combined. In addition, it overcomes some of the limitations of those techniques by being able to analyse events that develop over time. Cause-consequence analysis provides a comprehensive view of the system.

Limitations are that it is more complex than fault tree and event tree analysis, both to construct and in the manner in which dependencies are dealt with during quantification.

B.17 Cause-and-effect analysis

B.17.1 Overview

Cause-and-effect analysis is a structured method to identify possible causes of an undesirable event or problem. It organizes the possible contributory factors into broad categories so that all possible hypotheses can be considered. It does not, however, by itself point to the actual causes, since these can only be determined by real evidence and empirical testing of hypotheses. The information is organized in either a Fishbone (also called Ishikawa) or sometimes a tree diagram (see B.17.4).

B.17.2 Use

Cause-and-effect analysis provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.

It is used to enable consideration of all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes which can then be tested empirically or by evaluation of available data. It is most valuable at the beginning of an analysis to broaden thinking about possible causes and then to establish potential hypotheses that can be considered more formally.

Constructing a cause-and-effect diagram can be undertaken when there is need to:

- identify the possible root causes, the basic reasons, for a specific effect, problem or condition;
- sort out and relate some of the interactions among the factors affecting a particular process;
- analyse existing problems so that corrective action can be taken.

Benefits from constructing a cause-and-effect diagram include:

- concentrates review members' attention on a specific problem;
- to help determine the root causes of a problem using a structured approach;
- encourages group participation and utilizes group knowledge for the product or process;
- uses an orderly, easy-to-read format to diagram cause-and-effect relationships;
- indicates possible causes of variation in a process;
- identifies areas where data should be collected for further study.

Cause-and-effect analysis can be used as a method in performing root cause analysis (see Clause B.12).

B.17.3 Input

The input to a cause-and-effect analysis may come from expertise and experience from participants or a previously developed model that has been used in the past.

B.17.4 Process

The cause-and-effect analysis should be carried out by a team of experts knowledgeable with the problem requiring resolution.

The basic steps in performing a cause-and-effect analysis are as follows:

- establish the effect to be analysed and place it in a box. The effect may be positive (an objective) or negative (a problem) depending on the circumstances;
- determine the main categories of causes represented by boxes in the Fishbone diagram. Typically, for a system problem, the categories might be people, equipment, environment, processes, etc. However, these are chosen to fit the particular context;
- fill in the possible causes for each major category with branches and sub-branches to describe the relationship between them;
- keep asking “why?” or “what caused that?” to connect the causes;
- review all branches to verify consistency and completeness and ensure that the causes apply to the main effect;
- identify the most likely causes based on the opinion of the team and available evidence.

The results are normally displayed as either a Fishbone or Ishikawa diagram or tree diagram. The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone) with branches and sub-branches that describe more specific causes in those categories.

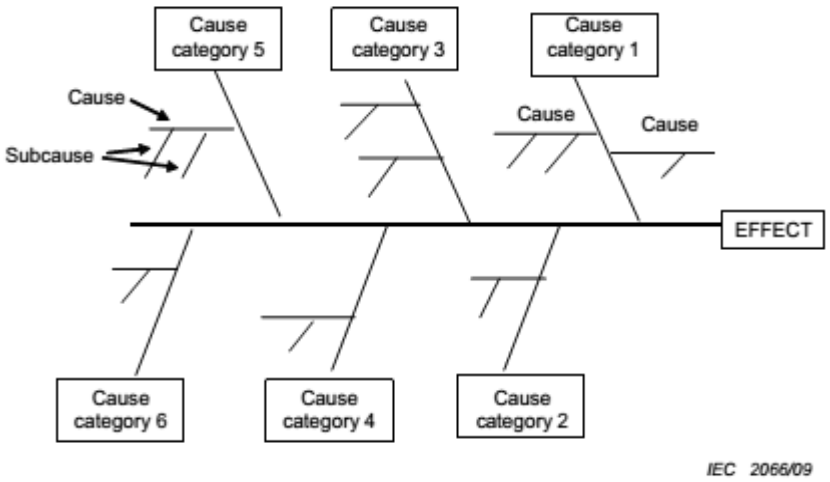


Figure B.5 – Example of Ishikawa or Fishbone diagram

The tree representation is similar to a fault tree in appearance, although it is often displayed with the tree developing from left to right rather than down the page. However, it cannot be quantified to produce a probability of the head event as the causes are possible contributory factors rather than failures with a known probability of occurrence.

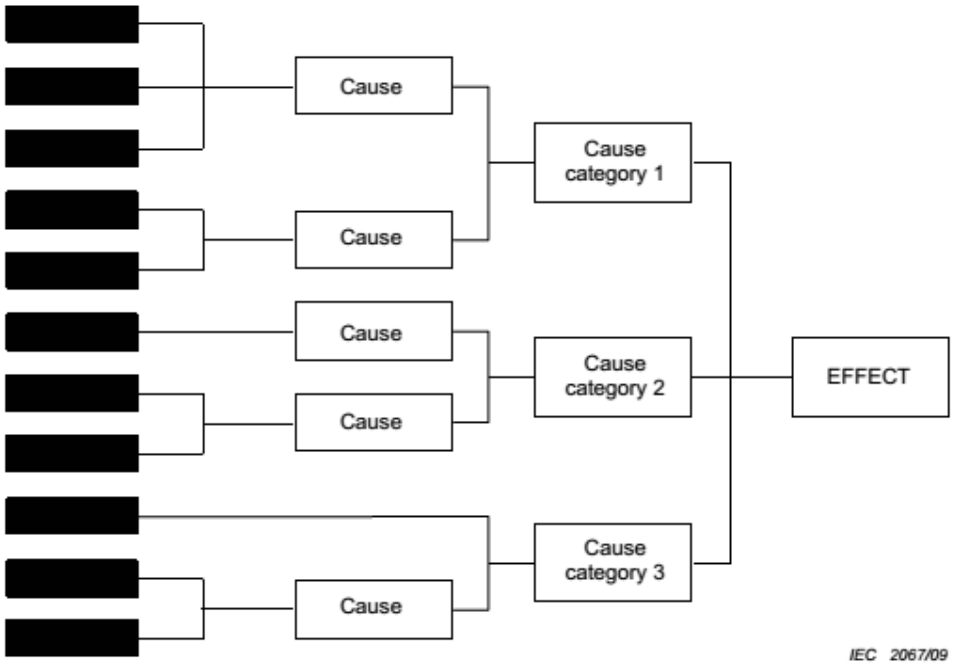


Figure B.6 – Example of tree formulation of cause-and-effect analysis

Cause-and-effect diagrams are generally used qualitatively. It is possible to assume the probability of the problem is 1 and assign probabilities to generic causes, and subsequently to the sub-causes, on the basis of the degree of belief about their relevance. However, contributory factors often interact and contribute to the effect in complex ways which make quantification invalid.

B.17.5 Output

The output from a cause-and-effect analysis is a Fishbone or tree diagram that shows the possible and likely causes. This has then to be verified and tested empirically before recommendations can be made.

B.17.6 Strengths and limitations

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- graphical easy-to-read illustration of results;
- areas identified where further data is needed;
- can be used to identify contributory factors to wanted as well as unwanted effects. Taking a positive focus on an issue can encourage greater ownership and participation.

Limitations include:

- the team may not have the necessary expertise;
- it is not a complete process in itself and needs to be a part of a root cause analysis to produce recommendations;
- it is a display technique for brainstorming rather than a separate analysis technique;

- the separation of causal factors into major categories at the start of the analysis means that interactions between the categories may not be considered adequately, e.g. where equipment failure is caused by human error, or human problems are caused by poor design.

B.18 Layers of protection analysis (LOPA)

B.18.1 Overview

LOPA is a semi-quantitative method for estimating the risks associated with an undesired event or scenario. It analyses whether there are sufficient measures to control or mitigate the risk.

A cause-consequence pair is selected and the layers of protection which prevent the cause leading to the undesired consequence are identified. An order of magnitude calculation is carried out to determine whether the protection is adequate to reduce risk to a tolerable level.

B.18.2 Uses

LOPA may be used qualitatively simply to review the layers of protection between a hazard or causal event and an outcome. Normally a semi-quantitative approach would be applied to add more rigour to screening processes for example following HAZOP or PHA.

LOPA provides a basis for the specification of independent protection layers (IPLs) and safety integrity levels (SIL levels) for instrumented systems, as described in the IEC 61508 series and in IEC 61511, in the determination of safety integrity level (SIL) requirements for safety instrumented systems. LOPA can be used to help allocate risk reduction resources effectively by analysing the risk reduction produced by each layer of protection.

B.18.3 Inputs

Inputs to LOPA include

- basic information on risks including hazards, causes and consequences such as provided by a PHA;
- information on controls in place or proposed;
- causal event frequencies, and protection layer failure probabilities, measures of consequence and a definition of tolerable risk;
- initiating cause frequencies, protection layer failure probabilities, measures of consequence and a definition of tolerable risk.

B.18.4 Process

LOPA is carried out using a team of experts who apply the following procedure:

- identify initiating causes for an undesired outcome and seek data on their frequencies and consequences;
- select a single cause-consequence pair;
- layers of protection which prevent the cause proceeding to the undesired consequence are identified and analysed for their effectiveness;
- identify independent protection layers (IPLs) (not all layers of protection are IPLs);
- estimate the probability of failure of each IPL;
- the frequency initiating cause is combined with the probabilities of failure of each IPL and the probabilities of any conditional modifiers (a conditional modifier is for example whether

a person will be present to be impacted) to determine the frequency of occurrence of the undesired consequence. Orders of magnitude are used for frequencies and probabilities;
- the calculated level of risk is compared with risk tolerance levels to determine whether further protection is required.

An IPL is a device system or action that is capable of preventing a scenario proceeding to its undesired consequence, independent of the causal event or any other layer of protection associated with the scenario.

IPLs include:

- design features;
- physical protection devices;
- interlocks and shutdown systems;
- critical alarms and manual intervention;
- post event physical protection;
- emergency response systems (procedures and inspections are not IPLs).

B.18.5 Output

Recommendations for any further controls and the effectiveness of these controls in reducing risk shall be given.

LOPA is one of the techniques used for SIL assessment when dealing with safety related/instrumented systems

B.18.6 Strengths and limitations

Strengths include:

- it requires less time and resources than a fault tree analysis or fully quantitative risk assessment but is more rigorous than qualitative subjective judgments;
- it helps identify and focus resources on the most critical layers of protection;
- it identifies operations, systems and processes for which there are insufficient safeguards;
- it focuses on the most serious consequences.

Limitations include:
- LOPA focuses on one cause-consequence pair and one scenario at a time. Complex interactions between risks or between controls are not covered;
- quantified risks may not account for common mode failures;
- LOPA does not apply to very complex scenarios where there are many cause-consequence pairs or where there are a variety of consequences affecting different stakeholders.

B.18.7 Reference documents

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

B.19 Decision tree analysis

B.19.1 Overview

A decision tree represents decision alternatives and outcomes in a sequential manner which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made.

B.19.2 Use

A decision tree is used in managing project risks and in other circumstances to help select the best course of action where there is uncertainty. The graphical display can also help communicate reasons for decisions.

B.19.3 Input

A project plan with decision points. Information on possible outcomes of decisions and on chance events which might affect decisions.

B.19.4 Process

A decision tree starts with an initial decision, for example to proceed with project A rather than project B. As the two hypothetical projects proceed, different events will occur and different predictable decisions will need to be made. These are represented in tree format, similar to an event tree. The probability of the events can be estimated together with the cost or utility of the final outcome of the pathway.

Information concerning the best decision pathway is logically that which produces the highest expected value calculated as the product of all the conditional probabilities along the pathway and the outcome value.

B.19.5 Outputs

Outputs include:

- a logical analysis of the risk displaying different options that may be taken
- a calculation of the expected value for each possible path

B.19.6 Strengths and limitations

Strengths include:
- they provide a clear graphical representation of the details of a decision problem;
- they enable a calculation of the best pathway through a situation.

Limitations include:
- large decisions trees may become too complex for easy communication with others;
- there may be a tendency to oversimplify the situation so as to be able to represent it as a tree diagram.

B.20 Human reliability assessment (HRA)

B.20.1 Overview

Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system.

Many processes contain potential for human error, especially when the time available to the operator to make decisions is short. The probability that problems will develop sufficiently to

become serious can be small. Sometimes, however, human action will be the only defence to prevent an initial failure progressing towards an accident.

The importance of HRA has been illustrated by various accidents in which critical human errors contributed to a catastrophic sequence of events. Such accidents are warnings against risk assessments that focus solely on the hardware and software in a system. They illustrate the dangers of ignoring the possibility of human error contribution. Moreover, HRAs are useful in highlighting errors that can impede productivity and in revealing ways in which these errors and other failures (hardware and software) can be "recovered" by the human operators and maintenance personnel.

B.20.2 Use

HRA can be used qualitatively or quantitatively. Qualitatively, it is used to identify the potential for human error and its causes so the probability of error can be reduced. Quantitative HRA is used to provide data on human failures into FTA or other techniques.

B.20.3 Input

Inputs to HRA include:
- information to define tasks that people should perform;
- experience of the types of error that occur in practice and potential for error;
- expertise on human error and its quantification.

B.20.4 Process

The HRA process is as follows:
- **Problem definition**, what types of human involvements are to be investigated/assessed?
- **Task analysis**, how will the task be performed and what type of aids will be needed to support performance?
- **Human error analysis**, how can task performance fail: what errors can occur and how can they be recovered?
- **Representation**, how can these errors or task performance failures be integrated with other hardware, software, and environmental events to enable overall system failure probabilities to be calculated?
- **Screening**, are there any errors or tasks that do not require detailed quantification?
- **Quantification**, how likely are individual errors and failures of tasks?
- **Impact assessment**, which errors or tasks are most important, i.e. which ones have the highest contribution to reliability or risk?
- **Error reduction**, how can higher human reliability be achieved?
- **Documentation**, what details of the HRA need to be documented?

In practice, the HRA process proceeds step-wise although sometimes with parts (e.g. tasks analysis and error identification) proceeding in parallel with one another.

B.20.5 Output

Outputs include:
- a list of errors that may occur and methods by which they can be reduced – preferably through redesign of the system;
- error modes, error types causes and consequences;
- a qualitative or quantitative assessment of the risk posed by the errors.

B.20.6 Strengths and limitations

Strengths of HRA include:

- HRA provides a formal mechanism to include human error in consideration of risks associated with systems where humans often play an important role;
- formal consideration of human error modes and mechanisms can help reduce the probability of failure due to error.

Limitations include:

- the complexity and variability of humans, which make defining simple failure modes and probabilities difficult;
- many activities of humans do not have a simple pass/fail mode. HRA has difficulty dealing with partial failures or failure in quality or poor decision-making.

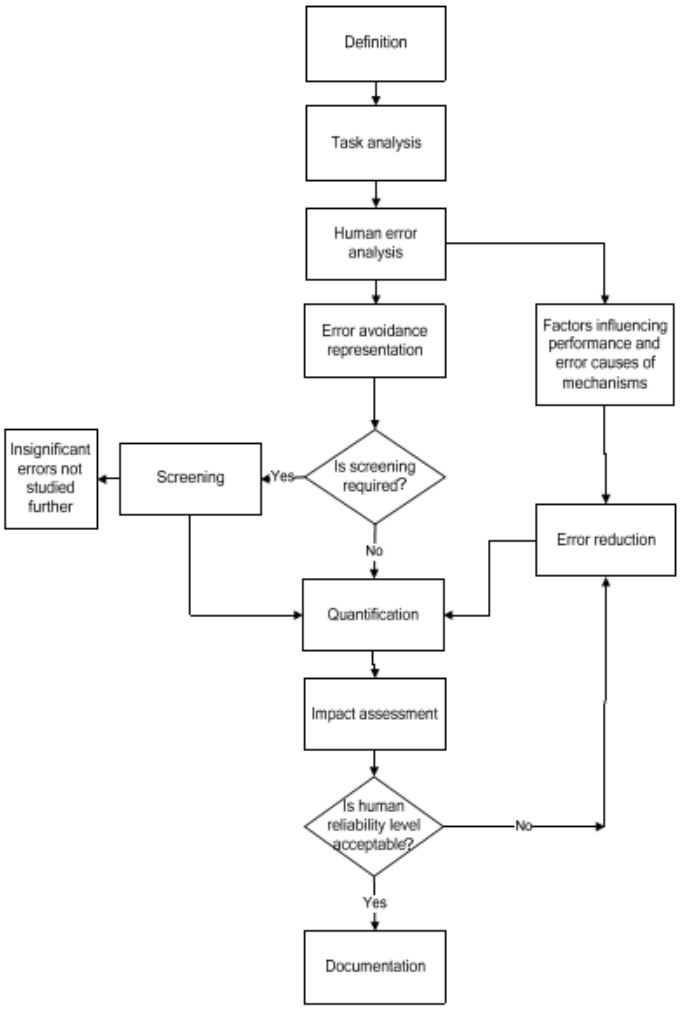


Figure B.7 – Example of human reliability assessment

B.21 Bow tie analysis

B.21.1 Overview

Bow tie analysis is a simple diagrammatic way of describing and analysing the pathways of a risk from causes to consequences. It can be considered to be a combination of the thinking of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an

event tree analysing the consequences. However the focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences. Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly from a brainstorming session.

B.21.2 Use

Bow tie analysis is used to display a risk showing a range of possible causes and consequences. It is used when the situation does not warrant the complexity of a full fault tree analysis or when the focus is more on ensuring that there is a barrier or control for each failure pathway. It is useful where there are clear independent pathways leading to failure.

Bow tie analysis is often easier to understand than fault and event trees, and hence can be a useful communication tool where analysis is achieved using more complex techniques.

B.21.3 Input

An understanding is required of information on the causes and consequences of a risk and the barriers and controls which may prevent, mitigate or stimulate it.

B.21.4 Process

The bow tie is drawn as follows:

a) A particular risk is identified for analysis and represented as the central knot of a bow tie.
b) Causes of the event are listed considering sources of risk (or hazards in a safety context).
c) The mechanism by which the source of risk leads to the critical event is identified.
d) Lines are drawn between each cause and the event forming the left-hand side of the bow tie. Factors which might lead to escalation can be identified and included in the diagram.
e) Barriers which should prevent each cause leading to the unwanted consequences can be shown as vertical bars across the line. Where there were factors which might cause escalation, barriers to escalation can also be represented. The approach can be used for positive consequences where the bars reflect ‘controls’ that stimulate the generation of the event.
f) On the right-hand side of the bow tie different potential consequences of the risk are identified and lines drawn to radiate out from the risk event to each potential consequence.
g) Barriers to the consequence are depicted as bars across the radial lines. The approach can be used for positive consequences where the bars reflect ‘controls’ that support the generation of consequences.
h) Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control.

Some level of quantification of a bow tie diagram may be possible where pathways are independent, the probability of a particular consequence or outcome is known and a figure can be estimated for the effectiveness of a control. However, in many situations, pathways and barriers are not independent and controls may be procedural and hence the effectiveness unclear. Quantification is often more appropriately carried out using FTA and ETA.

B.21.5 Output

The output is a simple diagram showing main risk pathways and the barriers in place to prevent or mitigate the undesired consequences or stimulate and promote desired consequences.

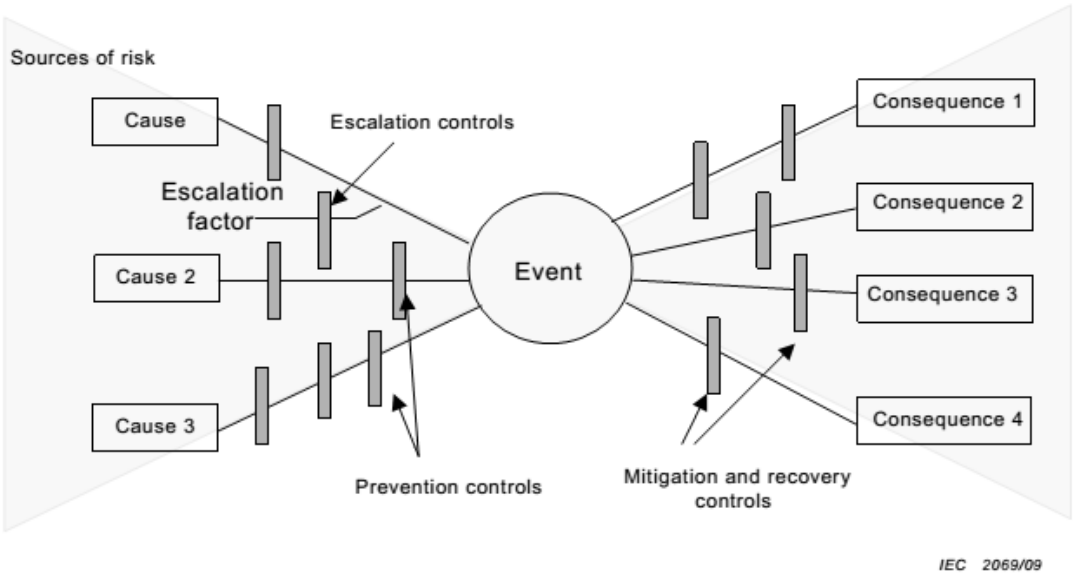


Figure B.8 – Example bow tie diagram for unwanted consequences

B.21.6 Strengths and limitations

Strengths of bow tie analysis:
- it is simple to understand and gives a clear pictorial representation of the problem;
- it focuses attention on controls which are supposed to be in place for both prevention and mitigation and their effectiveness;
- it can be used for desirable consequences;
- it does not need a high level of expertise to use.

Limitations include:
- it cannot depict where multiple causes occur simultaneously to cause the consequences (i.e. where there are AND gates in a fault tree depicting the left-hand side of the bow);
- it may over-simplify complex situations, particularly where quantification is attempted.

B.22 Reliability centred maintenance

B.22.1 Overview

Reliability centred maintenance (RCM) is a method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment.

RCM is now a proven and accepted methodology used in a wide range of industries.

RCM provides a decision process to identify applicable and effective preventive maintenance requirements for equipment in accordance with the safety, operational and economic consequences of identifiable failures, and the degradation mechanism responsible for those failures. The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes. Details regarding the use and application of RCM are provided in IEC 60300-3-11.

B.22.2 Use

All tasks are based on safety in respect of personnel and environment, and on operational or economic concerns. However, it should be noted that the criteria considered will depend on the nature of the product and its application. For example, a production process will need to be economically viable, and may be sensitive to strict environmental considerations, whereas an item of defence equipment should be operationally successful, but may have less stringent safety, economic and environmental criteria. Greatest benefit can be achieved through targeting of the analysis to where failures would have serious safety, environmental, economic or operational effects.

RCM is used to ensure that applicable and effective maintenance is performed, and is generally applied during the design and development phase and then implemented during operation and maintenance.

B.22.3 Input

Successful application of RCM needs a good understanding of the equipment and structure, the operational environment and the associated systems, subsystems and items of equipment, together with the possible failures, and the consequences of those failures.

B.22.4 Process

The basic steps of an RCM programme are as follows:
- initiation and planning;
- functional failure analysis;
- task selection;
- implementation;
- continuous improvement.

RCM is risk based since it follows the basic steps in risk assessment. The type of risk assessment is a failure mode, effect and criticality analysis (FMECA) but requires a specific approach to analysis when used in this context.

Risk identification focuses on situations where potential failures may be eliminated or reduced in frequency and/or consequence by carrying out maintenance tasks. It is performed by identifying required functions and performance standards and failures of equipment and components that can interrupt those functions

Risk analysis consists of estimating the frequency of each failure without maintenance being carried out. Consequences are established by defining failure effects. A risk matrix that combines failure frequency and consequences allows categories for levels of risk to be established.

Risk evaluation is then performed by selecting the appropriate failure management policy for each failure mode.

The entire RCM process is extensively documented for future reference and review. Collection of failure and maintenance-related data enables monitoring of results and implementation of improvements.

B.22.5 Output

RCM provides a definition of maintenance tasks such as condition monitoring, scheduled restoration, scheduled replacement, failure-finding or non preventive maintenance. Other possible actions that can result from the analysis may include redesign, changes to operating

or maintenance procedures or additional training. Task intervals and required resources are then identified.

B.22.6 Reference documents

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.23 Sneak analysis (SA)and sneak circuit analysis (SCI)

B.23.1 Overview

Sneak analysis (SA) is a methodology for identifying design errors. A sneak condition is a latent hardware, software or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel.

B.23.2 Use

Sneak circuit analysis (SCA) was developed in the late 1960s for NASA to verify the integrity and functionality of their designs. It served as a useful tool for discovering unintentional electrical circuit paths, and assisted in devising solutions to isolate each function. However, as technology advanced, the tools for sneak circuit analysis also had to advance. Sneak analysis includes and far exceeds the coverage of sneak circuit analysis. It can locate problems in both hardware and software using any technology. The sneak analysis tools can integrate several analyses such as fault trees, failure mode and effects analysis (FMEA), reliability estimates, etc. into a single analysis saving time and project expenses.

B.23.3 Input

Sneak analysis is unique from the design process in that it uses different tools (network trees, forests, and clues or questions to help the analyst identify sneak conditions) to find a specific type of problem. The network trees and forests are topological groupings of the actual system. Each network tree represents a sub-function and shows all inputs that may affect the sub-function output. Forests are constructed by combining the network trees that contribute to a particular system output. A proper forest shows a system output in terms of all of its related inputs. These, along with others, become the input to the analysis.

B.23.4 Process

The basic steps in performing a sneak analysis consist of:
- data preparation;
- construction of the network tree;
- evaluation of network paths;
- final recommendations and report.

B.23.5 Output

A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed

into the system, coded into the software program, or triggered by human error. There are four categories of sneak circuits:

a) sneak paths: unexpected paths along which current, energy, or logical sequence flows in an unintended direction;
b) sneak timing: events occurring in an unexpected or conflicting sequence;
c) sneak indications: ambiguous or false displays of system operating conditions that may cause the system or an operator to take an undesired action;
d) sneak labels: incorrect or imprecise labelling of system functions, e.g. system inputs, controls, display buses that may cause an operator to apply an incorrect stimulus to the system.

B.23.6 Strengths and limitations

Strengths include:

- sneak analysis is good for identifying design errors;
- it works best when applied in conjunction with HAZOP;
- it is very good for dealing with systems which have multiple states such as batch and semi-batch plant.

Limitations may include:

- the process is somewhat different depending on whether it is applied to electrical circuits, process plants, mechanical equipment or software;
- the method is dependent on establishing correct network trees.

B.24 Markov analysis

B.24.1 Overview

Markov analysis is used where the future state of a system depends only upon its present state. It is commonly used for the analysis of repairable systems that can exist in multiple states and the use of a reliability block analysis would be unsuitable to adequately analyse the system. The method can be extended to more complex systems by employing higher order Markov processes and is only restricted by the model, mathematical computations and the assumptions.

The Markov analysis process is a quantitative technique and can be discrete (using probabilities of change between the states) or continuous (using rates of change across the states).

While a Markov analysis can be performed by hand, the nature of the techniques lends itself to the use of computer programmes, many of which exist in the market.

B.24.2 Use

The Markov analysis technique can be used on various system structures, with or without repair, including:

- independent components in parallel;
- independent components in series;
- load-sharing system;
- stand-by system, including the case where switching failure can occur;
- degraded systems.

The Markov analysis technique can also be used for calculating availability, including taking into account the spares components for repairs.

B.24.3 Input

The inputs essential to a Markov analysis are as follows:

- list of various states that the system, sub-system or component can be in (e.g. fully operational, partially operation (i.e. a degraded state), failed state, etc);
- a clear understanding of the possible transitions that are necessary to be modelled. For example, failure of a car tyre needs to consider the state of the spare wheel and hence the frequency of inspection;
- rate of change from one state to another, typically represented by either a probability of change between states for discrete events, or failure rate (λ) and/or repair rate (μ) for continuous events.

B.24.4 Process

The Markov analysis technique is centred around the concept of “states”, e.g. “available” and “failed”, and the transition between these two states over time based on a constant probability of change. A stochastic transitional probability matrix is used to describe the transition between each of the states to allow the calculation of the various outputs.

To illustrate the Markov analysis technique, consider a complex system that can be in only three states; functioning, degraded and failed, defined as states S1, S2, S3 respectively. Each day, the system exists in one of these three states. Table B.3 shows the probability that tomorrow, the system is in state S*i* where *i* can be 1, 2 or 3.

Table B.2 – Markov matrix

		State today		
		S1	S2	S3
State tomorrow	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

This array of probabilities is called a Markov matrix, or transition matrix. Notice that the sum for each of the columns is 1 as they are the sum of all the possible outcomes in each case. The system, can also be represented by a Markov diagram where the circles represent the states, and the arrows represent the transition, together with the accompanying probability.

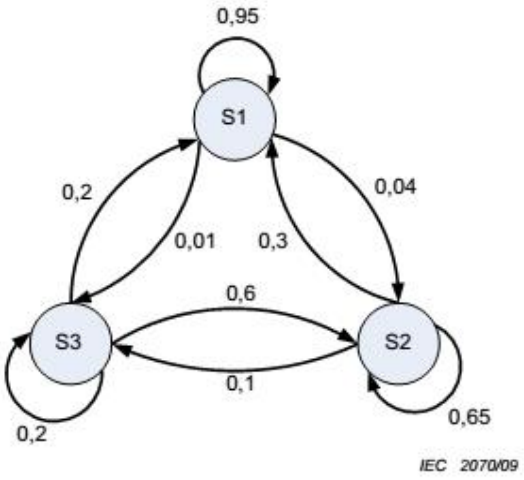


Figure B.9 – Example of system Markov diagram

The arrows from a state to itself are not usually shown, but are shown within these examples for completeness.

Let P*i* represent the probability of finding the system in state *i* for *i* = 1, 2, 3, then the simultaneous equations to be solved are:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \quad \text{(B.1)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \quad \text{(B.2)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \quad \text{(B.3)}$$

These three equations are not independent and will not solve the three unknowns. The following equation should be used and one of the above equations discarded.

$$1 = P1 + P2 + P3 \quad \text{(B.4)}$$

The solution is 0,85, 0,13, and 0.02 for the respective states 1, 2, 3. The system is fully functioning for 85 % of the time, in the degraded state for 13 % of the time and failed for 2 % of the time.

Consider two items operating in parallel with either required to be operational for the system to function. The items can either be operational or failed and the availability of the system is dependent upon the status of the items.

The states can be considered as:

State 1 Both items are functioning correctly;

State 2 One item has failed and is undergoing repair, the other is functioning;

State 3 Both items have failed and one is undergoing repair.

If the continuous failure rate for each item is assumed to be λ and the repair rate to be μ, then the state transition diagram is:

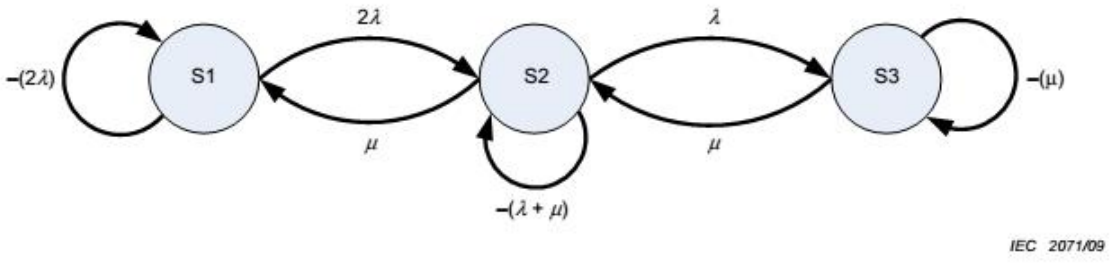


Figure B.10 – Example of state transition diagram

Note that the transition from state 1 to state 2 is 2λ as failure of either of the two items will take the system to state 2.

Let P$i(t)$ be the probability of being in an initial state i at time t; and

Let P$i(t + \delta t)$ be the probability of being in a final state at time $t + \delta t$

The transition probability matrix becomes:

Table B.3 – Final Markov matrix

		Initial state		
		P1(t)	P2(t)	P3(t)
	P1($t + \delta t$)	-2λ	μ	0
Final state	P2($t + \delta t$)	2λ	$-(\lambda + \mu)$	μ
	P3($t + \delta t$)	0	λ	$-\mu$

It is worth noting that the zero values occur as it is not possible to move from state 1 to state 3 or from state 3 to state 1. Also, the columns sum to zero when specifying rates.

The simultaneous equations become:

$$dP1/dt = -2\lambda P1(t) + \mu P2(t) \quad \text{(B.5)}$$

$$dP2/dt = 2\lambda P1(t) + (\lambda + \mu) P2(t) + \mu P3(t) \quad \text{(B.6)}$$

$$dP3/dt = \lambda P2(t) + \mu P3(t) \quad \text{(B.7)}$$

For simplicity, it will be assumed that the availability required is the steady state availability.

When δt tends to infinity, dPi/dt will tend to zero and the equations become easier to solve. The additional equation as shown in Equation (B.4) above should also be used:

Now the equation A(t) = P1(t) + P2(t) can be expressed as:

$A = P1 + P2$

Hence $A = (\mu 2 + 2\lambda\mu) / (\mu 2 + 2\lambda\mu + \lambda 2)$

B.24.5 Output

The output from a Markov analysis is the various probabilities of being in the various states, and therefore an estimate of the failure probabilities and/or availability, one of the essential components of a system.

B.24.6 Strengths and limitations

Strengths of a Markov analysis include:

- ability to calculate the probabilities for systems with a repair capability and multiple degraded states.

Limitations of a Markov analysis include:
- assumption of constant probabilities of change of state; either failure or repairs;
- all events are statistically independent since future states are independent of all past states, except for the state immediately prior;
- needs knowledge of all probabilities of change of state;
- knowledge of matrix operations;
- results are hard to communicate with non-technical personnel.

B.24.7 Comparisons

Markov analysis is similar to a Petri-Net analysis by being able to monitor and observe system states, although different since Petri-Net can exist in multiple states at the same time.

B.24.8 Reference documents

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

B.25 Monte Carlo simulation

B.25.1 Overview

Many systems are too complex for the effects of uncertainty on them to be modelled using analytical techniques, but they can be evaluated by considering the inputs as random variables and running a number N of calculations (so-called simulations) by sampling the input in order to obtain N possible outcomes of the wanted result.

This method can address complex situations that would be very difficult to understand and solve by an analytical method. Systems can be developed using spreadsheets and other conventional tools, but more sophisticated tools are readily available to assist with more complex requirements, many of which are now relatively inexpensive. When the technique was first developed, the number of iterations required for Monte Carlo simulations made the process slow and time consuming, but advances in computers and theoretical developments, such as Latin-hypercube sampling, have made processing time almost insignificant for many applications.

B.25.2 Use

Monte Carlo simulation provides a means of evaluating the effect of uncertainty on systems in a wide range of situations. It is typically used to evaluate the range of possible outcomes and the relative frequency of values in that range for quantitative measures of a system such as cost, duration, throughput, demand and similar measures. Monte Carlo simulation may be used for two different purposes:

- uncertainty propagation on conventional analytical models;
- probabilistic calculations when analytical techniques do not work.

B.25.3 Input

The input to a Monte Carlo simulation is a good model of the system and information on the types of inputs, the sources of uncertainty that are to be represented and the required output. Input data with uncertainty is represented as random variables with distributions which are more or less spread according to the level of uncertainties. Uniform, triangular, normal and log normal distributions are often used for this purpose.

B.25.4 Process

The process is as follows:

a) A model or algorithm is defined which represents as closely as possible the behaviour of the system being studied.
b) The model is run multiple times using random numbers to produce outputs of the model (simulations of the system); Where the application is to model the effects of uncertainty the model is in the form of an equation providing the relationship between input parameters and an output. The values selected for the inputs are taken from appropriate probability distributions that represent the nature of the uncertainty in these parameters.
c) In either case a computer runs the model multiple times (often up to 10,000 times) with different inputs and produces multiple outputs. These can be processed using conventional statistics to provide information such as average values, standard deviation, confidence intervals.

An example of a simulation is given below.

Consider the case of two items operating in parallel and only one is required for the system to function. The first item has a reliability of 0,9 and the other 0,8.

It is possible to construct a spreadsheet with the following columns:

Table B.4 – Example of Monte Carlo simulation

	Item 1		Item 2		
Simulation number	Random number	Functions?	Random number	Functions?	System
1	0,577 243	YES	0,059 355	YES	1
2	0,746 909	YES	0,311 324	YES	1
3	0,541 728	YES	0,919 765	NO	1
4	0,423 274	YES	0,643 514	YES	1
5	0,917 776	NO	0,539 349	YES	1
6	0,994 043	NO	0,972 506	NO	0
7	0,082 574	YES	0,950 241	NO	1
8	0,661 418	YES	0,919 868	NO	1
9	0,213 376	YES	0,367 555	YES	1
10	0,565 657	YES	0,119 215	YES	1

The random generator creates a number between 0 and 1 which is used to compare with the probability of each item to determine if the system is operational. With just 10 runs, the result of 0,9 should not be expected to be an accurate result. The usual approach is to build in a calculator to compare the total result as the simulation progresses to achieve the level of accuracy required. In this example, a result of 0,979 9 was achieved after 20 000 iterations.

The above model can be extended in a number of ways. For example:

- by extending the model itself (such as considering the second item becoming immediately operational only when the first item fails);
- by changing the fixed probability to a variable (a good example is the triangular distribution) when the probability cannot be accurately defined;
- using failure rates combined with the randomizer to derive a time of failure (exponential, Weibull, or other suitable distribution) and building in repair times.

Applications include, amongst other things, the assessment of uncertainty in financial forecasts, investment performance, project cost and schedule forecasts, business process interruptions and staffing requirements.

Analytical techniques are not able to provide relevant results or when there is uncertainty in the input data and so in the outputs.

B.25.5 Output

The output could be a single value, as determined in the above example, it could be a result expressed as the probability or frequency distribution or it could be the identification of the main functions within the model that has the greatest impact on the output.

In general, a Monte Carlo simulation will be used to assess either the entire distribution of outcomes that could arise or key measures from a distribution such as:

- the probability of a defined outcome arising;
- the value of an outcome in which the problem owners have a certain level of confidence that it will not be exceeded or beaten, a cost that there is less than a 10 % chance of exceeding or a duration that is 80 % certain to be exceeded.

An analysis of the relationships between inputs and outputs can throw light on the relative significance of the factors at work and identify useful targets for efforts to influence the uncertainty in the outcome.

B.25.6 Strengths and limitations

Strengths of the Monte Carlo analysis include the following:

- the method can, in principle, accommodate any distribution in an input variable, including empirical distributions derived from observations of related systems;
- models are relatively simple to develop and can be extended as the need arises;
- any influences or relationships arising in reality can be represented, including subtle effects such as conditional dependencies;
- sensitivity analysis can be applied to identify strong and weak influences;
- models can be easily understood as the relationship between inputs and outputs is transparent;
- efficient behavioural models such as Petri Nets (future IEC 62551) are available which prove to be very efficient for Monte Carlo simulation purposes;
- provides a measure of the accuracy of a result;
- software is readily available and relatively inexpensive.

Limitations are as follows:

- the accuracy of the solutions depends upon the number of simulations which can be performed (this limitation is becoming less important with increased computer speeds);
- it relies on being able to represent uncertainties in parameters by a valid distribution;
- large and complex models may be challenging to the modeller and make it difficult for stakeholders to engage with the process;
- the technique may not adequately weigh high-consequence/low probability events and therefore not allow an organization's risk appetite to be reflected in the analysis.

B.25.7 Reference documents

IEC 61649, *Weibull analysis*

IEC 62551, *Analysis techniques for dependability – Petri net techniques* [1]

ISO/IEC Guide 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)*

B.26 Bayesian statistics and Bayes Nets

B.26.1 Overview

Bayesian statistics are attributed to the Reverend Thomas Bayes. Its premise is that any already known information (the Prior) can be combined with subsequent measurement (the

[1] Currently under consideration

Posterior) to establish an overall probability. The general expression of the Bayes Theorem can be expressed as:

$$P(A \mid B) = \{P(A)\, P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

where

the probability of X is denoted by $P(X)$;
the probability of X on the condition that Y has occurred is denoted by $P(X|Y)$; and
E_i is the ith event.

In its simplest form this reduces to $P(A|B) = \{P(A)P(B|A)\} / P(B)$.

Bayesian statistics differs from classical statistics in that is does not assume that all distribution parameters are fixed, but that parameters are random variables. A Bayesian probability can be more easily understood if it is considered as a person's degree of belief in a certain event as opposed to the classical which is based upon physical evidence. As the Bayesian approach is based upon the subjective interpretation of probability, it provides a ready basis for decision thinking and the development of Bayesian nets (or Belief Nets, belief networks or Bayesian networks).

Bayes nets use a graphical model to represent a set of variables and their probabilistic relationships. The network is comprised of nodes that represent a random variable and arrows which link a parent node to a child node, (where a parent node is a variable that directly influences another (child) variable).

B.26.2 Use

In recent years, the use of Bays' theory and Nets has become widespread partly because of their intuitive appeal and also because of the availability of software computing tools. Bayes nets have been used on a wide range of topics: medical diagnosis, image modelling, genetics, speech recognition, economics, space exploration and in the powerful web search engines used today. They can be valuable in any area where there is the requirement for finding out about unknown variables through the utilization of structural relationships and data. Bayes nets can be used to learn causal relationships to give an understanding about a problem domain and to predict the consequences of intervention.

B.26.3 Input

The inputs are similar to the inputs for a Monte Carlo model. For a Bayes net, examples of the steps to be taken include the following:

- define system variables;
- define causal links between variables;
- specify conditional and prior probabilities;
- add evidence to net;
- perform belief updating;
- extract posterior beliefs.

B.26.4 Process

Bayes theory can be applied in a wide variety of ways. This example will consider the creation of a Bayes table where a medical test is used to determine if the patient has a disease. The belief before taking the test is that 99 % of the population do not have this

disease and 1 % have the disease, i.e the Prior information. The accuracy of the test has shown that if the person has the disease, the test result is positive 98 % of the time. There is also a probability that if you do not have the disease, the test result is positive 10 % of the time. The Bayes table provides the following information:

Table B.5 – Bayes' table data

	PRIOR	PROBABILITY	PRODUCT	POSTERIOR
Have disease	0,01	0,98	0,009 8	0,090 1
No disease	0,99	0,10	0,099 0	0,909 9
SUM	1		0,108 8	1

Using Bayes rule, the product is determined by combining the prior and probability. The posterior is found by dividing the product value by the product total. The output shows that a positive test result indicates that the prior has increased from 1 % to 9 % .More importantly, there is a strong chance that even with a positive test, having the disease is unlikely. Examining the equation (0,01×0,98)/((0,01×0,98)+(0,99×0,1)) shows that the 'no disease-positive result' value plays a major role in the posterior values.

Consider the following Bayes net:

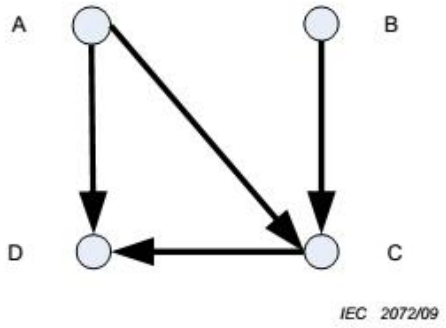


Figure B.11 – Sample Bayes' net

With the conditional prior probabilities defined within the following tables and using the notation that Y indicates positive and N indicates negative, the positive could be "have disease" as above, or could be High and N could be Low.

Table B.6 – Prior probabilities for nodes A and B

P (A = Y)	P (A = N)	P (A = Y)	P (B = Y)	P (B = N)
0,9	0,1	0,6	0,9	0,4

Table B.7 – Conditional probabilities for node C with node A and node B defined

A	B	P (C = Y)	P (C = N)
Y	Y	0,5	0,5

Y	N	0,9	0,1
N	Y	0,2	0,8
N	N	0,7	0,3

Table B.8 – Conditional probabilities for node D with node A and node C defined

A	C	P (D = Y)	P (D = N)
Y	Y	0,6	0,4
Y	N	1,0	0,0
N	Y	0,2	0,8
N	N	0,6	0,4

To determine the posterior probability of P(A|D=N,C=Y), it is necessary to first calculate P(A,B|D=N,C=Y).

Using Bayes' rule, the value P(D|A,C)P(C|A,B)P(A)P(B) is determined as shown below and the last column shows the normalized probabilities which sum to 1 as derived in the previous example (result rounded).

Table B.9 – Posterior probability for nodes A and B with node D and node C defined

A	B	P(D|A,C)P(C|A,B)P(A)P(B)	P(A|D=N,C=Y)
Y	Y	0,4 x 0,5 x 0,9 x 0,6 = 0,110	0,4
Y	N	0,4 x 0,9 x 0,9 x 0,4 = 0,130	0,48
N	Y	0,8 x 0,2 x 0,1 x 0,6 = 0,110	0,04
N	N	0,8 x 0,7 x 0,1 x 0,4 = 0,022	0,08

Table B.10 – Posterior probability for node A with node D and node C defined

P(A=Y|D=N,C=Y)	P(A=N|D=N,C=Y)
0,88	0,12

This shows that the prior for P(A=N) has increased from 0,1 to a posterior of 0,12 which is only a small change. On the other hand, P(B=N|D=N,C=Y) has changed from 0,4 to 0,56 which is a more significant change.

B.26.5 Outputs

The Bayesian approach can be applied to the same extent as classical statistics with a wide range of outputs, e.g. data analysis to derive point estimators and confidence intervals. Its recent popularity is in relation to Bayes nets to derive posterior distributions. The graphical

output provides an easily understood model and the data can be readily modified to consider correlations and sensitivity of parameters.

B.26.6 Strengths and limitations

Strengths:

- all that is needed is knowledge on the priors;
- inferential statements are easy to understand;
- Bayes' rule is all that is required;
- it provides a mechanism for using subjective beliefs in a problem.

Limitations:

- defining all interactions in Bayes nets for complex systems is problematic;
- Bayesian approach needs the knowledge of a multitude of conditional probabilities which are generally provided by expert judgment. Software tools can only provide answers based on these assumptions.

B.27 FN curves

B.27.1 Overview

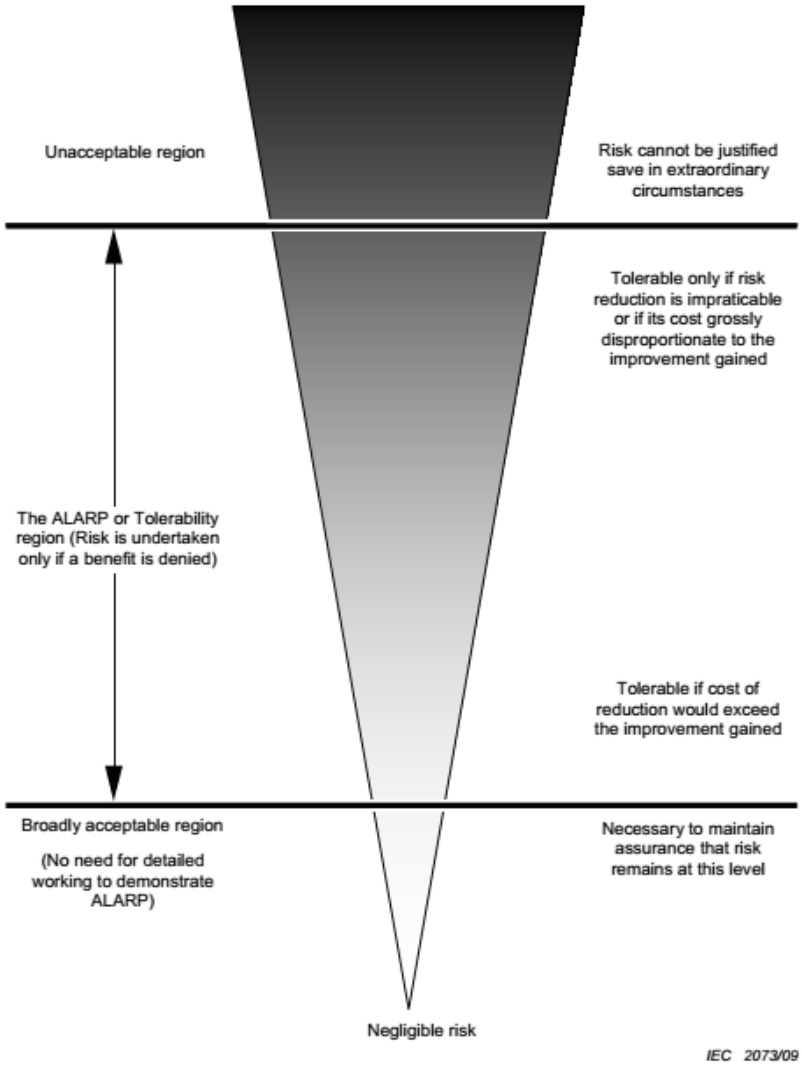


Figure B.12 – The ALARP concept

FN curves are a graphical representation of the probability of events causing a specified level of harm to a specified population. Most often they refer to the frequency of a given number of casualties occurring.

FN curves show the cumulative frequency (*F*) at which *N* or more members of the population that will be affected. High values of *N* that may occur with a high frequency *F* are of significant interest because they may be socially and politically unacceptable.

B.27.2 Use

FN curves are a way of representing the outputs of risk analysis. Many events have a high probability of a low consequence outcome and a low probability of a high consequence outcome. The FN curves provide a representation of the level of risk that is a line describing this range rather than a single point representing one consequence probability pair.

FN curves may be used to compare risks, for example to compare predicted risks against criteria defined as an FN curve, or to compare predicted risks with data from historical incidents, or with decision criteria (also expressed as an F/N curve).

FN curves can be used either for system or process design, or for management of existing systems.

B.27.3 Input

The inputs are either:

- sets of the probability consequence pairs over a given period of time;
- the output of data from a quantitative risk analysis giving estimated probabilities for specified numbers of casualties;
- data from both historical records and a quantitative risk analysis.

B.27.4 Process

The available data is plotted onto a graph with the number of casualties (to a specified level of harm, i.e. death) forming the abscissa with the probability of N or more casualties forming the ordinate. Because of the large range of values, both axes are normally on logarithmic scales.

FN curves may be constructed statistically using “real” numbers from past losses or they can be calculated from simulation model estimates. The data used and assumptions made may mean that these two types of FN curve give different information and should be used separately and for different purposes. In general, theoretical FN curves are most useful for system design, and statistical FN curves are most useful for management of a particular existing system.

Both derivation approaches can be very time-consuming so it is not uncommon to use a mixture of both. Empirical data will then form fixed points of precisely known casualties that occurred in known accidents/incident in a specified period of time and the quantitative risk analysis providing other points by extrapolation or interpolation.

The need to consider low-frequency, high-consequence accidents may require consideration of long periods of time to gather enough data for a proper analysis. This in turn may make the available data suspect if the initiating events happen to change over time.

B.27.5 Output

A line representing risk across a range of values of consequence that can be compared with criteria that are appropriate for the population being studied and the specified level of harm.

B.27.6 Strengths and limitations

FN curves are a useful way of presenting risk information that can be used by managers and system designers to help make decisions about risk and safety levels. They are a useful way of presenting both frequency and consequence information in an accessible format.

FN curves are appropriate for comparison of risks from similar situations where sufficient data is available. They should not be used to compare risks of different types with varying characteristics in circumstances where quantity and quality of data varies.

A limitation of FN curves is that they do not say anything about the range of effects or outcomes of incidents other than the number of people impacted, and there is no way of identifying the different ways in which the level of harm may have occurred. They map a particular consequence type, usually harm to people. FN curves are not a risk assessment method, but one way of presenting the results of risk assessment.

They are a well established method for presenting risk assessment results but require preparation by skilled analysts and are often difficult for non specialists to interpret and evaluate

B.28 Risk indices

B.28.1 Overview

A risk index is a semi-quantitative measure of risk which is an estimate derived using a scoring approach using ordinal scales. Risk indices can be used to rate a series of risks using similar criteria so that they can be compared. Scores are applied to each component of risk, for example contaminant characteristics (sources), the range of possible exposure pathways and the impact on the receptors.

Risk indices are essentially a qualitative approach to ranking and comparing risks. While numbers are used, this is simply to allow for manipulation. In many cases where the underlying model or system is not well known or not able to be represented, it is better to use a more overtly qualitative approach.

B.28.2 Use

Indices can be used for classifying different risks associated with an activity if the system is well understood. They permit the integration of a range of factors which have an impact on the level of risk into a single numerical score for level of risk

Indices are used for many different types of risk usually as a scoping device for classifying risk according to level of risk. This may be used to determine which risks need further in-depth and possibly quantitative assessment.

B.28.3 Input

The inputs are derived from analysis of the system, or a broad description of the context. This requires a good understanding of all the sources of risk, the possible pathways and what might be affected. Tools such as fault tree analysis, event tree.analysis and general decision analysis can be used to support the development of risk indices

Since the choice of ordinal scales is, to some extent, arbitrary, sufficient data is needed to validate the index.

B.28.4 Process

The first step is to understand and describe the system. Once the system has been defined, scores are developed for each component in such a way that they can be combined to provide a composite index. For example, in an environmental context, the sources, pathway and receptor(s) will be scored, noting that in some cases there may be multiple pathways and receptors for each source. The individual scores are combined according to a scheme that takes account of the physical realities of the system. It is important that the scores for each part of the system (sources, pathways and receptors) are internally consistent and maintain

their correct relationships. Scores may be given for components of risk (e.g. probability, exposure, consequence) or for factors which increase risk.

Scores may be added, subtracted, multiplied and/or divided according to this high level model. Cumulative effects can be taken into account by adding scores (for example, adding scores for different pathways). It is strictly not valid to apply mathematical formulae to ordinal scales. Therefore, once the scoring system has been developed, the model should be validated by applying it to a known system. Developing an index is an iterative approach and several different systems for combining the scores may be tried before the analyst is comfortable with the validation.

Uncertainty can be addressed by sensitivity analysis and varying scores to find out which parameters are the most sensitive.

B.28.5 Output

The output is a series of numbers (composite indices) that relate to a particular source and which can be compared with indices developed for other sources within the same system or which can be modelled in the same way.

B.28.6 Strengths and limitations

Strengths:

- indices can provide a good tool for ranking different risks;
- they allow multiple factors which affect the level of risk to be incorporated into a single numerical score for the level of risk.

Limitations:

- if the process (model) and its output are not well validated, the results may be meaningless. The fact that the output is a numerical value for risk may be misinterpreted and misused, for example in subsequent cost/benefit analysis;
- in many situations where indices are used, there is no fundamental model to define whether the individual scales for risk factors are linear, logarithmic or of some other form, and no model to define how factors should be combined. In these situations, the rating is inherently unreliable and validation against real data is particularly important.

B.29 Consequence/probability matrix

B.29.1 Overview

The consequence/probability matrix is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk or risk rating.

The format of the matrix and the definitions applied to it depend on the context in which it is used and it is important that an appropriate design is used for the circumstances.

B.29.2 Use

A consequence/probability matrix is used to rank risks, sources of risk or risk treatments on the basis of the level of risk. It is commonly used as a screening tool when many risks have been identified, for example to define which risks need further or more detailed analysis, which risks need treatment first, or which need to be referred to a higher level of management. It may also be used to select which risks need not be considered further at this

time. This kind of risk matrix is also widely used to determine if a given risk is broadly acceptable, or not acceptable (see 5.4) according to the zone where it is located on the matrix.

The consequence/probability matrix may also be used to help communicate a common understanding for qualitative levels of risks across the organization. The way risk levels are set and decision rules assigned to them should be aligned with the organization's risk appetite.

A form of consequence/probability matrix is used for criticality analysis in FMECA or to set priorities following HAZOP. It may also be used in situations where there is insufficient data for detailed analysis or the situation does not warrant the time and effort for a more quantitative analysis

B.29.3 Input

Inputs to the process are customized scales for consequence and probability and a matrix which combines the two.

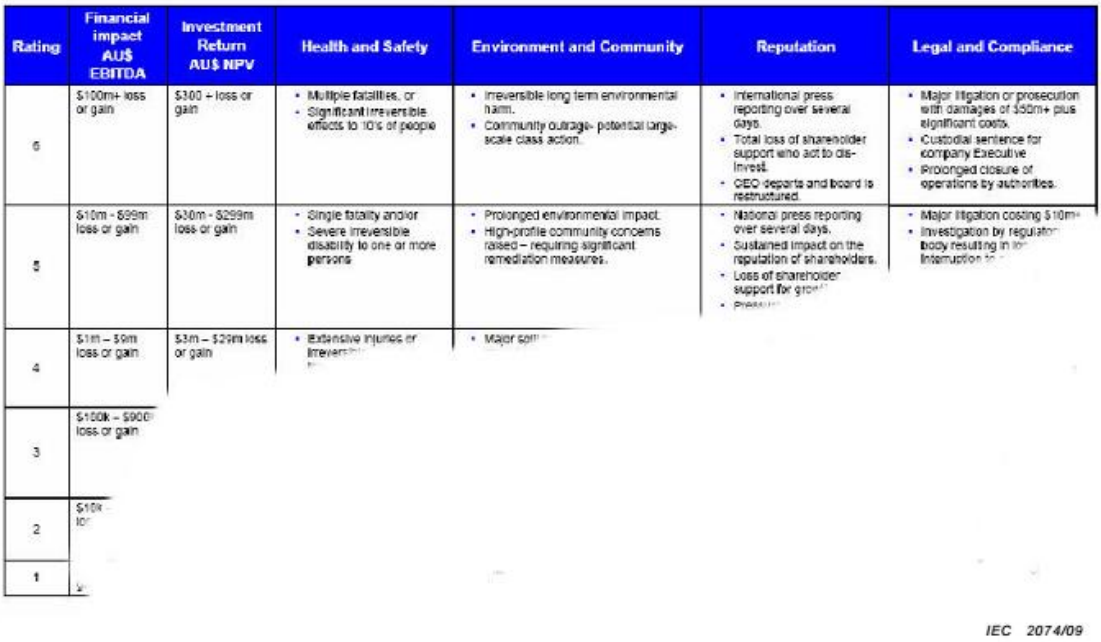
The consequence scale (or scales) should cover the range of different types of consequence to be considered (for example: financial loss; safety; environment or other parameters, depending on context) and should extend from the maximum credible consequence to the lowest consequence of concern. A part example is shown in Figure B.6.

The scale may have any number of points. 3, 4 or 5 point scales are most common.

The probability scale may also have any number of points. Definitions for probability need to be selected to be as unambiguous as possible. If numerical guides are used to define different probabilities, then units should be given. The probability scale needs to span the range relevant to the study in hand, remembering that the lowest probability must be acceptable for the highest defined consequence, otherwise all activities with the highest consequence are defined as intolerable. A part example is shown in Figure B.7.

A matrix is drawn with consequence on one axis and probability on the other. Figure B.8 shows part of an example matrix with a 6 point consequence and 5 point probability scales.

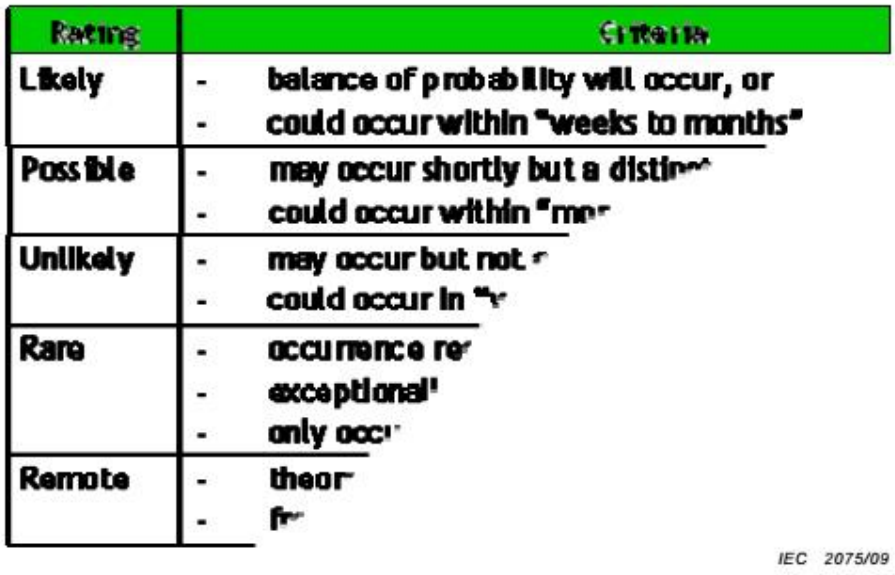
The risk levels assigned to the cells will depend on the definitions for the probability/ consequence scales. The matrix may be set up to give extra weight to consequences (as shown) or to probability, or it may be symmetrical, depending on the application. The levels of risk may be linked to decision rules such as the level of management attention or the time scale by which response is needed.



Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$300 + loss or gain	• Multiple fatalities, or • Significant irreversible effects to 10's of people	• Irreversible long term environmental harm. • Community outrage- potential large-scale class action.	• International press reporting over several days. • Total loss of shareholder support who act to dis-invest. • CEO departs and board is restructured.	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$30m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact. • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for gro	• Major litigation costing $10m • Investigation by regulato body resulting in lo interruption to
4	$1m – $9m loss or gain	$3m – $29m loss or gain	• Extensive injuries or irrever	• Major sm		
3	$100k – $900 loss or gain					
2	$10k lo					
1	v					

IEC 2074/09

Figure B.13 – Part example of a consequence criteria table



Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distin - could occur within "mo
Unlikely	- may occur but not - could occur in "y
Rare	- occurrence re - exceptional - only occ
Remote	- theor - fr

IEC 2075/09

Figure B.14 – Part example of a risk ranking matrix

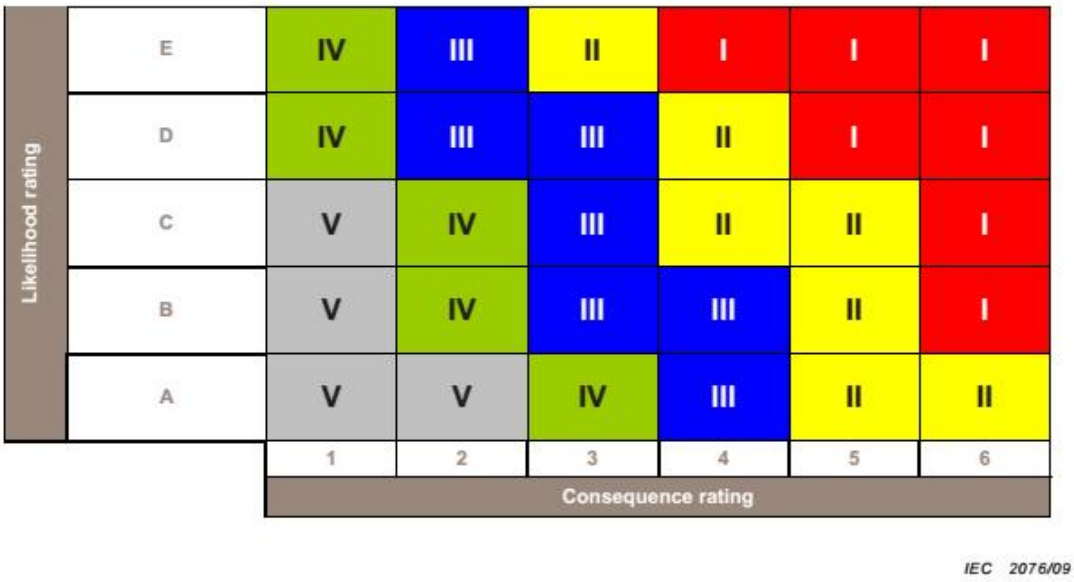


Figure B.15 – Part example of a probability criteria matrix

Rating scales and a matrix may be set up with quantitative scales. For example, in a reliability context the probability scale could represent indicative failure rates and the consequence scale the dollar cost of failure.

Use of the tool needs people (ideally a team) with relevant expertise and such data as is available to help in judgements of consequence and probability.

B.29.4 Process

To rank risks, the user first finds the consequence descriptor that best fits the situation then defines the probability with which those consequences will occur. The level of risk is then read off from the matrix.

Many risk events may have a range of outcomes with different associated probability. Usually, minor problems are more common than catastrophes. There is therefore a choice as to whether to rank the most common outcome or the most serious or some other combination. In many cases, it is appropriate to focus on the most serious credible outcomes as these pose the largest threat and are often of most concern. In some cases, it may be appropriate to rank both common problems and unlikely catastrophes as separate risks. It is important that the probability relevant to the selected consequence is used and not the probability of the event as a whole.

The level of risk defined by the matrix may be associated with a decision rule such as to treat or not to treat the risk.

B.29.5 Output

The output is a rating for each risk or a ranked list of risk with significance levels defined.

B.29.6 Strengths and limitations

Strengths:

- relatively easy to use;
- provides a rapid ranking of risks into different significance levels.

Limitations:
- a matrix should be designed to be appropriate for the circumstances so it may be difficult to have a common system applying across a range of circumstances relevant to an organization;
- it is difficult to define the scales unambiguously;
- use is very subjective and there tends to be significant variation between raters;
- risks cannot be aggregated (i.e. one cannot define that a particular number of low risks or a low risk identified a particular number of times is equivalent to a medium risk);
- it is difficult to combine or compare the level of risk for different categories of consequences.

Results will depend of the level of detail of the analysis, i.e. the more detailed the analysis, the higher the number of scenarios, each with a lower probability. This will underestimate the actual level of risk. The way in which scenarios are grouped together in describing risk should be consistent and defined at the start of the study.

B.30 Cost/benefit analysis (CBA)

B.30.1 Overview

Cost/benefit analysis can be used for risk evaluation where total expected costs are weighed against the total expected benefits in order to choose the best or most profitable option. It is an implicit part of many risk evaluation systems. It can be qualitative or quantitative or involve a combination of quantitative and qualitative elements. Quantitative CBA aggregates the monetary value of all costs and all benefits to all stakeholders that are included in the scope and adjusts for different time periods in which costs and benefits accrue. The net present value (NPV) which is produced becomes an input into to decisions about risk. A positive NPV associated with an action would normally mean the action should occur. However, for some negative risks, particularly those involving risks to human life or damage to the environment the ALARP principle may be applied. This divides risks into three regions: a level above which negative risks are intolerable and should not be taken except in extraordinary circumstances; a level below which risks are negligible and need only to be monitored to ensure they remain low; and a central band where risks are made as low as reasonably practicable (ALARP). Towards the lower risk end of this region, a strict cost benefit analysis may apply but where risks are close to intolerable, the expectation of the ALARP principle is that treatment will occur unless the costs of treatment are grossly disproportionate to the benefit gained.

B.30.2 Uses

Cost/benefit analysis can be used to decide between options which involve risk.

For example

- as input into a decision about whether a risk should be treated,
- to differentiate between and decide on the best form of risk treatment,
- to decide between different courses of action.

B.30.3 Inputs

Inputs include information on costs and benefits to relevant stakeholders and on uncertainties in those costs and benefits. Tangible and intangible costs and benefits should be considered.

Costs include resources expended and negative outcomes, benefits include positive outcomes, negative outcomes avoided and resources saved.

B.30.4 Process

The stakeholders who may experience costs or receive benefits are identified. In a full cost benefit analysis all stakeholders are included.

The direct and indirect benefits and costs to all relevant stakeholders of the options being considered are identified. Direct benefits are those which flow directly from the action taken, while indirect or ancillary benefits are those which are coincidental but might still contribute significantly to the decision. Examples of indirect benefits include reputation improvement, staff satisfaction and “peace of mind”. (These are often weighted heavily in decision-making).

Direct costs are those that are directly associated with the action. Indirect costs are those additional, ancillary and sunk costs, such as loss of utility, distraction of management time or the diversion of capital away from other potential investments. When applying a cost benefit analysis to a decision on whether to treat a risk, costs and benefits associated with treating the risk, and with taking the risk, should be included

In quantitative cost/benefit analysis, when all tangible and intangible costs and benefits have been identified, a monetary value is assigned to all costs and benefits (including intangible costs and benefits). There are a number of standard ways of doing this including the ‘willingness to pay’ approach and using surrogates. If, as often happens, the cost is incurred over a short period of time (e.g. a year) and the benefits flow for a long period thereafter, it is normally necessary to discount the benefits to bring them into “today’s money” so that a valid comparison can be obtained. All costs and benefits are expressed as a present value. The present value of all costs and all benefits to all stakeholders can be combined to produce a net present value (NPV). A positive NPV implies that the action is beneficial. Benefit cost ratios are also used see B30.5

If there is uncertainty about the level of costs or benefits, either or both terms can be weighted according to their probabilities.

In qualitative cost benefit analysis no attempt is made to find a monetary value for intangible costs and benefits and, rather than providing a single figure summarizing the costs and benefits, relationships and trade-offs between different costs and benefits are considered qualitatively.

A related technique is a cost-effectiveness analysis. This assumes that a certain benefit or outcome is desired, and that there are several alternative ways to achieve it. The analysis looks only at costs and which is the cheapest way to achieve the benefit.

B.30.5 Output

The output of a cost/benefit analysis is information on relative costs and benefits of different options or actions. This may be expressed quantitatively as a net present value (NPV) an internal rate of return (IRR) or as the ratio of the present value of benefits to the present value of costs. Qualitatively the output is usually a table comparing costs and benefits of different types of cost and benefit, drawing attention to trade offs.

B.30.6 Strengths and limitations

Strengths of cost benefit analysis:

- it allows costs and benefits to be compared using a single metric (money);
- it provides transparency of decision making;
- it requires detailed information to be collected on all possible aspects of the decision. This can be valuable in revealing ignorance as well as communicating knowledge.

Limitations:

- quantitative CBA can yield dramatically different numbers, depending on the methods used to assign economic values to non-economic benefits;
- in some applications it is difficult to define a valid discounting rate for future costs and benefits;
- benefits which accrue to a large population are difficult to estimate, particularly those relating to public good which is not exchanged in markets;
- the practice of discounting means that benefits gained in the long term future have negligible influence on the decision depending on the discounting rate chosen. The method becomes unsuitable for consideration of risks affecting future generations unless very low or zero discount rates are set.

B.31 Multi-criteria decision analysis (MCDA)

B.31.1 Overview

The objective is to use a range of criteria to objectively and transparently assess the overall worthiness of a set of options. In general, the overall goal is to produce a preference of order between the available options. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option.

B.31.2 Use

MCDA can be used for

- comparing multiple options for a first pass analysis to determine preferred and potential options and inappropriate option,

- comparing options where there are multiple and sometimes conflicting criteria,

- reaching a consensus on a decision where different stakeholders have conflicting objectives or values.

B.31.3 Inputs

A set of options for analysis. Criteria, based on objectives that can be used equally across all options to differentiate between them.

B.31.4 Process

In general a group of knowledgeable stakeholders undertakes the following process:

a) define the objective(s);
b) determine the attributes (criteria or performance measures) that relate to each objective;
c) structure the attributes into a hierarchy;
d) develop options to be evaluated against the criteria;
e) determine the importance of the criteria and assign corresponding weights to them;
f) evaluate the alternatives with respect to the criteria. This may be represented as a matrix of scores.

g) combine multiple single-attribute scores into a single aggregate multi attribute score;
h) evaluate the results.

There are different methods by which the weighting for each criteria can be elicited and different ways of aggregating the criteria scores for each option into a single multi-attribute score. For example, scores may be aggregated as a weighted sum or a weighted product or using the analytic hierarchy process, an elicitation technique for the weights and scores based on pairwise comparisons. All these methods assume that the preference for any one criterion does not depend on the values of the other criteria. Where this assumption is not valid, different models are used.

Since scores are subjective, sensitivity analysis is useful to examine the extent to which the weights and scores influence overall preferences between options.

B.31.5 Outputs

Rank order presentation of the options goes from best to least preferred. If the process produces a matrix where the axes of the matrix are criteria weighted and the criteria score for each option, then options that fail highly weighted criteria can also be eliminated.

B.31.6 Strengths and limitations

Strengths:

- provides a simple structure for efficient decision-making and presentation of assumptions and conclusions;
- can make complex decision problems, which are not amenable to cost/benefit analysis, more manageable;
- can help rationally consider problems where tradeoffs need to be made;
- can help achieve agreement when stakeholders have different objectives and hence criteria.

Limitations:

- can be affected by bias and poor selection of the decision criteria;
- most MCDA problems do not have a conclusive or unique solution;
- aggregation algorithms which calculate criteria weights from stated preferences or aggregate differing views can obscure the true basis of the decision.

Bibliografi

[1]. IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

[2]. IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[3]. IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

[4]. ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

[5]. ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

[6]. IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

[7]. IEC 61649, *Weibull analysis*

[8]. IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[9]. IEC 61165, *Application of Markov techniques*

[10]. ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

[11]. IEC 62551, *Analysis techniques for dependability – Petri net techniques 2*

[12]. IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

Informasi pendukung terkait perumus standar

[1] Komtek/SubKomtek perumus SNI

Komite Teknis 03-10 *Manajemen risiko*

[2] Susunan keanggotaan Komtek perumus SNI

Ketua : Antonius Alijoyo

Sekretaris : Hendro Kusumo

Anggota :

1. Arif Budiman
2. Bernado A. Mochtar
3. Charles Reinier Vorst
4. D.S. Priyarsono
5. Hidayat Prabowo
6. Johan Candra
7. Miryam L. Wijaya
8. Mohammad Mukhlis
9. Nursepdal Verliandri
10. Ridwan Hendra
11. Roy Urich Kusumawardhana

[3] Konseptor rancangan SNI

1. Arif Budiman
2. Bernado A. Mochtar
3. Johan Candra

[4] Sekretariat pengelola Komtek perumus SNI

Pusat Perumusan Standar

Kedeputian bidang Penelitian dan Kerjasama Standardisasi

Badan Standardisasi Nasional