

KENEXIS CONSULTING CORPORATION

BUKU PANDUAN REKAYASA SAFETY INSTRUMENTED SYSTEMS (SIS)

Safety Instrumented Systems Engineering Handbook

Kenexis Consulting Corporation • Columbus, Ohio, USA

Penulis Utama:

Kevin J. Mitchell • Peter Hereña • Todd M. Longendelpher • Matthew C. Kuhn

Edisi Terjemahan Lengkap Bahasa Indonesia

Panduan Standar Desain dan Siklus Hidup Keselamatan Industri Proses Kimia, Minyak, dan Gas
Berdasarkan Standar Internasional IEC 61511 / ISA 84.00.01 & IEC 61508

Kenexis © 2010 • Seluruh Hak Cipta Dilindungi Undang-Undang

INFORMASI HAK CIPTA DAN PENERBITAN

Hak Cipta © 2010 oleh Kenexis Consulting Corporation

Columbus, Ohio, Amerika Serikat

Kenexis Consulting Corporation

2929 Kenny Road, Suite 225, Columbus, OH 43221

E-mail: info@kenexis.com • Situs Web: <http://www.kenexis.com>

Telepon: (614) 451-7031

Seluruh Hak Cipta Dilindungi Undang-Undang (All Rights Reserved).

Dilarang memperbanyak, menyimpan dalam sistem penelusuran (retrieval system), atau mentransmisikan bagian mana pun dari karya ini dalam bentuk apa pun atau dengan cara apa pun, baik secara elektronik, mekanis, fotokopi, rekaman, atau cara lainnya, tanpa izin tertulis terlebih dahulu dari Kenexis Consulting Corporation.

PEMBERITAHUAN HUKUM RESMI

Penafian Hukum, Paten, dan Batasan Tanggung Jawab:

Dalam mempersiapkan karya ini, Kenexis Consulting Corporation tidak meneliti atau mempertimbangkan paten yang mungkin berlaku untuk materi subjek yang terkandung di dalam buku ini. Merupakan tanggung jawab pembaca dan pengguna materi yang terkandung dalam buku ini untuk melindungi diri mereka sendiri dari tanggung jawab hukum atas pelanggaran paten.

Informasi dan rekomendasi yang terkandung dalam buku ini tidak dimaksudkan untuk aplikasi atau penerapan spesifik tertentu, dan bersifat informatif umum. Akibatnya, Kenexis Consulting Corporation tidak bertanggung jawab dan melepaskan seluruh tanggung jawab hukum dalam bentuk apa pun, bagaimanapun timbulnya, sebagai akibat dari penggunaan informasi yang terkandung dalam buku ini.

Setiap peralatan yang mungkin dirujuk dalam karya ini telah dipilih oleh penulis semata-mata sebagai contoh teknologi. Kenexis Consulting Corporation tidak membuat dukungan atau jaminan terhadap produk apa pun, baik tersurat maupun tersirat. Dalam semua keadaan, prosedur dari produsen peralatan harus selalu diutamakan terkait penggunaan peralatan spesifik. Tidak ada pernyataan, baik tersurat maupun tersirat, yang dibuat sehubungan dengan ketersediaan peralatan, proses, formula, atau prosedur lain yang terkandung dalam buku ini.

Data Pengatalogan dalam Terbitan Perpustakaan Kongres (Library of Congress Cataloging-in-Publication Data)

TENTANG KENEXIS

Kenexis adalah perusahaan konsultan rekayasa global yang berfokus pada implementasi perlindungan berteknologi rekayasa (*engineered safeguards*) di pabrik-pabrik proses. Perlindungan rekayasa adalah perangkat fisik yang dapat mendeteksi bahwa situasi yang tidak diinginkan atau di luar kendali sedang terjadi di pabrik proses dan mengambil tindakan pemulihan untuk mengembalikan proses ke kondisi yang aman (*safe state*). Beberapa contoh tipikal dari perlindungan rekayasa yang diterapkan di industri proses ditunjukkan di bawah ini:

- **Safety Instrumented Systems (SIS):** Sistem berinstrumen keselamatan otomatis.
- **Fire and Gas Detection and Suppression Systems:** Sistem deteksi dan pemadaman kebakaran dan gas.
- **Emergency Isolation Valve Systems:** Sistem katup isolasi darurat untuk menghentikan aliran bahan berbahaya.
- **Alarm Systems:** Sistem alarm kritis untuk intervensi operator.
- **Pressure Relief Systems:** Sistem pelepasan tekanan darurat mekanis (katup relief dan rupture disk).
- **Cyber Security Systems:** Sistem keamanan siber industri (deteksi dan pencegahan intrusi pada jaringan kendali).
- **Machine Safeguarding Systems:** Sistem pengamanan mesin dan peralatan berputar.

Kenexis membantu klien kami untuk menerapkan sistem-sistem ini dengan bertindak sebagai penasihat ahli pihak ketiga independen yang membantu dalam pengembangan basis desain (*design basis*) dari sistem ini dan validasi bahwa sistem ini diimplementasikan sesuai dengan basis desain di seluruh siklus hidupnya (*safety lifecycle*). Karena Kenexis tidak menjual atau merekomendasikan perangkat keras apa pun atau melakukan layanan rekayasa terperinci, Kenexis memiliki posisi unik untuk bertindak sebagai penasihat independen tanpa konflik kepentingan yang mungkin membiaskan arah keputusan dalam pengembangan basis desain.

Kenexis menerapkan pendekatan berbasis risiko (*risk-based approach*) dalam membantu klien kami menentukan kebutuhan perlindungan rekayasa mereka. Risiko yang ditimbulkan oleh proses yang dioperasikan klien kami dapat ditentukan dan dikembangkan melalui Analisis Bahaya Proses (*Process Hazards Analysis - PHA*) di mana Kenexis dapat memfasilitasi dan berpartisipasi secara aktif. Setelah kebutuhan perlindungan rekayasa teridentifikasi, basis desain untuk perlindungan tersebut dikembangkan lebih lanjut dengan mempertimbangkan kode dan standar yang berlaku bersama dengan tingkat pengurangan risiko yang dipersyaratkan.

Dokumen basis desain Kenexis sangat unik dalam kemampuannya untuk memungkinkan pengguna akhir membandingkan alternatif dari berbagai vendor dan memilih solusi yang paling sesuai dengan kebutuhan mereka. Setelah basis desain selesai, klien kami bekerja sama dengan vendor peralatan, integrator sistem, dan perusahaan EPC untuk mengimplementasikan solusi fisik. Setelah itu, Kenexis membantu klien dengan melakukan layanan validasi dan dukungan berkelanjutan guna memastikan sistem tetap terpelihara secara *evergreen*.

TENTANG PENULIS

Kevin J. Mitchell

Kevin J. Mitchell memiliki pengalaman yang tak tertandingi di bidang manajemen risiko dan keselamatan proses. Mitchell telah terlibat dalam ratusan proyek yang mencakup berbagai operasi yang beragam seperti produksi minyak & gas bumi, pengilangan, petrokimia, kimia khusus, dan manufaktur umum.

Beliau berspesialisasi dalam penilaian mutakhir (*state-of-the-art assessment*) mengenai risiko material beracun, mudah terbakar, dan mudah meledak terhadap manusia, properti, lingkungan, dan pada akhirnya, kelangsungan bisnis. Beliau secara luas menggunakan penilaian risiko dan Analisis Biaya-Manfaat (*Cost-Benefit Analysis*) untuk membantu dalam pengambilan keputusan rekayasa teknik dan keputusan bisnis strategis.

Peter Hereña

Peter Hereña memiliki pengalaman luas dalam perancangan dan instalasi sistem kendali serta implementasi sistem berinstrumen keselamatan (SIS) untuk industri proses. Beliau telah bekerja pada berbagai proyek yang berkaitan dengan produksi minyak & gas bumi, pengilangan, petrokimia, dan manufaktur kimia.

Pengalaman beliau mencakup perancangan perangkat lunak, verifikasi lapangan sistem kendali dan instrumen, serta dukungan start-up untuk proyek-proyek di seluruh dunia. Beliau telah mendampingi klien di hampir setiap aspek siklus hidup keselamatan (*safety lifecycle*), mulai dari fasilitasi HAZOP, melalui pemilihan dan verifikasi SIL, hingga pengembangan Spesifikasi Persyaratan Keselamatan (*Safety Requirements Specifications - SRS*) dan rencana pengujian fungsional terperinci.

TENTANG PENULIS (LANJUTAN)

Todd M. Longendelpher

Todd M. Longendelpher memiliki pengalaman mendalam dalam perancangan sistem berinstrumen keselamatan dan metode analisis risiko. Beliau bertanggung jawab atas pengembangan persyaratan SIL dan verifikasi persyaratan SIL untuk sistem berinstrumen keselamatan.

Beliau memanfaatkan teknik analisis risiko untuk menilai desain SIS yang ada terhadap potensi bahaya yang menghasilkan konsekuensi parah. Beliau telah memimpin aktivitas LOPA / Pemilihan SIL dan Verifikasi SIL untuk pelanggan di sektor pengilangan minyak bumi, petrokimia, dan produksi minyak & gas hulu di Amerika Serikat maupun lokasi internasional. Saat ini beliau mengawasi implementasi desain SIS pada berbagai anjungan produksi hulu minyak dan gas di Teluk Meksiko.

Matthew C. Kuhn

Matthew C. Kuhn adalah *Lead Engineer* di Kenexis dan memiliki pengalaman signifikan dalam perancangan sistem berinstrumen keselamatan serta proyek analisis konsekuensi dan bahaya proses.

Kuhn telah bertanggung jawab atas beberapa proyek basis desain SIS yang melibatkan seluruh ladang produksi minyak dan gas bumi, mulai dari kepala sumur (*wellhead*), fasilitas pemrosesan terpusat, hingga fasilitas pemuatan dan pengapalan produk akhir. Proyek-proyek ini mencakup rangkaian lengkap kegiatan siklus hidup keselamatan SIS termasuk penetapan target SIL melalui analisis lapisan perlindungan (LOPA - baik teknik implisit maupun eksplisit), verifikasi desain konseptual yang ada maupun yang diusulkan menggunakan teknik perhitungan verifikasi SIL, penyusunan laporan kesenjangan (*gap reports*) basis desain SIS, serta perumusan rekomendasi terperinci. Kuhn juga memimpin fasilitasi pertemuan di lokasi proyek bersama dengan pelaksanaan perhitungan terperinci untuk produk kerja akhir.

PRAKATA

Sistem Berinstrumen Keselamatan (*Safety Instrumented Systems* - SIS) membentuk beberapa perlindungan rekayasa yang paling banyak digunakan dan paling sulit untuk dirancang di industri proses. Sebelum diterbitkannya standar berbasis risiko untuk perancangan SIS, desain secara tradisional diimplementasikan menggunakan aturan praktis (*rules of thumb*) yang cukup efektif, tetapi tidak sepenuhnya memuaskan.

Setelah implementasi analisis berbasis risiko, para pengguna SIS menyadari bahwa perlindungan rekayasa ini sendiri memiliki fleksibilitas desain yang memungkinkan terciptanya desain yang sangat beragam dengan kemampuan pengurangan risiko yang sangat beragam pula. Hanya SIS yang dapat dirancang dengan pendekatan bertingkat: baik (*good*), lebih baik (*better*), dan terbaik (*best*), yang membatasi jumlah pengurangan risiko yang disediakan agar sesuai secara presisi dengan jumlah pengurangan risiko yang benar-benar dibutuhkan oleh proses.

Kelemahan dari fleksibilitas yang disediakan oleh pengambilan keputusan berbasis risiko adalah besarnya kompleksitas yang kemudian diperkenalkan ke dalam proses perancangan. Untuk membuat keputusan berbasis risiko, seseorang perlu memahami risiko dari proses kimia yang bersangkutan—suatu pencapaian yang tidak mudah dan biasanya berada di luar 'zona nyaman' perancang SIS tradisional—serta harus memahami secara mendalam rincian rekayasa keandalan (*reliability engineering*) sebagaimana diterapkan pada perancangan SIS modern.

Pada tahun-tahun setelah dirilisnya standar berbasis kinerja yang mendefinisikan rekayasa SIS, banyak buku, standar, laporan teknis, dan makalah telah ditulis tentang proses Rekayasa SIS (termasuk buku dan makalah yang ditulis oleh para penulis buku ini).

PRAKATA (LANJUTAN)

Para penulis buku ini berkesimpulan bahwa akan sangat berharga untuk menyarikan seluruh informasi tersebut ke dalam format buku panduan (*handbook*) ringkas yang memungkinkan para praktisi sehari-hari memiliki referensi cepat terhadap poin-poin paling penting dari proses perancangan sistem keselamatan.

Buku ini menyajikan diskusi yang sangat praktis mengenai siklus hidup keselamatan SIS dan menyajikannya dengan cara yang condong pada bantuan dalam pelaksanaan tugas-tugas teknis di lapangan, tanpa memperpanjang landasan teoretis dari persamaan matematika dan data yang telah disajikan dalam buku-buku lain dan laporan teknis rujukan.

Selain itu, buku ini mencerminkan metodologi yang paling terbukti dan diterima secara luas untuk melaksanakan tugas-tugas rekayasa, terutama di area di mana standar memberikan fleksibilitas besar kepada pengguna untuk memilih dari banyak opsi guna mematuhi standar tersebut.

Sebagai contoh, tugas memilih tingkat integritas keselamatan (*Safety Integrity Level* - SIL) dapat dilakukan dengan memanfaatkan berbagai metode termasuk grafik risiko (*risk graphs*) dan analisis lapisan perlindungan (*layer of protection analysis* - LOPA). Namun karena sebagian besar industri telah memilih untuk menggunakan LOPA, hanya metodologi LOPA yang dieksplorasi secara terperinci dalam buku ini.

Buku ini juga berfokus pada aspek rekayasa SIS dari siklus hidup keselamatan, sementara tugas-tugas penting yang berada di luar ranah rekayasa instrumentasi dan kendali diserahkan kepada disiplin ilmu lain. Sebagai contoh, analisis bahaya proses (PHA) yang baik sangat penting untuk mengidentifikasi di mana perlindungan berinstrumen seperti SIS diperlukan, tetapi pelaksanaan PHA biasanya bukan merupakan tanggung jawab insinyur instrumentasi dan kendali, dan oleh karena itu dibahas secara prinsip namun tidak dikembangkan secara mendalam.

Para penulis buku ini berharap Anda menikmati isi materi buku ini dan menemukan informasi di dalamnya mendidik serta bermanfaat secara langsung dalam aktivitas pekerjaan sehari-hari.

DAFTAR ISI

Bab / Bagian	Sub-Bagian & Topik Bahasan	Halaman Ref
Tentang Penulis	Profil Kevin J. Mitchell, Peter Hereña, Todd Longendelpher, Matthew Kuhn	v
Prakata	Latar Belakang, Pendekatan Berbasis Kinerja & Tujuan Panduan	vii
Daftar Isi	Struktur Sistematis Buku Panduan Rekayasa SIS	ix
Bab 1: Pendahuluan	Mengapa Saya Memerlukan SIS?	1
	Apa itu SIS? (Perbedaan Mendasar SIS vs BPCS)	2
	Perundang-undangan dan Regulasi (OSHA PSM & EPA RMP)	4
	Mengapa Mengembangkan Standar SIS? (Pelajaran Investigasi Bencana)	5
	Apa yang Diperkirakan oleh Standar? (Klausul Grandfathering)	7
Bab 2: Siklus Hidup Keselamatan	The Safety Lifecycle menurut IEC 61511 & Alur Kerja Kenexis	9
Bab 3: Desain Proses Konseptual	Informasi Keselamatan Proses (Process Safety Information - PSI)	13
Bab 4: Analisis Bahaya Proses	Process Hazards Analysis (PHA), Metodologi HAZOP & Safeguards	14
Bab 5: Definisi SIF	Karakterisasi Safety Instrumented Functions & SIF List	18
Bab 6: Pemilihan SIL	Mendefinisikan SIL, PFDavg, Availability, & RRF	22
	Proses Pemilihan SIL & Representasi Risiko Grafis	24
	Merepresentasikan Risiko Ditoleransi (Matriks Risiko & TMEL)	26
	Layer of Protection Analysis (LOPA Implisit & Eksplisit)	30
Bab 7: Desain Konseptual & Verifikasi	Parameter Penentu SIL, Pemilihan Komponen, Toleransi Kesalahan	35

DAFTAR ISI (LANJUTAN)

Bab / Bagian	Sub-Bagian & Topik Bahasan	Halaman Ref
Bab 7: Verifikasi SIL (Lanjutan)	Interval Uji, Common Cause, Diagnostik, Persamaan PFD/STR	40
Bab 8: Spesifikasi SRS	29 Persyaratan Wajib Safety Requirements Specifications	44
Bab 9: Desain Rinci & Spesifikasi	Spesifikasi Teknis, Lembar Loop, Pengkabelan, Pemrograman PLC	49
Bab 10: Pengembangan Prosedur	Prosedur Operasi, Pemeliharaan, Uji Penuh & Filosofi Bypass	50
Bab 11: Konstruksi & Komisioning	Pengadaan, Pemasangan Fisik, FAT, dan SAT Lapangan	53
Bab 12: Uji Penerimaan PSAT	Pre-Startup Acceptance Testing & Validasi Kepatuhan SRS	54
Bab 13: Operasi & Pemeliharaan	Rutinitas Operasional, Tanggapan Alarm & Perbaikan Subsistem	56
Bab 14: Manajemen Perubahan	Prosedur MOC, Rekalkulasi Keandalan SIL & Revalidasi 5 Tahun	57
Bab 15: Kesimpulan	Rangkuman Prinsip Utama Desain Berbasis Kinerja	59
Lampiran A — Akronim	Daftar Singkatan Teknis Internasional Rekayasa SIS	61
Lampiran B — Definisi	Glosarium Terminologi Keselamatan Fungsional Lengkap	63
Lampiran C — Frekuensi Pemicu	Tabel Frekuensi Initiating Events Tipikal Industri Proses	71
Lampiran D — Lapisan Proteksi	Kredit Pengurangan Risiko IPL, Operator Response, dan CMS	73
Lampiran E — Persamaan Sederhana	Rumus Lengkap PFDavg, STR, Voting Kelompok, dan Arsitektur MooN	82
Lampiran F — Toleransi Kesalahan	Tabel Batasan Arsitektural Perangkat Tipe A & B (IEC 61508/61511)	97
Lampiran G — Data Komponen	Pangkalan Data Laju Kegagalan Sensor, Antarmuka, dan Final Element	102
Lampiran H — Kriteria Risiko	Risiko Individu (IR), Rentang ALARP, Kalibrasi TMEL & Matriks Risiko	106
Lampiran I — Referensi	Daftar Standar Industri, Regulasi Pemerintah, dan Buku Rujukan	115

BAB 1: PENDAHULUAN

Sistem Berinstrumen Keselamatan (*Safety Instrumented Systems* - SIS) adalah perlindungan rekayasa yang paling fleksibel dan salah satu yang paling umum digunakan di pabrik proses saat ini. Perancangan SIS, sesuai dengan praktik saat ini, adalah proses berbasis risiko di mana peralatan yang dipilih serta prosedur pemeliharaan dan pengujian terkait disesuaikan dengan persyaratan spesifik dari suatu aplikasi. Pendekatan berbasis risiko ini menghasilkan desain superior yang memberikan pengurangan risiko yang dipersyaratkan sekaligus meminimalkan biaya.

Perancangan SIS telah menjadi proses yang lebih kompleks karena kebutuhan untuk memahami lebih dari sekadar rekayasa instrumentasi dan kendali tradisional. Selain konsep-konsep dasar, perancangan SIS membutuhkan keahlian dalam menganalisis risiko proses yang dikendalikan (yang tentunya memerlukan pemahaman tentang proses itu sendiri) untuk menetapkan target desain, dan juga keahlian dalam rekayasa keandalan untuk memastikan bahwa target yang dipilih telah terpenuhi.

Tujuan dari buku ini adalah untuk memberikan tinjauan singkat tentang Siklus Hidup Keselamatan (*Safety Lifecycle*) yang digunakan untuk merancang SIS, bersama dengan informasi umum untuk membantu dalam melakukan tugas-tugas yang didefinisikan dalam siklus hidup keselamatan. Ini termasuk tabel data, daftar definisi dan akronim, persamaan matematika, dan penjelasan untuk menggunakan sumber daya ini.

Mengapa Saya Memerlukan SIS?

Pabrik proses menciptakan nilai dengan mengubah bahan mentah menjadi produk bernilai ekonomi tinggi. Proses yang digunakan untuk melakukan konversi ini sering kali menciptakan kondisi berbahaya yang dapat mengakibatkan konsekuensi signifikan jika proses tersebut tidak dikendalikan secara memadai. Kondisi-kondisi berbahaya tersebut meliputi:

- **Bahan Mudah Terbakar (Flammable Materials):** Gas dan cairan hidrokarbon yang rentan memicu kebakaran dan ledakan.
- **Bahan Beracun (Toxic Materials):** Bahan kimia berbahaya yang membahayakan pekerja dan masyarakat sekitar jika terlepas.
- **Tekanan Tinggi (High Pressures):** Potensi pelepasan energi katastrofik dan pecahnya peralatan proses.
- **Suhu Tinggi (High Temperatures):** Memicu degradasi mekanis material atau kebakaran spontan.

Pengendalian risiko yang ditimbulkan oleh pabrik proses dilakukan melalui kombinasi dari **Kendali Administratif (Administrative Controls)** dan **Perlindungan Rekayasa (Engineered Safeguards)**. Safety Instrumented System (SIS) adalah salah satu perlindungan yang digunakan dalam pemrosesan minyak bumi dan kimia modern untuk mengurangi risiko hingga ke tingkat yang dapat ditoleransi. SIS merupakan kendali rekayasa, dan berpadu dengan perlindungan rekayasa lainnya serta kendali administratif untuk mencapai keseimbangan keseluruhan perlindungan yang mengurangi risiko ke tingkat yang dapat diterima.

Aplikasi SIS yang umum mencakup sistem penghentian darurat (*emergency shutdown systems* - ESD), sistem manajemen pembakar (*burner management systems* - BMS) untuk boiler dan tungku pemanas lainnya; sistem perlindungan tekanan integritas tinggi (*high integrity pressure protection systems* - HIPPS) di fasilitas pengolahan minyak bumi atau kimia, serta aplikasi spesifik industri lainnya.

Apa itu SIS?

Safety Instrumented System adalah sistem instrumentasi dan kendali yang mendeteksi kondisi proses di luar kendali, dan secara otomatis mengembalikan proses ke kondisi yang aman. Sistem ini merupakan garis pertahanan terakhir atau mendekati garis pertahanan terakhir terhadap bahaya proses kimia, dan sistem ini **bukan** merupakan bagian dari Sistem Kendali Proses Dasar (*Basic Process Control System* - BPCS). Status sebagai garis pertahanan terakhir inilah yang membedakan Safety Instrumented System dari Basic Process Control System, yang digunakan untuk kendali proses regulasi normal sehari-hari.

Gambar 1 menunjukkan bagaimana Safety Instrumented System berbeda dari Basic Process Control System, atau BPCS. Dalam contoh ini, tekanan adalah potensi bahaya. Tekanan biasanya dikendalikan oleh loop kendali regulasi normal, yang ditunjukkan sebagai Basic Process Control System, yang memodulasi katup kendali tekanan (PV-101) berdasarkan pembacaan pemancar tekanan (PT-101) melalui pengontrol (PIC-101).

ILUSTRASI SISTEM: GAMBAR 1 — SIS VERSUS BPCS

GAMBAR 1: PERBANDINGAN ARSITEKTURAL ANTARA SIS DAN BPCS

- **Sistem Kendali Proses Dasar (BPCS):**

Pemancar Tekanan Proses (PT-101) → Pengendali Indikator Tekanan (PIC-101) → Katup Kendali Tekanan Regulasi (PV-101). Sistem ini memodulasi pembukaan katup secara kontinu untuk menjaga tekanan operasional normal.

- **Sistem Berinstrumen Keselamatan (SIS):**

Pemancar Tekanan Keselamatan Mandiri (PT-102) → Logic Solver Keselamatan Terdedikasi (USC-102) → Katup Penghenti Aliran Darurat (UV-102). Sistem ini berada dalam posisi siaga dan hanya bertindak menutup aliran saat tekanan melampaui batas aman.

Prinsip Esensial Kemandirian: Komponen BPCS dan SIS terpisah secara fisik dan fungsional. Ini mencakup komponen sensor, logic solver, dan elemen kendali akhir. SIS umumnya independen dari BPCS guna memastikan bahwa kondisi apa pun yang mengakibatkan parameter proses di luar kendali di BPCS akan tetap dilindungi secara aman oleh SIS, terlepas dari apakah BPCS berfungsi atau mengalami kegagalan.

Fungsi penghentian darurat tekanan tinggi (high-pressure shutdown function) yang independen diimplementasikan dalam Safety Instrumented System. Sistem ini independen sejauh komponen yang digunakan dalam BPCS dan SIS terpisah, baik secara fisik maupun fungsional.

Tiga Komponen Pembentuk SIS

SIS mencakup tiga jenis komponen utama yang bekerja secara sinergis:

1. **Komponen Sensor:** Perangkat instrumen lapangan yang mengukur variabel proses kritis (misalnya tekanan, suhu, level cairan, laju aliran, deteksi api) dan mengirimkan sinyal ke logic solver.
2. **Komponen Logic Solver:** Pengendali logika yang memproses sinyal masukan dari sensor, mengevaluasi kondisi terhadap batas trip keselamatan yang telah diprogram, dan memerintahkan tindakan keluaran. Logic solver dapat berupa sistem yang dapat diprogram (*programmable electronic system* seperti Safety PLC) atau sistem non-programmable (seperti relai kabel-keras / *hard-wired relays*).
3. **Elemen Kendali Akhir (Final Control Elements):** Perangkat fisik yang secara langsung melakukan tindakan koreksi di proses untuk mencapai kondisi aman, seperti katup on-off penutup darurat (*shutdown valves*), katup ventilasi (*vent valves*), atau kontaktor pemutus daya motor pompa.

Secara bersama-sama, komponen-komponen ini membentuk Safety Instrumented System, yang mendeteksi kondisi proses di luar kendali, dan secara otomatis mengembalikan proses ke kondisi yang aman, terlepas dari berfungsinya Basic Process Control System.

Perundang-undangan dan Regulasi

Persyaratan hukum untuk Safety Instrumented Systems di Amerika Serikat berasal dari berbagai peraturan manajemen keselamatan proses, serta undang-undang yang berfungsi sebagai dasar dari peraturan tersebut. Meskipun pembahasan dalam buku panduan ini berfokus pada Amerika Serikat, kerangka kerja yang serupa digunakan di sebagian besar wilayah di dunia.

Peraturan perundangan mewajibkan kepatuhan terhadap **praktik rekayasa yang diakui dan diterima secara umum (Recognized And Generally Accepted Good Engineering Practices - RAGAGEP)** untuk kendali-kendali kritis keselamatan, termasuk SIS. Peraturan ini mewajibkan RAGAGEP untuk memastikan bahwa industri mematuhi norma-norma operasi yang telah ditetapkan untuk industri tersebut.

Peraturan dan standar yang berlaku untuk Safety Instrumented Systems berawal pada akhir 1980-an ketika regulator industri, termasuk Administrasi Keselamatan dan Kesehatan Kerja AS (OSHA), serta Badan Perlindungan Lingkungan AS (EPA), menyimpulkan bahwa kinerja industri sehubungan dengan pencegahan bahaya besar tidak memadai.

Hal ini melahirkan Standar Manajemen Keselamatan Proses (*Process Safety Management - PSM*) oleh OSHA, yang diundangkan pada tahun 1992 di bawah **29 CFR 1910.119**. Pada tahun 1996, EPA mengundang *Accidental Release Prevention Program*, atau **40 CFR Part 68**, yang juga disebut *Risk Management Program (RMP)*. Standar peraturan ini secara substansial serupa dalam persyaratannya dengan Standar Manajemen Keselamatan Proses OSHA. Sebagian besar sebagai tanggapan terhadap peraturan ini, International Society for Automation (ISA) serta International Electrotechnical Commission (IEC) mengembangkan standar industri untuk sistem kendali kritis keselamatan guna memberikan panduan terperinci tentang cara mematuhi peraturan OSHA dan EPA tersebut.

Mengapa Mengembangkan Standar SIS?

Sebagaimana dicatat sebelumnya, peraturan mengenai keselamatan proses muncul karena adanya persepsi mengenai ketidakcukupan kebijakan dan prosedur mengenai keselamatan di industri proses. Banyak pelajaran yang telah dipetik dari investigasi kecelakaan besar menunjukkan kurangnya keselamatan fungsional (*functional safety*) sebagai penyebab utama hilangnya nyawa manusia, serta kerusakan properti lainnya dan insiden kehilangan produksi di industri minyak bumi dan kimia.

Setelah meninjau sejarah kecelakaan di industri proses sehubungan dengan skenario di mana kegagalan SIS berkontribusi terhadap insiden, beberapa tema kelemahan umum berkembang:

- **Sering kali tidak ada SIS yang dipasang:** Pada banyak kasus kecelakaan fatal, tidak ada sistem otomatis yang dipasang padahal dapat dibuktikan bahwa otomasi sangat penting untuk keselamatan. Bahkan, dalam banyak kasus ini, tidak ada studi untuk menilai risiko yang ditimbulkan oleh proses yang dilakukan sama sekali.
- **Proses pengambilan keputusan yang buruk:** Digunakan proses pengambilan keputusan yang lemah untuk menentukan kapan keselamatan harus diotomatisasi versus kapan diserahkan kepada sistem lain. Ini termasuk keputusan keliru yang menganggap intervensi operator atau kendali proses dasar (BPCS) sudah memadai sebagai pengganti sistem instrumen terpisah yang didedikasikan untuk keselamatan.
- **Pemilihan peralatan yang meragukan:** Riwayat insiden juga menunjukkan pemilihan peralatan yang dipertanyakan sebagai penyebab lain dari kurangnya keselamatan fungsional yang mengakibatkan kecelakaan dan kerugian besar.
- **Kurangnya redundansi dan diagnostik:** Kurangnya redundansi arsitektural dan ketiadaan fitur diagnostik pada SIS merupakan penyebab sering lainnya.
- **Metode dan frekuensi pengujian yang buruk:** Metode pengujian yang buruk dan penentuan frekuensi yang tidak tepat untuk pengujian fungsional berkala juga menjadi penyebab banyak kerugian terkait keselamatan fungsional, di samping teknik pembypasan (*bypassing*) yang tidak tepat dan pemilihan peralatan yang keliru.

Secara bersama-sama, penyebab-penyebab ini menunjukkan kebutuhan mendesak akan praktik-praktik yang ditingkatkan untuk memastikan manajemen keselamatan fungsional tercapai secara efektif di industri.

Implikasi Data Kecelakaan terhadap Rekayasa SIS

Implikasi dari data kecelakaan industri terhadap rekayasa Sistem Berinstrumen Keselamatan tercantum di bawah ini, dan telah dimasukkan ke dalam standar **IEC 61511 (ISA 84.00.01)** untuk desain dan implementasi SIS:

- **Kriteria Alarm vs Otomasi:** Kita harus memilih kriteria yang jelas kapan harus menggunakan alarm dan penilaian operator versus kapan harus menggunakan penghentian otomatis (automatic shutdown) dengan SIS, ketika batas operasi aman yang telah ditentukan sebelumnya telah dilanggar dan risikonya cukup signifikan sehingga tindakan manual tidak lagi memadai.
- **Strategi Pertahanan Berlapis (Defense in Depth):** Penting untuk diakui bahwa guna mencegah bahaya besar, strategi pertahanan berlapis yang melibatkan banyak lapisan perlindungan atau perlindungan yang independen diperlukan untuk mencegah kecelakaan besar. Kita menyadari hal ini karena dalam beberapa kasus, perlindungan dapat gagal sehingga menghasilkan permintaan beban (demand) pada SIS.
- **Spesifikasi SIS yang Memadai:** Kita juga mengakui bahwa spesifikasi SIS yang tidak memadai sering kali merupakan penyebab mendasar dari kecelakaan di mana keselamatan fungsional tidak tercapai. Ini mencakup spesifikasi komponen, arsitektur sistem, pengujian diagnostik, serta uji pembuktian fungsional (proof tests).
- **Pengendalian Bypass:** Dalam banyak kasus, data kecelakaan menunjukkan bahwa pembypasan (bypass) dan penonaktifan sistem kritis keselamatan juga merupakan kontributor signifikan terhadap riwayat kasus kecelakaan.

Menanggapi faktor-faktor ini, serta pendorong lain di industri, ISA dan IEC mengembangkan Standar untuk SIS yang mengatasi banyak penyebab tersebut. Standar ini menyediakan **Siklus Hidup Keselamatan (Safety Lifecycle)** sebagai fondasi untuk menangani keselamatan fungsional. Siklus Hidup Keselamatan mencakup identifikasi, desain, pengujian, pemeliharaan, dan manajemen perubahan. Ini adalah pendekatan 'dari buaian hingga liang lahat' (*cradle-to-grave*) terhadap keselamatan yang menangani masalah mendasar yang dapat terjadi pada setiap langkah selama desain, operasi, pemeliharaan, dan perubahan sistem.

Di AS, OSHA mewajibkan fasilitas industri yang dicakup oleh peraturan Manajemen Keselamatan Proses (PSM) untuk mematuhi praktik rekayasa yang diakui dan diterima secara umum (RAGAGEP). ISA mengajukan pertanyaan kepada OSHA mengenai apakah standar mereka, ISA 84.00.01 untuk Safety Instrumented Systems, mematuhi persyaratan OSHA untuk PSM. OSHA, dalam menanggapi pertanyaan ini, setuju bahwa standar ISA merupakan salah satu contoh kepatuhan terhadap persyaratan integritas mekanis untuk kendali kritis keselamatan dan sistem shutdown. Sejak saat itu sebagian besar perusahaan operasi industri proses telah sepakat bahwa siklus hidup keselamatan yang terkandung dalam IEC 61511 (ISA 84.00.01) adalah metodologi optimal untuk mengelola desain dan implementasi SIS.

Apa yang Dipersyaratkan oleh Standar?

Tidak seperti standar dan praktik lain yang digunakan sebelum dirilisnya IEC 61511 (ISA 84.00.01), standar ini tidak memberikan serangkaian aturan baku yang mendikte secara rinci bagaimana suatu sistem harus dirancang. Sebaliknya, standar ini menetapkan kerangka kerja untuk memungkinkan setiap pengguna individu menentukan apa yang tepat untuk situasi spesifik mereka. Ini adalah **pendekatan berbasis kinerja (performance-based approach)** terhadap SIS, bukan pendekatan preskriptif.

Dengan kata lain, standar tidak mengambil posisi mendiktekan: jenis komponen apa yang wajib dibeli, jenis arsitektur apa yang harus dipasang, jenis pengujian diagnostik apa yang harus digunakan, seberapa sering pengujian dilakukan, dan bagaimana menguji sistem berinstrumen keselamatan secara fungsional? Sebaliknya, standar menetapkan pendekatan penetapan tujuan kinerja (*goal-setting approach*). Pengguna harus memilih target kinerja yang sesuai untuk suatu fungsi sistem berinstrumen keselamatan, dan merancang sistem tersebut sedemikian rupa untuk mencapai tingkat kinerja tersebut.

Standar mendefinisikan Siklus Hidup Keselamatan dengan beberapa langkah yang harus diambil untuk mencapai keselamatan fungsional dalam pendekatan 'Cradle-to-Grave' untuk manajemen keselamatan fungsional. Standar mewajibkan pemilihan dan pencapaian tingkat kinerja target. Tingkat kinerja utama tersebut adalah **Safety Integrity Level (SIL)**, yang dipilih untuk setiap Safety Instrumented Function dalam SIS menggunakan pendekatan berbasis risiko. SIL adalah metrik fundamental untuk semua pengambilan keputusan berikutnya tentang perancangan SIS.

Ketentuan Peralatan Lama (Grandfathering Clause)

Badan standar (IEC dan ISA) dan regulator pemerintah (misalnya OSHA di AS) umumnya sepakat mengenai pendekatan yang berbeda untuk peralatan yang ada (*existing equipment*) versus desain rekayasa baru. Praktik rekayasa yang baik untuk desain baru mencakup kepatuhan terhadap standar rekayasa yang diakui dan diterima secara umum, termasuk IEC 61511. Namun, peralatan yang ada dapat diperlakukan sedikit berbeda, tergantung pada bagaimana masing-masing perusahaan memutuskan untuk menangani pendekatan terhadap klausul kakek (*grandfathering*) dari peralatan yang ada.

Klausul 'Grandfathering' dari peralatan yang ada diizinkan di AS di bawah Standar Manajemen Keselamatan Proses OSHA, dan juga diizinkan di bawah versi ISA 84.00.01 dari standar SIS IEC 61511. Standar menyatakan: *'Untuk sistem yang ada, yang dirancang dan dibangun sesuai dengan kode, standar, atau praktik sebelum diterbitkannya standar ini, pemilik/operator harus menentukan, dan memastikan apakah peralatan dirancang, dirawat, diinspeksi, diuji, dan dioperasikan dengan cara yang aman.'*

Dengan kata lain, standar tidak mewajibkan bahwa peralatan lama yang dirancang dengan standar rekayasa sebelumnya harus dirombak agar memenuhi standar SIS saat ini; melainkan sebuah sistem harus ada untuk memverifikasi bahwa peralatan tersebut dioperasikan, diuji, diinspeksi, dirawat, dan dirancang sesuai dengan standar keselamatan pada masa pembuatannya. Keberterimaan klausul 'grandfathering' dapat bervariasi tergantung pada yurisdiksi dan lokasi di mana SIS digunakan.

BAB 2: SIKLUS HIDUP KESELAMATAN (THE SAFETY LIFECYCLE)

Gambar 2 menyajikan Siklus Hidup Keselamatan SIS sebagaimana ditentukan dalam standar IEC 61511 (ISA 84.00.01). Siklus Hidup Keselamatan mencakup sejumlah langkah spesifik mulai dari desain konseptual hingga operasi, pemeliharaan, pengujian berkala, dan bahkan dekomisioning, untuk menangani keselamatan di sepanjang masa pakai Sistem Berinstrumen Keselamatan dalam proses perminyakan atau kimia.

STRUKTUR RESMI SIKLUS HIDUP IEC 61511

GAMBAR 2: SIKLUS HIDUP KESELAMATAN SISTEM MENURUT STANDAR IEC 61511

- **Aktivitas Manajemen & Verifikasi Menyeluruh (Sepanjang Siklus Hidup):**

- Manajemen Keselamatan Fungsional, Asesmen Keselamatan Fungsional, dan Audit (Klausul 5)
- Struktur dan Perencanaan Siklus Hidup Keselamatan (Klausul 6.2)
- Verifikasi Teknis pada Setiap Tahapan Siklus Hidup (Klausul 7, 12.4, 12.7)

- **Tahapan Utama Alur Eksekusi Siklus Hidup:**

1. Penilaian Bahaya dan Risiko (*Hazard and Risk Assessment* - Klausul 8)
2. Alokasi Fungsi Keselamatan ke Lapisan Perlindungan (*Allocation of Safety Functions to Protection Layers* - Klausul 9)
3. Spesifikasi Persyaratan Keselamatan SIS (*Safety Requirements Specification for the SIS* - Klausul 10 & 12)
4. Desain dan Rekayasa SIS (Klausul 11 & 12) berdampingan dengan Desain & Pengembangan Sarana Reduksi Risiko Lainnya (Klausul 9)
5. Instalasi, Komisioning, dan Validasi Lapangan (Klausul 14 & 15)
6. Operasi dan Pemeliharaan (Klausul 16)
7. Modifikasi Sistem (Klausul 17)
8. Dekomisioning / Penonaktifan Sistem (Klausul 18)

Langkah pertama dalam Siklus Hidup Keselamatan adalah '**Hazard and Risk Assessment**' (**Penilaian Bahaya dan Risiko**). Dasar pemikiran dari langkah ini adalah bahwa untuk merancang Sistem Berinstrumen Keselamatan secara memadai, kita harus memahami sepenuhnya bahaya-bahaya yang ingin dicegah oleh sistem tersebut. Jika kita tidak memiliki pemahaman yang memadai tentang bahaya-bahaya tersebut, sistem dapat dirancang secara tidak tepat sehubungan dengan jenis komponen yang digunakan, jenis redundansi atau arsitektur yang dipilih, dan faktor-faktor lain yang berkaitan dengan desain rekayasa SIS.

Langkah berikutnya, '**Allocation of Safety Functions**' (**Alokasi Fungsi Keselamatan**), melibatkan penetapan tingkat integritas tertentu untuk masing-masing perlindungan yang digunakan dalam proses, termasuk Fungsi Berinstrumen Keselamatan (SIF), serta fungsi non-instrumen untuk mencapai tingkat keselamatan keseluruhan yang dapat diterima oleh perusahaan yang mengoperasikan proses tersebut.

Tahapan Siklus Hidup Keselamatan (Lanjutan)

Langkah ketiga dalam Siklus Hidup Keselamatan adalah '**Safety Requirement Specifications**' (**Spesifikasi Persyaratan Keselamatan - SRS**). Ini adalah langkah yang sangat penting untuk mencapai keselamatan fungsional secara keseluruhan. Dalam desain konseptual suatu proses, kita harus memastikan bahwa persyaratan keselamatan telah ditentukan secara memadai sebelum melanjutkan ke langkah-langkah lain dalam siklus hidup desain rekayasa, termasuk desain terperinci, konstruksi, instalasi, dan komisioning. Langkah ini adalah tempat di mana tujuan dan sarana untuk mencapai tujuan tersebut didefinisikan. Setelah selesai, Spesifikasi Persyaratan Keselamatan (SRS) membentuk dasar untuk semua kegiatan desain terperinci dan validasi berikutnya.

Langkah-langkah setelah SRS (yang sering dilakukan secara paralel oleh kelompok yang berbeda) adalah '**Detail Design and Engineering**' (**Desain dan Rekayasa Terperinci**) untuk SIS dan '**Design and Development of Other Means of Risk Reduction**' untuk perlindungan non-SIS lainnya. Tahap ini adalah tempat di mana informasi dalam SRS diperluas menjadi dokumentasi yang lebih terperinci yang digunakan untuk pembelian peralatan, konfigurasi peralatan, dan instalasi fisik. Ini mencakup tugas-tugas seperti membuat daftar peralatan, diagram tata letak kabinet, diagram pengkabelan internal, diagram pengkabelan interkoneksi, dan program PLC keselamatan.

Setelah desain terperinci dari SIS selesai, langkah berikutnya adalah '**Installation, Commissioning, and Validation**' (**Instalasi, Komisioning, dan Validasi**) dari Sistem Berinstrumen Keselamatan itu sendiri. Tahap ini melibatkan uji penerimaan pabrik (*Factory Acceptance Testing - FAT*), instalasi fisik logic solver SIS dan semua instrumentasi lapangan, komisioning perangkat-perangkat tersebut, dan langkah validasi yang akan mencakup uji penerimaan lokasi (*Site Acceptance Testing - SAT*) dan uji penerimaan pra-startup (*Pre-Startup Acceptance Testing - PSAT*).

Setelah SIS dipasang dan beroperasi, fase siklus hidup yang berbeda dimulai di mana tim desain mengalihkan tanggung jawab peralatan kepada tim operasi dan pemeliharaan dari perusahaan operasi. Tahap '**Operation and Maintenance**' (**Operasi dan Pemeliharaan**) melibatkan interaksi rutin sehari-hari dengan sistem yang berfungsi. Selama fase ini, staf operasi akan menanggapi alarm sistem yang nyata menggunakan prosedur yang ditulis untuk tujuan tersebut. Selain itu, bagian pemeliharaan akan memperbaiki sistem dalam menanggapi kesalahan yang terdeteksi dan juga melakukan pengujian fungsional berkala (*proof testing*) untuk memastikan sistem beroperasi dengan baik.

Langkah '**Decommissioning**' (**Penonaktifan**) dan '**Modification**' (**Modifikasi**) memiliki sifat yang sangat mirip. Jika perubahan pada SIS atau pada proses yang dikendalikan terjadi, tindakan harus diambil agar kemampuan SIS dalam menyediakan jumlah pengurangan risiko yang dipersyaratkan tidak terganggu. Selama fase ini persyaratan Manajemen Perubahan (*Management of Change - MOC*) berlaku untuk memastikan bahwa ketika perubahan dilakukan pada proses di luar SRS, perubahan tersebut dianalisis secara memadai untuk potensi bahaya sebelum menerapkan perubahan tersebut. Dekomisioning adalah bentuk khusus dari modifikasi di mana analisis peralatan yang dihapus harus dianalisis sehubungan dengan dampaknya terhadap peralatan yang akan tetap beroperasi.

Ada tiga langkah lain dari Siklus Hidup Keselamatan yang terjadi di seluruh rentang umur SIS: Manajemen Keselamatan Fungsional dan Asesmen/Audit Keselamatan Fungsional, Struktur dan Perencanaan Siklus Hidup Keselamatan, serta Verifikasi. Standar mewajibkan bahwa pada setiap langkah, kita memverifikasi bahwa keluaran dari setiap langkah dalam Siklus Hidup Keselamatan telah tercapai dan konsisten dengan masukan untuk langkah tersebut.

Alur Kerja Siklus Hidup Rekayasa Kenexis

Kenexis telah menyiapkan siklus hidup perancangan SIS tipikal dalam representasi yang sedikit berbeda yang mengasosiasikan dirinya lebih dekat dengan langkah-langkah aktual yang diambil selama perancangan suatu SIS di industri. Siklus hidup terapan ini ditunjukkan pada Gambar 3.

DIAGRAM ALIR PROYEK SIS KENEXIS

GAMBAR 3: ALUR KERJA SIKLUS HIDUP DESAIN SIS KENEXIS (KENEXIS SAFETY LIFECYCLE)

- **Fase 1: Analisis dan Definisi Front-End**
 - Desain Proses Konseptual (*Conceptual Process Design*)
 - Analisis Bahaya Proses (*Process Hazards Analysis - PHA*)
 - Definisi Fungsi Berinstrumen Keselamatan (*SIF Definition*)
 - Pemilihan Tingkat Integritas Keselamatan (*SIL Selection*)
- **Fase 2: Desain Konseptual & Verifikasi Teknis**
 - Desain Konseptual (*Conceptual Design*)
 - Verifikasi SIL (*SIL Verification Calculations*)
 - Spesifikasi Persyaratan Desain (*Design Specifications / SRS*)
- **Fase 3: Implementasi, Instalasi, & Prosedur**
 - Pengembangan Prosedur (*Procedure Development*)
 - Konstruksi, Instalasi, dan Komisioning (*Construction, Installation, and Commissioning*)
 - Pengujian Penerimaan Pra-Startup (*Pre-Startup Acceptance Testing - PSAT*)
- **Fase 4: Operasi Berkelanjutan & Pengelolaan Siklus Hidup**
 - Operasi, Pemeliharaan, dan Pengujian Berkala (*Operation, Maintenance, and Testing*)
 - Manajemen Perubahan (*Management of Change - MOC*)

Langkah-langkah dalam Siklus Hidup Keselamatan Kenexis lebih granular daripada apa yang ditunjukkan dalam standar IEC 61511, dan dengan demikian berfungsi lebih efektif sebagai diagram alir pelaksanaan proyek SIS dunia nyata daripada representasi siklus hidup dalam standar formal. Setiap tahapan menghasilkan dokumen luaran (deliverable) terukur yang memicu tahapan rekayasa berikutnya secara berurutan dan terverifikasi.

BAB 3: DESAIN PROSES KONSEPTUAL

KERANGKA KERJA DESAIN PROSES KONSEPTUAL

ALUR KERJA TAHAP DESAIN PROSES KONSEPTUAL:

- **Masukan (Input):** Kebutuhan Bisnis, Karakteristik Kimia Bahan Baku, Kapasitas Produksi Pabrik.
- **Tugas Rekayasa (Task):** Desain Proses Konseptual (Conceptual Process Design).
- **Perangkat (Tools):** Simulator Proses Termodinamika, Neraca Massa & Energi, Templat Desain Lisensor.
- **Luaran (Deliverable):** Informasi Keselamatan Proses (Process Safety Information - PSI) → Masukan untuk Analisis Bahaya Proses (PHA).

Desain Proses Konseptual adalah titik awal dari Siklus Hidup Keselamatan. Meskipun terdaftar sebagai langkah dalam IEC 61511, langkah ini biasanya dianggap berada di luar lingkup (*out-of-scope*) untuk rekayasa Sistem Berinstrumen Keselamatan itu sendiri. Langkah ini dimasukkan dalam siklus hidup keselamatan sebagai referensi untuk tugas yang mengarah ke standar, dan menyediakan masukan untuk tugas siklus hidup keselamatan pertama, tetapi standar tidak memberikan persyaratan khusus pada desain proses konseptual.

Desain proses konseptual dikembangkan baik oleh perusahaan operasi itu sendiri, atau dilisensikan dari perusahaan yang mengkhususkan diri dalam pengembangan teknologi proses (lisensor proses). Proses desain konseptual akan menghasilkan dokumen-dokumen desain yang akan membentuk dasar untuk rekayasa selanjutnya, dan juga membentuk dasar dari **Informasi Keselamatan Proses (Process Safety Information - PSI)** yang akan digunakan sebagai masukan utama untuk analisis bahaya proses (PHA).

Informasi Keselamatan Proses (PSI) mencakup informasi yang sangat penting bagi analisis keselamatan, seperti:

- Diagram Perpipa dan Instrumentasi (*Piping and Instrumentation Diagrams - P&ID*)
- Diagram Alir Proses (*Process Flow Diagrams - PFD*) disertai kondisi operasi desain
- Neraca massa dan energi (*heat and mass balances*)
- Diagram blok aliran (*block flow diagrams*)
- Batas-batas operasi yang aman (*safe operating limits*) dan konsekuensi penyimpangannya
- Spesifikasi bahan konstruksi metalurgi dan data bahaya bahan kimia (MSDS / SDS)

BAB 4: ANALISIS BAHAYA PROSES (PROCESS HAZARDS ANALYSIS)

KERANGKA KERJA ANALISIS BAHAYA PROSES

ALUR KERJA TAHAP ANALISIS BAHAYA PROSES:

- **Masukan (Input):** Informasi Keselamatan Proses (PSI), P&ID, PFD, Neraca Massa, Filosofi Kontrol.
- **Tugas Rekayasa (Task):** Analisis Bahaya Proses (Process Hazards Analysis - PHA).
- **Perangkat (Tools):** Templat Kenexis PHA, Perangkat Lunak PHA-Pro / Perangkat Lunak Fasilitas HAZOP.
- **Luaran (Deliverable):** Laporan PHA (PHA Report) → Masukan untuk Definisi SIF dan Pemilihan SIL.

Analisis Bahaya Proses (*Process Hazards Analysis* - PHA) adalah analisis kualitatif terhadap bahaya proses yang dilakukan oleh tim multidisiplin. Ini bukan konsep baru. PHA telah diimplementasikan dalam industri selama lebih dari 15 tahun. Peraturan manajemen keselamatan proses OSHA yang diberlakukan pada tahun 1992 menyebabkan PHA menjadi jauh lebih umum, tetapi sebagian besar metodologi PHA sebenarnya telah dikembangkan dan diterapkan jauh lebih awal.

Masukan untuk langkah Siklus Hidup Keselamatan ini mencakup Informasi Keselamatan Proses (PSI), seperti usulan Diagram Alir Proses (PFD), Diagram Perpipa dan Instrumentasi (P&ID), dan dokumentasi lain yang diperlukan untuk menganalisis potensi penyimpangan dari tujuan normal operasi proses. PHA melibatkan analisis penyimpangan tersebut dari maksud desain dan menentukan apakah penyimpangan tersebut dapat mengakibatkan bahaya yang kredibel.

Jika demikian, konsekuensi dari bahaya tersebut diidentifikasi, dan perlindungan (*safeguards*) yang ada untuk mencegah bahaya tersebut diidentifikasi secara cermat. Penilaian risiko kualitatif dibuat oleh tim PHA, sering kali menggunakan pedoman risiko dari perusahaan operasi, seperti matriks risiko korporat. Jika perlindungan dianggap tidak memadai, maka tim PHA membuat rekomendasi untuk mengurangi atau menghilangkan bahaya atau menambahkan perlindungan baru.

Hasil dari langkah ini adalah Laporan Analisis Bahaya Proses (*PHA Report*) yang mengidentifikasi bahaya proses secara menyeluruh. Laporan PHA kemudian dapat digunakan pada langkah berikutnya dalam siklus hidup rekayasa SIS.

Rangkaian Studi Analisis Bahaya Proses (PHA)

Sehubungan dengan rekayasa SIS, tujuan utama dari langkah PHA adalah untuk mengidentifikasi perlindungan yang diperlukan guna mengurangi risiko proses dan memahami bahaya apa yang dilindungi oleh perlindungan tersebut. PHA biasanya dianggap sebagai studi formal tunggal seperti Studi Bahaya dan Kemampuan Operasi (*Hazards and Operability Study* - HAZOP) yang hasilnya didokumentasikan dalam satu laporan.

Namun, dalam kenyataannya PHA harus dianggap sebagai serangkaian studi terpadu dan tugas rekayasa yang menghasilkan rekomendasi untuk perlindungan potensial. Tugas-tugas ini harus mencakup hal-hal berikut:

- Pengembangan Paket Desain dari Lisensor Teknologi Proses dan Perusahaan Rekayasa.
- Penelaahan Standar Desain, Kode, dan Pedoman Praktik Rekayasa yang Baik untuk Item Peralatan Spesifik.
- Studi Penilaian Bahaya Awal (*Preliminary Hazard Assessment*), seperti HAZID.
- Studi Basis Desain Sistem Pelepasan Tekanan (*Relief System Design Basis Studies*).
- Studi Rasionalisasi dan Manajemen Alarm (*Alarm Rationalization Studies*).
- Pengujian dan Analisis Reaktivitas Kimiawi Bahan Proses.
- Studi Analisis Bahaya Proses Formal (seperti HAZOP atau What-If).

Desain proses awal jarang dilakukan mulai dari kertas kosong. Sering kali, desain proses didasarkan pada teknologi terbukti yang telah digunakan selama bertahun-tahun. Sering kali terdapat templat desain proses dari lisensor yang berisi informasi penting tentang bahaya dan perlindungan utama. Paket lisensor ini mengidentifikasi Fungsi Berinstrumen Keselamatan (SIF) yang telah disertakan berdasarkan pengalaman masa lalu.

Selain itu, sebagian besar pabrik proses mencakup sejumlah besar peralatan proses umum yang memerlukan perlindungan melalui SIS, seperti pompa, kompresor, dan peralatan berbahan bakar (*fired equipment*). Sering kali, peralatan ini dirancang dan dilindungi sesuai dengan standar khusus peralatan seperti standar National Fire Protection Association (NFPA) untuk boiler dan tungku pemanas, serta praktik yang direkomendasikan American Petroleum Institute (API) untuk kompresor dan mesin berputar.

Integrasi PHA dengan Siklus Hidup Rekayasa SIS

Studi basis desain perlindungan rekayasa lainnya juga dapat menghasilkan persyaratan untuk sistem berinstrumen keselamatan. Studi seperti basis desain sistem pelepasan, studi manajemen alarm, atau studi reaktivitas kimia sering kali menghasilkan rekomendasi untuk SIS terutama ketika cara perlindungan lain dinilai tidak tepat atau kurang efektif.

Tugas yang secara tradisional dianggap sebagai PHA pada dasarnya adalah teknik 'curah pendapat terstruktur' (*structured brainstorming*) di mana seorang fasilitator terlatih membimbing diskusi di antara sekelompok ahli dengan menggunakan kata pandu (*guide words*) deviasi dari maksud desain untuk bagian proses tertentu, seperti aliran berkurang atau level cairan berlebih. Pada saat PHA akhir dilakukan, sebagian besar perlindungan rekayasa telah didokumentasikan dalam desain pabrik dan PHA bertindak sebagai pemeriksaan akhir dari desain yang baik.

CONTOH LEMBAR KERJA HAZOP DI INDUSTRI PROSES

GAMBAR 4: TIPIKAL KELUARAN PHA BERGAYA HAZOP (HAZOP-STYLE PHA WORKSHEET)

- **Node 1:** Jalur Umpan 2"-P-101 & 102 menuju Kolom Stripper.
- **Deviasi:** Tekanan Tinggi (High Pressure).
- **Penyebab 1:** Tube penukar panas EX-102 pecah.
 - *Konsekuensi:* Tekanan berlebih pada stripper dengan potensi pelepasan zat berbahaya (Keparahan S = 3, Kemungkinan L = 2).
 - *Perlindungan (Safeguards):* PSV-105 melepas ke flare; PV-105 membuka ke flare.
 - *Rekomendasi:* Periksa ukuran PSV-105 untuk memastikan kapasitas pelepasan memadai untuk semua skenario (kebakaran, pecah tube, kehilangan refluks total).
- **Penyebab 2:** Katup kendali PV-105 gagal menutup sehingga kondensat panas tidak dapat dikeluarkan.
 - *Konsekuensi:* Tekanan berlebih pada stripper (S = 3, L = 4 → Risiko Kritis / Merah).
 - *Perlindungan:* PSV-105 melepas ke flare.
 - *Rekomendasi:* Tindakan koreksi diperlukan; perlindungan saat ini tidak mencukupi untuk menurunkan risiko ke batas toleransi.

Gambar 4 menyajikan tipikal laporan PHA bergaya HAZOP. Laporan ini dapat dibedah untuk mengembangkan informasi yang membantu penentuan target SIL. Skenario bahaya diberi kategori konsekuensi, penyebab dapat digunakan sebagai kejadian pemicu (*initiating events*), dan perlindungan dapat dievaluasi sebagai lapisan perlindungan independen (IPL). Rekomendasi PHA juga dapat mengidentifikasi kebutuhan SIF baru.

BAB 5: DEFINISI SAFETY INSTRUMENTED FUNCTION (SIF)

KERANGKA KERJA TAHAP DEFINISI SIF

ALUR KERJA TAHAP DEFINISI SIF:

- **Masukan (Input):** Laporan PHA/HAZOP, Diagram P&ID, Diagram Sebab-Akibat (Cause-and-Effect).
- **Tugas Rekayasa (Task):** Definisi Fungsi Berinstrumen Keselamatan (SIF Definition).
- **Perangkat (Tools):** SIS Toolkit – PHA-Pro.
- **Luaran (Deliverable):** Daftar SIF (SIF List) → Masukan untuk Pemilihan SIL & Desain Konseptual.

Definisi Fungsi Berinstrumen Keselamatan (*Safety Instrumented Function* - SIF) adalah langkah penting dalam siklus hidup keselamatan SIS, dan merupakan sumber dari banyak kesalahan dalam perancangan SIS sebagai akibat dari kesalahpahaman umum tentang apa yang sebenarnya merupakan sebuah SIF.

Definisi SIF membutuhkan pemahaman yang memadai tentang bahaya yang terkait dengan proses kimia, dan instrumen spesifik yang digunakan untuk melindungi dari bahaya tersebut. **Fungsi Berinstrumen Keselamatan dimaksudkan untuk melindungi dari bahaya yang spesifik dan teridentifikasi**, bukan bahaya umum seperti kebakaran dan ledakan gas secara global.

Hasil dari langkah ini adalah **Daftar Fungsi Berinstrumen Keselamatan (SIF List)**. Daftar SIF adalah kompilasi dari fungsi-fungsi yang harus diimplementasikan dalam keseluruhan Sistem Berinstrumen Keselamatan yang dapat mencakup banyak Fungsi Berinstrumen Keselamatan dalam logic solver yang sama, dan menggunakan komponen serupa atau identik seperti sensor dan elemen kendali akhir.

Tujuan dari definisi SIF adalah untuk membuat daftar semua fungsi yang perlu dianalisis dalam langkah-langkah selanjutnya dari Siklus Hidup Keselamatan termasuk pemilihan SIL, Spesifikasi Persyaratan Keselamatan (SRS), pengembangan Prosedur Uji Fungsional, dan seterusnya. Fungsi Berinstrumen Keselamatan diidentifikasi berdasarkan **basis bahaya-per-bahaya (hazard-by-hazard basis)**, bukan secara ketat mempertimbangkan fungsionalitas yang dieksekusi oleh SIF semata.

Oleh karena itu, sangat penting bahwa langkah ini dilakukan secara memadai, dengan pertimbangan yang cukup mengenai bahaya-bahaya yang terlibat dalam proses, dan peralatan atau komponen yang dapat digunakan untuk mendeteksi dan mengambil tindakan korektif setelah bahaya tersebut teridentifikasi.

Konsep Hubungan Fisik dan Fungsional: SIF versus SIS

Beberapa komponen perangkat keras mungkin digunakan di beberapa SIF sekaligus, sebagaimana ditunjukkan secara visual dalam diagram Gambar 5. Memahami perbedaan antara SIS (perangkat fisik terpadu) dan SIF (fungsi perlindungan keselamatan spesifik) adalah kunci utama keberhasilan perancangan.

ILUSTRASI: PERBEDAAN ANTARA SIS DAN SIF

GAMBAR 5: REPRESENTASI KONSEPTUAL SIF VERSUS SIS

- **Sistem Berinstrumen Keselamatan (SIS):** Ditunjukkan oleh lingkaran putus-putus hijau besar di luar. SIS mencakup keseluruhan kabinet logic solver, rak I/O, seluruh pemancar sensor di lapangan, dan seluruh katup penutup keselamatan.
- **Fungsi Berinstrumen Keselamatan (SIF):** Ditunjukkan oleh elips-elips merah yang membentang horizontal:
 - *SIF 1 (Elips Atas):* Menggabungkan sensor tekanan trip tinggi → modul masukan logic solver → program logika keselamatan → modul keluaran → katup penghenti aliran gas masuk.
 - *SIF 2 (Elips Bawah):* Menggabungkan sensor level cairan trip rendah → logic solver yang sama → memicu katup penghenti cairan keluar dan mematikan motor pompa.

Prinsip Penggunaan Bersama (Shared Components): Beberapa SIF yang berbeda dapat berbagi logic solver yang sama, bahkan dapat berbagi sensor yang sama atau memicu aksi shutdown pada katup akhir yang sama. Setiap SIF tetap memiliki peringkat SIL individualnya sendiri sesuai dengan tingkat bahaya spesifik yang dicegahnya.

Identifikasi Fungsi Berinstrumen Keselamatan dilakukan dengan mempertimbangkan berbagai dokumentasi desain termasuk Diagram Sebab dan Akibat (*Cause and Effect Diagrams*), dan Diagram Perpipaan dan Instrumentasi (P&ID).

Daftar SIF adalah daftar semua fungsi yang perlu dianalisis. Setiap SIF diberikan Tingkat Integritas Keselamatan (SIL) tersendiri, secara individual, untuk mewakili pengurangan risiko yang diperlukan guna memitigasi bahaya spesifik yang terkait dengan fungsi tersebut. Tingkat integritas mendefinisikan kinerja fungsi dalam hal kemampuannya mencapai target risiko yang dapat ditoleransi.

Tipikal Daftar SIF (SIF List) & Parameter Wajib

Gambar 6 menyajikan tipikal Daftar SIF (*SIF List*), sebagaimana terdapat dalam Toolkit Basis Desain SIS Kenexis (*Kenexis SIS Design Basis Toolkit™*). Daftar ini mendefinisikan batas-batas fungsional SIF secara lengkap.

STRUKTUR TABEL SIF LIST

GAMBAR 6: CONTOH TAMPILAN SIF LIST PADA TOOLKIT BASIS DESAIN SIS KENEXIS

• **SIF ID 417-1:**

- *Deskripsi SIF:* Api padam akibat tekanan gas bahan bakar rendah memicu shutdown Boiler B-508.
- *Status SIF:* Ya (Aktif) | *Target SIL Terpilih:* SIL 2.
- *Tag Masukan (Inputs):* PSL-505 (3 unit pemancar) | *Voting Masukan:* 2oo3.
- *Tag Keluaran (Outputs):* XV-505-1, XV-505-2 (Katup isolasi gas ganda) | *Voting Keluaran:* 1oo2.
- *Lokasi Logika:* Logic Solver Boiler SIS.

• **SIF ID 417-2:**

- *Deskripsi SIF:* Api padam akibat tekanan gas bahan bakar tinggi memicu shutdown Boiler B-508.
- *Status SIF:* Ya | *Target SIL:* SIL 2 | *Input:* PSHH-505 (3 unit) | *Voting Input:* 2oo3 | *Output:* XV-505-1/2 | *Voting:* 1oo2.

• **SIF ID 417-3:**

- *Deskripsi SIF:* Tekanan uap tinggi memicu shutdown burner Boiler B-508.
- *Status SIF:* Ya | *Target SIL:* SIL 1 | *Input:* PSHH-507-1 (1 unit) | *Voting Input:* 1oo1 | *Output:* XV-505-1/2 | *Voting:* 1oo2.

Untuk setiap SIF, deskripsi disediakan yang mendefinisikan maksud fungsi dan tindakan yang diperlukan untuk membawa proses ke kondisi aman. Semua masukan kritis keselamatan dicantumkan, khususnya semua sensor yang dapat mendeteksi bahaya yang dicegah. Semua keluaran kritis keselamatan dicantumkan, yaitu semua keluaran yang **perlu dan cukup** untuk membawa proses ke kondisi aman. Ini adalah konsep yang sangat berbeda daripada sekadar mendaftarkan semua keluaran yang diaktifkan sesuai diagram sebab-akibat unit.

Daftar SIF harus mendefinisikan setiap SIF secara menyeluruh, mencakup: Tag nama untuk perangkat masukan, Deskripsi tujuan SIF, Voting masukan, Tag nama untuk perangkat keluaran, Voting keluaran, Lokasi logika SIF, serta nomor interlock dan gambar P&ID acuan.

BAB 6: PEMILIHAN TINGKAT INTEGRITAS KESELAMATAN (SIL SELECTION)

KERANGKA KERJA TAHAP PEMILIHAN SIL

ALUR KERJA TAHAP PEMILIHAN SIL:

- **Masukan (Input):** Laporan PHA, Daftar SIF (SIF List), Diagram P&ID, Kriteria Risiko Korporat.
- **Tugas Rekayasa (Task):** Pemilihan Tingkat Integritas Keselamatan (Safety Integrity Level Selection).
- **Perangkat (Tools):** SIS Toolkit – PHA-Pro, Matriks Risiko Terkalibrasi, Lembar Kerja LOPA.
- **Luaran (Deliverable):** Laporan Pemilihan SIL (SIL Selection Report) → Masukan Desain Konseptual & SRS.

Setelah semua fungsi yang berada dalam lingkup analisis didefinisikan dalam daftar SIF, Pemilihan Tingkat Integritas Keselamatan (*Safety Integrity Level* - SIL) dilakukan. Pada tahap ini, SIF dianalisis secara berurutan dengan melihat bahaya, mengidentifikasi parameter yang sesuai yang mempengaruhi risiko bahaya tersebut, dan memilih SIL yang sesuai untuk mencapai ambang toleransi risiko yang diinginkan.

Penting untuk diingat bahwa **tujuan Pemilihan SIL adalah untuk menentukan kriteria kinerja untuk sistem**. Ini bukan untuk merancang perangkat keras SIF secara fisik, melainkan untuk menetapkan berapa banyak pengurangan risiko yang diperlukan dari masing-masing SIF tersebut.

Mendefinisikan SIL (Defining SIL)

Sesuai dengan definisinya dalam IEC 61511 (ISA 84.00.01), SIL adalah rentang pita orde besaran (*order of magnitude bands*) dari rata-rata probabilitas kegagalan saat diminta (*average probability of failure on demand* - PFDavg). PFDavg ini juga mewakili jumlah pengurangan risiko yang dapat disediakan oleh fungsi keselamatan berinstrumen preventif.

Rentang untuk masing-masing dari empat tingkat SIL yang didefinisikan dalam standar tidak hanya disajikan dalam istilah PFDavg, tetapi juga dalam **Ketersediaan Keselamatan (Safety Availability)** dan **Faktor Reduksi Risiko (Risk Reduction Factor - RRF)**. Safety Availability adalah komplemen dari PFDavg (yaitu $1 - \text{PFDavg}$), dan RRF adalah kebalikan matematis dari PFDavg (yaitu $1 / \text{PFDavg}$). Semua metrik ini umum digunakan di industri.

Metrik Tingkat Integritas Keselamatan (SIL Metrics)

Gambar 7 menyajikan metrik tingkat integritas keselamatan lengkap sesuai standar IEC 61511 dan IEC 61508 untuk mode operasi permintaan rendah (*low-demand mode*):

Safety Integrity Level (SIL)	Ketersediaan Keselamatan (Safety Availability)	Rata-rata Probabilitas Kegagalan saat Dibutuhkan (PFDavg)	Faktor Reduksi Risiko (Risk Reduction Factor - RRF)
SIL 4	> 99,99%	0,001% hingga 0,01% ($10^{-5} \leq \text{PFD} < 10^{-4}$)	100.000 hingga 10.000
SIL 3	99,9% hingga 99,99%	0,01% hingga 0,1% ($10^{-4} \leq \text{PFD} < 10^{-3}$)	10.000 hingga 1.000
SIL 2	99% hingga 99,9%	0,1% hingga 1% ($10^{-3} \leq \text{PFD} < 10^{-2}$)	1.000 hingga 100
SIL 1	90% hingga 99%	1% hingga 10% ($10^{-2} \leq \text{PFD} < 10^{-1}$)	100 hingga 10

Gambar 7 — Metrik Tingkat Integritas Keselamatan (Safety Integrity Level)

SIL 1 adalah tingkat integritas keselamatan terendah yang didefinisikan dengan ketersediaan keselamatan setidaknya 90% hingga 99%, yang pada dasarnya memberikan satu orde besaran pengurangan risiko (faktor 10 hingga 100).

SIL 2 adalah satu orde besaran lebih aman daripada SIL 1 dalam hal ketersediaan keselamatannya. Ketersediaan keselamatan dari fungsi SIL 2 adalah setidaknya 99% dan hingga 99,9% (faktor pengurangan risiko 100 hingga 1.000).

SIL 3 adalah satu orde besaran di atas SIL 2 dalam hal ketersediaan keselamatannya, dengan ketersediaan 99,9% hingga 99,99% (RRF 1.000 hingga 10.000).

SIL 4 jarang atau bahkan tidak pernah terlihat di industri proses kimia dan perminyakan, dan sering kali dicadangkan untuk aplikasi pada industri terkait non-proses (seperti industri nuklir atau perkeretaapian komersial berkecepatan tinggi) yang dicakup oleh standar IEC 61508. Jika proses pemilihan SIL menghasilkan persyaratan untuk SIL 4, pengguna harus melanjutkan dengan sangat hati-hati dan memperoleh bantuan dari para ahli keselamatan proses, karena mendesain ulang proses kimia yang mendasarinya biasanya jauh lebih disukai daripada mencoba membangun sistem instrumen SIL 4.

Proses Pemilihan SIL (SIL Selection Process)

Karena SIL adalah ukuran jumlah pengurangan risiko yang disediakan oleh Fungsi Berinstrumen Keselamatan, pemilihan SIL adalah latihan dalam menganalisis risiko bahaya dan menentukan berapa banyak pengurangan risiko yang diperlukan untuk mencapai tingkat risiko yang dapat ditoleransi.

Pengurangan risiko dapat direpresentasikan secara grafis melalui diagram yang terdapat pada Gambar 8, di mana setidaknya dua parameter yang mempengaruhi risiko dipertimbangkan: **Konsekuensi (Consequence)** dan **Kemungkinan (Likelihood)**.

ILUSTRASI: REPRESENTASI GRAFIS PEMILIHAN SIL

GAMBAR 8: REPRESENTASI GRAFIS PEMILIHAN SIL (GRAPHICAL SIL SELECTION)

- **Sumbu Diagram:** Sumbu X mewakili Konsekuensi (Keparahan Bahaya); Sumbu Y mewakili Kemungkinan (Likelihood). Risiko meningkat ke arah kanan-atas.

- **Tiga Wilayah Risiko:**

1. *Wilayah Risiko Tidak Dapat Diterima (Unacceptable Risk Region - Merah):* Risiko terlalu tinggi, tidak dapat ditoleransi dalam kondisi apa pun, dan wajib diturunkan.
2. *Wilayah ALARP (As Low As Reasonably Practicable - Kuning):* Wilayah transisi di mana risiko harus dikurangi serendah mungkin yang dapat dicapai secara praktis dengan menyeimbangkan efektivitas dan biaya.
3. *Wilayah Risiko yang Dapat Ditoleransi (Tolerable Risk Region - Hijau):* Risiko dianggap dapat diterima secara luas tanpa memerlukan perlindungan tambahan.

- **Alur Pengurangan Risiko:**

Titik awal adalah *Inherent Risk of the Process* (di wilayah merah). Reduksi risiko non-SIS pertama-tama diterapkan: reduksi konsekuensi (tanggul pengaman, proteksi fisik) menggeser titik ke kiri, dan reduksi kemungkinan (katup relief mekanis PSV) menggeser titik ke bawah. Sisa celah risiko kemudian dipenuhi oleh SIS dengan target SIL 1, SIL 2, atau SIL 3 untuk membawa risiko masuk ke wilayah hijau yang dapat ditoleransi.

Konsekuensi adalah potensi keparahan dari bahaya kecelakaan. Kemungkinan adalah representasi dari seberapa sering kecelakaan diperkirakan terjadi. Jika seseorang mempertimbangkan satu bahaya tunggal dalam suatu proses, bahaya tersebut akan memiliki risiko proses inheren, yang merupakan fungsi dari keparahan konsekuensi inherennya dan kemungkinan inheren dari bahaya tersebut terjadi tanpa adanya perlindungan apa pun.

Merepresentasikan Risiko yang Dapat Ditoleransi untuk Pemilihan SIL

Untuk tujuan melakukan pemilihan SIL, perusahaan sering kali mewakili toleransi risiko mereka dalam bentuk **Matriks Risiko** (*Risk Matrix*) atau **Tabel Kemungkinan Kejadian Maksimum yang Dapat Ditoleransi** (*Tolerable Maximum Event Likelihood - TMEL*). Gambar 9 menunjukkan contoh matriks risiko terkalibrasi.

Keparahan / Kemungkinan	L = 0	L = 1	L = 2	L = 3	L = 4	L = 5
S = 5 (Kematian Ganda)	0	3	4	5		7
S = 4 (Kematian Tunggal)	0	2	3	4	5	
S = 3 (Cedera Parah)	0	1	2	3	4	5
S = 2 (Cedera Hari Kerja Hilang)	0	0	1	2	3	4
S = 1 (Cedera Ringan P3K)	0	0	0	1	2	3
S = 0 (Tanpa Konsekuensi)	0	0	0	0	0	0

Gambar 9 — Matriks Risiko Terkalibrasi (Angka dalam sel = orde besaran reduksi risiko yang diperlukan)

Alat-alat risiko ini digunakan untuk tugas-tugas rekayasa risiko sehari-hari, dan dikalibrasi terhadap pedoman risiko yang dapat ditoleransi dari korporasi. Rincian kalibrasi untuk contoh alat risiko ini dimuat dalam Lampiran H.

Tabel Kategori Konsekuensi dan Kemungkinan

Gambar 10 menyajikan tabel kategorisasi konsekuensi yang mencakup angka TMEL untuk setiap kategori konsekuensi, mencakup kriteria keselamatan manusia, lingkungan, dan kerugian finansial komersial:

S	Kategori	Keselamatan Manusia	Lingkungan Hidup	Komersial	TMEL (/thn)
0	Tidak Ada	Tanpa konsekuensi keselamatan	Tidak ada dampak	Tidak ada	N/A
1	Sangat Rendah	Cedera ringan – P3K	Tumpahan kecil, pembersihan minimal	\$50.000	1×10^{-2}
2	Rendah	Cedera hari kerja hilang tanpa rawat inap panjang	Tumpahan sedang, terbatas di dalam area pabrik	\$500.000	1×10^{-3}
3	Sedang	Cedera parah (rawat inap panjang, cacat permanen)	Pelepasan besar dengan dampak terbatas ke luar area	\$5 Juta	1×10^{-4}
4	Tinggi	Kematian tunggal (single fatality)	Pelepasan besar ke luar pabrik, kerusakan area sensitif	\$50 Juta	1×10^{-5}
5	Sangat Tinggi	Kematian ganda (multiple fatalities)	Pelepasan sangat besar ke luar area, kerusakan permanen	\$500 Juta	1×10^{-6}

Gambar 10 — Tabel Kategori Konsekuensi dengan TMEL

Gambar 11 menunjukkan contoh tabel kategori kemungkinan yang akan digunakan dalam kombinasi dengan tabel konsekuensi saat menggunakan pendekatan Matriks Risiko:

Kemungkinan (L)	Deskripsi Kategori	Periode Keberulangan (Recurrence Period)	Frekuensi Rata-rata (/tahun)
0	Tidak Ada (None)	N/A	0
1	Sangat Jarang (Very Unlikely)	1 kali dalam 1.000 tahun	1×10^{-3}
2	Jarang (Unlikely)	1 kali dalam 100 tahun	1×10^{-2}
3	Kadang-kadang (Occasional)	1 kali dalam 10 tahun	1×10^{-1}
4	Sering (Frequent)	1 kali dalam 1 tahun	1
5	Sangat Sering (Very Frequent)	1 kali dalam 0,1 tahun	10

Gambar 11 — Tabel Kategori Kemungkinan (Likelihood Category Table)

Layer of Protection Analysis (LOPA)

Meskipun berbagai macam teknik dapat digunakan untuk memilih SIL yang dipersyaratkan, **Layer of Protection Analysis (LOPA)** adalah metode yang paling umum karena kemudahan penggunaan dan efektivitasnya. LOPA dapat menggunakan pendekatan Matriks Risiko atau tabel TMEL untuk merepresentasikan risiko.

Ketika matriks risiko digunakan, analisis secara ketat menggunakan orde besaran (yaitu 'eksponen') dan disebut sebagai **LOPA Implisit (Implicit LOPA)**. Sedangkan ketika tabel TMEL digunakan, angka-angka risiko dihitung menggunakan angka frekuensi dan probabilitas aktual dan disebut sebagai **LOPA Eksplisit (Explicit LOPA)**.

Manfaat dari lapisan-lapisan perlindungan dapat diperhitungkan dalam analisis Lapisan Perlindungan terpisah, di mana kita melihat efektivitas potensial dari masing-masing lapisan perlindungan ini.

ILUSTRASI: KONSEP BOLA LAPISAN PERLINDUNGAN

GAMBAR 12: DEPIKSI GRAFIS BOLA KONSENTRIS LAPISAN PERLINDUNGAN (SPHERES OF PROTECTION)

Gambar 12 menyajikan penggambaran grafis dari konsep analisis lapisan perlindungan, di mana setiap bola konsentris mengandung risiko proses di dalamnya. Agar bahaya proses dapat lolos dan menimbulkan dampak buruk pada masyarakat atau lingkungan, bahaya tersebut harus menembus seluruh lapisan perlindungan secara berurutan:

- **Lapisan Inti:** Proses Fisik/Kimia Itu Sendiri (Process)
- **Lapisan 1:** Sistem Kendali Dasar & Pengawasan Operator (BPCS Controls, Process Alarms, & Operator Supervision)
- **Lapisan 2:** Alarm Kritis & Intervensi Manual Operator (Critical Alarms & Manual Intervention)
- **Lapisan 3:** Tindakan Otomatis Sistem Berinstrumen Keselamatan (Automatic Action SIS)
- **Lapisan 4:** Proteksi Fisik Pelepasan Tekanan Mekanis (Physical Protection: Relief Devices / PSV)
- **Lapisan 5:** Proteksi Fisik Penampungan Sekunder (Physical Protection: Containment Dikes)
- **Lapisan 6:** Tanggap Darurat Pabrik (Plant Emergency Response)
- **Lapisan 7:** Tanggap Darurat Komunitas / Masyarakat (Community Emergency Response)

Karakteristik Lapisan Perlindungan Independen (IPL)

Industri proses memanfaatkan sejumlah lapisan perlindungan independen sebagai bagian dari desain pabrik yang khas. Beberapa lapisan perlindungan umum, bersama dengan probabilitas kegagalan lapisan-lapisan tersebut dapat ditemukan dalam Lampiran D.

ILUSTRASI: PERTAHANAN DINDING BERLAPIS

GAMBAR 13: DINDING PERTAHANAN BERLAPIS (LAYERS OF PROTECTION)

- **Basic Process Control System (BPCS):** Garis kendali proses normal.
- **Operator Intervention (Intervensi Operator):** Berdasarkan alarm proses sebelum kondisi mencapai trip point.
- **Emergency Shutdown (SIS):** Sistem otomatis yang membawa proses ke kondisi aman saat batas trip terlampaui.
- **Physical Devices (Perangkat Fisik):** Katup pengaman tekanan (PSV/PRV) yang membuka pada relief set point.
- **Consequence Mitigation (Mitigasi Konsekuensi):** Tanggul penahan tumpahan cairan, sistem tirai air (water spray).
- **Emergency Response (Tanggap Darurat):** Pemadam kebakaran pabrik dan evakuasi personel.

Prinsip Pertahanan: Satu atau lebih lapisan dapat gagal ketika terjadi permintaan (demand). Kecelakaan dengan konsekuensi tinggi memerlukan beberapa lapisan proteksi independen yang kuat untuk menurunkan risiko ke tingkat yang dapat ditoleransi.

Filosofi lapisan perlindungan mengakui bahwa satu atau lebih dari lapisan-lapisan ini dapat gagal ketika kondisi permintaan (demand) terjadi padanya. Oleh karena itu, kecelakaan dengan potensi keparahan konsekuensi yang tinggi serta kemungkinan yang tinggi dapat memerlukan lebih dari satu desain SIS yang tangguh, atau lapisan perlindungan lainnya untuk mengurangi risiko ke tingkat yang dapat ditoleransi.

Kita memperhitungkan lapisan-lapisan perlindungan dalam analisis LOPA terpisah di mana kita memverifikasi bahwa **setiap lapisan perlindungan memenuhi tiga kriteria ketat**:

1. **Independen (Independent):** Benar-benar independen dari penyebab pemicu (initiating event) dan independen dari semua lapisan perlindungan lainnya.
2. **Spesifik (Specific):** Dirancang secara spesifik untuk mendeteksi dan mencegah bahaya khusus yang telah diidentifikasi.
3. **Efektif (Effective):** Terbukti mampu memberikan pengurangan risiko setara dengan setidaknya 1 orde besaran (probabilitas kegagalan saat diminta $\leq 10\%$ atau $PFD \leq 0,1$).

Formulasi Matematika LOPA Implisit dan LOPA Eksplisit

Varian LOPA eksplisit dan implisit menangani efektivitas lapisan perlindungan dengan cara yang sedikit berbeda, tetapi secara matematis setara.

Ketika menggunakan target TMEL sebagai dasar untuk risiko yang dapat ditoleransi (LOPA Eksplisit), frekuensi kecelakaan yang tidak diinginkan harus dihitung dan dibandingkan dengan target. Perhitungan frekuensi ini dilakukan dengan mengalikan frekuensi kejadian pemicu dengan probabilitas kegagalan saat diminta dari semua lapisan perlindungan independen yang bertindak terhadap kejadian pemicu spesifik tersebut. Jika ada beberapa kejadian pemicu, maka frekuensi yang dihasilkan harus dijumlahkan.

Target kinerja yang dipilih untuk SIF kemudian dihitung sebagai probabilitas kegagalan maksimum yang diizinkan bagi SIF untuk tetap mencapai TMEL.

Ketika menggunakan matriks risiko (LOPA Implisit), jumlah orde besaran pengurangan risiko yang diperlukan diambil langsung dari matriks. Setiap kredit untuk lapisan perlindungan independen (IPL) mengurangi risiko sebesar 1 orde besaran (setara dengan $PFD = 0,1$). Dengan demikian, target SIL yang dipilih untuk SIF adalah jumlah orde besaran pengurangan risiko yang dipersyaratkan dikurangi jumlah kredit lapisan perlindungan. Pengurangan kredit lapisan perlindungan setara dengan perkalian probabilitas karena mengalikan angka atau menambahkan eksponennya menghasilkan hasil yang sama.

FORMULA LOPA RESMI STANDAR REKAYASA

PERSAMAAN PERHITUNGAN SIL PADA ANALISIS LAPISAN PERLINDUNGAN (LOPA):

1. LOPA Implisit (Pendekatan Matriks Risiko):

$$SIL = RR(S, L) - \sum (Kredit\ IPL)$$

Di mana:

- SIL : Tingkat integritas keselamatan yang dipilih untuk SIF.
- $RR(S, L)$: Jumlah pengurangan risiko yang dipersyaratkan (dalam orde besaran, diperoleh dari matriks risiko terkalibrasi berdasarkan keparahan S dan kemungkinan L).
- $\sum(Kredit\ IPL)$: Jumlah dari semua kredit untuk semua lapisan perlindungan independen yang valid.
- *Konversi Kredit IPL ke PFD*: 1 kredit $\rightarrow PFD = 0,1$; 2 kredit $\rightarrow PFD = 0,01$; 3 kredit $\rightarrow PFD = 0,001$.

2. LOPA Eksplisit (Pendekatan Target TMEL):

$$F(\text{kejadian, Tanpa-SIS}) = \sum [IE_i \times \prod_j (PFD_{IPL_j})]$$

$$SIL\ Target\ (RRF) = F(\text{kejadian, Tanpa-SIS}) / TMEL$$

Di mana:

- $TMEL$ (*Target Maximum Event Likelihood*): Frekuensi kejadian yang dapat ditoleransi per tahun dari tabel konsekuensi.
- $F(\text{kejadian, Tanpa-SIS})$: Frekuensi kejadian yang terjadi tanpa adanya SIS yang terpasang.
- IE_i : Frekuensi dari kejadian pemicu (initiating event) ke-i per tahun (Lampiran C).
- $\prod(PFD_{IPL})$: Hasil kali probabilitas kegagalan saat diminta dari semua IPL yang valid untuk kejadian pemicu tersebut.

BAB 7: DESAIN KONSEPTUAL / VERIFIKASI SIL

KERANGKA KERJA TAHAP VERIFIKASI SIL

ALUR KERJA TAHAP DESAIN KONSEPTUAL & VERIFIKASI SIL:

- **Masukan (Input):** Laporan Pemilihan SIL (SIL Selection Report), Data Kegagalan Komponen (Lampiran G).
- **Tugas Rekayasa (Task):** Desain Konseptual SIS & Verifikasi SIL (Iteratif).
- **Perangkat (Tools):** SIS Toolkit – FaultTree+, Persamaan Matematis Sederhana ISA-TR84.00.02.
- **Luaran (Deliverable):** Laporan Verifikasi SIL (SIL Verification Report) → Masukan untuk SRS.

Setelah Tingkat Integritas Keselamatan dipilih untuk masing-masing Fungsi Berinstrumen Keselamatan yang diidentifikasi, tugas-tugas berikutnya dalam Siklus Hidup Keselamatan SIS yang perlu diselesaikan adalah '**Conceptual Design of the Safety Instrumented System**' (**Desain Konseptual SIS**) dan '**SIL Verification**' (**Verifikasi SIL**). Tahap ini adalah tempat di mana verifikasi bahwa masing-masing SIL yang dipersyaratkan telah dicapai oleh sistem yang telah dirancang diselesaikan.

Kedua langkah ini benar-benar berjalan beriringan, dan sering kali bersifat iteratif. Titik awal tipikal adalah Desain Konseptual SIF yang didasarkan pada pengalaman sebelumnya dengan aplikasi tersebut, atau pertimbangan rekayasa berdasarkan SIL yang dipersyaratkan. Desain ini kemudian dievaluasi untuk menentukan apakah SIL telah tercapai. Desain Konseptual kemudian dimodifikasi secara iteratif sampai semua aspek dari peringkat SIL telah dicapai oleh desain; termasuk jenis komponen, arsitektur, toleransi kesalahan, pengujian fungsional, dan kemampuan diagnostik.

LIMA PARAMETER PENENTU KINERJA SIL

GAMBAR 14: PARAMETER YANG MEMPENGARUHI SIL YANG DICAPAI (PARAMETERS IMPACTING ACHIEVED SIL)

Sebagaimana ditunjukkan pada Gambar 14, terdapat lima parameter fundamental dalam perancangan SIS yang secara langsung mempengaruhi ketercapaian tingkat integritas keselamatan:

1. **Pemilihan Komponen (Component Selection):** Kelayakan teknologi instrumen dan rekam jejak keandalan.
2. **Toleransi Kesalahan (Fault Tolerance):** Arsitektur pemungutan suara (Moon voting) dan batasan arsitektural HFT.
3. **Interval Uji Fungsional (Functional Test Interval - TI):** Seberapa sering pengujian bukti penuh dilakukan.
4. **Kegagalan Penyebab Umum (Common Cause Failures - β):** Potensi kejadian tunggal yang melumpuhkan saluran ganda.
5. **Cakupan Diagnostik (Diagnostic Coverage - DC):** Persentase kegagalan berbahaya yang dideteksi otomatis.

Pemilihan Komponen (Component Selection)

Proses pemilihan komponen mempertimbangkan aspek kualitatif dan kuantitatif dari serangkaian sifat komponen. Aspek kualitatif meliputi dua kriteria penting yang tidak boleh diabaikan:

1. **Kesesuaian untuk Aplikasi Terpilih (Suitability for the Selected Application)**
2. **Kesesuaian untuk Penggunaan dalam Keselamatan (Suitability for Use in Safety)**

Kriteria pertama mengacu pada kemampuan komponen untuk bereaksi secara akurat dalam aplikasi proses spesifik, dan kriteria kedua mengacu pada keandalan komponen untuk aplikasi keselamatan. Kedua kriteria ini sangat penting, dan tidak ada yang bisa diabaikan.

Agar suatu perangkat cocok untuk aplikasi tertentu, prinsip-prinsip yang digunakan perangkat harus memiliki riwayat kinerja efektif yang terbukti dalam aplikasi proses spesifik tersebut. Misalnya, meteran vortex (*vortex meters*) dan meteran magnetik (*magnetic meters*) keduanya mengukur aliran, tetapi tidak dapat dipertukarkan di semua aplikasi karena efektivitasnya tidak sama dalam semua kasus, dan sangat tergantung pada zat yang diukur. Ini adalah pertimbangan penting saat menggunakan peralatan 'bersertifikat'. Bahkan jika peralatan 'bersertifikat' untuk kepatuhan IEC 61508, peralatan tersebut tetap tidak dapat digunakan kecuali penilaian dibuat oleh pengguna bahwa teknologi yang digunakan perangkat tersebut cocok untuk aplikasi fluida tersebut.

Agar suatu perangkat 'cocok untuk keselamatan', pengguna harus memiliki pengalaman sukses penggunaan sebelumnya (*proven-in-use / prior use*) dengan perangkat tersebut atau harus diproduksi sesuai dengan standar yang diakui industri untuk pemasok komponen Sistem Berinstrumen Keselamatan; khususnya **IEC 61508**. Ini biasanya diverifikasi oleh sertifikasi pihak ketiga independen (seperti TÜV). Tindakan ini dimaksudkan untuk menunjukkan 'keandalan' perangkat yang sesuai. Dalam kasus 'prior use', pengguna akhir menganalisis kinerja masa lalu perangkat untuk menentukan keberterimaannya, dan dalam kasus 'sertifikasi' diasumsikan bahwa proses perancangan dan manufaktur yang sangat terkontrol akan menghasilkan keandalan yang tinggi.

Selain dua kriteria kualitatif, teknologi perangkat juga akan memainkan peran dalam peralatan apa yang dipilih. Keputusan antara teknologi yang dapat diprogram (*programmable*), dibandingkan dengan perangkat elektromekanis kabel-keras (*hard-wired*), biasanya dibuat dengan menyeimbangkan biaya rendah dari sistem kecil kabel-keras dengan penurunan biaya dan upaya rekayasa yang terkait dengan sistem besar yang dapat diprogram. Selain itu, teknologi juga akan mempengaruhi parameter kuantitatif lainnya seperti laju kegagalan, fraksi kegagalan aman (SFF), dan cakupan diagnostik.

Toleransi Kesalahan (Fault Tolerance)

Toleransi kesalahan adalah kemampuan SIS untuk dapat melakukan tindakan yang dimaksudkan (dan tidak melakukan tindakan yang tidak diinginkan) dengan adanya kegagalan satu atau lebih komponen SIS. Toleransi kesalahan biasanya dicapai melalui penggunaan beberapa komponen redundan yang diatur untuk melakukan 'pemungutan suara' (*voting*) atas tindakan SIF. Pengaturan beberapa komponen redundan ini disebut sebagai 'arsitektur' dari subsistem SIF. Beberapa arsitektur pemungutan suara berpotensi mengakibatkan hilangnya keselamatan saat terjadi kegagalan komponen, sementara yang lain berpotensi meningkatkan tingkat keselamatan jika satu atau lebih komponen dalam arsitektur gagal.

Arsitektur yang paling umum digunakan sebagai subsistem SIS dijelaskan dalam sistem M-out-of-N (MooN), di mana M adalah jumlah komponen yang harus berfungsi untuk mengambil tindakan keselamatan dan N adalah jumlah total komponen:

- **1oo1 (One-out-of-One / Simpleks):** Merupakan komponen tunggal, dan berfungsi sebagai dasar perbandingan arsitektur. Memiliki toleransi kesalahan 0.
- **1oo2 (One-out-of-Two):** Merupakan opsi 'paling aman', memberikan PFDavg terendah. Jika salah satu dari dua pemancar memilih trip, tindakan penghentian diambil. Menyediakan satu tingkat toleransi kesalahan terhadap kegagalan berbahaya, tetapi tidak ada toleransi terhadap kegagalan spurious. Pengaturan 1oo2 akan menghasilkan trip palsu dua kali lebih sering daripada perangkat tunggal.
- **2oo2 (Two-out-of-Two):** Memberikan satu tingkat toleransi kesalahan terhadap trip palsu, tetapi tidak ada terhadap keselamatan. PFDavg-nya dua kali lebih besar dari komponen tunggal (lebih berbahaya), tetapi memiliki tingkat gangguan trip yang satu orde besaran lebih rendah.
- **2oo3 (Two-out-of-Three):** Menawarkan kompromi optimal antara 1oo2 dan 2oo2. Pengaturan ini memiliki PFDavg yang lebih rendah dan tingkat trip palsu yang lebih rendah daripada perangkat tunggal, meskipun tidak seaman 1oo2 dan tidak setahan trip 2oo2.

Selain dampak kuantitatif dari arsitektur, tingkatan SIL memerlukan pencapaian '**Batasan Arsitektural**' (**Architectural Constraints**) yang pada dasarnya merupakan pembatasan pada toleransi kesalahan minimum yang harus disediakan untuk subsistem tertentu. Umumnya, SIL 1 tidak memerlukan toleransi kesalahan perangkat keras kecuali jika diperlukan untuk mencapai target PFDavg. SIL 2 membutuhkan setidaknya satu derajat toleransi kesalahan (misalnya arsitektur 1oo2 atau 2oo3). Rincian batasan arsitektural dimuat dalam Lampiran F.

Interval Uji Fungsional (Functional Test Interval)

Pengujian fungsional berkala (*proof testing*) dari suatu SIF menurunkan probabilitas kegagalannya, dan meningkatkan SIL efektifnya, dengan secara efektif mengurangi fraksi waktu di mana SIF berada dalam kondisi gagal tersembunyi (*latent failed state*).

Ketika pengujian SIF dilakukan, setiap kegagalan laten dalam sistem diidentifikasi dan selanjutnya diperbaiki. Ketika interval pengujian menjadi lebih pendek (yaitu pengujian lebih sering dilakukan), SIF yang gagal tidak akan tetap berada dalam kondisi gagal tersebut untuk jangka waktu yang lama, sehingga mengurangi ketidaktersediaan sistem (*unavailability*).

KURVA GERGAJI KETIDAKANDALAN DAN EFEK UJI BUKTI

GAMBAR 15: DAMPAK INTERVAL UJI TERHADAP SIL (IMPACT OF TEST INTERVAL ON SIL)

Gambar 15 menunjukkan konsep ini dari perspektif ketidakandalan (unreliability):

- **Sumbu Horizontal:** Waktu Operasi Berjalan.
- **Sumbu Vertikal:** Probabilitas Kegagalan Akumulatif (Unreliability Curve) → Berbanding terbalik dengan SIL (Pita SIL 1 di atas, SIL 2 di tengah, SIL 3 di bawah).

• Dinamika Kurva Gergaji:

Seiring bertambahnya waktu operasi, ketidakandalan meningkat secara bertahap sampai uji fungsional dilakukan. Setelah pengujian mengonfirmasi operasi sistem yang berhasil (atau menghasilkan perbaikan komponen yang gagal), probabilitas kegagalan kemudian disetel ulang kembali mendekati nol.

Kesimpulan Teknis: Jika suatu sistem diuji lebih sering (interval uji lebih pendek), kurva ketidakandalan tidak akan naik terlalu tinggi sebelum direset ke nol, sehingga rata-rata PFDavg tetap berada dalam pita target SIL yang lebih tinggi (SIL 2 atau SIL 3). Sebaliknya, interval uji yang terlalu panjang akan menyebabkan PFDavg terdegradasi ke tingkat SIL yang lebih rendah.

Kegagalan Penyebab Umum (Common Cause Failures)

Konsep Penyebab Umum (*Common Cause*) mengakui bahwa potensi kejadian tunggal atau stres eksternal pada suatu SIF dapat mengakibatkan beberapa kegagalan simultan dari komponen-komponen SIF yang redundan secara bersamaan.

Sebagai contoh, dua atau lebih pemancar tekanan redundan dapat gagal pada saat yang sama jika saluran tap impuls proses mereka tersumbat oleh lilin, polimer, atau es beku. Kegagalan Penyebab Umum sering ditangani menggunakan analisis persentase Kegagalan Penyebab Umum yang mempengaruhi SIL yang dicapai. Ini disebut **Metode Faktor Beta (*Beta Factor Method*)**.

Kegagalan Penyebab Umum dapat dihilangkan, atau dikurangi secara substansial, dengan tidak hanya menggunakan arsitektur redundan, tetapi dengan menggunakan **berbagai jenis peralatan yang beragam (*diverse equipment*)** dalam arsitektur redundan tersebut, serta menerapkan pemisahan fisik jalur impuls dan perkabelan.

Cakupan Diagnostik (Diagnostic Coverage)

Cakupan Diagnostik (*Diagnostic Coverage*) adalah faktor lain yang memungkinkan pencapaian target SIL yang berpotensi lebih tinggi.

Diagnostik pada dasarnya adalah pengujian pembuktian otomatis dari komponen SIS individual yang terjadi secara cepat dan otomatis di latar belakang, tetapi hanya mendeteksi sebagian dari potensi kegagalan perangkat. Fraksi kegagalan yang dapat dideteksi secara otomatis ini disebut sebagai cakupan diagnostik.

Diagnostik menurunkan probabilitas kegagalan keseluruhan dari suatu SIF dengan secara efektif mengurangi laju kegagalan berbahaya tak terdeteksi (λ_{DU}). Jika kegagalan berbahaya dari komponen SIF terdeteksi oleh diagnostik internal, kegagalan tersebut kemudian dapat diubah menjadi kegagalan yang aman dengan mengonfigurasi SIF untuk secara otomatis beralih ke kondisi aman jika terjadi kegagalan yang terdeteksi, atau mengaktifkan alarm degradasi yang memungkinkan operator melakukan intervensi perbaikan segera sebelum terjadi permintaan bahaya proses.

Perhitungan PFD dan Persamaan yang Disederhanakan

Perhitungan probabilitas kegagalan keseluruhan, yang mempertimbangkan semua faktor yang dijelaskan sebelumnya, dilakukan menggunakan model keandalan seperti Analisis Pohon Kesalahan (*Fault Tree Analysis - FTA*), persamaan matematika yang disederhanakan, atau model rantai Markov untuk mengevaluasi setiap SIF.

Standar industri mewajibkan verifikasi kuantitatif bahwa target SIL yang dipilih telah dicapai untuk desain yang dipilih. Meskipun masing-masing metode potensial memiliki kelebihan dan kekurangan, **opsi persamaan yang disederhanakan terutama digunakan oleh para praktisi industri** jika memungkinkan. Dalam kasus di mana situasi yang dimodelkan tidak dapat dijelaskan menggunakan kumpulan standar persamaan yang disederhanakan, alat yang lebih kuat tetapi lebih sulit digunakan, seperti FTA, digunakan untuk mendukung persamaan yang disederhanakan.

Perhitungan PFDavg keseluruhan dari suatu SIF dimulai dengan penggunaan salah satu persamaan yang ditunjukkan di bawah ini untuk setiap subsistem: sensor, logic solver, antarmuka elemen akhir, dan elemen akhir. Persamaan yang digunakan mempertimbangkan laju kegagalan spesifik dari perangkat yang dianalisis dan interval pengujian yang diusulkan:

FORMULA RESMI ISA-TR84.00.02

PERSAMAAN MATEMATIKA SEDERHANA UNTUK PFDavg SUBSISTEM:

- **1001:** $PFD_{avg} = \lambda^{DU} \times (TI / 2)$
- **1001D-NT:** $PFD_{avg} = [\lambda^{DU} \times (TI / 2)] + [(\lambda^{DD} + \lambda^{SD}) \times MTTR]$
- **1002:** $PFD_{avg} = [(\lambda^{DU})^2 \times (TI^2 / 3)] + [\beta \times \lambda^{DU} \times (TI / 2)]$
- **2002:** $PFD_{avg} = \lambda^{DU} \times TI$
- **2003:** $PFD_{avg} = [(\lambda^{DU})^2 \times TI^2] + [\beta \times \lambda^{DU} \times (TI / 2)]$

PERSAMAAN UNTUK LAJU TRIP PALSU (SPURIOUS TRIP RATE - STR):

- **1001:** $STR = \lambda^S + \lambda^{DD}$
- **1001D-NT:** $STR = \lambda^{SU}$
- **1002:** $STR = 2 \times (\lambda^S + \lambda^{DD})$
- **2002:** $STR = [2 \times (\lambda^S + \lambda^{DD})^2 \times MTTR] + [\beta \times (\lambda^S + \lambda^{DD})]$
- **2003:** $STR = [6 \times (\lambda^S + \lambda^{DD})^2 \times MTTR] + [\beta \times (\lambda^S + \lambda^{DD})]$

BAB 8: SPESIFIKASI PERSYARATAN KESELAMATAN (SRS)

KERANGKA KERJA TAHAP PENYUSUNAN SRS

ALUR KERJA TAHAP SPESIFIKASI PERSYARATAN KESELAMATAN:

- **Masukan (Input):** Laporan Pemilihan SIL, Hasil Perhitungan Verifikasi SIL, Diagram P&ID.
- **Tugas Rekayasa (Task):** Pengembangan Spesifikasi Persyaratan Keselamatan (SRS Development).
- **Perangkat (Tools):** Templat SRS Kenexis (Excel / Word), Diagram Matriks Sebab-Akibat.
- **Luaran (Deliverable):** Paket Dokumen SRS (Safety Requirements Specifications) → Masukan Desain Terperinci.

Tugas 'Safety Requirements Specifications' (Spesifikasi Persyaratan Keselamatan) adalah langkah berikutnya dalam Siklus Hidup Keselamatan. Pengembangan Spesifikasi Persyaratan Keselamatan (SRS) terjadi pada akhir fase Desain Konseptual / Verifikasi SIL setelah desain yang diusulkan telah dikonfirmasi mencapai target integritasnya.

Tujuan dari SRS adalah untuk **mendefinisikan persyaratan fungsional dan kinerja yang berkaitan dengan keselamatan**. SRS disiapkan secara cukup terperinci sehingga fungsionalitas seluruh SIS (khususnya logic solver) didefinisikan dengan ketelitian yang memadai agar tugas-tugas rekayasa desain terperinci dapat dilanjutkan (biasanya oleh kelompok yang berbeda dari yang menyiapkan paket basis desain SRS).

Standar IEC 61511 / ISA 84.00.01-2004 menyediakan daftar komprehensif dari informasi yang harus didokumentasikan, atau setidaknya dipertimbangkan selama fase ini.

29 Butir Persyaratan Wajib SRS menurut Standar (Bagian 1)

Standar IEC 61511 / ISA 84.00.01-2004 menetapkan daftar informasi yang harus didokumentasikan dalam Spesifikasi Persyaratan Keselamatan (SRS). Butir 1 hingga 15 adalah sebagai berikut:

- **1. Deskripsi dari semua fungsi berinstrumen keselamatan (SIF)** yang diperlukan untuk mencapai keselamatan fungsional yang dipersyaratkan.
- **2. Persyaratan untuk mengidentifikasi dan memperhitungkan kegagalan penyebab umum (common cause failures).**
- **3. Definisi kondisi proses yang aman (safe state)** untuk setiap fungsi keselamatan berinstrumen yang diidentifikasi.
- **4. Definisi mengenai kondisi-kondisi proses aman individual** yang, apabila terjadi secara bersamaan, dapat menciptakan bahaya terpisah (misalnya, kelebihan beban pada tangki penyimpanan darurat, pelepasan simultan ganda ke sistem flare).
- **5. Asumsi sumber permintaan (demand)** dan laju permintaan (demand rate) pada fungsi berinstrumen keselamatan.
- **6. Persyaratan untuk interval uji pembuktian fungsional berkala (proof-test intervals).**
- **7. Persyaratan waktu respons bagi SIS** untuk membawa proses ke kondisi aman (process safety time).
- **8. Tingkat integritas keselamatan (SIL)** dan mode operasi (permintaan rendah / terus menerus) untuk setiap SIF.
- **9. Deskripsi pengukuran variabel proses SIS** dan titik-titik trip pengamannya (trip setpoints).
- **10. Deskripsi tindakan keluaran proses SIS** dan kriteria untuk keberhasilan operasi (misalnya persyaratan katup penutup kedap gelembung Class VI).
- **11. Hubungan fungsional antara masukan dan keluaran proses**, termasuk logika, fungsi matematika, dan setiap kondisi izin (permissives) yang diperlukan.
- **12. Persyaratan fasilitas penghenti proses darurat manual (manual shutdown).**
- **13. Persyaratan yang berkaitan dengan tindakan logika de-energize to trip** (hilangkan daya untuk trip) atau energize to trip (beri daya untuk trip).
- **14. Persyaratan untuk menyetel ulang (reset) SIS** setelah terjadi shutdown.
- **15. Laju trip palsu maksimum yang diizinkan (maximum allowable spurious trip rate).**

29 Butir Persyaratan Wajib SRS menurut Standar (Bagian 2)

Kelanjutan persyaratan wajib Spesifikasi Persyaratan Keselamatan (SRS) menurut standar IEC 61511 / ISA 84.00.01 (butir 16 hingga 29):

- **16. Moda kegagalan dan respons yang diinginkan dari SIS** (misalnya, alarm diagnostik saja, atau shutdown otomatis).
- **17. Setiap persyaratan khusus yang berkaitan dengan prosedur untuk menyalakan (start-up) dan menyalakan kembali (restart) SIS.**
- **18. Semua antarmuka antara SIS dan sistem lainnya** (termasuk BPCS/DCS dan antarmuka operator HMI).
- **19. Deskripsi moda operasi pabrik dan identifikasi fungsi berinstrumen keselamatan yang diperlukan untuk beroperasi dalam setiap moda.**
- **20. Persyaratan keselamatan perangkat lunak aplikasi (application software safety requirements).**
- **21. Persyaratan untuk overrides / inhibits / bypasses** termasuk bagaimana penonaktifan sementara tersebut akan dilepaskan (cleared).
- **22. Spesifikasi tindakan apa pun yang diperlukan untuk mencapai atau mempertahankan kondisi aman jika terjadi kesalahan yang terdeteksi pada SIS, dengan mempertimbangkan semua faktor manusia yang relevan.**
- **23. Waktu rata-rata untuk memperbaiki (MTTR) yang layak untuk SIS, dengan mempertimbangkan waktu perjalanan, lokasi, suku cadang, kontrak servis, dan batasan lingkungan.**
- **24. Identifikasi kombinasi berbahaya dari status keluaran SIS yang perlu dihindari.**
- **25. Kondisi lingkungan ekstrem yang mungkin dihadapi SIS harus diidentifikasi** (suhu, kelembapan, kontaminan, pentanahan, EMI/RFI, getaran, pelepasan elektrostatis, klasifikasi area berbahaya listrik, banjir, petir).
- **26. Identifikasi moda normal dan abnormal untuk pabrik secara keseluruhan (start-up pabrik) dan prosedur operasional individu pabrik (pemeliharaan peralatan, kalibrasi/perbaikan sensor).**
- **27. Definisi persyaratan untuk setiap SIF yang diperlukan untuk bertahan dalam peristiwa kecelakaan besar (misalnya waktu yang dibutuhkan katup untuk tetap beroperasi jika terjadi kebakaran eksternal).**
- **28. Persyaratan kualifikasi personel dan sertifikasi kompetensi teknis untuk pemeliharaan sistem.**
- **29. Persyaratan keandalan pasokan utilitas listrik dan udara instrumen (fail-safe upon utility loss).**

Pendekatan Praktis Penyusunan Paket SRS Holistik Kenexis

Meskipun semua informasi yang dijelaskan di atas harus dikembangkan untuk mendefinisikan SIS secara lengkap, **bukanlah praktik yang baik untuk mencoba menggabungkan semua informasi tersebut ke dalam satu dokumen tunggal dengan format mengisi titik-titik.**

Sering kali, insinyur yang baru mengenal SIS dan belum memiliki pengalaman signifikan dalam spesifikasi sistem instrumentasi dan kendali, menggunakan pembacaan standar sebagai satu-satunya dasar mereka tentang cara menentukan sistem kendali. Mereka secara keliru mencoba menggunakan IEC 61511 / ISA 84.00.01 sebagai panduan desain alih-alih sebagai kumpulan persyaratan kinerja. Ini sering kali menghasilkan dokumen SRS yang menggunakan daftar butir-butir standar sebagai 'kerangka garis besar' dan kemudian melanjutkan untuk 'mengisi bagian yang kosong' untuk setiap SIF.

Proses ini biasanya menghasilkan hasil yang sangat buruk. Dokumen menjadi sangat sulit digunakan oleh integrator sistem dan vendor peralatan, karena tidak menyajikan pandangan yang komprehensif tentang sistem, dan juga mencakup sejumlah besar data berulang yang tidak berguna bagi perancang sistem, serta sering kali tidak dimutakhirkan ketika perubahan berikutnya terjadi.

Pendekatan yang jauh lebih baik adalah menyediakan **paket komprehensif yang menggambarkan seluruh SIS secara holistik**. Paket jenis ini biasanya berisi:

1. **Deskripsi Logika Fungsional:** Sering disajikan dalam format Diagram Sebab dan Akibat (*Cause and Effect Diagram*) yang ringkas dan mudah digunakan.
2. **Dokumen Persyaratan Umum (General Requirements Document):** Kumpulan persyaratan yang diterapkan secara seragam untuk semua SIF—seperti persyaratan bypass dan tindakan respons kegagalan—sangat baik dimuat dalam dokumen persyaratan umum tunggal ini.
3. **Dokumen Catatan Spesifik (Specific Notes Document):** Kompleksitas sistem yang unik untuk satu SIF tunggal dan terlalu rumit untuk dijelaskan dalam konteks diagram sebab-akibat dapat dijelaskan dalam dokumen catatan spesifik.

Menggunakan metodologi ini, pandangan sistem holistik disediakan, pengulangan informasi diminimalkan, dan informasi yang tidak relevan bagi pengguna paket SRS (seperti rincian pemilihan SIL) tidak disertakan. Setelah disiapkan, paket SRS ini dapat diberikan kepada kontraktor desain terperinci dan vendor peralatan untuk mengimplementasikan sistem yang konsisten dengan SIL.

BAB 9: DESAIN TERPERINCI DAN SPESIFIKASI (DETAILED DESIGN)

KERANGKA KERJA DESAIN TERPERINCI

ALUR KERJA TAHAP DESAIN TERPERINCI & SPESIFIKASI:

- **Masukan (Input):** Paket Dokumen SRS (Safety Requirements Specifications), Diagram Sebab-Akibat.
- **Tugas Rekayasa (Task):** Desain Rekayasa Terperinci & Spesifikasi (Detailed Design & Specifications).
- **Perangkat (Tools):** Templat Spesifikasi Perangkat Keras/Lunak, Software CAD, Tool Rekayasa PLC.
- **Luaran (Deliverable):** Paket Desain Terperinci (Detailed Design Package) → Masukan untuk Konstruksi.

Fase 'Desain Rekayasa Terperinci dan Spesifikasi' terjadi setelah tim Basis Desain SIS menyelesaikan Spesifikasi Persyaratan Keselamatan (SRS), yang kemudian berfungsi sebagai dasar untuk semua tugas desain berikutnya. Dalam langkah ini, perancangan SIS sangat mirip dengan perancangan sistem kendali non-keselamatan lainnya.

Beberapa tugas utama yang dilakukan selama fase rekayasa terperinci ini meliputi hal-hal berikut:

- **Pengembangan spesifikasi instrumentasi dan rekuisisi:** Membuat lembar data teknis spesifikasi instrumen lapangan dan pesanan pembelian resmi.
- **Pengembangan lembar loop (loop sheets):** Menggambarkan konfigurasi listrik dan terminasi lengkap dari setiap simpal instrumen keselamatan.
- **Pengembangan daftar input/output logic solver:** Menyusun rincian alokasi titik I/O analog dan digital pada modul logic solver SIS.
- **Pengembangan tata letak kabinet logic solver:** Merancang pengaturan fisik internal dan eksternal kabinet kendali, manajemen termal, dan distribusi daya.
- **Pengembangan diagram pengkabelan internal kabinet:** Menggambar skema kabel dari terminal blok ke kartu I/O, catu daya, dan relai pembatas.
- **Persiapan diagram pengkabelan interkoneksi dan jadwal kabel:** Mengatur jalur kabel lapangan dari kotak persimpangan (junction box) ke ruang kendali.
- **Pengembangan program PLC keselamatan:** Menulis dan menguji kode logika aplikasi keselamatan menggunakan bahasa terstandarisasi IEC 61131-3.

BAB 10: PENGEMBANGAN PROSEDUR (PROCEDURE DEVELOPMENT)

KERANGKA KERJA PENGEMBANGAN PROSEDUR

ALUR KERJA TAHAP PENGEMBANGAN PROSEDUR:

- **Masukan (Input):** Spesifikasi Desain Terperinci, Paket SRS, Pedoman Pabrikan Peralatan.
- **Tugas Rekayasa (Task):** Pengembangan Prosedur Operasi, Pemeliharaan, dan Pengujian.
- **Perangkat (Tools):** Templat Prosedur Operasi Standar (SOP), Database Pemeliharaan Pabrik (CMMS).
- **Luaran (Deliverable):** Buku Prosedur Operasi dan Pemeliharaan SIS → Masukan untuk Komisioning & PSAT.

Langkah berikutnya dalam Siklus Hidup Keselamatan adalah 'Pengembangan Prosedur'. Yang dimaksud di sini adalah **Prosedur Operasi**, serta **Prosedur Pemeliharaan dan Pengujian** dari Sistem Berinstrumen Keselamatan. Prosedur harus mengatur berbagai moda operasi SIS, termasuk operasi start-up, bypass, dan reset. Prosedur juga harus mengatur respons manual terhadap kegagalan SIS yang terdeteksi, serta persyaratan pengujian fungsional untuk mencapai SIL yang dipersyaratkan.

Filosofi Pengujian Fungsional Penuh (Full Functional Testing)

Sebelum prosedur dapat ditulis, pengguna akhir harus menetapkan filosofi yang dipilih tentang bagaimana SIS akan diuji, dirawat, dan dioperasikan. Rincian yang tampaknya kecil dapat memiliki dampak besar pada efektivitas SIS.

Umumnya lebih disukai untuk melakukan **pengujian fungsional penuh (full functional test)** setiap kali memungkinkan secara praktis, yang secara simultan menguji semua komponen SIF mulai dari perangkat penginderaan (sensor), melalui logic solver, dan keluar ke elemen akhir. Contoh uji fungsional penuh adalah mengisolasi pemancar tekanan dari saluran impuls proses, menghubungkan pompa tangan ke port uji pemancar, memberi tekanan pada sensor ke titik trip dan mengonfirmasi fungsi diaktifkan pada nilai yang benar dan katup akhir menutup penuh (misalnya uji kebocoran Class VI bubble-tight).

Uji fungsional penuh memiliki peluang terbaik untuk menemukan kegagalan tersembunyi (*covert failures*). Ini membuat pengguna akhir lebih mudah mencapai laju kegagalan berbahaya yang diklaim dalam perhitungan verifikasi SIL. Sebaliknya, menghubungkan simulator sinyal listrik ke terminal lapangan adalah contoh praktik pengujian inferior yang hanya menguji sebagian kecil sirkuit I/O dan logika, tetapi gagal mendeteksi penyumbatan saluran impuls, kerusakan diafragma sensor, atau masalah mekanis katup lapangan.

Filosofi Pengendalian Bypass dan Faktor Manusia

Ketika menetapkan filosofi bypass, pengguna akhir harus memperhitungkan faktor manusia; dalam sebagian besar kecelakaan besar industri, pembypassan yang tidak disengaja atau disengaja disebut sebagai faktor kontribusi utama.

Ada nilai yang diakui dalam kemampuan untuk menempatkan elemen penginderaan (sensor) pada status bypass sementara. Jika sensor memerlukan kalibrasi ulang, pemeliharaan, atau penggantian rutin, bypass sensor dapat memungkinkan aktivitas tersebut berlangsung tanpa memerlukan penghentian (shutdown) fasilitas pabrik secara menyeluruh. Tindakan bypass dapat dilakukan melalui perangkat lunak atau sakelar kabel-keras, meskipun perangkat lunak biasanya lebih nyaman.

Ketika bypass perangkat lunak diterapkan dan dapat diaktifkan melalui sistem kendali terdistribusi (DCS), komunikasi antara SIS dan DCS harus dirancang secara cermat untuk memastikan bahwa SIS dapat dengan cepat kembali dari mode 'bypass diaktifkan' ke mode 'normal' tanpa mengharuskan operator melepaskan setiap sensor yang dibypass secara manual satu per satu. Selain itu, diagnostik komunikasi SIS-DCS harus digunakan yang memungkinkan SIS berfungsi dengan baik jika terjadi kehilangan komunikasi antara kedua sistem.

BAHAYA PEMBYPASAN ELEMEN AKHIR

PERINGATAN KESELAMATAN KRITIS: LARANGAN MEMBYPASS ELEMEN KELUARAN AKHIR

Antarmuka SIS harus dirancang sedemikian rupa sehingga **operator, teknisi instrumen, dan insinyur TIDAK MAMPU membypass keluaran (elemen akhir)**.

Alasan Teknis: Sebagian besar keluaran (seperti katup penutup bahan bakar utama) diaktifkan oleh beberapa sensor yang berbeda secara bersamaan. Sebagai contoh, dalam tungku pemanas berbahan bakar (fired heater), katup pasokan bahan bakar dapat ditutup karena:

1. Tekanan kotak api (firebox) tinggi,
2. Tekanan gas bahan bakar tinggi atau rendah,
3. Suhu proses tinggi berlebih,
4. Analisator oksigen / gas mudah terbakar mendeteksi bahaya, atau
5. Kegagalan kipas draft udara pembakaran.

Kondisi abnormal dalam salah satu dari variabel-variabel yang berbeda ini dapat memerlukan aktivasi shutdown. **Jika suatu elemen keluaran akhir dibypass, tindakan tersebut secara efektif MEMBYPASS SEMUA interlock kritis ini secara simultan!** Hal ini melumpuhkan seluruh sistem pertahanan keselamatan fasilitas.

BAB 11: KONSTRUKSI, INSTALASI, DAN KOMISIONING

KERANGKA KERJA TAHAP KONSTRUKSI

ALUR KERJA KONSTRUKSI, INSTALASI, DAN KOMISIONING:

- **Masukan:** Paket Desain Terperinci, Perangkat Keras Logic Solver & Lapangan, Rencana Validasi.
- **Tugas:** Pengadaan Peralatan, Instalasi Fisik, Penarikan Kabel, Komisioning Lapangan.
- **Luaran:** Sistem Terpasang Siap Uji → Masukan untuk Pre-Startup Acceptance Testing (PSAT).

Langkah berikutnya dari Siklus Hidup Keselamatan adalah '**Construction, Installation, and Commissioning**' (**Konstruksi, Instalasi, dan Komisioning**). Langkah ini sangat mirip dengan kegiatan desain, komisioning, dan start-up sistem kendali standar non-SIS lainnya. Ini melibatkan pembelian peralatan, instalasi fisik di lokasi pabrik, pengimporan dan pemuatan program perangkat lunak aplikasi, dan penyambungan kabel instrumen. Semua ini harus diselesaikan secara tuntas sebelum Uji Penerimaan Pra-Startup dilaksanakan.

BAB 12: UJI PENERIMAAN PRA-STARTUP (PSAT) — BAGIAN 1

KERANGKA KERJA TAHAP PSAT

ALUR KERJA TAHAP PRE-STARTUP ACCEPTANCE TESTING (PSAT):

- **Masukan (Input):** Rencana Validasi (Validation Plan), Paket Dokumen SRS, Sistem Terpasang.
- **Tugas Rekayasa (Task):** Pre-Startup Acceptance Testing (PSAT).
- **Perangkat (Tools):** Templat Daftar Periksa (Checklist Template), Prosedur Uji Lapangan.
- **Luaran (Deliverable):** Daftar Temuan (Punchlists) & Laporan Validasi Sistem Siap Operasi.

'**Pre-Startup Acceptance Testing**' (**PSAT**) adalah langkah berikutnya dalam Siklus Hidup Keselamatan. Dalam langkah ini, persyaratannya adalah memverifikasi bahwa peralatan dan perangkat lunak yang dipasang sesuai dengan Spesifikasi Persyaratan Keselamatan (SRS). Ini adalah kegiatan yang berlangsung di lokasi proyek selama kegiatan komisioning, instalasi, dan start-up.

Insinyur desain meninjau perangkat keras dan perangkat lunak untuk memastikan semua persyaratan yang ditetapkan dalam Spesifikasi Persyaratan Keselamatan telah dicapai secara penuh. Setiap penyimpangan yang relevan harus dicatat dalam daftar punchlist dan diperbaiki sebelum peralatan ditempatkan dalam layanan operasional.

Uji Penerimaan Pra-Startup (PSAT) — Bagian 2

Selain peninjauan dokumentasi dan inspeksi fisik, **pengujian fungsional penuh (*full-functional test*) dari sistem umumnya diwajibkan selama pengujian penerimaan pra-startup** untuk membuktikan secara empiris bahwa sistem berperilaku tepat seperti yang ditentukan dalam Spesifikasi Persyaratan Keselamatan.

Metode yang benar dalam melakukan PSAT adalah mengonfirmasi bahwa desain sesuai dengan SRS. Hal ini karena SRS berisi keputusan desain kritis, preferensi operasional, dan persyaratan yang membentuk dasar dari sistem yang dirancang dengan baik. Jika seorang integrator SIS telah salah menafsirkan suatu persyaratan dalam SRS, PSAT adalah kesempatan terakhir bagi cacat desain tersebut untuk ditemukan dan diperbaiki sebelum sistem menjadi operasional dan dialiri bahan berbahaya.

VERIFIKASI INDEPENDEN SEBELUM START-UP

PENTINGNYA PENILAI PIHAK KETIGA INDEPENDEN DALAM PSAT:

Ini adalah alasan kuat mengapa **pihak ketiga yang independen dari integrator SIS**, dan yang memiliki pemahaman menyeluruh tentang persyaratan SRS, harus memimpin atau mendampingi pelaksanaan PSAT.

Pihak ketiga independen akan mampu memberikan penilaian objektif mengenai integritas desain dan dapat mengonfirmasi tanpa bias komersial bahwa sistem telah diimplementasikan dengan mematuhi seluruh persyaratan pengguna akhir serta standar keselamatan internasional sebelum start-up fasilitas dilakukan.

Pelaksanaan PSAT yang ketat memastikan tidak ada celah antara asumsi teoretis yang digunakan dalam studi analisis bahaya dan kondisi fisik peralatan yang terpasang di lapangan.

BAB 13: OPERASI DAN PEMELIHARAAN (OPERATION AND MAINTENANCE)

KERANGKA KERJA OPERASI DAN PEMELIHARAAN

ALUR KERJA TAHAP OPERASI DAN PEMELIHARAAN:

- **Masukan (Input):** Prosedur Operasi & Pemeliharaan, Jadwal Uji Fungsional Berkala (TI).
- **Tugas Rekayasa (Task):** Operasi, Pemeliharaan, Pengujian Rutin, Respons Alarm Diagnostik.
- **Perangkat (Tools):** Sistem Manajemen Pemeliharaan Terkomputerisasi (CMMS), Logbook Operasi.
- **Luaran (Deliverable):** Catatan Kinerja Keandalan Lapangan → Masukan untuk Manajemen Perubahan (MOC).

Langkah berikutnya dalam Siklus Hidup Keselamatan adalah '**Operation And Maintenance**' (**Operasi dan Pemeliharaan**).

Selama fase ini, jika semuanya berjalan sesuai rencana, sangat sedikit aktivitas luar biasa yang akan terjadi sehubungan dengan SIS. Aktivitas terkait SIS yang rutin dan terencana mencakup:

1. **Pengujian fungsional berkala (proof testing):** Melaksanakan uji bukti berkala pada instrumen sensor, logic solver, dan katup akhir sesuai interval pengujian (TI) yang ditetapkan dalam SRS guna mengungkap kegagalan laten.
2. **Menanggapi kesalahan nyata (overt faults):** Merespons alarm kerusakan komponen SIS yang terdeteksi secara otomatis oleh fitur diagnostik internal.
3. **Perbaikan dan pemulihan subsistem:** Respons ini biasanya mencakup perbaikan atau penggantian subsistem yang gagal dalam batas waktu perbaikan rata-rata (MTTR) yang diasumsikan dalam perhitungan keandalan.

Kedisiplinan dalam menjalankan pengujian berkala dan dokumentasi pemeliharaan selama fase ini sangat menentukan apakah tingkat ketersediaan keselamatan yang telah dirancang akan tetap bertahan sepanjang masa pakai pabrik.

BAB 14: MANAJEMEN PERUBAHAN (MANAGEMENT OF CHANGE)

KERANGKA KERJA TAHAP MANAJEMEN PERUBAHAN

ALUR KERJA TAHAP MANAJEMEN PERUBAHAN:

- **Masukan (Input):** Usulan Perubahan Peralatan/Proses, Data Komponen Baru, Laporan SIL Asli.
- **Tugas Rekayasa (Task):** Manajemen Perubahan (Management of Change - MOC) & Verifikasi Ulang SIL.
- **Perangkat (Tools):** Prosedur MOC Fasilitas, Toolkit Verifikasi SIL, Pemutakhiran SRS.
- **Luaran (Deliverable):** Persetujuan Perubahan & Basis Desain SIS Terkini (Evergreen).

Manajemen Perubahan (*Management of Change* - MOC) terjadi ketika perubahan diusulkan pada Sistem Berinstrumen Keselamatan, yang bukan merupakan penggantian jenis yang serupa (*not like-in-kind changes*).

Prosedur Manajemen Perubahan di lokasi pabrik harus diikuti untuk mengevaluasi dan menangani perubahan tersebut secara memadai sebelum implementasi, guna mengidentifikasi potensi bahaya yang dapat timbul dari perubahan tersebut. Langkah ini penting untuk memastikan bahwa modifikasi konsisten dengan Spesifikasi Persyaratan Keselamatan (SRS), dan mempertahankan Tingkat Integritas Keselamatan (SIL) yang dipersyaratkan.

Ketika perubahan terjadi dalam sistem, komponen baru cenderung memiliki laju kegagalan (λ) dan cakupan diagnostik yang berbeda dari aslinya. Jika ini benar, maka **perhitungan verifikasi SIL yang ada menjadi tidak benar** dan memverifikasi bahwa komponen baru mampu mencapai SIL yang dipersyaratkan adalah langkah pertama dalam proses MOC.

Tergantung pada komponen baru tersebut, desain Fungsi Berinstrumen Keselamatan (SIF) yang baru mungkin dapat mencapai SIL yang ada atau mungkin tidak. Jika tidak tercapai, frekuensi pengujian dapat disesuaikan (diperpendek), instrumentasi tambahan mungkin diperlukan (menambah redundansi), atau bagian lain dari SIF mungkin memerlukan modifikasi desain.

Setelah perhitungan verifikasi SIL baru selesai, perangkat keras harus ditinjau untuk memastikan perangkat keras tersebut mampu memenuhi semua persyaratan yang ditentukan sebagai bagian dari SRS. Jika perangkat keras baru memiliki persyaratan tambahan, atau tidak memenuhi beberapa persyaratan SRS yang ada, SRS harus dimodifikasi untuk memperhitungkan hal ini.

Revalidasi Berkala Pemilihan SIL dan Basis Desain

Terkadang faktor-faktor lain memerlukan MOC untuk bagian dari SIS. Misalnya, jika pedoman toleransi risiko korporat berubah, hal itu dapat mempengaruhi implementasi banyak SIF. Dalam kasus seperti itu proses pemilihan SIL harus ditinjau untuk menetapkan (atau mengonfirmasi) target SIL untuk fungsi-fungsi tersebut.

Jika analisis risiko kuantitatif (QRA) dilakukan yang menyediakan informasi yang lebih akurat tentang bahaya spesifik, SIF untuk fungsi tersebut dapat berubah sehubungan dengan hasil analisis. Contoh terakhir adalah di mana lapisan perlindungan yang diklaim selama pemilihan SIL ternyata kurang (atau lebih) efektif daripada yang diklaim, berdasarkan data operasional terbaru. Ketika ini terjadi, hasil pemilihan SIL harus ditinjau untuk menentukan SIL baru untuk fungsi yang terpengaruh. Setiap contoh yang disebutkan dapat memerlukan penambahan instrumen, modifikasi instrumen, atau interval uji fungsional baru.

Untuk alasan ini, **laporan pemilihan SIL harus ditinjau dan divalidasi ulang secara berkala (pada frekuensi yang sama yang disarankan untuk revalidasi PHA — yaitu lima tahun sekali)** untuk memastikan bahwa SIL yang dipilih konsisten dengan filosofi korporat saat ini, praktik terbaik industri, dan data pemodelan yang paling akurat.

BAB 15: KESIMPULAN — BAGIAN 1

Safety Instrumented Systems digunakan di pabrik proses untuk **mengurangi risiko — bukan untuk menghilangkan risiko secara mutlak — tetapi untuk menguranginya ke apa yang dianggap sebagai tingkat yang dapat ditoleransi** oleh operator pabrik tersebut.

Di Amerika Serikat, peraturan dari OSHA, serta EPA, mengatur perancangan, pengujian, pemeliharaan, dan pengoperasian Sistem Berinstrumen Keselamatan. Anda harus mengetahui persyaratan peraturan ini sebelum memulai proyek perancangan Sistem Berinstrumen Keselamatan. Sebagian besar perusahaan memiliki beberapa jenis program untuk perancangan dan implementasi Sistem Berinstrumen Keselamatan.

Semakin banyak perusahaan yang menyesuaikan diri dengan standar rekayasa SIS dari ISA dan IEC. Standar baru ini berbasis kinerja, bukan preskriptif. Standar tersebut mengharuskan Anda menetapkan tingkat kinerja, atau tujuan, yang harus dicapai oleh desain rekayasa SIS, alih-alih mendiktekan seperti apa bentuk desain tersebut.

BAB 15: KESIMPULAN — BAGIAN 2

Buku panduan ini telah menyajikan ringkasan Siklus Hidup Desain Rekayasa SIS. Sebelum fasilitas Anda menerapkan siklus hidup ini, hal ini harus dipertimbangkan dan dipahami secara cermat.

Fungsi Berinstrumen Keselamatan dalam desain proses yang ada maupun yang baru memerlukan analisis mendalam untuk mengidentifikasi fungsi-fungsi tersebut, dan menangani persyaratan Tingkat Integritas Keselamatan untuk setiap fungsi. Tingkat Integritas Keselamatan dapat dioptimalkan untuk memperhitungkan kemungkinan kejadian pemicu dan perlindungan yang masuk akal, dengan demikian mengidentifikasi desain yang memenuhi tujuan keselamatan tanpa peralatan dan instrumentasi yang tidak perlu.

Peralatan yang Ada dan Efisiensi Desain Sejak Awal Proyek

Penggantian perangkat keras yang ada (*existing hardware*) tidak diwajibkan oleh standar, dan dalam banyak kasus, tidak dapat dibenarkan. Analisis persyaratan Tingkat Integritas Keselamatan memang diperlukan, dan dalam beberapa kasus — bahkan dalam banyak kasus — peralatan yang ada dapat dibuktikan mampu mencapai target Tingkat Integritas Keselamatan yang dipersyaratkan oleh perusahaan Anda.

Meskipun dalam banyak kasus peralatan yang ada sudah cukup untuk mencapai Tingkat Integritas Keselamatan, untuk beberapa fungsi tertentu modifikasi atau penambahan peralatan mungkin diperlukan. Biaya tambahan ini **selalu paling diminimalkan dengan menerapkan perubahan ini pada awal fase desain proyek**.

Banyak 'cerita horor' yang menggambarkan kesulitan dalam mengimplementasikan IEC 61511 / ISA 84.00.01 terjadi karena standar ini diterapkan di tengah-tengah proyek yang luas, atau setelah desain lapangan diselesaikan. Sama seperti desain proses yang tepat, **perancangan Sistem Berinstrumen Keselamatan yang tepat harus dilakukan pada awal proyek, bukan sebagai pemikiran susulan (*afterthought*)**.

LAMPIRAN A — DAFTAR AKRONIM (ACRONYMS)

Daftar singkatan dan akronim teknis internasional yang digunakan dalam rekayasa Sistem Berinstrumen Keselamatan (SIS):

Akronim	Kepanjangan Teknis Bahasa Inggris	Penjelasan Bahasa Indonesia
BPCS	Basic Process Control System	Sistem Kendali Proses Dasar (kontrol regulasi)
CMS	Consequence Mitigation System	Sistem Mitigasi Konsekuensi
DCS	Distributed Control System	Sistem Kendali Terdistribusi
EPA	Environmental Protection Agency (USA)	Badan Perlindungan Lingkungan Hidup AS
HAZOP	Hazards and Operability Study	Studi Bahaya dan Kemampuan Operasi Fasilitas
HSE	Health, Safety, and Environmental	Kesehatan, Keselamatan Kerja, dan Lingkungan (K3L)
HSE	Health and Safety Executive (UK)	Badan Eksekutif Kesehatan & Keselamatan Kerja Inggris
IEC	International Electrotechnical Commission	Komisi Elektroteknik Internasional
ISA	International Society for Automation	Masyarakat Otomasi Internasional
IPL	Independent Protection Layer	Lapisan Perlindungan Independen
HIPPS	High Integrity Pressure Protection System	Sistem Proteksi Tekanan Berintegritas Tinggi
LOPA	Layer of Protection Analysis	Analisis Lapisan Perlindungan
NFPA	National Fire Protection Association	Asosiasi Perlindungan Kebakaran Nasional AS
OSHA	Occupational Safety and Health Admin (USA)	Badan Keselamatan & Kesehatan Kerja AS
PFD	Probability of Failure on Demand	Probabilitas Kegagalan saat Dibutuhkan
P&ID	Piping and Instrumentation Diagram	Diagram Perpipaan dan Instrumentasi
PHA	Process Hazards Analysis	Analisis Bahaya Proses
PLC	Programmable Logic Controller	Pengendali Logika Terprogram
PRV	Pressure Relief Valve	Katup Pelepas Tekanan
PSV	Pressure Safety Valve	Katup Pengaman Tekanan
SIL	Safety Integrity Level	Tingkat Integritas Keselamatan
SIS	Safety Instrumented System	Sistem Berinstrumen Keselamatan
SOP	Standard Operating Procedure	Prosedur Operasi Standar
TMEL	Target Maximum Event Likelihood	Kemungkinan Kejadian Maksimum yang Ditargetkan

LAMPIRAN B — DEFINISI DAN TERMINOLOGI (BAGIAN 1)

Glosarium istilah teknis keselamatan fungsional dan keandalan sistem berinstrumen keselamatan (Bagian 1):

Terminologi	Definisi dan Penjelasan Teknis
% Safe Failures (% Kegagalan Aman)	Faktor yang digunakan untuk membagi laju kegagalan keseluruhan untuk suatu perangkat menjadi kegagalan aman (yaitu, kegagalan perangkat yang cenderung memulai kondisi trip) dan kegagalan berbahaya (yaitu, kegagalan perangkat yang cenderung menghambat kondisi trip). Ini berbeda dari Safe Failure Fraction (SFF) sebagaimana didefinisikan oleh IEC 61508 dan IEC 61511 yang mencakup kegagalan berbahaya yang dapat dideteksi.
Architectural Constraints (Batasan Arsitektural)	Batasan yang dikenakan pada komponen dan arsitektur yang dipilih untuk implementasi fungsi berinstrumen keselamatan, terlepas dari kinerja yang dihitung untuk subsistem dalam hal PFDavg. Batasan ditentukan (dalam IEC 61508-2 Tabel 2 dan IEC 61511 Tabel 5) dan memerlukan derajat minimum toleransi kesalahan. Batasan arsitektural ditetapkan sesuai dengan SIL yang dipersyaratkan dari subsistem, 'tipe' komponen yang digunakan, dan Safe Failure Fraction (SFF) komponen. Perangkat Tipe A adalah perangkat sederhana non-mikroprosesor dengan moda kegagalan yang dipahami penuh, dan perangkat Tipe B adalah perangkat kompleks berbasis mikroprosesor.
Availability (Ketersediaan)	Probabilitas terhitung bahwa suatu perangkat beroperasi dengan sukses pada saat tertentu. Ini adalah ukuran waktu aktif (uptime), yang mempertimbangkan kemampuan deteksi dan kemampuan perbaikan kegagalan selain laju kegagalannya.
Beta Factor (β) (Faktor Beta)	Persentase kegagalan untuk perangkat tertentu yang diatribusikan pada moda kegagalan penyebab umum (common cause failure modes).
Common Cause (Penyebab Umum)	Mengacu pada kegagalan yang menyebabkan dua atau lebih perangkat berada dalam kondisi gagal berdasarkan peristiwa kegagalan tunggal. Peristiwa kegagalan tunggal dapat bersifat internal atau eksternal terhadap sistem.
Cd	Cakupan diagnostik dari kegagalan berbahaya (Dangerous Diagnostic Coverage). Kemampuan sistem untuk mendeteksi dan mendiagnosis kegagalan yang telah atau akan menyebabkan perangkat gagal ke kondisi berbahaya.
Cs	Cakupan diagnostik dari kegagalan aman (Safe Diagnostic Coverage). Kemampuan sistem untuk mendeteksi dan mendiagnosis kegagalan yang telah atau akan menyebabkan perangkat gagal ke kondisi aman.
Diagnostic Coverage (Cakupan Diagnostik)	Ukuran kemampuan sistem untuk mendeteksi kegagalan sendiri. Untuk SIS dengan kemampuan deteksi kesalahan aktif, ini adalah rasio antara laju kegagalan untuk kegagalan yang terdeteksi terhadap laju kegagalan untuk semua kegagalan dalam sistem.
Demand (Permintaan)	Suatu kondisi atau peristiwa proses yang memerlukan SIS untuk mengambil tindakan guna mencegah terjadinya peristiwa berbahaya.
DTT (De-energize to Trip)	Keluaran dan perangkat SIS diberi energi di bawah operasi normal. Penghapusan sumber daya (listrik, udara pneumatik) menyebabkan trip.
ETT (Energize to Trip)	Keluaran dan perangkat SIS dihilangkan energinya di bawah operasi normal. Penerapan daya menyebabkan trip.
Failure Category (Kategori Kegagalan)	Suatu perangkat dapat gagal dalam salah satu dari empat kategori kegagalan yang menggambarkan arah kegagalan (aman atau berbahaya) dan kemampuan kegagalan untuk didiagnosis: Safe Detected (SD), Dangerous Detected (DD), Safe Undetected (SU), dan Dangerous Undetected (DU) sesuai ISA TR84.0.02.
Fault Tolerance (Toleransi Kesalahan)	Kemampuan subsistem (sensor, logic solver, elemen akhir) untuk terus melakukan fungsi yang dipersyaratkan dengan adanya sejumlah kesalahan peralatan yang terbatas.
Fail-safe (Aman saat Gagal)	Kemampuan Fungsi Berinstrumen Keselamatan untuk beralih ke kondisi aman yang telah ditentukan sebelumnya jika terjadi malfungsi spesifik, terutama kehilangan energi listrik atau pneumatik.

LAMPIRAN B — DEFINISI DAN TERMINOLOGI (BAGIAN 2)

Glosarium istilah teknis keselamatan fungsional dan keandalan sistem berinstrumen keselamatan (Bagian 2):

Terminologi	Definisi dan Penjelasan Teknis
FMEDA	<i>Failure Modes Effects and Diagnostics Analysis</i> berarti analisis moda kegagalan untuk item peralatan, efek dari moda kegagalan tersebut, dan kemampuan perangkat untuk mendiagnosis kegagalan. Ini adalah metode untuk menentukan laju kegagalan, Safe Failure Fraction (SFF), dan cakupan diagnostik, persyaratan untuk sertifikasi peralatan terhadap persyaratan IEC 61508.
MTTF	<i>Mean Time to Failure</i> adalah jumlah waktu rata-rata yang berlalu antara menempatkan sistem ke dalam layanan operasi dan saat sistem tersebut mengalami kegagalan.
MTTF_{SPURIOUS}	<i>Mean Time to Fail Spurious</i> adalah waktu rata-rata hingga kegagalan sistem menyebabkan trip proses ketika tidak ada kondisi trip aktual yang ada di proses. Ini disebut trip palsu (spurious trip) karena menyiratkan kegagalan sistem instrumentasi dan kendali, tetapi kegagalan tersebut berada dalam arah yang 'aman'.
MTTR	<i>Mean Time to Repair</i> adalah waktu rata-rata terhitung untuk memperbaiki komponen yang gagal dari waktu deteksi hingga waktu untuk menyelesaikan perbaikan dan memulihkan komponen ke layanan.
Proof Test Coverage (Cakupan Uji Bukti)	Persentase kegagalan yang terdeteksi dan diperbaiki selama uji pembuktian fungsional peralatan. Cakupan uji bukti 100% berarti sistem dipulihkan ke kondisi kerja penuh, dan probabilitas kegagalan teoretis nol segera setelah sistem dipulihkan ke layanan.
Proof Test Interval (Interval Uji Bukti)	Interval waktu antara uji pembuktian dari item peralatan atau fungsi berinstrumen keselamatan.
PFD (Probability of Failure on Demand)	Probabilitas Kegagalan saat Dibutuhkan berarti probabilitas bahwa Fungsi Berinstrumen Keselamatan akan gagal secara berbahaya, dan tidak dapat melakukan fungsi keselamatannya saat diperlukan. PFD dapat ditentukan sebagai probabilitas rata-rata (PFDavg) atau probabilitas maksimum selama periode waktu yang ditentukan, yang biasanya merupakan interval uji bukti. IEC 61508/61511 dan ISA 84.01 menggunakan PFD rata-rata sebagai metrik sistem di mana SIL yang dicapai didefinisikan.
Random Hardware Failure (Kegagalan Acak Perangkat Keras)	Kegagalan yang terjadi pada waktu acak, yang dihasilkan dari satu atau lebih kemungkinan mekanisme degradasi pada perangkat keras fisik. Kegagalan perangkat keras acak bukan merupakan hasil dari kegagalan manusia dalam desain, pemrograman, atau pemeliharaan perangkat.
Redundancy (Redundansi)	Penggunaan beberapa komponen untuk melakukan fungsi yang sama. Redundansi dapat diimplementasikan oleh elemen identik (redundansi identik) atau oleh elemen yang beragam (redundansi beragam). Redundansi terutama digunakan untuk meningkatkan keandalan atau ketersediaan sistem.
Reliability (Keandalan)	Probabilitas bahwa suatu perangkat dapat melakukan fungsi yang dimaksudkan dalam kondisi yang dinyatakan untuk periode waktu tertentu tanpa kegagalan.

LAMPIRAN B — DEFINISI DAN TERMINOLOGI (BAGIAN 3)

Glosarium istilah teknis keselamatan fungsional dan keandalan sistem berinstrumen keselamatan (Bagian 3):

Terminologi	Definisi dan Penjelasan Teknis
RRF (Risk Reduction Factor)	Faktor Pengurangan Risiko untuk Fungsi Berinstrumen Keselamatan adalah kebalikan matematis dari PFDavg dari fungsi tersebut ($RRF = 1 / PFD_{avg}$). Ini adalah ukuran jumlah pengurangan risiko yang disediakan oleh SIF dengan asumsi fungsi tersebut digunakan secara preventif dan memiliki cakupan diagnostik 100% dari kondisi proses yang akan menghasilkan bahaya. $RRF = 100$ menyiratkan pengurangan risiko dengan faktor 100.
SFF (Safe Failure Fraction)	Fraksi dari laju kegagalan keseluruhan suatu perangkat yang menghasilkan kegagalan aman atau kegagalan berbahaya yang terdiagnosis (terdeteksi). Perhitungan SFF mencakup kegagalan berbahaya yang dapat dideteksi ketika kegagalan tersebut diberitahukan dan terjadi perbaikan atau proses dimatikan setelah deteksi kesalahan. Istilah ini didefinisikan secara ketat dalam IEC 61508.
SIF (Safety Instrumented Function)	Fungsi Berinstrumen Keselamatan adalah serangkaian tindakan spesifik yang harus diambil dalam keadaan tertentu, yang akan memindahkan proses kimia dari kondisi yang berpotensi tidak aman ke kondisi yang aman. Untuk mendefinisikan SIF secara memadai, enam pertimbangan harus dipenuhi: (i) Bahaya yang dicegah/dimitigasi; (ii) Kejadian pemicu / penyebab; (iii) Masukan untuk mendeteksi bahaya; (iv) Logika penghubung masukan dan keluaran; (v) Keluaran untuk membawa proses ke kondisi aman; (vi) Waktu yang diperlukan untuk membawa proses ke kondisi aman.
SIL (Safety Integrity Level)	Tingkat Integritas Keselamatan adalah ukuran kuantitatif dari efektivitas Fungsi Berinstrumen Keselamatan. SIL didefinisikan oleh ISA 84.00.01 dan IEC 61511/61508 sebagai pita orde besaran PFD: SIL 4 (PFD 10^{-4} hingga 10^{-5} , RRF 10.000-100.000); SIL 3 (PFD 10^{-3} hingga 10^{-4} , RRF 1.000-10.000); SIL 2 (PFD 10^{-2} hingga 10^{-3} , RRF 100-1.000); SIL 1 (PFD 10^{-1} hingga 10^{-2} , RRF 10-100).
SIS (Safety Instrumented System)	Implementasi dari satu atau lebih Fungsi Berinstrumen Keselamatan. SIS adalah sistem yang terdiri dari kombinasi sensor, logic solver, dan elemen akhir.
Spurious Trip (Trip Palsu)	Mengacu pada penghentian proses karena alasan yang tidak terkait dengan masalah dalam proses yang dirancang untuk dilindungi oleh SIS (misalnya kesalahan perangkat keras, kesalahan perangkat lunak, transien, interferensi bidang tanah). Istilah lain yang digunakan mencakup trip gangguan (nuisance trip) dan shutdown palsu (false shutdown).
Voting (Pemungutan Suara)	Sistem redundan (misalnya m dari n, 1oo2 untuk trip, 2oo3 untuk trip) yang memerlukan setidaknya m dari n saluran berada dalam kesepakatan sebelum SIS dapat mengambil tindakan keselamatan.

LAMPIRAN C — FREKUENSI KEJADIAN PEMICU TIPIKAL

Beberapa lapisan perlindungan independen umum dan kredit efektivitas tipikal ditunjukkan di bawah ini bersama dengan frekuensi kejadian pemicu tipikal:

Kejadian Pemicu (Initiating Event)	Kemungkinan Kegagalan (Kejadian per Tahun)
Kegagalan loop instrumen BPCS, termasuk sensor, pengontrol, dan elemen akhir. Mencakup kegagalan peralatan serta kesalahan operasional. <i>Catatan: IEC 61511 membatasi kemungkinan kegagalan BPCS tidak kurang dari 9×10^{-2} / tahun (IEC, 2003).</i>	10^{-1} (0,1 / tahun)
Kesalahan operator untuk mengeksekusi prosedur rutin, dengan asumsi terlatih dengan baik, tidak stres, tidak lelah.	10^{-2} per peluang
Kegagalan persiapan untuk pemeliharaan atau pengembalian pabrik dari pemeliharaan – kegagalan prosedur LOTO (lock-out tag-out).	10^{-3} per peluang
Kegagalan Pompa (pompa tunggal yang biasanya beroperasi) karena masalah mekanis. Tidak termasuk kehilangan daya listrik.	10^{-1} (atau lebih tinggi berdasarkan pengalaman lokasi)
Kegagalan kompresor atau blower karena masalah mekanis. Tidak termasuk kehilangan daya listrik.	10^{-1} (atau lebih tinggi berdasarkan pengalaman lokasi)
Kegagalan regulator (misalnya regulator tekanan self-contained).	10^{-1}
Kegagalan air pendingin (pompa CW redundan, penggerak beragam).	10^{-1}
Kehilangan Daya Listrik (catu daya redundan).	10^{-1}
Kegagalan Peralatan Tetap (misalnya kegagalan tabung penukar panas).	10^{-2}
Kegagalan bejana tekan (pressure vessel rupture).	10^{-6}
Kegagalan perpipaan – bagian 100 meter Robek Penuh (Full Breach).	10^{-5}
Kebocoran pipa 100 m.	10^{-3}
Kegagalan tangki penyimpanan atmosferik.	10^{-3}
Gasket / packing blowout (jebol).	10^{-2}
Kegagalan selang bongkar muat (loading / unloading hose).	10^{-1}
Kejadian Pemicu Lainnya	Dikembangkan menggunakan pengalaman tim ahli

LAMPIRAN D — LAPISAN PERLINDUNGAN TIPIKAL (BAGIAN 1)

Pengurangan risiko yang disarankan untuk Lapisan Perlindungan Independen (IPL):

IPL	IPL Kredit (Tipikal)	Batasan Lebih Lanjut untuk Dipertimbangkan sebagai IPL
Intervensi Operator menggunakan Prosedur Operasi	-	Tindakan harus independen dari penyebab pemicu dan IPL lainnya. JIKA tindakan operator adalah penyebab pemicu, tidak ada IPL yang boleh ditetapkan untuk tindakan operator yang semata-mata bergantung pada operator yang sama untuk mengenali masalah dan segera memperbaikinya. Jika penyebab pemicu adalah BPCS, tidak ada IPL yang boleh ditetapkan untuk tindakan operator yang semata-mata bergantung pada tampilan informasi BPCS.
Putaran & Inspeksi Terkait Proses	1	Frekuensi putaran operator harus memadai untuk mendeteksi potensi insiden. Operator harus mencatat nilai spesifik dari sensor/katup independen. Log harus menunjukkan nilai di luar rentang yang tidak dapat diterima. SOP harus menjelaskan respons.
Observasional	1	Frekuensi putaran cukup untuk mendeteksi potensi insiden. Insiden yang akan terjadi harus jelas bagi operator melalui penglihatan/pendengaran normal (suara keras, getaran tinggi, kebocoran serius).
Tinjauan (Review)	1	Tinjauan pengawasan independen dan persetujuan tertulis bahwa pekerjaan telah selesai dan benar sebelum start-up atau mengembalikan komponen ke layanan.
Tindakan (Action)	1	Tindakan operator yang menggunakan operator berbeda, mengandalkan pengamatan independen.
Tindakan Korektif	1	Tindakan operator yang diambil berdasarkan skenario di mana perambatan peristiwa cukup lambat sehingga operator memiliki cukup waktu untuk mengenali kesalahan dan memperbaikinya.
Alarm	Lihat Tabel Waktu	Alarm dengan respons operator harus diperiksa untuk memastikan independen dari penyebab pemicu dan IPL lainnya. Ini mencakup instrumentasi lapangan independen dan saluran independen di BPCS serta independen dari operator (operator berbeda). Hanya satu alarm berbasis BPCS atau fungsi BPCS yang dapat digunakan sebagai IPL.
Basic Process Control System (BPCS)	1	BPCS harus independen dari penyebab pemicu dan IPL lainnya. Jika penyebab pemicu adalah loop kendali BPCS, loop kendali lain dalam BPCS tidak boleh ditetapkan sebagai IPL kecuali studi terperinci dilakukan. Kredit IPL terkait dengan BPCS dibatasi hingga 1 per IEC 61511.
Loop kendali normal	1	Aksi normal memitigasi skenario. Harus berjalan dalam mode otomatis selama semua fase operasional di mana skenario kecelakaan ada.
Interlock BPCS (terverifikasi independen)	1	Interlock tidak diimplementasikan dalam logic solver terpisah, di mana semua penyebab dapat diverifikasi independen dari kegagalan logic solver BPCS.
Interlock BPCS (tidak terverifikasi)	0	Penyebab tidak dapat diverifikasi independen dari kegagalan logic solver BPCS.

LAMPIRAN D — LAPISAN PERLINDUNGAN TIPIKAL (BAGIAN 2)

Pengurangan Risiko yang Disarankan untuk Respons Operator sebagai IPL

Waktu (menit)	Lokasi	Berapa Banyak	Batasan Operasional	Kredit IPL
< 10	Mana saja	Siapa saja	Operator harus memecahkan masalah alarm dan menentukan respons yang tepat.	(tidak ada)
2 hingga 10	Ruang Kendali	Operator Tunggal	Respons yang dilatihkan (drilled response / never deviate). Tindakan spesifik diambil tanpa penundaan setiap saat. Staf memadai 24/7. Jika responsnya memecahkan masalah, < 10 menit tidak memadai (tidak ada kredit).	1
> 10	Ruang Kendali	Operator Tunggal	Tindakan operator rumit (banyak alarm dihasilkan oleh penyebab pemicu dan respons tidak jelas atau tidak terdokumentasi).	(tidak ada)
> 10	Ruang Kendali	Operator Tunggal	Operator terlatih pada respons alarm, memiliki prosedur yang tersedia, dan mempraktikkan tindakan secara berkala.	1
> 10	Ruang Kendali	Dua Operator	Semua operator menerima informasi yang sama. Kedua operator dapat membuat respons independen yang sepenuhnya memitigasi peristiwa. Prosedur tersedia dan dilatihkan.	2
> 30	Lapangan	Operator Tunggal	Operator terlatih pada respons alarm lapangan, prosedur tersedia dan dipraktikkan.	1
> 30	Lapangan	Dua Operator	Semua operator menerima informasi sama. Kedua operator membuat respons independen.	2

Pengurangan Risiko untuk Sistem Mitigasi Konsekuensi (CMS)

CMS	Batasan Lebih Lanjut untuk Dipertimbangkan sebagai IPL	Kredit IPL
Pressure Relief Valve (PRV)	Servis Bersih (Clean Service). PRV harus berukuran tepat untuk memitigasi penuh skenario.	2
Lebih dari 1 PRV	Lebih dari satu PRV tersedia. Masing-masing mampu meredakan tekanan secara independen.	2 atau 3
PRV Bertingkat (Staged)	Lebih dari satu PRV diperlukan untuk memitigasi beban penuh. Perhitungan harus ditinjau.	1
Servis Menyumbat (Plugging)	Rentan terhadap penyumbatan, polimerisasi, pengendapan. PRV tanpa pelindung tidak cukup.	(tidak ada)
PRV Redundan (Plugging)	PRV redundan dengan koneksi proses terpisah pada servis menyumbat.	1
PRV dengan Rupture Disk	PRV dengan rupture disk terintegrasi untuk servis menyumbat.	1
PRV + Rupture Disk + Purging	PRV dengan rupture disk terintegrasi dan sistem pembersihan (purging).	1 atau 2
Rupture Disk Bejana Tekan	Harus dirancang untuk memitigasi skenario. Pelepasan harus dievaluasi untuk potensi risiko.	2
Blast-wall / Bunker	Dinding tahan ledak terkait proses. Dirancang untuk mengarahkan/menahan ledakan.	Cari Panduan

LAMPIRAN E — PERSAMAAN SEDERHANA PFD_{avg} DAN STR (BAGIAN 1)

Bagian ini berisi persamaan matematika yang disederhanakan, umumnya sebagaimana disajikan dalam laporan teknis ISA-TR84.00.02 untuk perhitungan probabilitas rata-rata kegagalan saat diminta (PFD_{avg}) untuk SIF dan subsistem SIF. Penerapan yang benar dari persamaan ini bergantung pada asumsi umum mengenai desain sistem:

- Laju kegagalan sensor terdiri dari semua komponen sensor (elemen penginderaan, sistem elektronik internal dan pneumatik, pemancar, perkabelan lapangan, terminasi blok hingga modul masukan logic solver). Tidak termasuk isolator sinyal eksternal khusus kecuali diperhitungkan secara spesifik.
- Laju kegagalan logic solver terdiri dari semua komponen sistem kendali SIS (modul I/O, prosesor, catu daya, dan peralatan lain yang mempengaruhi fungsi SIF).
- Laju kegagalan antarmuka elemen akhir terdiri dari modul keluaran logic solver ke komponen elektronik/pneumatik yang digunakan (misalnya katup solenoid, relai interposing, transduser I/P).
- Laju kegagalan elemen akhir terdiri dari semua komponen antara antarmuka dan elemen kendali akhir yang digunakan untuk memengaruhi kondisi aman dalam proses (biasanya katup proses atau kontaktor motor).
- Laju kegagalan yang disertakan dalam perhitungan adalah konstan selama periode pengujian fungsional. Kegagalan wear-in (awal) dan wear-out (aus) tidak dimasukkan.
- Laju kegagalan untuk komponen redundan yang digunakan dalam Kelompok Pemungutan Suara Sensor adalah identik.
- Laju kegagalan adalah untuk elemen tunggal dari sistem. Jika konfigurasi pemungutan suara adalah pemancar 2oo3, laju kegagalan TIDAK boleh dikalikan tiga.
- Interval Uji (TI) terjadi jauh lebih sering daripada Waktu Rata-rata Hingga Kegagalan (MTTF) perangkat.
- Waktu Rata-rata untuk Memperbaiki (MTTR) mencakup waktu deteksi dan waktu perbaikan, diasumsikan lebih pendek daripada MTTF (standar: 72 jam).
- Uji fungsional yang sukses adalah 100% efektif (sistem kembali 'seperti baru').
- Elemen akhir dirancang, dikonfigurasi, dan dipasang untuk gagal dalam kondisi aman (fail-safe, misalnya katup uap fail-closed).
- Kegagalan penggerak utama (motor listrik atau turbin pompa/kompresor) diasumsikan berada pada kondisi tanpa daya (de-energized) yang aman.

Perhitungan PFD_{avg} Subsistem: Suatu SIF tersusun dari Sensor, Logic Solver, Antarmuka Elemen Akhir, dan Elemen Akhir. PFD_{avg} total adalah penjumlahan dari keempat subsistem: $PFD_{avg} = PFD_{avg,S} + PFD_{avg,LS} + PFD_{avg,FEI} + PFD_{avg,FE}$

LAMPIRAN E — PERSAMAAN SEDERHANA PFD_{avg} DAN STR (BAGIAN 2)

Perhitungan Pemungutan Suara Kelompok (Group Voting Calculations)

Terkadang subsistem akan berisi dua atau lebih kelompok sensor dari tipe yang tidak identik (misalnya pemancar DP level 2oo2 bersama dengan float level 1oo1). Jika SATU kelompok sensor dapat mengaktifkan fungsi secara independen, logikanya disebut **1ooX**. Jika SEMUA kelompok sensor harus memilih aktif untuk mengambil tindakan, logikanya disebut **XooX**.

PERSAMAAN VOTING KELOMPOK & RRF

FORMULA LOGIKA KELOMPOK (GROUP LOGIC):

- **Logika Kelompok 1ooX Sensor:** $PFD_{avg, S} = \prod PFD_{avg, Si}$
- **Logika Kelompok XooX Sensor:** $PFD_{avg, S} = \sum PFD_{avg, Si} - \prod PFD_{avg, Si}$
- **Logic Solver Majemuk:** $PFD_{avg, LS} = \sum PFD_{avg, LSi}$
- **Logika Kelompok 1ooX Elemen Akhir:** $PFD_{avg, FE} = \prod PFD_{avg, FEi}$
- **Logika Kelompok XooX Elemen Akhir:** $PFD_{avg, FE} = \sum PFD_{avg, FEi} - \prod PFD_{avg, FEi}$

Faktor Reduksi Risiko yang Dicapai (Achieved RRF): $RRF = 1 / PFD_{avg}$

Perhitungan Laju Trip Palsu (Spurious Trip Rate - STR)

Kegagalan perangkat keras acak yang menempatkan sistem dalam kondisi aman atau mati disebut 'spurious trip', 'nuisance trip', atau 'safe failure'. Namun dalam dunia nyata tidak ada kegagalan yang benar-benar 'aman' karena sering kali menciptakan gangguan proses yang parah dan dapat memicu bahaya saat menyalakan ulang peralatan yang rumit (seperti tungku pemanas atau kompresor).

STR dihitung secara terpisah untuk sensor, elemen akhir (termasuk antarmuka), dan logic solver: $STR_{SIF} = \sum STR_S + \sum STR_{FE} + \sum STR_{LS}$. Hubungannya dengan MTTF Spurious adalah: $MTTF^{Spurious} = 1 / STR$.

PERSAMAAN RESMI LAJU SPURIOUS TRIP (STR)

PERSAMAAN LENGKAP STR BERDASARKAN ARSITEKTUR VOTING:

- **1oo1:** $STR = \lambda^S + \lambda^{DD}$
- **1oo1D-NT:** $STR = \lambda^{SU}$ (kesalahan terdeteksi hanya menghasilkan alarm degradasi)
- **1oo2:** $STR = 2 \times (\lambda^S + \lambda^{DD})$
- **2oo2:** $STR = [2 \times (\lambda^S + \lambda^{DD})^2 \times MTTR] + [\beta \times (\lambda^S + \lambda^{DD})]$
- **2oo3:** $STR = [6 \times (\lambda^S + \lambda^{DD})^2 \times MTTR] + [\beta \times (\lambda^S + \lambda^{DD})]$

LAMPIRAN F — TABEL TOLERANSI KESALAHAN MINIMUM (BAGIAN 1)

Toleransi kesalahan (*fault tolerance*) adalah ekspresi dari jumlah kesalahan yang dapat ditoleransi oleh suatu komponen, subsistem, atau SIF keseluruhan dan terus melakukan fungsi yang dimaksudkan dengan adanya kesalahan tersebut. Secara praktis, ini diukur sebagai bilangan bulat yaitu 0 (derajat nol), 1 (satu derajat), atau 2 (dua derajat toleransi kesalahan). Sistem sederhana (non-redundan) memiliki nol derajat toleransi kesalahan secara definisi.

Toleransi kesalahan minimum yang dipersyaratkan menurut IEC 61511 adalah fungsi dari tingkat SIL target:

Target SIL	Toleransi Kesalahan Minimum yang Diperkirakan (IEC 61511)
SIL 1	0 (Tidak memerlukan redundansi wajib)
SIL 2	1 (Memerlukan redundansi perangkat keras)
SIL 3	2 (Memerlukan toleransi kesalahan ganda)

Toleransi kesalahan yang dicapai untuk setiap Kelompok Sensor adalah fungsi dari arsitekturnya (voting):

Arsitektur Sub-sistem (Voting)	Toleransi Kesalahan yang Dicapai (Achieved Fault Tolerance)
1oo1	0
1oo1D-NT	0
1oo2	1
2oo2	0
2oo3	1
1oo3	2

Jika SIF berisi beberapa kelompok sensor (misalnya pemungutan suara 2oo3 pada tekanan dan 1oo2 pada aliran), aturan berikut berlaku: Untuk 1oo1 tidak ada penyesuaian; untuk **1ooX** toleransi kesalahan adalah jumlah matematis toleransi kesalahan kelompok ditambah jumlah kelompok dikurangi 1; untuk **XooX** toleransi kesalahan adalah nilai terendah dari kelompok mana pun dalam subsistem tersebut.

LAMPIRAN F — BATASAN ARSITEKTURAL IEC 61508 (BAGIAN 2)

Jika toleransi kesalahan yang dicapai tidak memenuhi toleransi kesalahan minimum menurut IEC 61511, maka prosedur alternatif menggunakan standar **IEC 61508** diizinkan. Perangkat Tipe B adalah perangkat apa pun yang mengandung mikroprosesor; Perangkat Tipe A adalah semua perangkat lainnya (tanpa mikroprosesor):

Tabel Perangkat Tipe A (Perangkat Sederhana Non-Mikroprosesor):

Safe Failure Fraction (SFF)	HFT = 0	HFT = 1	HFT = 2
< 60%	SIL 1	SIL 2	SIL 3
60% hingga 90%	SIL 2	SIL 3	SIL 4 *
90% hingga 99%	SIL 3	SIL 4 *	SIL 4 *
> 99%	SIL 3	SIL 4 *	SIL 4 *

Tabel Perangkat Tipe B (Perangkat Kompleks Berbasis Mikroprosesor):

Safe Failure Fraction (SFF)	HFT = 0	HFT = 1	HFT = 2
< 60%	Tidak Diizinkan	SIL 1	SIL 2
60% hingga 90%	SIL 1	SIL 2	SIL 3
90% hingga 99%	SIL 2	SIL 3	SIL 4 *
> 99%	SIL 3	SIL 4 *	SIL 4 *

Ketentuan Pengurangan HFT Berdasarkan 'Proven in Use': Untuk semua subsistem kecuali PE logic solver, toleransi kesalahan minimum dapat dikurangi satu jika perangkat mematuhi: Perangkat keras dipilih berdasarkan 'prior use' bukan sertifikasi; Hanya mengizinkan penyesuaian parameter terkait proses; Penyesuaian dilindungi; SIL yang diperlukan dari SIF adalah kurang dari SIL 4.

Batasan Khusus Logic Solver PE: Terlepas dari PFD yang dicapai, semua logic solver elektronik terprogram (PE) harus **dibatasi untuk mengklaim tidak lebih dari SIL 1** kecuali vendor telah memasok sertifikasi resmi bahwa sistem tersebut mampu mencapai kinerja SIL 2 atau lebih tinggi (sertifikasi oleh otoritas independen yang memenuhi syarat seperti TÜV).

LAMPIRAN G — DATA KEGAGALAN KOMPONEN SIS (BAGIAN 1)

Lampiran ini berisi data laju kegagalan tipikal untuk komponen yang umum digunakan dalam SIS di industri proses perminyakan dan kimia. Data ini mencerminkan operasi proses aktual (bukan teknik prediktif semata). Karakteristik kegagalan mencakup laju kegagalan keseluruhan (semua mode kegagalan) dalam kegagalan per jam, persentase kegagalan aman (% Safe Failure), faktor cakupan diagnostik aman [C(S)], dan faktor cakupan diagnostik berbahaya [C(D)]:

Tabel Data Sensor (Bagian 1):

Item Komponen Sensor	Laju Gagal (/jam)	% Gagal Aman	C(S) %	C(D) %
Sakelar Tekanan Pneumatik (Pneumatic Pressure Switch)	2,37E-05	83,5	0,0	0,0
Relai Pneumatik dengan Pilot (Pneumatic Relay with Pilot)	9,20E-07	13,0	0,0	0,0
Sakelar Tekanan Listrik (Pressure Switch)	6,50E-06	41,0	0,0	0,0
Pemancar Tekanan Trip Tinggi (Pressure Transmitter High Trip)	1,50E-06	10,0	100,0	55,6
Pemancar Tekanan Trip Rendah (Pressure Transmitter Low Trip)	1,50E-06	50,0	100,0	20,0
Turbine Meter - Trip Tinggi	1,50E-05	3,0	0,0	89,0
Turbine Meter - Trip Rendah	1,50E-05	90,0	97,0	0,0
Sensor Suhu RTD	4,90E-08	81,6	100,0	0,0
Sakelar Suhu (Temperature Switch)	4,00E-06	40,0	0,0	0,0
Pemancar Suhu - Trip Tinggi (Temperature Transmitter High Trip)	5,00E-06	30,0	100,0	50,0
Pemancar Suhu - Trip Rendah (Temperature Transmitter Low Trip)	5,00E-06	50,0	100,0	20,0
Termokopel - Trip Tinggi (Thermocouple High Trip)	1,20E-06	0,0	100,0	97,0
Termokopel - Trip Rendah (Thermocouple Low Trip)	1,20E-06	95,0	100,0	0,0
Sensor Level - Kapasitansi (Level Sensor - Capacitance)	4,00E-06	50,0	0,0	0,0
Sakelar Level Pelampung / Displacer (Level Switch Float)	5,00E-06	60,0	0,0	0,0
Sakelar Level Piezo-Elektrik - Trip Tinggi	6,00E-07	30,0	0,0	66,7
Sakelar Level Piezo-Elektrik - Trip Rendah	6,00E-07	67,0	0,0	0,0

LAMPIRAN G — DATA KEGAGALAN KOMPONEN SIS (BAGIAN 2)

Sensor (Lanjutan)	Laju (/jam)	% Aman	C(S)%	C(D)%
Sakelar Level Pneumatik	9,00E-07	50,0	0,0	0,0
Pemancar Level Displacement - Trip Tinggi	7,00E-06	10,0	100,0	50,0
Pemancar Level Displacement - Trip Rendah	7,00E-06	60,0	100,0	10,0
Pemancar Level Magnetostriktif - Trip Tinggi	1,80E-06	50,0	100,0	50,0
Pemancar Level Radar - Trip Tinggi / Rendah	1,20E-06	55,0	100,0	30,0
Sakelar Aliran (Flow Switch)	8,00E-06	60,0	0,0	0,0
Pemancar Aliran Coriolis Meter - Trip Tinggi	3,70E-06	20,0	100,0	50,0
Pemancar Aliran Vortex Shedding - Trip Tinggi	3,50E-06	20,0	100,0	50,0
Pemindai Api Pembakar (Flame Scanner Burner)	6,00E-06	50,0	0,0	0,0
Sakelar Kedekatan (Proximity Switch)	3,00E-07	50,0	0,0	0,0
Pemancar Kecepatan (Speed Transmitter)	2,00E-06	23,0	0,0	0,0
Antarmuka Elemen Akhir	Laju (/jam)	% Aman	C(S)%	C(D)%
Transduser I/P (I/P Transducer)	4,00E-06	40,0	0,0	0,0
Relai Perantara (Interposing Relay)	2,00E-07	20,0	0,0	0,0
Regulator Pneumatik (Pneumatic Regulator)	3,00E-06	80,0	0,0	0,0
Katup Solenoid 2-Arah Deenergize to Trip	4,00E-06	60,0	0,0	0,0
Katup Solenoid 3-Arah Deenergize to Trip	2,00E-06	60,0	0,0	0,0
Katup Solenoid 3-Arah Energize to Trip	1,00E-05	20,0	0,0	91,0
Elemen Kendali Akhir	Laju (/jam)	% Aman	C(S)%	C(D)%
Katup Bola Operasi Udara (Air Operated Ball Valve)	3,00E-06	60,0	0,0	0,0
Katup Kupu-kupu Operasi Udara (Butterfly Valve)	3,00E-06	55,0	0,0	0,0
Katup Sorong Operasi Udara (Gate Valve)	2,00E-06	40,0	0,0	0,0
Katup Globe Operasi Udara (Globe Valve)	2,50E-06	55,0	0,0	0,0
Katup Bola Operasi Hidrolik (Hydraulic Ball)	3,00E-06	55,0	0,0	0,0
Katup Geser Operasi Hidrolik (Slide Valve)	5,00E-06	50,0	0,0	0,0
Katup Operasi Motor Listrik (MOV)	5,00E-06	10,0	0,0	0,0
Sirkuit Starter Motor / Kontaktor	1,50E-06	80,0	0,0	0,0
Damper Cerobong Tungku (Stack Damper)	6,00E-06	55,0	0,0	0,0
Katup Trip and Throttle Turbin Kompresor	3,80E-06	39,0	0,0	0,0

LAMPIRAN H — CONTOH KRITERIA RISIKO (RISK CRITERIA)

Salah satu aspek yang paling penting namun sulit dari Siklus Hidup Keselamatan SIS adalah menentukan tingkat risiko yang dapat diterima dalam situasi tertentu. Meskipun tolerabilitas risiko dapat direpresentasikan dalam banyak cara, semuanya biasanya merujuk kembali ke metrik tunggal yang disebut '**Risiko Kematian Individu**' (*Individual Risk of Fatality - IR*). Semua representasi risiko lainnya diturunkan dari nilai tunggal ini.

IR biasanya direpresentasikan sebagai rentang, di mana awal rentang (frekuensi tertinggi) mewakili frekuensi di mana risiko tidak dapat ditoleransi dalam keadaan apa pun, dan akhir rentang (frekuensi terendah) mewakili titik di mana risiko dapat diabaikan. Di tengahnya, risiko harus dikurangi '**As Low As Reasonably Practicable**' (**ALARP**).

METODOLOGI KALIBRASI KRITERIA RISIKO SIS

KRITERIA RISIKO INDIVIDU NASIONAL & PERUSAHAAN (GAMBAR F.1 & F.2):

- **Kriteria Nasional:** Inggris (UK), Hong Kong, dan Australia (NSW) menetapkan rentang ALARP pekerja industri antara 10^{-3} hingga 10^{-5} per tahun. Belanda menetapkan batas ketat 10^{-5} hingga 10^{-8} per tahun.
- **Kriteria Perusahaan Proses (Company A hingga L):** Menunjukkan rentang target risiko individu perancangan SIS berpusat pada 1×10^{-4} hingga 1×10^{-5} per tahun.

KONVERSI RENTANG ALARP KE TITIK TUNGGAL TMEL:

Rekayasa membutuhkan satu titik target. Memilih titik tengah ALARP menghasilkan nilai 1×10^{-4} per tahun. Mengingat seorang pekerja terpapar sekitar 10 bahaya SIS berbeda namun hanya berada di pabrik selama ~25% jam kalender tahunan, faktor-faktor ini saling meniadakan. Akibatnya, nilai IR target fatalitas tunggal langsung diadopsi sebagai **TMEL = 1×10^{-5} per tahun**.

KESETARAAN KERUGIAN LAIN (GAMBAR F.5):

Berdasarkan penyelesaian hukum di AS, 1 kematian tunggal dikalibrasi setara dengan **\$50 Juta** kerugian komersial atau pelepasan kimia katastrofik ke luar area pabrik. Setiap perubahan tingkat keparahan (S=0 hingga S=5) berubah satu orde besaran (faktor 10x). Matriks risiko terkalibrasi persilangan S=4 (kematian) dan L=4 (frekuensi 1/tahun) menghasilkan angka 5 orde besaran reduksi risiko.

LAMPIRAN I — REFERENSI DAN PUSTAKA RUJUKAN

Daftar standar industri, regulasi pemerintah, dan publikasi rekayasa keandalan yang menjadi rujukan dalam penyusunan buku panduan ini:

1. **ANSI/ISA-84.00.01-2004 (IEC 61511-1:Mod):** *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, 2004.
2. **IEC 61511-1:** *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, International Electrotechnical Commission, Final Standard, 2003.
3. **IEC 61508 Parts 1-7:** *Functional safety of electrical/electronic/programmable electronic safety-related systems*, International Electrotechnical Commission, Final Standard, December 1999.
4. **ISA-TR84.00.02-2002:** *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, 2002.
5. **ISA-TR84.00.07:** *The Application of ANSI/ISA 84.00.01-2004 Parts 1-3 (IEC 61511 Parts 1-3 Modified) for Safety Instrumented Functions (SIFs) in Fire, Combustible Gas, & Toxic Gas Systems*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, December 2009.
6. **Marszal, Edward and Scharpf, Eric:** *Safety Integrity Level Selection with Layer of Protection Analysis*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, 2002.
7. **OSHA:** *Petroleum Refinery Process Safety Management National Emphasis Program*, Occupational Safety and Health Administration, Washington DC, 2007.
8. **EPA:** *Risk Management Program Guidance for Offsite Consequence Analysis*, Environmental Protection Agency, Washington DC, 1996.
9. **Smith, David J.:** *Reliability, Maintainability and Risk*, Butterworth-Heinemann, London, UK, 2007.
10. **Lees, F.P.:** *Loss Prevention in the Process Industries*, Butterworth-Heinemann, London, UK, 1980.
11. **Reliability Analysis Center:** *Nonelectronic Parts Reliability Data (NPRD)*, Reliability Analysis Center, Rome, NY, 1995.
12. **OREDA:** *OREDA-84: Offshore Reliability Data Handbook*, 1st edition, PennWell Publishing Company and distributed by DNV Technica, Houston, TX, 1984.
13. **CCPS / AIChE:** *Guidelines for Process Equipment Reliability Data, with Data Tables*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1989.
14. **CCPS / AIChE:** *Layer of Protection Analysis, Simplified Process Risk Assessment*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001.

*Akhir dari Buku Panduan Rekayasa SIS (Safety Instrumented Systems Engineering Handbook)
Edisi Lengkap Terjemahan Bahasa Indonesia • Kenexis Consulting Corporation*