Safety Instrumented Systems

- Contoh Perancangan Dasar
- Konsep Lapisan Pelindung
- ISA S84
- IEC 61508
- IEC 61511
- Rangkuman

ISA 84.01-1996

- Membedakan Instrumentasi Kontrol dan Instrumentasi Keamanan (safety instrumented systems)
- Standard berlaku bagi industri proses, dan karenanya tidak berlaku bagi
  - Reaktor Nuklir dan
  - Peralatn Mekanik.
- Bagian yang perlu diperhatikan :
  - Harus dipertimbangkan Clause 1 s/d 12
  - Untuk informasi Annex A s/d E
- Diakui didalam ANSI, dan akan disetarakan dengan IEC 61511

ISA TR 84.0.02

- Part 1 Development of the overall terms, symbols, explanation of SIS element failures, comparison of system analysis examples
- Part 2 Verification of SIL for SIF using Simplified Equation Methodology
- Part 3 Verification of SIL for SIF using Fault Tree Analysis Methodology
- Part 4 Verification of SIL for SIF using Markov Analysis Methodology
- Part 5 Guidance in determining PFD of E/E/PE logic solver(s) via Markov Analysis

ISTILAH

- Process Control System

  Instrumentasi dan kontrol Pengendalian Proses agar Pabrik dapat bekerja sesuai kapasitas

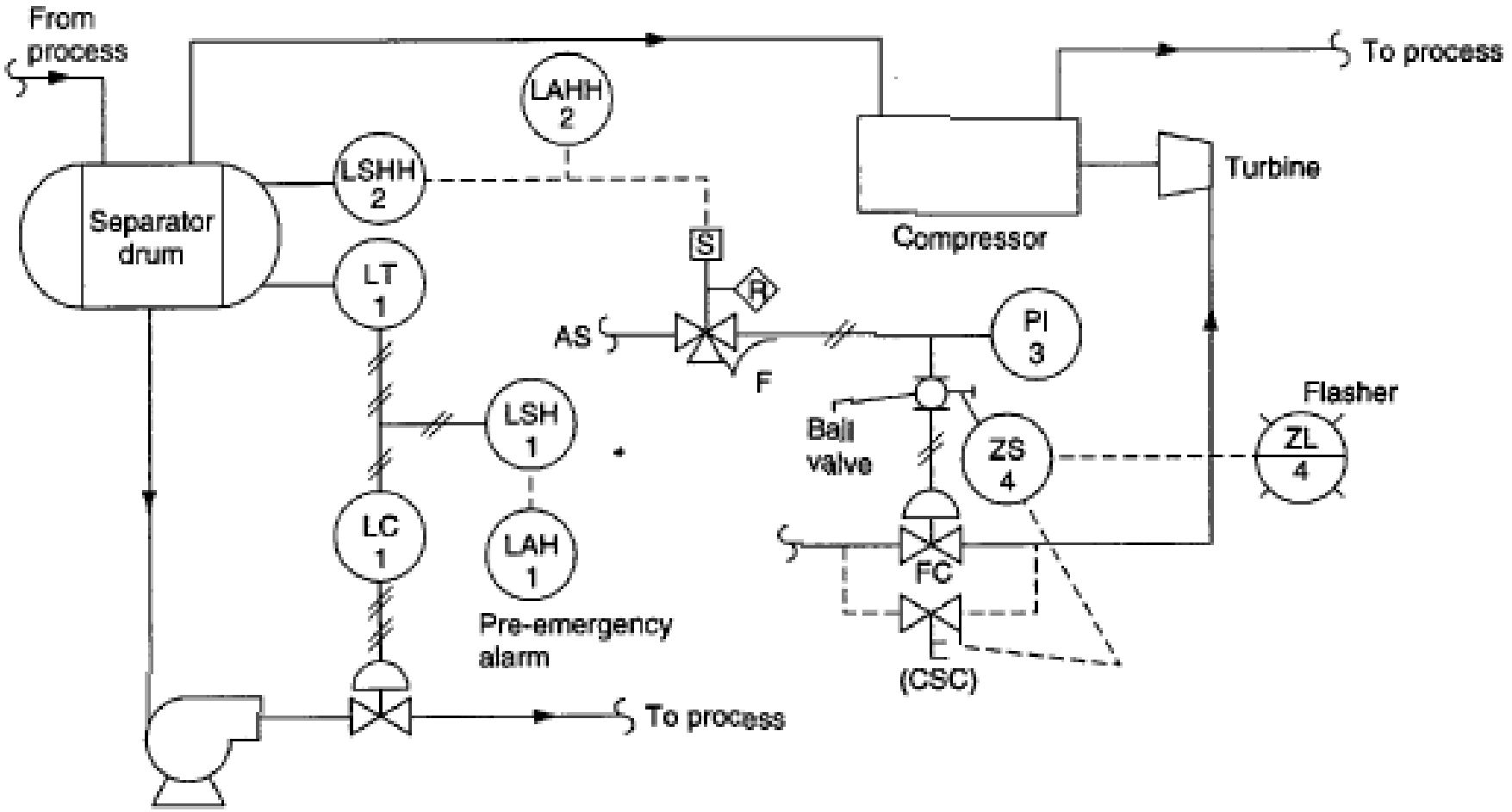
- Safety Instrumented System

  Instrumentasi dan Kontrol untuk Pengamanan Proses (Emergency Shut Down System) Disayaratkan tidak terkait dengan sistim Instrumentasi dan Kontrol Pengendalian Proses

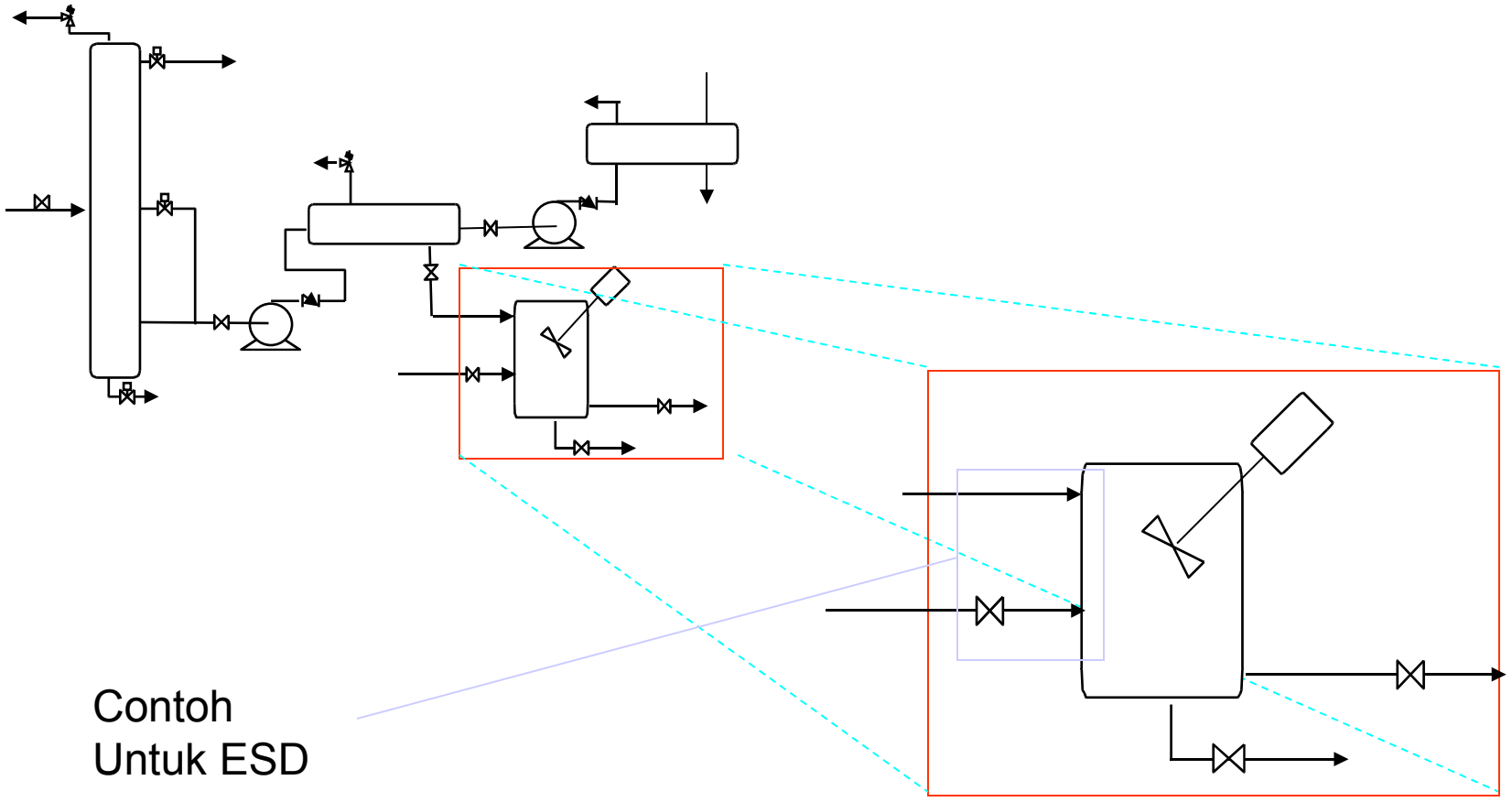
- Independent Protection Layer

  Adalah lapisan pelindung saling tidak terkait pada IPL lainnya, untuk menghasilkan tingkat keamanan yang disebut sebagai Safety Instrumented Level

shutdown can be initiated if selected variables, such as level in a suction knockout drum, vibration, lubrication flow, seal fluid pressure, and so forth, exceed limits. See API Stds 612, 614, 616, 617, 618, and 619 for additional details.

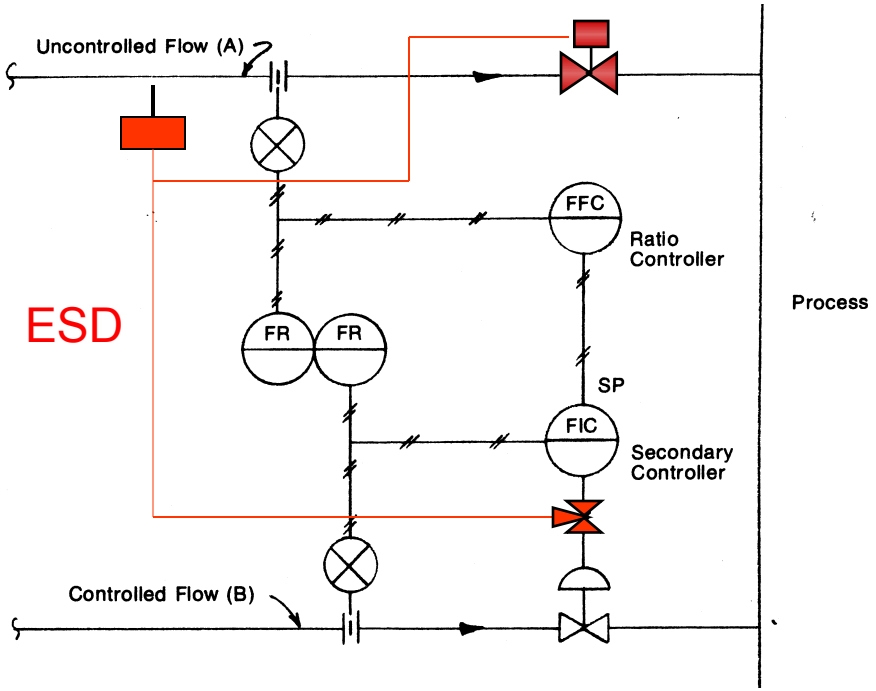


UNIT OPERATION



Contoh
Untuk ESD

INDEPENDENT PROTECTION LAYER



PABRIK

SITIM KONTROL PROSES

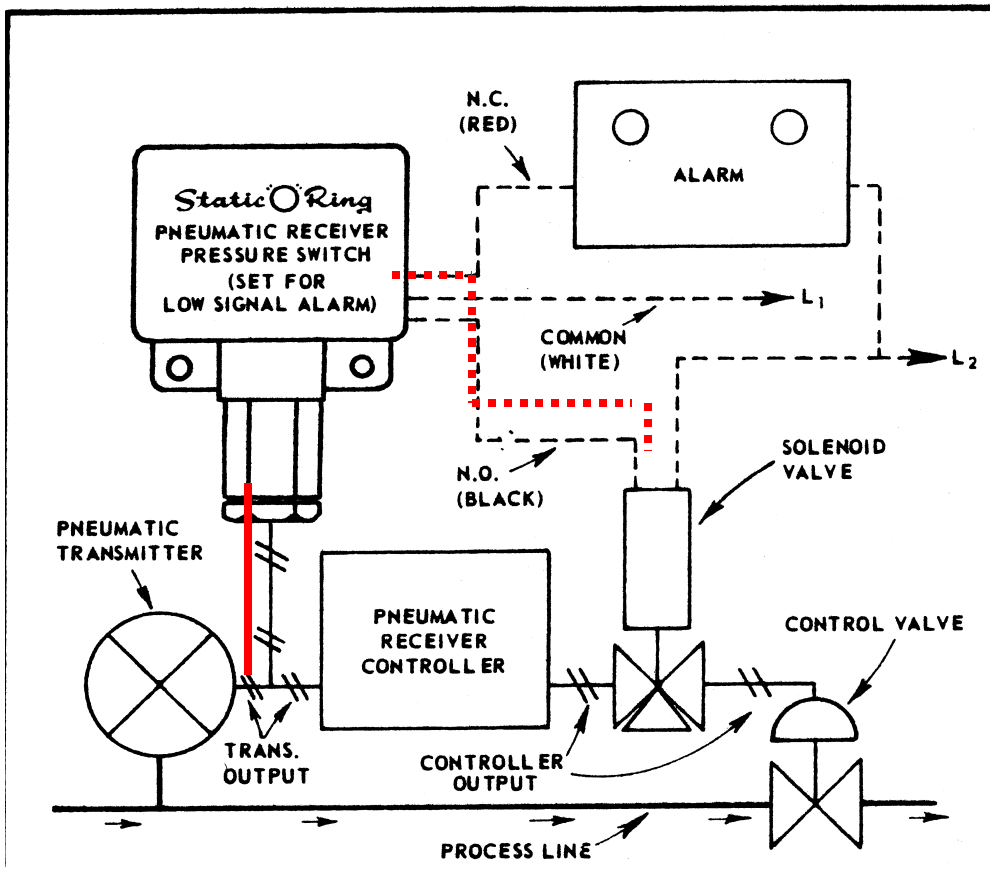
ALARM & TINDAKAN MANUAL

SAFETY INSTRUMENTED SYSTEM

PENGAMANAN FISIK

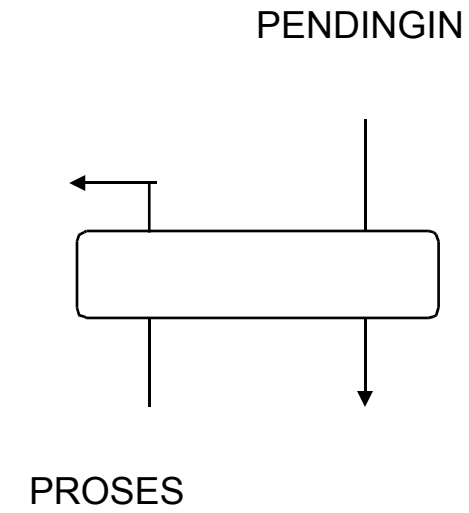
MASYARAKAT

Contoh Rangkaian ESD



PENUKAR PANAS
(HEAT EXCHANGER)

- Dari data Industri, kegagalan cairan pendingin terjadi 0.1 kali/tahun/alat, alat yang dirancang sesuai standard yang berlaku
- Dalam analisa oprasi pabrik yang berbahaya, kegagalan cairan pendingin dapat mengakibatkan situasi berbahaya



Lapisan Perlindungan

4.2.1.1.3 Primary Protection

Primary protection from overpressure in a pressure component should be provided by a PSH sensor to shut off inflow. If a vessel is heated, the PSH sensor should also shut off the fuel or source of heat. Primary protection for atmospheric components should be provided by an adequate vent system.

4.2.1.1.4 Secondary Protection

Secondary protection from overpressure in a pressure component should be provided by a PSV. Secondary protection for atmospheric components should be provided by a second vent. The second vent may be identical to the primary vent, a gauge hatch with a self-contained PSV or an independent PSV.

4.2.1.2.3 Primary Protection

Primary protection from leaks of sufficient rate to create an abnormal operating condition within a pressure component should be provided by a PSL sensor to shut off inflow and a FSV to minimize backflow. Primary protection from leaks from the liquid section may also be provided by an LSL sensor to shut off inflow. On an atmospheric component, primary protection from liquid leaks should be provided by an LSL sensor to shut off inflow. A containment system should provide primary protection from small liquid leaks that cannot be detected by the safety devices on a process component. Primary protection from small gas leaks that occur in an inadequately ventilated area and cannot be detected by component sensing devices should be provided by a combustible gas detection system.

4.2.1.2.4 Secondary Protection

Secondary protection from all detectable leaks and small gas leaks in an inadequately ventilated area should be provided by the Emergency Support Systems (ESS). Secondary protection from small liquid leaks should be provided by an LSH sensor installed on the sump tank to shut in all components that could leak into the sump.

Tingkat Lapisan Pelindung (IPL) untuk menghitung Tingkat Keandalan SIS

Kondisi Awal	Tingkat kegagalan proses/tahun	10^{-1}
IPL_1	Tingkat kegagalan peralatan	10^{-2}
IPL_2	Tingkat kegagalan Sistim Kontrol	10^{-1}
IPL_3	Tingkat Kegagalan alarm & tindakan operator	10^{-1}

Bila Sasaran tingkat kegagalan/tahun 10^{-6}

Maka tingkat keandalan SIS yang diperlukan adalah =

$$10^{-6}/(10^{-1}*10^{-2}*10^{-1}*10^{-1}) = 10^{-1}$$

2.5.2.11 Reliability

No more than 1 control loop or output device should fail to operate as specified in any continuous 12-month period for each group of 100 control loops and 2 out of 100 for non-control points.

The system should have on-line diagnostic programs for self-checking and security checking/correction so that the primary system and the backup system are periodically checked. It should also be able to disconnect the faulty component, or transfer to backup. The system should have a system status display and should also identify the source of any malfunction.

Brosur Chromatograph

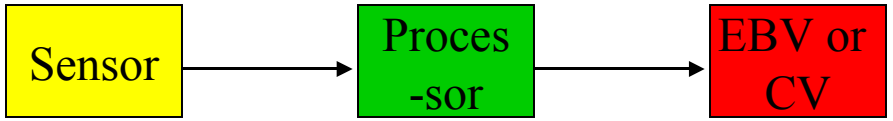
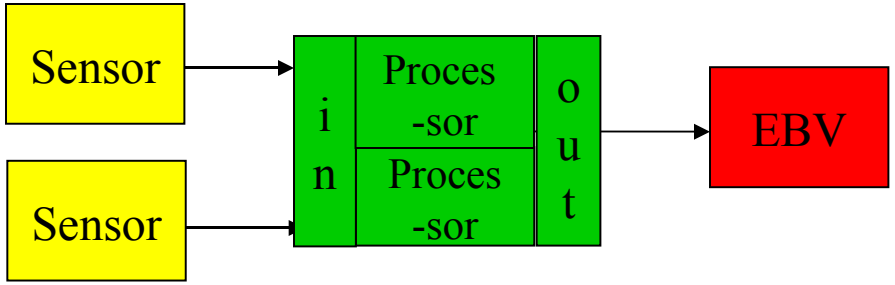
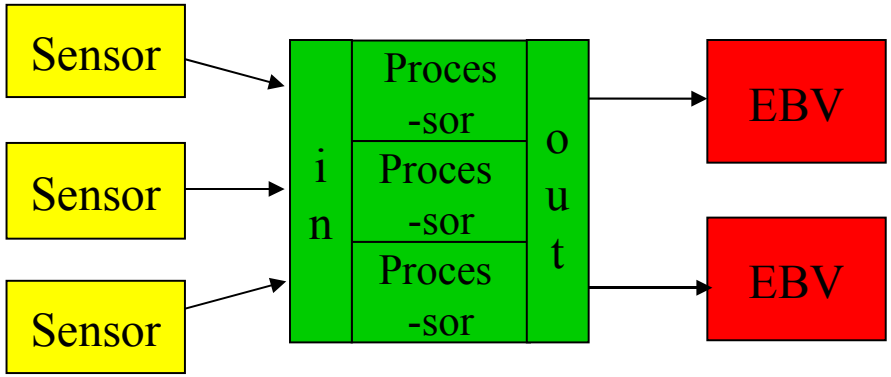
- Superior reliability of 1/2 BTU/1000 (0.05%) over the full ambient temperature range
- Broad application scope with single or dual detector capability
- Extreme ambient temperature operation minimizes installation and utility requirements
- Unique micro-packed columns for improved separations, reduced carrier consumption, fast analysis
- Powerful 2350A controller electronics offers unsurpassed communications, archiving, and I/O options (including internal modem and ethernet MODBUS/TCP communications)
- Easy to use MON2000 PC software for advanced diagnostics and simplified troubleshooting - simply the best in the industry

Sasaran Tingkat Keandalan

Tergantung pada Persyaratan dan jenis proses,

Contoh umum saat ini :

- Proses Sodium Silicate, mensyaratkan tingkat tingkat keandalan 5 x 10-3 (0.005)
- Untuk Proses dengan gas yang berbahaya, dapat disyaratkan tingkat keandalan sampai 2 x 10-6

Tingkat Keamanan	Jenis Sistim Instrumentasi	Tingkat keandalan (PFD)
SIL 1		0,1 sampai 0,01
SIL 2		0,01 sampai 0,001
SIL 3		0,001 sampai 0,0001
SIL 4	**Hanya pada IEC saja**	0,0001 sampai 0,00001

SIL Risk Graph Examples

- Case 1

A HAZOP Scenario is considered to have a high probability of happening. The risk to the tank farm operator is high, but he is only on site one hour per day. There is no local alarm. Determine the required SIL

- Case 2

A HAZOP Scenario is considered to have a low probability of happening. The risk to the trained maintenance crew is low. There are local alarms and manual isolation valves. Determine the required SIL

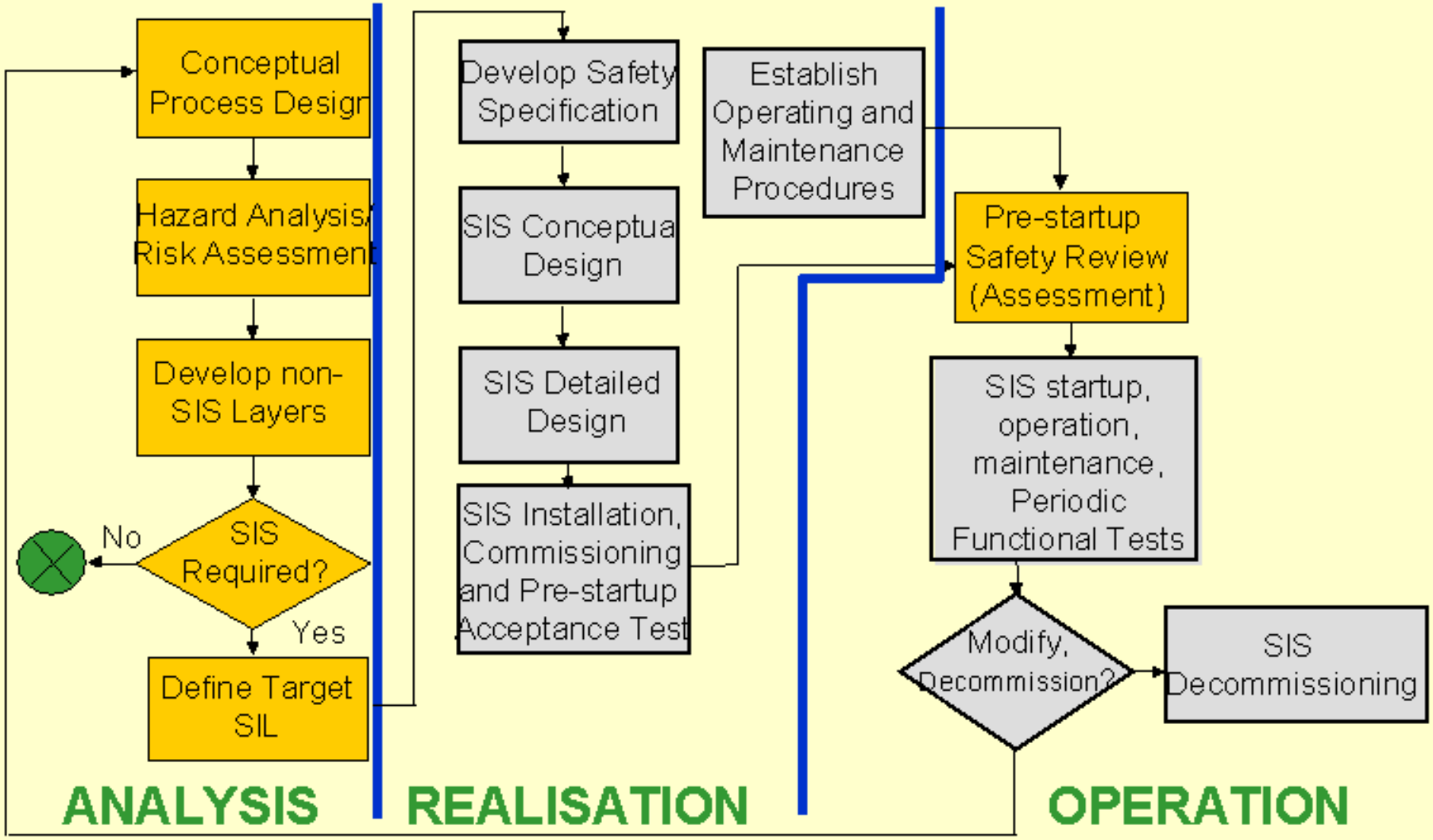
Pelaksanaan SIS

- PHA — **Safeguards for each Failure Mode**
- Scenario — **Target Risk for specific failure**
- LOPA — **Determine Required SIL**
- SIS Reliability — **Calculate SIL for specific ESD/SIS**

- Maintain Level of Safety / Risk

Safety Life Cycle

ISA 84.01 Safety Lifecycle



IEC 61508

- Berlaku bagi semua industri secara internasional
- Merumuskan fungsi dari Sistim Keamanan :
  - Mencakup penggunaan semua jenis teknologi (relay, solid state, programmable, dlsb)
  - Berlaku bagi Industri Proses, Manufacturer, Angkutan, Peralatan Medik dlsb.
- Digunakan sebagai dasar sertifikasi bagi peralatan, baik perangkat lunak maupun keras

IEC 61508
Functional Safety-Related Systems

- Part 1: General requirements
- Part 2: Requirements for Electrical /Electronic /Programmable Electronic Systems (E/E/PES)
- Part 3: Software requirements
- Part 4: Definitions and abbreviations of terms
- Part 5: Examples of the methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of part 2 and 3
- Part 7: Bibliography of techniques and measures

IEC 61511

Disusun berdasarkan IEC 61508, dan terdiri dari :

- Part 1: Framework, definitions, system, hardware and software requirements
- Part 2: Guidelines in the application of IEC 61511-1
- Part 3: Example methods for determining safety integrity in the application of Hazard & Risk Analysis

Instrumentasi Proses (BPCS) vs Instrumentasi Keamanan (SIS)

- Instrumentasi Keamanan dan Instrumentasi Proses harus dirancang terpisah dan tidak saling bergantungan
- Dalam hal terpaksa digunakannya satu pengolah data (Processor) bagi keperluan Proses dan Keamanan, maka sistim dianggap dan dikelola sebagai Instrumentasi Keamanan.
- Baik perngkat lunak maupun keras dari Instrumentasi keamanaan dirancang, ditest dan dikelola secara khusus menurut standard yang diberlakukan.
- Menurut IEC 61511 laju kegagalan Insrumentasi Prosees tidak bisa kurang dari 10^{-5} kegagalan/jam, dan nilai kemapuan mengurangi kegagalannya tidak bisa dinyatakan lebih besar dari 10

Kelebihan IEC 61511 terhadap ISA 84

Lapisan Perlindungan harus didefinisikan beserta dengan kemapuan pengurangan tingkat kegagalannya masing masing

Bersifat Performance Base dan karenanya penentuan penggunaannya diletakan pada pengguna.

Memberikan ketentuan mengenai Tata Laksana Fungsi keamanan, seperti :

- Penentuan peran jabatan dan departemennya
- Mensyaratkan dokumentassi kemampuan perorangan maupun prestasi Departemen
- Menentukan kapan dilaksanakannya pemeriksaan dan audit.
- Mensyaratkan adanya prosedur untuk mengevaluasi keandalan SIS selama oprasi.

Safety Instrumented Level membedakan antara demand mode dan continous mode dan dikembangkan ke SIL tingkat 4,

Dasar Standard Sistim Keamanan

- Siklus Keamanan (Safety Life Cycle) yang menjelaskan mengenai metoda analisa fungsi kemanan, yang banyak mencakup Pengelolaan Sitim Keamanan.

- Tingkat Keamanan (SIL) yang menjelaskan cara untuk mengenai penyeimbangan risiko proses dengan kebutuhan kemampuan yang dituntut pada Sistim Instrumentasi keamanan.

Sifat Standard Keamanan

- Standards hanya menerangkan mengenai konsep ataupun sasaran untuk menuntun kearah perancangan yang baik
- Standard tidak menjelaskan berapa nilai SIL yang harus digunakan
- Standard tidak menjelaskan mengenai cara merancang, menjalankan maupun memelihara suatu Sistim Instrumentasi Keamanan untuk memenuhi tingkat keandalan yang ditentukan