SIL VERIFICATION PROCEDURE

ENGINEERING TECHNICAL STANDARDS & PROCEDURES

PT KILANG PERTAMINA INTERNASIONAL

DIREKTORAT PROYEK INFRASTRUKTUR

00	Issued For Record	11/22	WHE/RW/AFM	VS/DC	HY	RMD	MHA
Rev.	Description	Date	Prepared by	Checked by	Verified by	Validated By	Approved By

REVISION HISTORY
RIWAYAT REVISI

Page / Section *Hal. / Bagian*	Date *Tanggal*	Description *Deskripsi*	Revised by *Direvisi oleh*

TABLE OF CONTENTS
DAFTAR ISI

1. INTRODUCTION

1.1 Introduction

Pertamina Engineering Technical Standards and Procedures (ETSP) provides procedure and guideline for the verification of Safety Integrated Levels (SIL) of safety instrumentedfunctions (SIF) for all projects Pertamina Refining & Petrochemicals Subholding (PT.KPI and its subsidiaries) (henceforth “COMPANY”) throughout facility lifecycle.

International Standard IEC 61511 defines the functional safety requirements established by IEC 61508 for the process industry sector and addresses the application of Safety Instrumented Systems (SIS) provided to prevent or mitigate a hazardous event.

A SIL determination process is carried out to assign a safety performance categoryto each safety function identified in the HAZOP study. The performance category assigned is defined as a Safety Integrity Level (SIL). The SIL verification process is performed to demonstrate that the Target Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF) has been achieved.

1.2 Purpose

The purpose of this procedure is to outline the processes to be followed for the verification of safety integrity levels for safety instrumented functions. This procedure shall be used for Pertamina Refining & Petrochemicals Subholding (PT.KPI and its subsidiaries) (henceforth “COMPANY”) projects

1. PENGANTAR

1.1 Pengantar

Pertamina *Engineering Technical Standards and Procedures (ETSP)* memberikan prosedur dan pedoman untuk verifikasi Safety Integrated Levels (SIL) dari safety instrumented functions (SIF) untuk semua proyek proyek Pertamina Refining & Petrochemicals Subholding (PT.KPI dan Anak Perusahaannya), yang untuk selanjutnya disebut [“COMPANY”] di seluruh siklus hidup fasilitas.

Standar Internasional IEC 61511 mendefinisikan persyaratan keselamatan fungsional yang ditetapkan oleh IEC 61508 untuk sektor industri proses dan membahas penerapan Sistem Instrumen Keselamatan (SIS) yang disediakan untuk mencegah atau mengurangi kejadian berbahaya.

Proses penentuan SIL dilakukan untuk menetapkan kategori performa keselamatan untuk setiap fungsi keselamatan yang diidentifikasi dalam studi HAZOP. Kategori performa yang ditetapkan didefinisikan sebagai Tingkat Integritas Keselamatan (SIL). Proses verifikasi SIL dilakukan untuk menunjukkan bahwa Target Safety Integrity Level (SIL) dari Safety Instrumented Function (SIF) telah tercapai.

1.2 Tujuan

Tujuan dari prosedur ini adalah untuk menguraikan proses yang harus diikuti untuk verifikasi tingkatan integritas keselamatan untuk fungsi instrumen keselamatan. Prosedur ini akan digunakan untuk proyek proyek Pertamina Refining & Petrochemicals Subholding (PT.KPI dan Anak Perusahaannya),yang untuk selanjutnya disebut “COMPANY”]

2. SCOPE

2.1 SIL Verification is required for Safety Instrumented Functions (SIFs) that have been assigned target integrity levels of 1 and above. The SIFs, where the target integrity level has been determined by Safety or Environmental levels, shall be verified to the highest SIL level determined (i.e. the higher of SIL & EIL).

2.2 Commercial (Asset) Integrity Levels are optional upon project requirements. For SIFs where the integrity level has been determined by safety or environmental consequences there will always be an associated commercial loss, however there are scenarios where equipment damage is the only consequence and caution is advised if verification is required since an inflated commercial loss may lead to a high integrity levels requiring additional redundant hardware to meet the required Risk Reduction Factor (RRF).

2.3 This document contains the procedure for performing the verification of safety instrumented functions and assigns the achieved safety integrity level and a Target Failure Measure, expressed as Risk Reduction Factor (RRF), or Probability of Failure on Demand (PFD) for low demand mode applications or dangerous failure rate per hour for high demand mode applications. Only when a safety instrumented function meets the criteria set by IEC 61508 / IEC 61511 in terms of architectural constraints, target failure measure and systematic capability.

2. LINGKUP

2.1 Verifikasi SIL diperlukan untuk Safety Instrumented Functions (SIFs) yang targetnya sudah ditetapkan tingkat integritas 1 ke atas. Target tingkat integritas SIF, yang telah ditentukan oleh tingkat Keselamatan atau Lingkungan, harus diverifikasi ke tingkat SIL tertinggi yang ditentukan (yaitu yang lebih tinggi dari SIL & EIL).

2.2 Tingkat Integritas Komersial (Aset) bersifat opsional berdasarkan persyaratan proyek. Untuk SIF yang tingkat integritasnya telah ditentukan untuk kepentingan keselamatan atau lingkungan akan selalu ada kerugian komersial yang terkait, namun ada skenario di mana kerusakan peralatan adalah satu-satunya akibat dan disarankan untuk hati hati apabila diperlukan verifikasi yang mungkin akan menyebabkan tingkat integritas tinggi yang pada akhirnya akan meningkatkan kerugian komersial karena harus menambah redundan perangkat keras untuk memenuhi Faktor Pengurangan Resiko (RRF)

2.3 Dokumen ini berisi prosedur untuk pelaksanaan verifikasi fungsi instrumentasi keselamatan dan menetapkan tingkat integritas keselamatan yang ingin dicapai dan Ukuran Kegagalan Target yang dinyatakan sebagai Faktor Pengurangan Risiko (RRF), atau Probabilitas Kegagalan Sesuai Permintaan (PFD) untuk aplikasi modus permintaan rendah atau tingkat kegagalan berbahaya per jam untuk aplikasi modus permintaan tinggi. SIL target dapat dikatakan tercapai hanya ketika fungsi instrumen keselamatan memenuhi kriteria yang ditetapkan oleh IEC 61508 / IEC 61511 dalam hal batasan arsitektur, ukuran kegagalan target dan kemampuan sistematis,

2.4 SIL Verification shall be developed, preferably during EPC or Detail Engineering Desain (DED) stage.

3. CONFLICTS AND DEVIATIONS

3.1 Any conflicts between this standard and other applicable Pertamina Engineering Technical Standards and Procedures (ETSP), or industry standards, codes, and forms shall be resolved in writing by the Vendor/Consultant/Contractor through to PT Kilang Pertamina Internasional (PT KPI) Where two or more references define requirements for the same subject, the more restrictive reference shall govern.

Where two or more references define requirements for the same subject, the more restrictive reference shall govern.

3.2 This document is made in the Indonesian language and the English language. Both texts are equally original. In the event of any inconsistency or different interpretation or conflict between the Indonesian text and English text, the English text shall prevails and the relevant Indonesian text shall be deemed to be automatically amended to conform with and to make the relevant Indonesian text consistent with the relevant English text.

4. ABBREVIATIONS

4.1 The reference documents listed below form an integral part of this ETSP.

BPCS	Basic Process Control System
C&E	Cause and Effects (Diagram)
CCF	Common Cause Failure
CMF	Common Mode Failure

2.4 Verifikasi SIL harus dikembangkan, sebaiknya selama EPC atau *Detail Engineering Desain* (DED).

3. KONFLIK DAN DEVIASI

3.1 Setiap konflik antara standar ini dengan *Engineering Technical Standards and Procedures (ETSP)* Pertamina lain yang berlaku, atau standar, kode, dan formulir industri harus diselesaikan secara tertulis oleh Vendor/Konsultan/Kontraktor melalui PT Kilang Pertamina Internasional (PT KPI). Jika dua atau lebih referensi menentukan persyaratan untuk subjek yang sama, referensi yang lebih ketat akan berlaku

Jika dua atau lebih referensi menentukan persyaratan untuk subjek yang sama, referensi yang lebih ketat akan berlaku

3.2 Dokumen ini dibuat dalam Bahasa Indonesia dan bahasa Inggris. Baik teks Bahasa Indonesia ataupun teks Bahasa Inggris kedua-duanya adalah asli (original). Jika terdapat ketidaksesuaian atau perbedaan interprestasi atau pertentangan antara teks bahasa Indonesia dan teks bahasa Inggris, maka teks bahasa Inggris akan menjadi acuan dan kemudian teks bahasa Indonesia harus dianggap sudah diubah secara otomatis sehingga menjadi sesuai dengan teks bahasa Inggris.

4. ABBREVIATIONS

4.1 Singkatan yang digunakan pada spesifikasi ini harus memiliki definisi sebagai berikut:

BPCS	*Basic Process Control System*
C&E	*Cause and Effects (Diagram)*
CCF	*Common Cause Failure*
CMF	*Common Mode Failure*

DC	Diagnostic Coverage	DC	*Diagnostic Coverage*
DCPST	Diagnostic Coverage for Partial Stroke Testing	DCPST	*Diagnostic Coverage for Partial Stroke Testing*
E/E/PE	Electrical/ Electronic/ Programmable Logic Device	E/E/PE	*Electrical/ Electronic/ Programmable Logic Device*
FIT	Failure in Time per billion hours (1x10-9 failures per hour)	FIT	*Failure in Time per billion hours (1x10-9 failures per hour)*
FMEDA	Failure Modes Effects and Diagnostic Analysis	FMEDA	*Failure Modes Effects and Diagnostic Analysis*
HFT	Hardware Fault Tolerance	HFT	*Hardware Fault Tolerance*
HIPPS	High Integrity Pressure Protection System	HIPPS	*High Integrity Pressure Protection System*
IPL	Independent Protection Layer	IPL	*Independent Protection Layer*
IS	Intrinsically Safe	IS	*Intrinsically Safe*
LOPA	Layer of Protection Analysis	LOPA	*Layer of Protection Analysis*
MOC	Management of Change	MOC	*Management of Change*
MRT	Mean Repair Time	MRT	*Mean Repair Time*
MT	Mission Time	MT	*Mission Time*
MTBF	Mean Time Between Failures	MTBF	*Mean Time Between Failures*
MTTFS	Mean Time to Fail Spurious	MTTFS	*Mean Time to Fail Spurious*
MTTR	Mean Time to Restoration	MTTR	*Mean Time to Restoration*
OREDA	Offshore Reliability Data	OREDA	*Offshore Reliability Data*
P&ID	Process and Instrumentation Diagram	P&ID	*Process and Instrumentation Diagram*
PDS	(PDS Data Hand book) Norwegian Acronym for Reliability of Safety Instrumented Systems	PDS	*(PDS Data Hand book) Norwegian Acronym for Reliability of Safety Instrumented Systems*
PERD	Process Equipment Reliability Database	PERD	*Process Equipment Reliability Database*

PFD	Probability of Dangerous Failure on Demand
PFDavg	Average Probability of Dangerous Failure on Demand
PFH	Probability (average frequency of dangerous failures) of Failure per hour
PTC	Proof Test Coverage
PTI	Proof Test Interval
PST	Partial Stroke Testing
RRF	Risk Reduction Factor
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System

PFD	*Probability of Dangerous Failure on Demand*
PFDavg	*Average Probability of Dangerous Failure on Demand*
PFH	*Probability (average frequency of dangerous failures) of Failure per hour*
PTC	*Proof Test Coverage*
PTI	*Proof Test Interval*
PST	*Partial Stroke Testing*
RRF	*Risk Reduction Factor*
SFF	*Safe Failure Fraction*
SIF	*Safety Instrumented Function*
SIL	*Safety Integrity Level*
SIS	*Safety Instrumented System*

5. DEFINITIONS

5.1 The following words shall have these special meanings when used herein:

Company	Pertamina Refining & Petrochemicals Subholding (PT.KPI and its subsidiaries)
Contractor/ Consultant	An independent third party safety contractor/consultant for SIL/LOPA Study in which is selected to conduct and engage SIL/LOPA Study for all projects under PT Pertamina (Persero) – Refining & Petrochemicals Subholding

5. DEFINISI

5.1 Penggunaan kata-kata berikut harus memiliki arti khusus sebagai berikut:

Company	Pertamina Refining & Petrochemicals Subholding (PT.KPI dan anak perusahannya)
Kontraktor/ Konsultan	Kontraktor/konsultan keselamatan pihak ketiga independen untuk Studi SIL/LOPA yang dipilih untuk melakukan dan terlibat dalam Studi SIL/LOPA untuk semua proyek di bawah PT Pertamina (Persero) – Subholding Refining & Petrochemicals

Controls	Any activity, facilities and equipment that is intended to help reducing the occurrence frequency of the hazard accident or to mitigate its consequences.	Kontrol	Setiap kegiatan, fasilitas dan peralatan yang dimaksudkan untuk membantu mengurangi frekuensi terjadinya bahaya kecelakaan atau untuk mengurangi konsekuensinya.
Equipment	Identifiable items of equipment such as vessels, pumps, instruments, etc.	Peralatan	Item peralatan yang dapat diidentifikasi seperti *vessel*, pompa, instrumen, dll.
Event	Thing that happens or takes place.	Peristiwa	Hal yang terjadi atau kejadian
Frequency	Number of the occurrences of defined event per unit time.	Frekuensi	Jumlah kemunculan peristiwa yang ditentukan per satuan waktu
Final Control Element	Any device that manipulates a process variable to achieve the control	Elemen Kontrol Akhir	Perangkat apa pun yang memanipulasi variabel proses untuk mencapai kontrol
Hazard	The potential to cause harm, including ill-health or injury; damage to property, installation, products or the environment; production losses or increased liabilities (e.g. pressurized hydrocarbons, high voltage equipment).	Bahaya	Potensi untuk menyebabkan kerugian, termasuk kesehatan yang buruk atau cedera; kerusakan properti, instalasi, produk atau lingkungan; kerugian produksi atau peningkatan kewajiban (misalnya hidrokarbon bertekanan, peralatan tegangan tinggi).
Impact	The ultimate potential result of a hazardous Event. This may be expressed in terms of numbers of injuries or fatalities, environmental or asset damage.	Dampak	Hasil potensial akhir dari Peristiwa berbahaya. Hal ini dapat dinyatakan dalam jumlah cedera atau kematian, kerusakan lingkungan atau aset.

Independent Protection Layer (IPL)	The device, system or action that is capable of preventing a scenario from proceeding to the undesired consequences of the initiating event or the action of any other protection layer associated with considered scenario.	Lapisan Perlindungan Independen (IPL)	Perangkat, sistem, atau tindakan yang mampu mencegah skenario dari melanjutkan ke konsekuensi yang tidak diinginkan dari peristiwa awal atau tindakan lapisan perlindungan lain yang terkait dengan skenario yang dipertimbangkan.
Initiating Cause	The Cause that initiates any hazardous scenario leading to the undesired Consequence.	Inisiasi Penyebab	Penyebab yang memulai skenario berbahaya apa pun yang mengarah ke Konsekuensi yang tidak diinginkan.
Mitigation	The act of causing a Consequence/Impact to be less severe	Mitigasi	Tindakan yang menyebabkan Akibat/Dampak menjadi lebih ringan
Prevention	The act of causing an event not to happen – reducing the Frequency/ Likelihood of the hazardous Cause occurrence.	Pencegahan	Tindakan menyebabkan suatu peristiwa tidak terjadi – mengurangi Frekuensi/ Kemungkinan terjadinya Penyebab berbahaya.
Recommendation	Activities identified during a desktop/workshop study for follow-up. These may comprise technical improvements in the design, modifications in the status of drawings and process descriptions and, procedural measures to be developed or further in-depth studies to be carried out.	Rekomendasi	Kegiatan yang diidentifikasi selama studi desktop/workshop untuk tindak lanjut Ini mungkin terdiri dari perbaikan teknis dalam desain, modifikasi status gambar dan deskripsi proses dan, langkah-langkah prosedural yang akan dikembangkan atau studi mendalam lebih lanjut yang akan dilakukan.
Risk	A measure combining the consequences of a	Resiko	Tindakan yang menggabungkan

	realized Hazard and the Frequency/Likelihood of its occurrence.		konsekuensi dari Bahaya yang disadari dan frekuensi atau kecenderungan kejadiannya.
Safeguard	The device, system or action that either would interrupt the chain of the events following the initiating event or that would mitigate the expected consequences	Safeguard	Perangkat, sistem, atau tindakan yang akan mengganggu rantai peristiwa setelah peristiwa awal atau yang akan mengurangi konsekuensi yang diperkirakan
Scenario	An Cause or sequence of Events that may result in undesirable Consequence.	Skenario	Penyebab atau urutan Peristiwa yang dapat mengakibatkan Akibat yang tidak diinginkan.
Severity	A measure indicating the hazardous Scenario impact on asset, personnel, public health, environment, and company reputation.	*Severity*	Ukuran yang menunjukkan dampak Skenario berbahaya terhadap aset, personel, kesehatan masyarakat, lingkungan, dan reputasi perusahaan.

6. CODES AND STANDARDS

This environmental design criteria shall be in accordance with the applicable laws, local regulations and standards. Reference codes and standards are as follows

1. IEC 61508 Parts 1-7 (2010) Functional Safety of Electrical/Electronic/Programmable
2. IEC 61511 Parts 1-3 (2016) Functional safety - Safety instrumented systems for the process industry sector
3. RP-ETS-PSE-EG- Project Risk Matrix and Tolerence Criteria

6. KODE DAN STANDAR

Kriteria desain lingkungan ini harus sesuai dengan hukum, peraturan dan standar setempat yang berlaku. Kode referensi dan standar adalah sebagai berikut.

1. IEC 61508 Parts 1-7 (2010) *Functional Safety of Electrical/Electronic/Programmable*
2. IEC 61511 Parts 1-3 (2016) *Functional safety - Safety instrumented systems for the process industry sector*
3. RP-ETS-PSE-EG- *Project Risk Matrix and Tolerence Criteria*

0001

4. RP-ETS-PSE-EG-0003 SIL Classification using LOPA Procedure.
5. SINTEF PDS Data Handbook (2013) Reliability Data for Safety Instrumented Systems.
6. OREDA (2015) Offshore Reliability Data handbook

7. SAFETY INSTRUMENTED SYSTEM (SIS)

A Safety Instrumented System (SIS) is an instrumented system used to implement one or more SIFs, comprising a logic solver that provides independent shutdown functionality, responsible for all identified SIFs with a SIL 1 or greater. A safety instrumented function is a safety function, with a specified safety integrity level, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event. A SIF typically comprises of sensor, logic solver and final element.

Safety Integrity Levels are performance categories for SIFs. The categories range from SIL 1 to SIL 4 as defined by IEC 61508 and IEC 61511, with SIL 4 representing the highest level of safety integrity. Each level represents an order of magnitude improvement in safety defined by the average probability of failure.

The Safety Instrument System provides independence from other Independent Protection Layers (IPLs) and is designed to prevent or mitigate a hazard if the process moves outside its normal operating

0001

4. RP-ETS-PSE-EG-0003 *SIL Classification using LOPA Procedure.*
5. SINTEF PDS Data Handbook (2013) *Reliability Data for Safety Instrumented Systems.*
6. OREDA (2015) *Offshore Reliability Data handbook*

7. SISTEM INSTRUMEN KESELAMATAN

Sistem Instrumen Keselamatan (SIS) adalah sistem instrumentasi yang digunakan untuk mengimplementasikan satu atau lebih SIF, yang meliputi *logic solver* yang menyediakan fungsi *shutdown* independen, yang bertanggung jawab untuk semua SIF yang teridentifikasi dengan SIL 1 atau lebih besar. Fungsi instrumen keselamatan adalah fungsi keselamatan, dengan tingkat integritas keselamatan tertentu, yang diharapkan untuk mencapai atau mempertahankan status aman proses dari peristiwa berbahaya tertentu. Sebuah SIF biasanya terdiri dari sensor, logic solver dan elemen akhir.

Tingkat Integritas Keselamatan adalah kategori performa untuk SIF. Kategori berkisar dari SIL 1 hingga SIL 4 seperti yang didefinisikan oleh IEC 61508 dan IEC 61511, dimana SIL 4 merupakan tingkat integritas keselamatan tertinggi. Setiap tingkat mewakili urutan peningkatan keselamatan yang ditentukan oleh probabilitas rata-rata kegagalan.

Sistem Instrumen Keselamatan terpisah dari Lapisan Perlindungan Independen (IPL) lainnya dan didesain untuk mencegah atau mengurangi bahaya jika proses beroperasi di luar kondisi operasi normal. Hal ini

envelope. It requires verification that the performance of each Safety Instrumented Function (SIF) is met throughout the safety lifecycle.

The performance criteria for each SIF operating in low demand mode are documented as part of the Safety Integrity Level (SIL) determination where a target average probability on demand (PFDavg), also known as Risk Reduction Factor (RRF), given by 1 / PFDavg, or the frequency of dangerous failures per hour for a high demand application must be achieved.

International Standard IEC 61508 written for functional safety of Electrical/Electronic/ Programmable Electronic (E/E/PE) for safety related systems was introduced, followed later by IEC 61511 written specifically for the process industry sector.

memerlukan verifikasi bahwa performa setiap *Safety Instrumented Function (SIF)* terpenuhi sepanjang siklus hidup keselamatan.

Kriteria performa untuk setiap SIF yang beroperasi dalam modus permintaan rendah didokumentasikan sebagai bagian dari penentuan Tingkat Integritas Keselamatan (SIL) di mana probabilitas rata-rata target sesuai permintaan (PFDavg), juga dikenal sebagai Faktor Pengurangan Risiko (RRF), diberikan oleh 1 / PFDavg, atau frekuensi kegagalan berbahaya per jam untuk aplikasi permintaan tinggi yang harus dicapai.

Standar Internasional IEC 61508 yang ditulis untuk keselamatan fungsional *Electrical/Electronic/ Programmable Electronic (E/E/PE)* untuk sistem keselamatan lain yang terkait sudah diperkenalkan, diikuti kemudian oleh IEC 61511 yang ditulis khusus untuk sektor industri proses.

7.1 Random, Systematic and Common Cause Failures

For compliance to either IEC61508 or IEC 61511 it has to be demonstrated that the SIF with a required integrity level of SIL 1 to SIL 3:

- Has sufficient reliability to achieve the overall target average Probability of Failure on Demand (PFDavg) for low demand applications and target frequency of dangerous failures per hour (PFH) for high demand or continuous modes of operation;
- Meets the architectural constraint requirements based on minimum hardware fault tolerance, and;
- Has sufficiently low probability of

7.1 Kegagalan dengan Penyebab Umum, Sistematis, dan tanpa pola/acak

Untuk memenuhi IEC61508 maupun IEC 61511, SIF dengan tingkat integritas yang dipersyaratkan dari SIL 1 hingga SIL 3 harus menunjukkan bahwa:

- Memiliki keandalan yang cukup untuk mencapai rata-rata target keseluruhan Probabilitas Kegagalan sesuai Permintaan (PFDavg) untuk aplikasi permintaan rendah dan frekuensi target kegagalan berbahaya per jam (PFH) untuk permintaan tinggi atau modus operasi berkelanjutan;
- Memenuhi persyaratan batasan arsitektur berdasarkan toleransi kesalahan perangkat keras minimum, dan;
- Memiliki probabilitas kegagalan

dangerous failure due to systematic faults.

The SIS may fail to operate on demand when one or more of its devices fail. This failure can be due to random, systematic and common cause events. The source of data to justify verification and any assumptions made will be indicated in the SIL verification report.

7.1.1. Random Hardware Failures

Random hardware failures can occur at any time during the life of a device. The failure of a device typically follows a “bathtub” curve with respect to time, where higher failure rates are expected during the early and latter stages in the life of the device. During the useful life of the device, the failure rate is assumed to be constant. Failure rates used for verification are based on statistical techniques, using Failure Mode Effects and Diagnostic Analysis (FMEDA) Methods or from reliable historical data collection based on failures whilst in service, e.g. OREDA. Failure due to random hardware faults are used to calculate the PFD of each SIF as described in this procedure.

7.1.2. Systematic Failures

Systematic integrity is difficult to quantify due to the diversity and opportunity for introducing faults due to human factors, manufacturing, operational and maintenance

berbahaya yang cukup rendah karena kesalahan sistematis.

SIS mungkin gagal beroperasi sesuai permintaan ketika satu atau lebih perangkatnya gagal. Kegagalan ini dapat disebabkan oleh peristiwa penyebab yang acak, sistematis dan umum. Sumber data untuk membenarkan verifikasi dan asumsi yang dibuat akan ditunjukkan dalam laporan verifikasi SIL.

7.1.1. Kegagalan Perangkat dengan Penyebab Acak

Kegagalan perangkat keras dengan penyebab acak dapat terjadi kapan saja selama masa pakai perangkat. Kegagalan perangkat biasanya mengikuti kurva “bath tub” yang berkaitan dengan waktu, di mana tingkat kegagalan yang lebih tinggi diharapkan selama tahap awal dan akhir dalam masa pakai perangkat. Selama masa manfaat perangkat, tingkat kegagalan diasumsikan konstan. Tingkat kegagalan yang digunakan untuk verifikasi didasarkan pada teknik statistik, menggunakan metoda *Failure Mode Effects and Diagnostic Analysis (FMEDA)* atau dari pengumpulan data historis yang dapat dipercaya berdasarkan kegagalan saat dalam servis, mis. OREDA. Kegagalan karena kesalahan perangkat keras acak digunakan untuk menghitung PFD dari setiap SIF seperti yang dijelaskan dalam prosedur ini.

7.1.2. Kegagalan Sistemtis

Integritas sistematis sulit untuk diukur karena keragaman dan kemungkinan penyebab kesalahan, karena faktor manusia, manufaktur, kegiatan operasional dan pemeliharaan

activities.

Systematic failures include many types of errors, such as:

- Specification and design errors during the development phase
- Manufacturing defects due to software or hardware errors
- Construction and testing errors, not meeting design specification
- Commissioning errors resulting in wrongly calibrated or configured equipment
- Maintenance and operational errors resulting in inadequate proof tests, failure to put the device back online, failure to remove a bypass
- Management of Change (MoC) errors

7.1.3. Common Cause Failures

Common Cause Failures (CCF) can be introduced due to errors in the design specification, during installation, or due to influence by the process or environmental conditions. CCF can dominate the overall PFD for redundant SIFs and errors made during the design and engineering phase can be eliminated by proven design guides which identify and address CCFs. Errors can be caught by using independent verification during the

Kegagalan sistematis mencakup banyak jenis kesalahan, seperti :

- Kesalahan spesifikasi dan desain selama fase pengembangan
- Cacat produksi karena kesalahan perangkat lunak atau perangkat keras
- Kesalahan konstruksi dan pengujian, tidak memenuhi spesifikasi desain
- Kesalahan pada saat komisioning yang mengakibatkan peralatan dikalibrasi atau dikonfigurasi secara salah
- Kesalahan pemeliharaan dan operasional yang mengakibatkan *proof tests* yang tidak memadai, kegagalan untuk mengembalikan perangkat secara *online,* kegagalan untuk menghapus *bypass*
- Kesalahan Manajemen Perubahan (MoC)

7.1.3. Kegagalan Penyebab Umum

Kegagalan Penyebab Umum (CCF) dapat terjadi karena kesalahan dalam spesifikasi desain, selama pemasangan, atau karena pengaruh proses atau kondisi lingkungan. CCF dapat mendominasi PFD keseluruhan untuk SIF yang berulang dan kesalahan yang dibuat selama fase desain dan *engineering* dapat dihilangkan dengan panduan desain yang telah terbukti yang mengidentifikasi dan menangani CCF. Kesalahan dapat ditangkap dengan

design and engineering phases of the project.

7.2 Selection of Software

The selection of SIL-certified devices in design, with available failure rate data, is essential for SIL Verification. The certificate ensures a Functional Safety Assessment has been carried out and will specify the SIL Capability based on systematic integrity, architectural constraints and PFD. The use of non-certified equipment or equipment type makes verification more conservative (i.e. higher PFD) since generic failure rates will be used in place of device- specific failure rates when computing the overall PFD. In addition, the Safe Failure Fraction (SFF) will be limited to a maximum of 50% for a Type 'A' device and 80% for a Type 'B' device, assuming 50% safe/ dangerous failures and 60% diagnostic coverage.

8. SIL VERIFICATION CRITERIA

Failure due to systematic errors can dominate the overall PFDavg for a SIF, for example leaving a differential pressure transmitter equalization manifold valve open or a bypass on will result in a failed SIF. Systematic errors need to be addressed at the relevant design and operational phases of the safety lifecycle with the goal to eliminate them by procedural and independent verification measures.

Whilst SIL Verification is an important process to verify the selected hardware achieves the required risk reduction for the Safety Integrity Level assigned, it is important to recognize that most failures of mission-critical systems are not caused by

menggunakan verifikasi independen selama fase desain dan engineering proyek.

7.2 Pemilihan Perangkat Lunak

Pemilihan perangkat bersertifikasi SIL dalam desain, dengan data tingkat kegagalan yang tersedia, sangat penting untuk Verifikasi SIL. Sertifikat memastikan Penilaian Keselamatan Fungsional telah dilakukan dan akan menentukan Kemampuan SIL berdasarkan integritas sistematis, kendala arsitektur dan PFD. Penggunaan peralatan atau jenis peralatan yang tidak bersertifikat membuat verifikasi lebih konservatif (yaitu PFD yang lebih tinggi) karena tingkat kegagalan umum akan digunakan sebagai pengganti tingkat kegagalan khusus perangkat saat menghitung PFD keseluruhan. Selain itu, Fraksi Kegagalan Aman (SFF) akan dibatasi hingga maksimum 50% untuk perangkat Tipe 'A' dan 80% untuk perangkat Tipe 'B' dengan asumsi 50% kegagalan aman/ berbahaya dan cakupan diagnostik 60%

8. KRITERIA VERIFIKASI SIL

Kegagalan karena kesalahan sistematis dapat mendominasi PFDavg keseluruhan untuk SIF, misalnya membiarkan sebuah *differential pressure transmitter equalization manifold valve* terbuka atau di *bypass* akan menghasilkan SIF yang gagal. Kesalahan sistematis perlu ditangani pada fase desain dan operasional yang relevan dari siklus hidup keselamatan dengan tujuan untuk menghilangkannya dengan langkah-langkah verifikasi prosedural dan independen.

Sementara Verifikasi SIL adalah proses penting dalam memverifikasi perangkat keras yang dipilih untuk mencapai pengurangan risiko yang diperlukan untuk Tingkat Integritas Keselamatan yang ditetapkan, penting untuk mengenali bahwa

hardware failure or software.They are caused by human error during design, maintenance and operational phases.

This procedure defines the verification steps required to meet the safety integrity level and addresses probability of failure on demand, hardware fault tolerance and systematic integrity of the equipment selected. It assumes all other failures due to systematic causes are addressed elsewhere.

The UK HSE published document HSG 238 (2003) : “Out of Control: Why control systems go wrong and how to prevent failure”. It documents the analysis based on 34 actual incidents which occurred resulting in a safety or environmental consequence. Refer to **Figure 1**., for typical mission critical system failures, where a significant proportion of the causes are due to errors made during the specification phase of a project. For SIL Verification, three criteria need to be satisfied for each SIF:

- PFDavg or PFH meets the risk reduction requirements for the assigned SIL
- Minimum Hardware Fault Tolerance is satisfied for the SIL target
- Equipment Systematic Integrity has been addressed

sebagian besar kegagalan sistem misi kritis tidak disebabkan oleh kegagalan perangkat keras atau perangkat lunak, tetapi disebabkan oleh faktor kesalahan manusia selama fase desain, pemeliharaan dan operasional.

Prosedur ini mendefinisikan langkah-langkah verifikasi yang diperlukan untuk memenuhi tingkat integritas keselamatan dan membahas kemungkinan kegagalan sesuai permintaan, toleransi kesalahan perangkat keras dan integritas sistematis dari peralatan yang dipilih. Ini dengan mengasumsikan semua kegagalan lain karena penyebab sistematis ditangani di tempat lain.

The UK HSE menerbitkan dokumen HSG 238 (2003): “*Out of Control*: Mengapa sistem kontrol salah dan bagaimana mencegah kegagalan”. Dokumen ini menganalisa berdasarkan 34 insiden aktual yang terjadi yang mengakibatkan konsekuensi keselamatan atau lingkungan. Berdasarkan Gambar 1., tipikal kegagalan sistem kritis misi, sebagian besar penyebabnya adalah karena kesalahan yang dibuat selama fase spesifikasi proyek. Untuk Verifikasi SIL, tiga kriteria harus dipenuhi untuk setiap SIF:

- PFDavg atau PFH memenuhi persyaratan pengurangan risiko untuk SIL yang ditetapkan
- Toleransi Kesalahan Perangkat Keras Minimum terpenuhi untuk target SIL
- Integritas Sistematis Peralatan telah ditangani

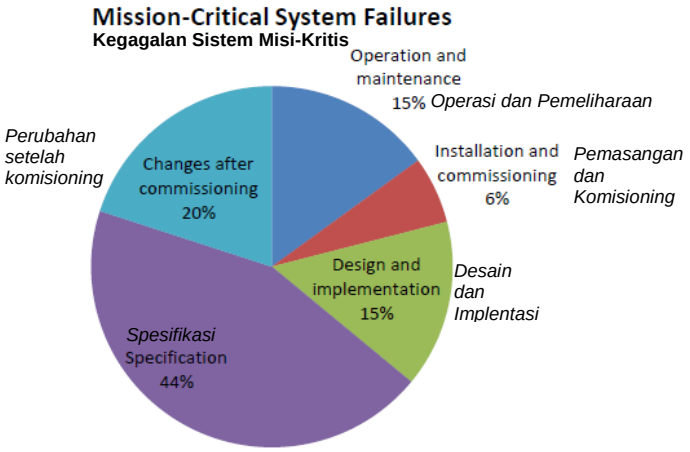

Figure 1. Mission-Critical System Failures by Cause

Gambar 1. Kegagalan Sistem Misi-Kritis dengan Penyebabnya

8.1 Probability of Failure On Demand (PFD) and Frequency Of Dangerous Failures (PFH)

The target average probability of failure on demand (PFDavg) or frequency of dangerousfailures (PFH) and the required SIL is specified through a separate SIL Determination exercise. Refer to the Project SIL Classification Procedure

a) If the SIL Determination exercise has provided a target PFDavg or PFH, then the probability of failure on demand or frequency of dangerous failures of each safety

b) If a target Safety Integrity Level (SIL) has been provided instead (typically from the risk graph method), the achieved PFDavg or PFH is to reside within the ranges specified in Table 1 and Table 2 below. This shall be verified by calculation.

8.1 Probabilitas Kegagalan Sesuai Permintaan (PFD) dan Frekuensi Kegagalan Berbahaya (PFH)

Target rata rata probabilitas kegagalan sesuai permintaan (PFDAvg) atau frekuensi kegagalan berbahaya (PFH) dan SIL yang diperlukan ditentukan melalui latihan Penentuan SIL yang terpisah. Mengacu kepada Prosedur Klasifikasi SIL Proyek

a) Jika latihan Penentuan SIL telah memberikan target PFDavg atau PFH, selanjutnya dilakukan latihan penentuan probabilitas kegagalan sesuai permintaan atau frekuensi kegagalan berbahaya dari setiap keselamatan

b) Jika target Tingkat Integritas Keselamatan (SIL) telah diberikan maka (biasanya dari metode grafik risiko), PFDavg atau PFH yang dicapai harus berada dalam kisaran yang ditentukan dalam Tabel 1 dan Tabel 2 di bawah. Ini harus diverifikasi dengan perhitungan.

8.1.1. Demand Mode

A demand mode safety instrumented function is a SIF that takes a specific action (e.g. closing a valve) in response to a process condition or demand. A potential hazard occurs only if dangerous failure of the SIF occurs simultaneously with a process failure which places a demand on the SIF.

In demand mode applications where the demand rate is more frequent than once per year, the hazard rate shall not be higher than the dangerous failure rate of the SIF. In such a case, it will normally be appropriate to use the continuous mode criteria. The SIL Determination exercise should have identified if the SIF is in low demand or high demand (continuous mode). The verification exercise must also distinguish between low demand and high demand modes.

For each SIF operating in low demand mode, the required SIL will be specified in accordance to IEC 61511-1:2016.

8.1.1. Mode Permintaan

Fungsi instrumentasi keselamatan mode permintaan adalah SIF yang mengambil tindakan tertentu (misalnya menutup *valve)* sebagai respons terhadap kondisi atau permintaan proses. Potensi bahaya hanya terjadi jika kegagalan berbahaya dari SIF terjadi bersamaan dengan kegagalan proses yang menempatkan permintaan pada SIF.

Dalam aplikasi mode permintaan di mana tingkat permintaan lebih dari sekali per tahun, tingkat bahaya tidak boleh lebih tinggi dari tingkat kegagalan berbahaya SIF. Dalam kasus seperti itu, biasanya akan tepat untuk menggunakan kriteria mode kontinyu. Latihan Penentuan SIL seharusnya mengidentifikasi apakah SIF dalam permintaan rendah atau permintaan tinggi (mode kontinyu). Latihan verifikasi juga harus membedakan antara mode permintaan rendah dan permintaan tinggi

Untuk setiap SIF yang beroperasi dalam mode permintaan rendah, SIL yang diperlukan akan ditentukan sesuai dengan IEC 61511-1:2016.

Table 1 : IEC 61511-1:2016 – Safety Integrity Requirements PFDavg

Tabel 1 : IEC 61511-1:2016 – Persyaratan Integritas Keselamatan PFDavg

LOW DEMAND MODE OF OPERATION *MODE OPERASI PERMINTAAN RENDAH*		
Safety Integrity Level (SIL) *Safety Integrity Level (SIL)*	Target average probability of failure on demand (PFDavg) *Target rata-rata probabilitas kegagalan sesuai permintaan (PFDAvg)*	Target risk reduction *Target pengurangan risiko*
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤100

The probability of failure on demand of the SIF is the sum of the dangerous failure rates for each subsystem, comprising sensors, logic solver and final elements. It includes all elements within the SIF, e.g. sensor, I.S. isolator, relay, solenoid, valve, actuator, positioner, booster valve, etc.

A simplified equation for 1oo1 (simplex) voting gives the average probability of failure on demand as:

$$PFD_{avg} = \frac{\lambda_{DU} PTI}{2}$$

Where λ_{DU} is the dangerous undetected failure rate and PTI is the proof test interval. This equation assumes dangerous detected λ_{DD} failures are detected by the logic solver, perfect Proof Test (100%) and no MTTR.

Probabilitas kegagalan sesuai permintaan SIF adalah jumlah dari tingkat kegagalan berbahaya untuk setiap subsistem, yang terdiri dari sensor, logic solver, dan elemen akhir, yang mencakup semua elemen dalam SIF, mis. *sensor, I.S. isolator, relay, solenoid, valve, actuator, positioner, booster valve,* dll.

Persamaan yang disederhanakan untuk pemungutan suara 1oo1 (simpleks) memberikan probabilitas rata-rata kegagalan pada permintaan sebagai:

$$PFD_{avg} = \frac{\lambda_{DU} PTI}{2}$$

Dimana λ_{DU} adalah tingkat kegagalan berbahaya yang tidak terdeteksi dan PTI adalah interval *proof test*. Persamaan ini mengasumsikan kegagalan berbahaya terdeteksi, λ_{DD} dapat dideteksi oleh logic solver, *Proof Test* yang sempurna (100%) dan tidak ada *MTTR.*

8.1.2. Continuous Mode

A continuous mode safety integrity function is one which in the event of a dangerous failure of the SIF, a potential hazard WILL occur without further failure unless action is taken to prevent it. Continuous mode covers those safety instrumented functions which implement continuous control to maintain functional safety.

The target failure measures for SIFs operating in continuous mode are defined in IEC 61511-1:2016 below.

8.1.2. Mode Kontinyu

Fungsi integritas keselamatan mode kontinyu adalah fungsi yang jika terjadi kegagalan yang berbahaya pada SIF, maka potensi bahaya AKAN terjadi tanpa kegagalan lebih lanjut kecuali jika tindakan diambil untuk mencegahnya. Mode kontinyu mencakup fungsi-fungsi instrumen keselamatan yang menerapkan kontrol berkelanjutan untuk menjaga keselamatan fungsional.

Ukuran kegagalan target untuk SIF yang beroperasi dalam mode kontinyu didefinisikan dalam IEC 61511-1:2016 di bawah ini.

Table 2. IEC 61511-1:2016 Safety Integrity Requirements: Average Frequency of Dangerous Failures of the SIF

Tabel 2. IEC 61511-1:2016 Persyaratan Integritas Keselamatan: Frekuensi Rata-rata Kegagalan Berbahaya SIF

CONTINUOUS MODE OR HIGH DEMAND MODE OF OPERATION[1] ***MODE KONTINYU ATAU MODE PERMINTAAN TINGGI OPERASI[1]***	
Safety Integrity Level (SIL) ***Tingkat Integrasi Keselamatan (SIL)***	**Average Frequency of Dangerous failures (failures per hour)** ***Frekuensi Rata-rata Kegagalan Berbahaya (kegagalan per jam)***
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

[1] IEC 61511-1:2016 Table 3-1 and Table 3-2 do not distinguish between low demand and high demand and state that for demand mode the SIL shall be specified in accordance with Table 3-1 or Table 3-2. This may be confusing to the user. High demand mode, where the frequency of demands is greater than one per year shall be determined in accordance with Table 3-2.

[1] IEC 61511-1:2016 Tabel 3-1 dan Tabel 3-2 tidak membedakan antara permintaan rendah dan permintaan tinggi dan menyatakan bahwa untuk mode permintaan SIL harus ditentukan sesuai dengan Tabel 3-1 atau Tabel 3-2. Ini mungkin membingungkan pengguna. Mode permintaan tinggi, di mana frekuensi permintaan lebih besar dari satu per tahun harus ditentukan sesuai dengan Tabel 3-2.

8.2 Hardware Fault Tolerance

The verification process must take into account the requirements for Hardware Fault Tolerance as detailed in IEC 61511-1:2016 Clause 11.4.

Hardware Fault Tolerance (HFT) is the ability of a component or subsystem to continue to undertake the required safety instrumented function in the presence of one or more dangerous faults in the hardware. A hardware fault tolerance of 1 means that for example there are two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring. 1oo2 or 2oo3 voting supports this level of fault tolerance.

The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in the SIF design that may result due to the number of assumptions made in the design of the SIF, along with the uncertainty in the failure rate of components or subsystems used in various process applications.

It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to IEC 61511-1:2016 Clause 11.9.

8.2 Toleransi Kesalahan Perangkat Keras

Proses verifikasi harus mempertimbangkan persyaratan untuk Toleransi Kerusakan Perangkat Keras sebagaimana dirinci dalam IEC 61511-1:2016 Klausul 11.4.

Toleransi Kegagalan Perangkat Keras (HFT) adalah kemampuan komponen atau subsistem untuk terus melakukan fungsi instrumentasi keselamatan yang diperlukan dengan adanya satu atau lebih kesalahan berbahaya pada perangkat keras. Toleransi kegagalan perangkat keras 1 dapat diartikan dengan contoh : ada dua perangkat dan arsitekturnya sedemikian rupa sehingga kegagalan berbahaya dari salah satu dari dua komponen atau subsistem tidak mencegah terjadinya tindakan keselamatan. Voting 1oo2 atau 2oo3 mendukung tingkat toleransi kesalahan ini.

Toleransi kesalahan perangkat keras minimum telah ditetapkan untuk mengurangi potensi kekurangan dalam desain SIF yang mungkin terjadi karena banyaknya asumsi yang dibuat dalam desain SIF, bersamaan dengan ketidakpastian dalam tingkat kegagalan komponen atau subsistem yang digunakan dalam berbagai aplikasi proses.

Penting untuk dicatat bahwa persyaratan toleransi kesalahan perangkat keras menggambarkan komponen minimum atau redundansi subsistem. Tergantung pada aplikasinya, tingkat kegagalan komponen dan *proof testing interval*, redundansi tambahan mungkin diperlukan untuk memenuhi SIL dari SIF menurut IEC 61511-1:2016 Klausul 11.9.

8.2.1. SIF Architectural Constraint

The safety integrity level of each safety instrumented function is determined by the average probability of failure on demand (PFDavg) of the SIF. However, the hardware fault tolerance and for the SIF architecture must also be considered to determine that the SIF meets the required SIL.

So, for example if the calculated PFDavg is low enough to achieve the required SIL, but the SIF architecture does not satisfy the hardware fault tolerance requirements, additional redundancy will be required to ensure the SIL is met.

It is important to recognize that the requirements for PFDavg and HFT are both met by adequate selection by type and redundancy for the SIF architecture.

a) Minimum Hardware Fault Tolerance

Clause 11.4.3 of IEC 61511-2:2016 defines the minimum Hardware Fault Tolerance (HFT) requirements for each SIF. This allows the determination in accordance with IEC 61511-1:2016 or IEC 61508-2:2010 as follows:

- ✓ 11.4.5 to 11.4.9 of IEC 61511-1:2016, clause 11 or,
- ✓ The requirements of 7.4.4.2 (route 1H) of IEC

8.2.1. Kendala Arsitektur SIF

Tingkat integritas keselamatan dari setiap fungsi instrumen keselamatan ditentukan oleh probabilitas rata-rata kegagalan sesuai permintaan (PFDavg) dari SIF. Namun, toleransi kesalahan perangkat keras dan untuk arsitektur SIF juga harus dipertimbangkan untuk menentukan bahwa SIF memenuhi apa yang dibutuhkan oleh SIL

Sehingga, misalnya PFDavg yang dihitung cukup rendah untuk mencapai apa yang dibutuhkan oleh SIL sedangkan arsitektur SIF tidak memenuhi persyaratan toleransi kesalahan perangkat keras, maka akan diperlukan tambahan redudansi untuk memastikan SIL terpenuhi.

Perlu diketahui bahwa persyaratan untuk PFDavg dan HFT dapat dipenuhi dengan pemilihan yang memadai berdasarkan jenis dan redundansi untuk arsitektur SIF.

a) Toleransi Minimum Kegagalan Perangkat Keras

Klausul 11.4.3 dari IEC 61511-2:2016 mendefinisikan persyaratan Toleransi minimum kegagagalan perangkat keras (HFT) untuk setiap SIF. Hal ini memungkinkan penetapannya sesuai dengan IEC 61511-1:2016 atau IEC 61508-2:2010 sebagai berikut:

- ✓ 11.4.5 to 11.4.9 of IEC 61511-1:2016, klausul 11 or,
- ✓ Persyaratan dari 7.4.4.2 (route 1H) of IEC 61508-

61508-2:2010 or,

- ✓ The requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

HFT for sensors and final elements may be determined by any one of the above three methods. The choice will be dependent on the selection of equipment and where certified, by the methodology used as stated on the SIL certificate. A SIL certified device will have been assessed in accordance with IEC 61508 and may have been determined by either Route 1H, Route 2H or both methods.

HFT for logic solvers shall be determined by the requirements of 7.4.4.2 (Route 1H) of IEC 61508-2:2010. This will be declared by the logic solver supplier and stated in the SIL certificate / assessment report. This methodology determines HFT by calculation of the Safe Failure Fraction (SFF).

Route 2H of IEC 61508-2:2010 uses proven in use (termed as prior use per IEC 61511) justification. This method has been adopted by IEC 61511-1:2016 and does not consider SFF during determination.

b) HFT Determination to IEC 61511-1:2016

Refer to below Table from

2:2010 or,

- ✓ Persyaratan dari 7.4.4.3 (route 2H) of IEC 61508-2:2010

HFT untuk sensor dan elemen akhir dapat ditentukan dengan salah satu dari tiga metode di atas. Pilihannya akan tergantung pada pemilihan peralatan dan di disertifikasi dengan metodologi yang digunakan sebagaimana dinyatakan pada sertifikat SIL. Perangkat bersertifikat SIL akan dinilai sesuai dengan IEC 61508 dan mungkin telah ditentukan dengan Rute 1H ataupun Rute 2H atau kedua metode.

HFT untuk *logic solver* harus ditentukan oleh persyaratan 7.4.4.2 (Rute 1H) dari IEC 61508-2:2010. Hal ini akan dinyatakan oleh pemasok *logic solver* dan dinyatakan dalam sertifikat / laporan penilaian SIL. Metodologi ini menentukan HFT dengan menghitung Fraksi Kegagalan Aman (SFF)

Rute 2H dari IEC 61508-2:2010 menggunakan justifikasi yang telah terbukti digunakan (disebut sebagai penggunaan sebelumnya menurut IEC 61511). Metode ini telah diadopsi oleh IEC 61511-1:2016 dan tidak mempertimbangkan SFF selama penentuan.

b) Penentuan HFT ke IEC 61511-1:2016

Berdasarkan Tabel dari Klausul

Clause 11.4.5:

11.4.5 dibawah ini :

Table 3. IEC 61511-1: 2016 – Minimum HFT Requirements According to SIL
Tabel 3. IEC 61511-1:2016 – Persyaratan HFT Minimum Menurut SIL

SIL *SIL*	Minimum required HFT *HFT minimum yang diperlukan*
1 (any mode) *1(Mode apa saja)*	0
2 (low demand mode) *2 (mode permintaan rendah)*	0
2 (high demand or continuous mode) *2 (mode pemintaan tinggi atau kontinyu*)	1
3 (any mode) *3 (mode apa saja)*	1
4 (any mode) *4 (mode apa saja)*	2

For a SIL 2 safety function operating in low demand mode there has been a reduction in HFT by one when compared to the previous version of IEC 61511.

Untuk fungsi keselamatan SIL 2 yang beroperasi dalam modus permintaan rendah, telah terjadi penurunan HFT sebesar satu jika dibandingkan dengan versi IEC 61511 sebelumnya.

The route developed in IEC 61511 is derived from route 2H of IEC 61508-2:2010. Route 2H justification uses field data based on proven in use concepts. Refer to 6.2.1.4 below for details. Equipment with a SIL certificate with Route 2H justification should be available to support HFT determined to IEC 61511.

Rute yang dikembangkan dalam IEC 61511 diturunkan dari rute 2H dari IEC 61508-2:2010. Justifikasi rute 2H menggunakan data lapangan berdasarkan konsep yang telah terbukti digunakan. Lihat 6.2.1.4 di bawah ini untuk detailnya. Peralatan dengan sertifikat SIL dengan justifikasi Rute 2H harus tersedia untuk mendukung HFT yang ditentukan pada IEC 61511.

c) HFT Determination to IEC 61508-2-1:2010 – Route 1H

c) Penentuan HFT ke IEC 61508-2-1:2010 – Rute 1H

Route 1H allows Hardware Fault Tolerance to be determined based on Safe Failure Fraction concepts using Table 4 and Table 5. IEC 61508-2:2010 Clause 7.4.4.2

Rute 1H memungkinkan Toleransi Kegagagalan Perangkat Keras ditentukan berdasarkan konsep Fraksi Kegagalan Aman menggunakan Tabel 4 dan Tabel 5. IEC 61508-

Table 2 for architectural constraints for Type A devices is detailed in Table 4:

2:2010 Klausul 7.4.4.2 Tabel 2 untuk batasan arsitektur untuk perangkat Tipe A dirinci dalam Tabel 4:

Table 4. IEC 61508-2:2010 Maximum allowable SIL for a safety function carried out by a type A Safety-Related Element or Subsystem

Tabel 4. IEC 61508-2:2010 SIL maksimum yang diizinkan untuk fungsi keselamatan yang dilakukan oleh tipe A Elemen atau Subsistem Terkait Keselamatan

SFF ***SFF***	**Hardware fault tolerance** *Toleransi Kegagalan Perangkat Keras*		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% -< 90%	SIL2	SIL3	SIL4
90% -< 99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

Definition of a type A device from IEC 61508-2 Clause 7.4.4.1.2; A subsystem can be regarded as type A if, for the components required to achieve the safety function:

Definisi perangkat tipe A dari IEC 61508-2 Klausul 7.4.4.1.2; Suatu subsistem dapat dianggap sebagai tipe A jika, untuk komponen yang diperlukan dalam mencapai fungsi keselamatan:

- ✓ The failure modes of all constituent components are well defined; and
- ✓ Mode kegagalan dari semua komponen konstituen didefinisikan dengan baik; dan
- ✓ The behaviour of the subsystem under fault conditions can be completely determined; and
- ✓ Perilaku subsistem di bawah kondisi gangguan dapat sepenuhnya ditentukan; dan
- ✓ There is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.
- ✓ Ada data kegagalan yang cukup dapat diandalkan dari pengalaman lapangan untuk menunjukkan bahwa tingkat kegagalan yang diklaim untuk kegagalan berbahaya yang terdeteksi dan tidak terdeteksi terpenuhi.

Examples of type A

- ✓ Contoh komponen tipe A

components are: switches, proximity switches, analogue transmitters (without digital processors), isolators/barriers, solenoid valves and valves.

adalah: sakelar, Sakelar proksimitas, transmitter analog (tanpa prosesor digital), isolator/penghalang, valve dan solenoid valves

A SIL certified valve with partial stroke testing (PST) functionality may satisfy the requirements of a type A device, depending on the selection of the partial stroke device.

✓ Valve bersertifikat SIL dengan fungsional partial stroke testing (PST) dapat memenuhi persyaratan perangkat tipe A, tergantung pada pemilihan perangkat partial stroke

IEC 61508-2:2010 Clause 7.4.4.2 Table 3 for architectural constraints for Type B devices is detailed in Table 5.:

✓ IEC 61508-2:2010 Klausul 7.4.4.2 Tabel 3 untuk batasan arsitektur untuk perangkat Tipe B dirinci dalam Tabel 5.:

Table 5. IEC 61508-2:2010 Maximum Allowable SIL for a Safety Function Carried Out by a Type B Safety-Related element or Subsystem

Tabel 5. IEC 61508-2:2010 SIL Maksimum yang Diperbolehkan untuk Fungsi Keselamatan yang Dilakukan oleh Elemen atau Subsistem Terkait Keselamatan Tipe B

SFF ***SFF***	**Hardware fault tolerance** ***Toleransi Kegagalan Perangkat Keras***		
	0	1	2
<60%	Not allowed	SIL1	SIL2
60% -< 90%	SIL1	SIL2	SIL3
90% -< 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

Definition of a type B device from IEC 61508-2 Clause 7.4.4.1.3; A subsystem shall be regarded as type B if, for the components required to achieve the safety function,

Definisi perangkat tipe B dari IEC 61508-2 Klausul 7.4.4.1.3; Suatu subsistem harus dianggap sebagai tipe B jika, untuk komponen yang diperlukan untuk mencapai fungsi keselamatan,

✓ The failure mode of at least one constituent

✓ Modus kegagalan setidaknya satu komponen

component is not well defined; or

- ✓ The behaviour of the subsystem under fault conditions cannot be completely determined; or
- ✓ There is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.

konstituen tidak didefinisikan dengan baik; atau

- ✓ Perilaku subsistem dalam kondisi gangguan tidak dapat ditentukan sepenuhnya; atau
- ✓ Tidak cukup data kegagalan yang dapat diandalkan dari pengalaman lapangan untuk mendukung klaim tingkat kegagalan untuk kegagalan berbahaya yang terdeteksi dan tidak terdeteksi.

NOTE:

This means that if at least one of the components of a subsystem itself satisfies the conditions for a type B subsystem then that subsystem must be regarded as type B rather than type A.

Examples of Type B components are; Transmitters with digital processors (HART), smart positioners and programmable logic solvers. Partial stroke device manufacturers have been successful in demonstrating certain products satisfy the requirements of a type ‘A’ device, despite the functionality being similar to a transmitter.

CATATAN:

Ini berarti bahwa jika setidaknya salah satu komponen dari subsistem itu sendiri memenuhi kondisi untuk subsistem tipe B, maka subsistem tersebut harus lebih dianggap sebagai tipe B dari pada tipe A.

Contoh komponen Tipe B adalah; *Transmitter* dengan prosesor digital (HART), *smart positioners and programmable logic solvers.* Produsen perangkat *partial stroke* telah berhasil menunjukkan produk tertentu memenuhi persyaratan perangkat tipe 'A', meskipun fungsinya mirip dengan transmitter

d) HFT Determination to IEC 61508-2-1:2010 – Route 2H

Route 2H allows Hardware Fault Tolerance to be

d) Penentuan HFT ke IEC 61508-2-1:2010 – Rute 2H

Route 2H memungkinkan Toleransi Kegagalan.

determined based on proven-in-use justification. This concept introduced in IEC 61508-2:2010 version is based on component reliability data from feedback from end users and hardware fault tolerance for specified safety integrity levels. Note that the Safe Failure Fraction is not considered by this method. Refer to Table 6. for minimum hardware fault tolerance requirements.

Perangkat Keras ditentukan berdasarkan justifikasi yang telah terbukti digunakan. Konsep yang diperkenalkan dalam versi IEC 61508-2:2010 ini didasarkan pada data keandalan komponen dari umpan balik dari pengguna akhir dan toleransi kesalahan perangkat keras untuk tingkat integritas keselamatan yang ditentukan. Perhatikan bahwa Fraksi Kegagalan Aman tidak dipertimbangkan dengan metode ini. Lihat Tabel 6. untuk persyaratan toleransi kegagalan perangkat keras minimum.

Table 6. IEC 61508-2:2010 Maximum Allowable SIL for a Safety Function

Tabel 6. IEC 61508-2:2010 SIL Maksimum yang Diizinkan untuk Fungsi Keselamatan

SIL ***SIL***	**Minimum HFT (Low Demand)** ***HFT Minimum (Permintaan Rendah)***	**Minimum HFT (High Demand or Continuous)** ***HFT Minimum (Permintaan Tinggi atau Kontinyu)***
1	0	0
2	0	1
3	1	1
4	2	2

For the majority of applications, SIL-certified equipment is available covering sensors, final elements and interface devices including certified safety relays for interface with electrical devices. It is strongly recommended that SIL certified equipment is always specified and used for safety instrumented functions (SIFs).

Untuk sebagian besar aplikasi, tersedia peralatan bersertifikasi SIL yang mencakup sensor, elemen akhir, dan perangkat *interface* termasuk *relay* keselamatan bersertifikat untuk *interface* dengan perangkat listrik. Sangat disarankan agar peralatan bersertifikasi SIL selalu ditentukan dan digunakan untuk fungsi yang dilengkapi dengan instrumen keselamatan (SIF).

All Type B elements used in

Semua elemen Tipe B yang

Route 2H shall have a minimum diagnostic coverage of not less than 60%. Route 1H method based on HFT and SFF was originally created as an additional design constraint for complex microprocessor devices which were being developed faster than reliable failure rate data being collected. The Route 2H method may be considered more appropriate for mechanical and electrical devices.

It is also acceptable to combine both methods for a sub-system, for an example a Type B transmitter (Route 1H) with Type A remote seal (Route 2H).

digunakan pada Rute 2H harus memiliki cakupan diagnostik minimum tidak kurang dari 60%. Metode Route 1H berdasarkan HFT dan SFF awalnya dibuat sebagai batasan desain tambahan untuk perangkat mikroprosesor kompleks yang dikembangkan lebih cepat daripada data tingkat kegagalan yang dapat diandalkan yang dikumpulkan. Metode Rute 2H dapat dianggap lebih tepat untuk perangkat mekanik dan listrik

Juga dapat diterima untuk menggabungkan kedua metode untuk sub-sistem, misalnya Transmitter Tipe B (Rute 1H) dengan remote seal Tipe A (Rute 2H).

8.3 Systematic Integrity

Systematic integrity refers to the part of the safety integrity of a SIF that is related to systematic failures in a dangerous mode of failure. Systematic safety integrity, unlike hardware safety integrity, cannot usually be quantified. It is typically assured through assessment of development procedures against IEC 61508.

A Systematic SIL Capable device has a development process that defines a safety lifecycle which meets the requirements for a safety lifecycle as documented in IEC 61508. Throughout all phases of this lifecycle, fault avoidance measures are included. Such measures include design reviews, FMEDA, code reviews, unit testing, integration testing, fault injection testing,

8.3 Integritas Sistematis

Integritas sistematis mengacu pada bagian dari integritas keselamatan SIF yang terkait dengan kegagalan sistematis dalam mode kegagalan yang berbahaya. Integritas keselamatan sistematis biasanya tidak bisa dikuantifikasi seperti pada integritas keselamatan perangkat keras. Hal ini biasanya diyakini melalui penilaian prosedur pengembangan terhadap IEC 61508.

Perangkat Berkemampuan SIL Sistematis memiliki proses pengembangan yang mendefinisikan siklus hidup keselamatan yang memenuhi persyaratan untuk siklus hidup keselamatan seperti yang didokumentasikan dalam IEC 61508. Sepanjang fase siklus hidup ini, langkah-langkah penghindaran kesalahan disertakan. Langkah-langkah tersebut termasuk tinjauan desain, FMEDA, tinjauan kode, pengujian unit, pengujian

etc.

The Systematic SIL Capability (SC)[2] of a device is documented on the device's certificate. A record of the investigation, prepared by the certification party, is available in the device's Functional Safety Assessment report. To ensure systematic integrity compliance, SIL-certified devices are preferred over non-SIL-certified equipment. SIL certified equipment ensures that the respective device has been allocated a systematic capability rating. A device with a rating of SC 3 means it is SIL 3 capable and can be used as part of a safety function up to SIL 3 providing the PFDavg and HFT are satisfied.

[2]Systematic Capability expressed as SC N (where N = 1 to 4) is a measure of the confidence that the systematic integrity of a device meets the requirements of the specified SIL level

8.4 Process Safety Time

The "process safety time" defined in IEC 61511-2:2016 as the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.

The SIF overall response time is defined as; from detection by the sensor to completion of the final element action. Control system failure or inadvertent human action may place a demand on a safety function at any time; it is assumed that the occurrence of the failure will be unrevealed until a demand is placed on the safety function. Based on this

integrasi, pengujian injeksi kesalahan, dll.

Kemampuan SIL Sistematis (SC)2 perangkat didokumentasikan pada sertifikat perangkat. Catatan investigasi, yang disiapkan oleh pihak sertifikasi, tersedia dalam laporan Penilaian Keselamatan Fungsional perangkat. Untuk memastikan kepatuhan terhadap integritas sistematis, perangkat bersertifikasi SIL lebih diutamakan daripada peralatan yang tidak bersertifikasi SIL. Peralatan yang bersertifikat SIL dijamin bahwa perangkat masing-masing telah dialokasikan peringkat kemampuan sistematisnya. Perangkat dengan peringkat SC 3 berarti mampu SIL 3 dan dapat digunakan sebagai bagian dari fungsi keselamatan hingga SIL 3 asalkan PFDavg dan HFT terpenuhi.

[2]Kemampuan Sistematis dinyatakan sebagai SC N (di mana N = 1 hingga 4) adalah ukuran keyakinan bahwa integritas sistematis perangkat memenuhi persyaratan tingkat SIL yang ditentukan

8.4 Waktu Keselamatan Proses

"Waktu keselamatan proses" yang didefinisikan dalam IEC 61511-2:2016 sebagai periode waktu antara kegagalan yang terjadi dalam proses atau sistem kontrol proses dasar (dengan potensi menimbulkan peristiwa berbahaya) dan terjadinya peristiwa berbahaya jika fungsi instrumentasi keselamatan tidak dilakukan

Waktu respons keseluruhan SIF didefinisikan sebagai; dari deteksi oleh sensor hingga penyelesaian tindakan elemen akhir. Kegagalan sistem kontrol atau tindakan manusia yang tidak disengaja dapat mengancam fungsi keselamatan setiap saat; diasumsikan bahwa terjadinya kegagalan tidak akan terungkap sampai permintaan ditempatkan

scenario the following approach has been taken, where, the response time target is calculated and based on the time period between initiation of the trip set-point and the time at the onset of the hazardous event. For over-pressure protection the system design pressure limit will be taken as the end value, this ensures that the safety function is independent of the mechanical protection layer where provided and the successful operation of the SIF will place the system in a safe state. The overall SIF response time shall be less that the response time target value.

As a guideline, the appropriate SIF response time should be less than half of process safety time.

pada fungsi keselamatan. Berdasarkan skenario ini, pendekatan berikut telah diambil, di mana, target waktu respons dihitung berdasarkan periode waktu antara permulaan *set-point trip* dan waktu pada permulaan peristiwa berbahaya. Untuk perlindungan tekanan berlebih, batas tekanan desain sistem akan diambil sebagai nilai akhir, ini memastikan bahwa fungsi keselamatan tidak bergantung pada lapisan perlindungan mekanis yang disediakan dan pengoperasian SIF yang berhasil akan menempatkan sistem dalam keadaan aman. Waktu respons SIF keseluruhan harus kurang dari nilai target waktu respons.

Sebagai pedoman, waktu respons SIF yang sesuai harus kurang dari setengah waktu keamanan proses.

9. SIL VERIFICATION INPUT AND ASSUMPTION

Key supporting documents in the verification exercise may include, but not limited to:

- Cause and Effect Diagrams
- SIL Determination Report (for the target SIL and PFDavg)
- Identification of the primary final element which removes the demand on the SIF

9.1 Methodology and Assumptions

9.1.1. Define Name and Tag for Safety Instrumented Function

A unique identifier should be created and assigned to each SIF for ease of identification and referencing. This may be based on the sensor tag number, e.g.

9. INPUT DAN ASUMSI VERIFIKASI SIL

Dokumen pendukung utama dalam pelaksanaan verifikasi dapat mencakup, namun tidak terbatas pada:

- Diagram Sebab Akibat
- Laporan Penetapan SIL (untuk SIL dan PFDavg target)
- Identifikasi elemen akhir utama yang menghilangkan permintaan pada SIF

9.1 Asumsi dan Metodologi

9.1.1. Penentuan Nama dan Tag untuk Fungsi Instrumen Keselamatan

Pengidentifikasi unik harus dibuat dan ditetapkan untuk setiap SIF untuk kemudahan identifikasi dan referensi. Ini mungkin didasarkan pada nomor tag sensor, mis.

LAHH-XXXX-XX.

9.1.2. Describe Safety Function, Hazard and Consequence

The function of the SIF shall be clearly described, along with the hazard and consequence to avoid ambiguity over the required executive action.

The sensors tag, and the final element tags should have been clearly recorded in the SIL Determination Report.

9.1.3. Define SIF Parameters The following typical assumptions may be used for verification.

LAHH-XXXX-XX.

9.1.2. Penjelasan Fungsi Keselamatan, Bahaya dan Konsekuensi

Fungsi SIF harus dideskripsikan dengan jelas, termasuk bahaya dan konsekuensi untuk menghindari ambiguitas atas tindakan eksekutif yang diperlukan

Tag sensor, dan tag elemen terakhir harus dicatat dengan jelas dalam Laporan Penentuan SIL.

9.1.3. Penentuan Parameter SIF , asumsi tipikal berikut dapat digunakan untuk verifikasi:

Table 7. SIF Assumptions
Tabel 7. Asumsi SIF

Parameter ***Parameter***	**Assumed Value** ***Nilai Asumsi***
Architectural Constraints *Kendala Arsitektur*	IEC 61511-1:2016 or IEC 61508:2010 Route 1H / Route 2H *IEC 61511-1:2016 atau IEC 61508:2010 Rute1H / Rute 2H*
IEC 61508 Systematic Capability *Kemampuan Sistematis IEC61508*	Yes *Ya*
Mission Time (sample) *Waktu Misi (contoh*)	15 to 20 years *15 – 20 tahun*
Startup Time (sample) *Waktu startup (contoh)*	24 hours *24 jam*

- Mission Time Considerations

  Mission time refers to the time from installation start-up to the replacement or refurbishment to as-new condition of the SIF or component of the SIF. The mission time should take into consideration the published “useful life” data provided by the manufacturer and the impact on the PFDavg due to imperfect proof testing. The

- Pertimbangan Waktu Misi

  Waktu misi mengacu pada saat mulai pemasangan hingga penggantian atau perbaikan hingga kondisi SIF atau komponen SIF seperti baru. Waktu misi harus mempertimbangkan data “masa pakai” yang dipublikasikan yang disediakan oleh pabrikan dan dampaknya pada PFDavg karena *proof testing* yang tidak

"useful life" information can be found in the Safety Manual provided by the supplier of the device, and also in the "Safety Equipment Reliability Handbook" (SERH) by Exida.	sempurna. Informasi "masa pakai" dapat ditemukan di Manual Keselamatan yang disediakan oleh pemasok perangkat, dan juga di "Buku Pegangan Keandalan Peralatan Keselamatan" (SERH) oleh Exida.
SIL verification is based on the relatively constant failure rate portion of the "bathtub curve". The documented product lifetime of a certified device typically stops short of the upward curve of the "bathtub". Therefore, extending the mission time beyond this limit can result in exceeding the required PFDavg for the SIF.	Verifikasi SIL didasarkan pada bagian tingkat kegagalan yang relatif konstan dari 'bathtub curve". Masa pakai produk yang didokumentasikan dari perangkat bersertifikat biasanya sedikit diatas "bathtub curve". Oleh karena itu, memperpanjang waktu misi di luar batas ini dapat mengakibatkan PFDavg yang diperlukan untuk SIF terlampaui.
Imperfect proof testing has the effect of limiting the achievable mission time for a given target SIL. The effect of the build-up of undetected failure mode contributions produces a saw-tooth curve (PFD vs. time) with an upward trend. Since PFDavg is the average over the complete mission time of the total PFD, the PFDavg for a shorter mission time will be lower than the PFDavg over a longer mission time.	*Proof testing* yang tidak sempurna berdampak membatasi waktu misi yang dapat dicapai untuk SIL target tertentu. Efek dari peningkatan kontribusi modekegagalan yang tidak terdeteksi menghasilkan kurva *saw-tooth* (PFD vs. waktu) dengan tren naik. Karena PFDavg adalah nilai rata-rata selama waktu misi lengkap dari total PFD maka PFDavg untuk waktu misi yang lebih pendek akan lebih rendah daripada PFDavg untuk waktu misi yang lebih lama.
Therefore, a too short mission time can provide a lower PFDavg but places a demand on Operations to refurbish to "as-new" or replace the device well before scheduled	Oleh karena itu, waktu misi yang terlalu singkat dapat memberikan PFDavg yang lebih rendah yang akan memaksa Operasi untuk melakukan *refurbishment* atau mengganti

maintenance. A too long mission time has the opposite effect of inflating the PFDavg, possibly placing additional requirements for redundant devices to achieve the target SIL.

perangkat jauh sebelum jadwal pemeliharaan. Waktu misi yang terlalu lama akan memberikan dampak sebaliknya yaitu akan memperbesar nilai PFDavg, memungkinkan untuk ditempatkan persyaratan tambahan pada perangkat yang berlebihan agar tercapainya target SIL.

9.2 Define Voting Configuration

The voting configuration, based on the Cause and Effects Diagram, is to be defined along with whether the equipment is identical or diverse.

9.2 Menentukan Konfigurasi *Voting*

Konfigurasi voting, yang berdasarkan Diagram Sebab-Akibat, harus ditentukan terlepas dari apakah peralatan itu identik atau beragam.

9.3 Define Common Cause Factor (Beta Factor β)

It is important that systematic failure due to common cause errors in design are identified and eliminated even if the probability is considered to be low. Verification that the hardware meets the required PFD does not address common cause design errors. A common cause failure (CCF) may cause multiple failures due to a shared cause and a common mode failure (CMF) where multiple items fail in the same mode.

9.3 Menentukan Faktor Penyebab Umum (*Beta Factor β*)

Suatu hal yang penting untuk mengidentifikasi dan menghilangkan kegagalan sistematis karena penyebab umum dalam desain walaupun kemungkinannya dianggap rendah. Hasil verifikasi yang menyatakan bahwa perangkat keras memenuhi PFD yang diperlukan, tidak mengatasi kesalahan desain kegagalan dengan penyebab umum. Kegagalan dengan penyebab umum (CCF) dapat menyebabkan beberapa kegagalan karena penyebab bersama dan kegagalan modus umum (CMF) di mana beberapa item gagal dalam mode yang sama.

- CCF example – A non-return valve (NRV) / check valve in a common hydraulic return line serving shutdown valves fails stuck in the closed position will result in all valves failing to danger on demand.

- Contoh CCF – Valve satu arah (NRV) / *check valve* di saluran balik hidraulik umum yang melayani *shutdown valves* gagal/ macet dalam posisi tertutup akan mengakibatkan semua valve gagal karena bahaya sesuai permintaan.

- CMF example – An undetected fault on a SIS analogue input module

- Contoh CMF – Kesalahan yang tidak terdeteksi pada modul input analog

causes all signals to read low resulting in all high trip functions connected to that module failing to danger immediately.

SIS menyebabkan semua sinyal terbaca rendah yang mengakibatkan semua fungsi trip tinggi yang terhubung ke modul tersebut gagal seketika.

Values of Common Cause Factor (Beta) are typically between 0% and 10%. 0% is used for non-redundant devices and 5% for identical devices in a voted configuration. Common causes can have a significant effect on the SIF reliability and assigning a high beta factor can dominate the overall PFD value therefore it is important to eliminate as many common cause sources as possible. Beta. β_D in Table 3-2 and Table 3-4 of IEC 61511 refer to failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere).

Nilai factor penyebab umum (Beta) biasanya antara 0% dan 10%. 0% digunakan untuk perangkat non-redundan dan 5% untuk perangkat identik dalam konfigurasi yang dipilih. Penyebab umum dapat memiliki pengaruh yang signifikan pada keandalan SIF dan menetapkan faktor beta yang tinggi dapat mendominasi nilai PFD keseluruhan oleh karena itu penting untuk menghilangkan sumber penyebab umum sebanyak mungkin. Beta β_D pada Tabel 3-2 dan Tabel 3-4 dari IEC 61511 mengacu pada kegagalan yang dideteksi oleh tes diagnostik, fraksi yang memiliki penyebab yang sama (dinyatakan sebagai fraksi dalam persamaan dan sebagai persentase di tempat lain).

During the engineering and design phase of the project, consideration shall be given to redundant systems to address; segregation / separation, diversity, design interfaces, test procedures and influences due to human interface and environmental conditions.

Selama fase engineering dan desain proyek, pertimbangan harus diberikan pada sistem redundan untuk mengatasi segregasi / pemisahan, keragaman, desain interface, prosedur pengujian dan pengaruh human interface dan kondisi lingkungan.

Typical assumptions in **Table 8.** below may be considered :

Asumsi umum pada **Tabel 8.** di bawah ini dapat dipertimbangkan:

Table 8. Beta Factor Assumptions

Tabel 8. Asumsi Faktor Beta

Device ***Perangkat***	**Assumed Beta Factor β** ***Asumsi Faktor Beta β***	**Remarks** ***Catatan***
Non-redundant devices *Perangkat Non-redundan*	0%	
Identical devices in a voted configuration *Perangkat identik dalam konfigurasi yang dipilih*	5%	Review FMEDA Report *Tinjauan Laporan FMEDA*

Diverse devices in a voted configuration *Beragam perangkat dalam konfigurasi yang dipilih*	0% for Shut-Off Valve and Pump 0% untuk Shut-Off Valve and Pompa 2-5% for Diverse Shut-Off Valves *2-5% for berbagai Shut-Off Valves*	

9.4 Define Mean Time to Repair Restoration (MTTR)

The mean time to restoration (MTTR) is the time from the detection of a dangerous fault to restoring the equipment or device to a fully functional state. Typical assumption for subsystem MTTR that may be considered are detailed in **Table 9.** below:

9.4 Penetapan *Mean Time to Repair Restoration (MTTR)*

Waktu rata-rata untuk restorasi (MTTR) adalah waktu saat deteksi kesalahan berbahaya sampai pemulihan peralatan atau perangkat ke keadaan berfungsi penuh. Asumsi tipikal untuk subsistem MTTR yang dapat dipertimbangkan dirinci dalam **Tabel 9.** di bawah ini:

Table 9. MTTR Assumptions

Tabel 9. Asumsi MTTR

Device type ***Jenis Perangkat***	**Assumed MTTR** ***Assumsi MTTR***
Sensors *Sensors*	8 to 72 hrs. *8 to 72 jam*
Logic Solver *Logic Solver*	8 to 72 hrs. *8 to 72 jam*
Final Elements *Elemen Akhir*	24 to 72 hrs. for Valves *24 to 72 jam untuk Valves* 8 to 72 hrs. for Electrical Drives / Heaters *8 to 72 hrs. for Penggerak Listrik / Pemanas*

This assumed time is required as part of the PFDavg calculation.

The assumption is that detection of a fault with redundant architecture is automatic by external diagnostics and an appropriate alarm is initiated for an operator to take the necessary action for maintenance to carry out a repair within the specified MTTR time. For redundant architecture voted 1oo2, the design can tolerate a single fault and SIF calculation takes into account the MTTR to maintain safe operation during

Asumsi waktu ini diperlukan sebagai bagian dari perhitungan PFDavg.

Asumsinya adalah bahwa deteksi kesalahan dengan arsitektur redundan dilakukan secara otomatis oleh diagnostik eksternal dan alarm sebagai tanda dimulainya bagi operator untuk mengambil tindakan yang diperlukan untuk pemeliharaan guna melakukan perbaikan dalam waktu MTTR yang ditentukan. Untuk arsitektur redundan yang dipilih 1oo2, desain dapat mentolerir kesalahan tunggal dan perhitungan SIF

the repair.

For non-redundant architecture, where the SIF is totally dependent on the availability of the failed device, additional measures are expected to be required to maintain safe operation whilst the repair is being undertaken. These additional measures shall be at least equal to the risk reduction provided by the SIF.

9.5 Input Proof Test Interval (PTI)

The Proof Test Interval (PTI) needs to be defined during SIL verification as the safety performance of each SIF is dependent on the SIF undergoing a full functional test at a specified interval.

The proof test requires a detailed inspection and a full functional test of the SIF from end to end or in parts; this covers the sensors, logic solver and final elements. The purpose of the proof test is to reveal any undetected dangerous failures in the SIF and restore it to the designed integrity. The aim is to provide 100% proof test coverage. In practice, no form of testing is perfect, and a human factor should be included since the test requires human intervention. A human error frequency for actions taken less than one month is 0.01 per year for an operator will trained with no stress. This corresponds to 99% so even with a theoretically perfect test procedure it should not be credited with more than 99%. Refer to proof test coverage in the next section.

sebagai pertimbangan untuk menentukan MTTR untuk menjaga operasi yang aman selama perbaikan.

Untuk arsitektur non-redundan, di mana SIF sepenuhnya bergantung pada ketersediaan perangkat yang gagal, langkah-langkah tambahan diharapkan diperlukan untuk menjaga operasi yang aman saat perbaikan sedang dilakukan. Tindakan tambahan ini setidaknya harus sama dengan pengurangan risiko yang diberikan oleh SIF.

9.5 Masukkan Interval *Proof Test (PTI*)

Interval *Proof Test* (PTI) perlu ditentukan selama verifikasi SIL karena performa keselamatan setiap SIF bergantung pada SIF yang menjalani uji fungsional penuh pada interval tertentu.

Proof test memerlukan pemeriksaan terperinci dan uji fungsional penuh SIF dari ujung ke ujung atau sebagian; ini mencakup *sensor, logic solver* dan elemen akhir. Tujuan dari proof test adalah untuk mengungkapkan kegagalan berbahaya yang tidak terdeteksi di SIF dan mengembalikannya ke integritas yang didesain. Tujuannya adalah untuk memberikan cakupan *proof test* 100%. Dalam praktiknya, tidak ada bentuk pengujian yang sempurna, dan faktor manusia harus dimasukkan karena pengujian memerlukan campur tangan manusia. Frekuensi kesalahan manusia untuk tindakan yang dilakukan kurang dari satu bulan adalah 0,01 per tahun untuk operator yang akan dilatih tanpa stres. Ini sesuai dengan akurasi 99% sehingga walaupun dengan prosedur pengujian yang secara teoritis sempurna, akurasi pengujian tidak boleh dianggap bisa lebih dari 99% Lihat cakupan *proof test* di bagian berikutnya.

The initial baseline proof test intervals assumed may be between 12 to 48 months. The PTI typically corresponds to the COMPANY's plant turnaround interval.

The Proof Test Intervals detailed above are the baseline for SIL Verification. There may be opportunity to increase these subject to the PFDavg being met. The manufacturer's recommendation for proof testing should be observed since these may specify a maximum test interval for a particular device. The design team is to be alerted if the manufacturer's recommended proof test intervals are unreasonably short as this may indicate that the integrity of the device is lower than claimed by the manufacturer. The target minimum test interval should be 12 months. Where the required proof test interval is less than 12 months, to ensure the PFDavg target is met, these shall be reviewed by the project team to accept or modify the design to provide additional redundancy.

Proof testing can be assumed to be conducted online for sensors and offline for final elements (referring to process online and offline).

9.6 Select Proof Test Coverage (PTC)

IEC 61508 and IEC 61511 provide detailed instructions for calculating diagnostic coverage (DC). This term applies to the ability to detect dangerous undetected failures by diagnostic tests and are automatic tests provided by logic solvers and safety transmitters.

PTC and DC should not be confused, and no guidance is given in either standard on how to calculate PTC. The manufacturer's safety manual for the equipment used in each safety function should have a

Dasar awal Interval *proof test* yang diasumsikan mungkin antara 12 hingga 48 bulan. PTI biasanya sesuai dengan interval *turnaround* pabrik PERUSAHAAN.

Interval *proof test* yang dirinci di atas adalah dasar untuk Verifikasi SIL. Mungkin ada peluang untuk meningkatkan subjek ini hingga PFDavg terpenuhi. Rekomendasi pabrikan untuk *proof test* harus diperhatikan karena ini dapat menentukan interval pengujian maksimum untuk perangkat tertentu. Tim desain harus diingatkan jika interval *proof test* yang direkomendasikan pabrikan terlalu pendek karena ini dapat mengindikasikan bahwa integritas perangkat lebih rendah daripada yang diklaim oleh pabrikan. Target interval tes minimum harus 12 bulan. Bila interval *proof test* yang diperlukan kurang dari 12 bulan, untuk memastikan target PFDavg terpenuhi, ini harus ditinjau oleh tim proyek, apakah bisa diterima atau memodifikasi desain untuk memberikan redundansi tambahan

Proof testing dapat diasumsikan dilakukan secara online untuk sensor dan offline untuk elemen akhir (mengacu pada proses online dan offline).

9.6 Pemilihan *Proof Test Coverage (PTC)*

IEC 61508 dan IEC 61511 memberikan petunjuk rinci untuk menghitung cakupan diagnostik (DC). Istilah ini berlaku untuk kemampuan mendeteksi kegagalan berbahaya yang tidak terdeteksi dengan tes diagnostik dan merupakan tes otomatis yang disediakan oleh *logic solvers* dan transmitters keselamatan

PTC dan DC tidak boleh membingungkan, dan tidak ada panduan yang diberikan dalam kedua standar tersebut diatas tentang cara menghitung PTC. Manual keselamatan pabrikan untuk peralatan

procedure detailing the proof test which should also provide a PTC factor claimed for the test.

yang digunakan dalam setiap fungsi keselamatan harus memiliki prosedur yang merinci *proof test* dan juga harus menyediakan faktor PTC yang diklaim untuk pengujian tersebut.

For Proof Testing of a valve, a witnessed full stroke test can detect a stuck or delayed stroking of the valve, providing good access is available for accurate visual inspection and confirmation. However, without any leak test monitoring measurement it is impossible to detect seat leakage failures, which account for approximately 30% of all dangerous undetected failures. Generally, PTC is based on confirmation of the valves ability to move to its fail-safe position for a full stroke application, but in reality, the PFD may be higher due to unrevealed seat leakage faults.

Untuk valve *Proof Testing*, pembuktian dengan uji full stroke dapat mendeteksi gerakan valve yang macet atau tertunda, menyediakan akses yang baik untuk inspeksi dan konfirmasi visual yang akurat. Akan tetapi, tanpa pengukuran, pemantauan uji kebocoran tidak mungkin mendeteksi kegagalan, karena kebocoran *valve seat* yang merupakan sekitar 30% dari semua kegagalan berbahaya yang tidak terdeteksi. Umumnya, PTC didasarkan pada konfirmasi kemampuan valve untuk pindah ke posisi gagal-aman untuk aplikasi *full stroke*, tetapi pada kenyataannya, PFD mungkin lebih tinggi karena kesalahan kebocoran *valve seat* yang tidak terungkap.

To explore further the effectiveness of the proof test on a valve and the consequence of the PTC assumed, IEC 61508 and IEC 61511 do not give guidance on selection of the proof test coverage factor and many suppliers and end users have assumed a “near perfect” or perfect proof test. If we use a 70% PTC for a valve proof test then there is an argument to suggest the proof test procedure is wrong, and in time this means some random hardware failures remaining will prevent the SIF from performing its safety function. At the end of the proof test the result of the test is “pass” or “fail” with a fail meaning the system cannot perform its safety function.

Untuk mengeksplorasi lebih lanjut efektivitas *proof test* pada *valve* dan konsekuensi dari asumsi PTC, IEC 61508 dan IEC 61511 tidak memberikan panduan tentang pemilihan faktor cakupan *proof test* dan banyak pemasok dan pengguna akhir telah mengasumsikan "hampir sempurna" atau *proof test* sempurna. Jika kita menggunakan PTC 70% untuk *valve proof test* maka ada argumen yang menyatakan prosedur *proof test* salah, dan ini dapat diartikan bahwa beberapa kegagalan perangkat keras acak yang tersisa akan menghalangi SIF melakukan fungsi keselamatannya. Pada akhir *proof test* hasil pengujiannya adalah “lulus” atau “gagal”, apabila “gagal” berarti sistem tidak dapat menjalankan fungsi keselamatannya

Random hardware failures may happen at any time; this type of sudden failure is likely to be revealed by the proof test; an

Kegagalan perangkat keras acak dapat terjadi kapan saja; jenis kegagalan mendadak ini kemungkinan besar akan

example being the valve is unable to fully close due to a failure. Degraded failure also needs to be considered as these results due to aging and can be caused by corrosion, erosion, or deposition on the seat and effects due to the process and environment. Failures due to these effects are not sudden but occur slowly over time. This is very different from a sudden failure which will result in a dangerous state if it happens, while a degraded failure can still achieve the safety function in a degraded state over a long period of time.

terungkap melalui proof test; sebagai contoh valve tidak dapat menutup sepenuhnya karena kegagalan. Kegagalan terdegradasi juga perlu dipertimbangkan karena akibat dari proses penuaan dan dapat juga disebabkan oleh korosi, erosi, atau deposisi pada *valve seat* dan karena efek proses dan lingkungan. Kegagalan karena efek ini tidak tiba-tiba tetapi terjadi perlahan seiring waktu. Hal ini sangat berbeda dengan kegagalan tiba-tiba yang akan mengakibatkan keadaan berbahaya jika terjadi, sedangkan kegagalan yang terdegradasi masih dapat mencapai fungsi keselamatan dalam keadaan terdegradasi dalam jangka waktu yang lama.

An example is corrosion of the valve seat, where the valve is able to perform its safety function, but eventually excessive corrosion may lead to failure of the safety function due to high leakage rates. This may be revealed by other monitoring functions on the process and may put a demand on the final layer of protection, e.g. lift the PSV.

Contohnya adalah korosi pada valve seat di mana valve dapat melakukan fungsi keamanannya, tetapi pada akhirnya korosi yang berlebihan dapat menyebabkan kegagalan fungsi pengaman karena tingkat kebocoran yang tinggi. Hal ini dapat diungkapkan oleh fungsi pemantauan lainnya pada proses dan dapat menempatkan permintaan pada lapisan perlindungan terakhir, mis. angkat PSV nya.

A preventative maintenance schedule needs to be in place to return the valve to "as good as new" in accordance with the manufacturers recommendations for the application. To apply a low proof test coverage factor will have a significant effect on increasing the PFD, and result in additional hardware requirements due to an overly pessimistic result; IEC 61508 and IEC 61511 do not take account of degraded failure in the PFD calculation, all failures are treated as random hardware so a constant failure rate with respect to time is applied. This is not true for degraded failure, which increases over time, it may have little or no effect on loss of the safety function and may only be

Jadwal pemeliharaan *preventif* perlu dibuat untuk mengembalikan valve ke kondisi "seperti baru" sesuai dengan rekomendasi pabrikan untuk aplikasi tersebut. Penerapan faktor cakupan *proof test* rendah akan memiliki efek signifikan pada peningkatan PFD, dan akan menghasilkan tambahan persyaratan perangkat keras karena hasil yang terlalu pesimis; IEC 61508 dan IEC 61511 tidak memperhitungkan kegagalan terdegradasi dalam perhitungan PFD, semua kegagalan diperlakukan sebagai kegagagalan perangkat keras acak sehingga tingkat kegagalan konstan terhadap waktu diterapkan. Ini tidak betul karena untuk kegagalan terdegradasi, yang meningkat

present after a number of years, yet these failure rates are treated exactly the same as a random hardware failure which may cause the valve to fail to operate on demand, i.e. remain open when demanded to close which will always result if failure of the safety function.

seiring waktu, mungkin memiliki sedikit atau tidak berpengaruh pada hilangnya fungsi keselamatan dan mungkin hanya ada setelah beberapa tahun, namun tingkat kegagalan ini diperlakukan persis sama dengan kegagalan perangkat keras acak, yang dapat menyebabkan valve gagal beroperasi sesuai permintaan, yaitu tetap terbuka ketika diminta untuk menutup, dan ini akan selalu terjadi jika ada kegagalan fungsi keselamatan

To allocate a PTC factor the user needs to be aware of the manufacturers recommendations for their equipment and have sufficient confidence the test procedure will be performed accordingly to reveal the declared fraction of random hardware faults.

Untuk mengalokasikan faktor PTC, pengguna perlu memperhatikan rekomendasi pabrikan untuk peralatan mereka dan meyakini bahwa prosedur pengujian akan dilakukan sesuai untuk mengungkapkan fraksi yang dinyatakan dari kegagalan perangkat keras acak.

Typical assumption for Proof Test Coverage is detailed in **Table 10.** below.

Asumsi tipikal untuk cakupan Proof Test dirinci dalam **Tabel 10.** di bawah ini.

Table 10. Proof Test Coverage Assumption

Tabel 10. Asumsi Cakupan Proof Test

Parameter ***Parameter***	**Assumed Value** ***Nilai Asumsi***	**Remarks** ***Catatan***
Proof Test Coverage – Offline Proof Test *Cakupan Proof Test – Proof Test Offline*	100% *100%*	Adjust as necessary in accordance with manufacturer's recommendation *Diatur seperlunya sesuai dengan rekomendasi pabrikan*

9.7 Safe Failure Fraction (SFF)

Safe Failure Fraction (SFF) is the fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure. From the random hardware failures, the SFF can be calculated. The SFF shall not include systematic failures. Failure rates for impulse line plugging or freezing shall be included in the PFD calculation as part of the sensor sub-system.

9.7 Fraksi *Kegagalan* Aman (SFF)

Fraksi Kegagalan Aman (SFF) adalah fraksi dari keseluruhan tingkat kegagalan perangkat keras acak dari perangkat yang menghasilkan kegagalan aman atau kegagalan berbahaya yang terdeteksi. Dari kegagalan perangkat keras acak, SFF dapat dihitung. SFF tidak boleh mencakup kegagalan sistematis. Tingkat kegagalan untuk penyumbatan atau pembekuan saluran impuls harus dimasukkan dalam perhitungan PFD sebagai bagian dari sub-sistem sensor

SFF can be determined by the following calculation:

$$SFF = \frac{(\lambda_S + \lambda_{DD})}{(\lambda_S + \lambda_D)}$$

Where λ_S is safe failure rate, λ_{DD} is diagnosed dangerous failure rate and λ_D is dangerous failure rate. Refer to IEC61508-2:2010, Annex C.1 for details on how to calculate SFF.

IMPORTANT CHANGE IN IEC 61508-2:2010 The method for calculating SFF in revision 2 of the standard has been revised so the “No-Effect” or “No-Part” failures shall not play any part in the calculation of the diagnostic coverage or the Safe Failure Fraction as defined in IEC61508-2:2010, C.1.c. This is a fundamental change to IEC61508:2000 and can significantly reduce the SFF for a device. Refer to the example in 4.1.11.1 (Table 4-12 and related text) where the calculation for a typical shutdown valve demonstrates a reduction in the SFF from 70% to 40%. The impact is severe since the hardware fault tolerance needs to be increased by one, therefore requiring two valves for a SIL 2 and three valves for a SIL 3 application. A safety transmitter is also affected by this new method; however, the effect is much less (typically reduces by 2-3%), this is because the transmitter has automatic diagnostics which detect additional failures, and these are classed as Dangerous Detected failures which improve the SFF value. The SFF is typically determined by the SIL verification software without further input and used to determine the SIL achieved considering architectural constraints.

SFF dapat ditentukan dengan perhitungan berikut:

$$SFF = \frac{(\lambda_S + \lambda_{DD})}{(\lambda_S + \lambda_D)}$$

Dimana λ_S adalah tingkat kegagalan aman, λ_{DD} adalah tingkat kegagalan berbahaya yang didiagnosis dan λ_D adalah tingkat kegagalan berbahaya. Lihat IEC61508-2:2010, Lampiran C.1 untuk rincian cara menghitung SFF.

PERUBAHAN PENTING DALAM IEC 61508-2:2010 Metode untuk menghitung SFF dalam revisi 2 standar telah direvisi sehingga kegagalan “Tanpa Efek” atau “Tanpa Bagian” tidak akan berperan dalam perhitungan cakupan diagnostik atau Fraksi Kegagalan Aman sebagaimana didefinisikan dalam IEC61508-2:2010, C.1.c. Ini adalah perubahan mendasar pada IEC61508:2000 dan dapat secara signifikan mengurangi SFF untuk sebuah perangkat. Lihat contoh pada 4.1.11.1 (Tabel 4-12 dan teks terkait) di mana perhitungan untuk *shutdown valve* tipikal menunjukkan penurunan SFF dari 70% menjadi 40%. Dampaknya parah karena toleransi kegagalan perangkat keras perlu ditingkatkan satu, oleh karena itu membutuhkan dua valve untuk aplikasi SIL 2 dan tiga *valve* untuk aplikasi SIL 3. Transmitter keselamatan juga dipengaruhi oleh metode baru ini; namun, efeknya jauh lebih sedikit (biasanya berkurang 2-3%), ini karena transmitter memiliki diagnostik otomatis yang mendeteksi kegagalan tambahan, dan ini digolongkan sebagai kegagalan Terdeteksi Berbahaya yang meningkatkan nilai SFF. SFF biasanya ditentukan oleh perangkat lunak verifikasi SIL tanpa masukan lebih lanjut dan digunakan untuk menentukan SIL yang dicapai dengan mempertimbangkan kendala arsitektur.

9.8 Field Reliability Data

Where SIL verification is required for equipment which has not been certified to IEC 61508, SINTEF PDS3 data handbook (latest edition) shall be used for reliability data. The PDS data is compiled from field reliability feedback data based on a number of sources, the most recognised in the industry is OREDA. The PDS method is used for safety instrumented systems (SIS) to quantify the safety unavailability due to dangerous failures and loss of production due to safe failures. The method includes all failures due to both random hardware and systematic failures. Random hardware failures will occur at some point in time and can be predicted by FMEDA.

PDS³ is a Norwegian acronym for reliability of safety instrumented systems.

Typical causes resulting in failure of the SIS are included in the PDS method, such as:

- Normal aging / wear out
- Software related failures
- Hardware related failures
- Stress induced failures
- Installation failures
- Operational failures

There is a requirement to justify selection of devices based on prior use as defined in IEC 61511-1:2016, clause 11.5.3.

Neither IEC 61508 nor IEC 61511 quantify the required amount of

9.8 Data Keandalan Lapangan

Ketika verifikasi SIL diperlukan untuk peralatan yang belum disertifikasi untuk IEC 61508, buku pegangan data SINTEF PDS3 (edisi terbaru) harus digunakan untuk data keandalan. Data PDS dikompilasi dari data umpan balik keandalan lapangan berdasarkan sejumlah sumber, yang paling dikenal di industri adalah OREDA. Metode PDS digunakan pada sistem instrumentasi keselamatan (SIS) untuk mengukur ketidak tersediaan keselamatan karena kegagalan berbahaya dan kehilangan produksi karena kegagalan aman. Metode ini mencakup semua kegagalan, kegagagalan perangkat keras acak dan kegagalan sistematis. Kegagalan perangkat keras acak akan terjadi di beberapa titik waktu dan dapat diprediksi oleh FMEDA.

PDS³ adalah singkatan dalam Bahasa Norwegia untuk keandalan sistem instrumen keselamatan.

Penyebab khusus yang mengakibatkan kegagalan SIS termasuk dalam metode PDS, seperti:

- Penuaan / keausan normal
- Kegagalan terkait perangkat lunak
- Kegagalan terkait perangkat keras
- Kegagalan akibat stres
- Kegagalan instalasi
- Kegagalan operasional

Ada persyaratan untuk membenarkan pemilihan perangkat berdasarkan penggunaan sebelumnya sebagaimana didefinisikan dalam IEC 61511-1:2016, klausul 11.5.3.

Baik IEC 61508 maupun IEC 61511 tidak menghitung jumlah pengalaman

operational experience to justify 'proven in use' or 'prior use', but state extensive operating experience can be used as a basis for the evidence.

Exida recommends a minimum of 10 million operational hours based on ten different applications. SINTEF PDS data handbook recommend a minimum of 2.5 million operational hours from at least two installations or at least 2 dangerous undetected failures should have been registered for the considered observation period.

Based on the data sources for equipment failure rates and inclusion of both random hardware and systematic failures used to compile the PDS data handbook the prior use requirement can be justified.

a) Reliability Data Uncertainties

The reliability data uncertainties can be evaluated according to the amount of field feedback. IEC 61508-2:2010 section 7.4.9.5 and IEC 61511-1:2016 section 11.9.4 require that the reliability data shall be assessed and taken into account when calculating the failure measure. An upper bound confidence limit of 70 % for dangerous undetected failure rate should be used instead of the mean value. This requirement is with respect to random hardware failures. This is to obtain conservative point estimates of the failure measure.

Upper bound 70% values are presented in PDS data hand book

operasional yang diperlukan untuk membenarkan 'terbukti digunakan' atau 'penggunaan sebelumnya', tetapi menyatakan pengalaman operasi ekstensif dapat digunakan sebagai dasar untuk bukti.

Exida merekomendasikan minimal 10 juta jam operasional berdasarkan sepuluh aplikasi yang berbeda. Buku pegangan data SINTEF PDS merekomendasikan minimal 2,5 juta jam operasional dari setidaknya dua instalasi atau setidaknya 2 kegagalan berbahaya yang tidak terdeteksi harus didaftarkan untuk periode pengamatan yang dipertimbangkan.

Buku pegangan data PDS disusun berdasarkan sumber data untuk tingkat kegagalan peralatan dan penyertaan kegagalan perangkat keras acak dan kegagalan sistematis persyaratan penggunaan sebelumnya dapat dibenarkan.

a) Ketidakpastian Data Keandalan

Ketidakpastian data keandalan dapat dievaluasi sesuai dengan jumlah umpan balik lapangan. IEC 61508-2:2010 pasal 7.4.9.5 dan IEC 61511-1:2016 pasal 11.9.4 mensyaratkan bahwa data keandalan harus dinilai dan diperhitungkan saat menghitung ukuran kegagalan. Batas atas tingkat kepercayaan 70% untuk tingkat kegagalan berbahaya yang tidak terdeteksi harus digunakan sebagai ganti nilai rata-rata. Persyaratan ini berkaitan dengan kegagalan perangkat keras acak. Ini untuk mendapatkan estimasi titik konservatif dari ukuran kegagalan.

Nilai batas atas 70% disajikan dalam buku pegangan data PDS bagian

section 3.5.2, Table 11. Where no upper bound 70 % values are provided due to insufficient data being available then a factor of 1.5 x mean value may be assumed as an estimated value.

9.9 SIL Certified Equipment Failure Rate Data

A Failure Modes Effects and Diagnostic Analysis (FMEDA) is a method to predict expected failure rates based on a constant failure rate for the equipment during its useful life.

Some SIL certified equipment has justified the dangerous failure rates presented using the proven in use method based on field returns to the Original Equipment Manufacturer (OEM) In some cases the failure rates given for shutdown valves are overly optimistic, with reliability being stated up to 3 orders of magnitude lower than generic failure rate data[4] In such cases it is potentially dangerous to perform SIL verification using this data since the actual performance for the SIF will be much lower than claimed.

[4]For this example it is likely that the calculation is based on assumed number of devices in service and the actual number of valves which have been returned to the OEM with a claimed dangerous failure. Where the reality is the majority of valves in service are maintained and serviced by a third party.

Dangerous failure rates should always be compared with generic data with a sensitivity check to confirm they are within upper and lower bound norms for failures

3.5.2, Tabel 11. Jika tidak ada batas atas nilai 70% yang diberikan karena data yang tersedia tidak mencukupi, maka faktor 1,5 x nilai rata-rata dapat diasumsikan sebagai nilai perkiraan .

9.9 Data Tingkat Kegagalan Peralatan Bersertifikat SIL

A Failure Modes Effects and Diagnostic Analysis (FMEDA) adalah metode untuk memprediksi tingkat kegagalan yang diperkirakan berdasarkan tingkat kegagalan yang konstan untuk peralatan selama masa manfaatnya.

Beberapa peralatan bersertifikat SIL telah membenarkan tingkat kegagalan berbahaya yang ditampilkan dengan menggunakan metode yang telah terbukti, yaitu yang berdasarkan data jumlah perangkat yang dikembalikan ke Original Equipment Manufacturer (OEM) dengan klaim kegagalan berbahaya. Dalam beberapa kasus, tingkat kegagalan yang diberikan untuk *shutdown valve* terlalu optimis, dengan keandalan dinyatakan hingga 3 urutan besarnya lebih rendah dari data tingkat kegagalan umum[4]. Apabila verifikasi SIL dilakukan dengan data seperti tersebut diatas maka akan menimbulkan potensi bahaya, karena kinerja sebenarnya untuk SIF akan jauh lebih rendah dari pada yang diklaim.

[4]Untuk contoh ini, kemungkinan perhitungan didasarkan pada asumsi jumlah perangkat yang digunakan dan jumlah sebenarnya dari valve yang telah dikembalikan ke OEM dengan klaim kegagalan berbahaya. Dimana kenyataannya mayoritas valve, servis dan pemeliharaannya dilakukan oleh pihak ketiga.

Tingkat kegagalan yang berbahaya harus selalu dibandingkan dengan data umum dengan pemeriksaan sensitivitas untuk memastikan bahwa mereka berada dalam

of the same device. If the dangerous failure rate is outside the limits, then further analysis shall be carried out to justify use of the data presented on the SIL certificate. If, however the difference is extreme as presented in the previous paragraph then generic data shall be used.

The failure rates from a FMEDA report are termed random hardware failures. FMEDA and model-specific data are preferred over generic field data.

a) Interpreting Failure Rates and Diagnostic Coverage from FMEDA Reports. Failure rates are expressed as lambda (λ), so λ_D for all dangerous failure and λ_S for all safe failures

Non-smart devices such as a relay, solenoid or valve do not have any internal diagnostics to detect failures. Smart devices have, and the term used for this is diagnostic coverage (DC), this usually refers to the detection of dangerous fault only because safe faults are inherently safe. DC is quoted as a percentage. Failure rates can now be broken down further into detected and undetected, giving:

- λ_T – Total Failure Rate
- λ_{SD} – Safe Detected
- λ_{SU} – Safe Undetected
- λ_{DD} – Dangerous Detected
- λ_{DU} – Dangerous Undetected

Failure rates are normally quoted in

standar batas atas dan bawah untuk kegagalan perangkat yang sama. Jika tingkat kegagalan berbahaya berada di luar batas, maka analisis lebih lanjut harus dilakukan untuk membenarkan penggunaan data yang disajikan pada sertifikat SIL. Namun, jika perbedaannya ekstrem seperti yang disajikan dalam paragraf sebelumnya, maka data umum harus digunakan

Tingkat kegagalan dari laporan FMEDA disebut kegagalan perangkat keras acak. FMEDA dan pemodelan data khusus lebih diutamakan daripada data lapangan umum.

a) Penafsiran Tingkat Kegagalan dan cakupan diagnostik dari Laporan FMEDA. Laju kegagalan dinyatakan sebagai lambda (λ), jadi λ_D untuk semua kegagalan berbahaya dan λ_S untuk semua kegagalan aman

Perangkat *non-smart* seperti relai, solenoid, atau *valve* tidak memiliki diagnostik internal untuk mendeteksi kegagalan. Perangkat smart memiliki diagnostik internal dan disebut dengan istilah cakupan diagnostik (DC), ini biasanya mengacu pada deteksi kegagalan berbahaya hanya karena kegagalan aman secara inheren aman. DC dinyatakan sebagai persentase. Tingkat kegagalan sekarang dapat dipecah lebih lanjut menjadi terdeteksi dan tidak terdeteksi, dengan perincian sebagai berikut:

- λ_T – Tingkat Kegagalan Total
- λ_{SD} – Aman Terdeteksi
- λ_{SU} – Aman Tidak Terdeteksi
- λ_{DD} – Terdeteksi Berbahaya
- λ_{DU} – Berbahaya Tidak Terdeteksi

Tingkat kegagalan biasanya dinyatakan

Failure in Time (FIT), these are faults per billion hours or 1 FIT = 1E-09 hours. Alternatively, failure rate in hours is quoted, for example 200 FITs = 200E-09 = 2.0E-07 hours.

If no FMEDA report or generic field data is available then the Mean Time to Fail (MTTF) can be used, and the following assumptions made. For example, from the vendor information a device has a MTTF of 40 years; λ_T = 1 / MTTF, then the total failure rate per hour is 1 / 40 / 365 / 24 = 2.85E-06 h. If no ratio is provided for safe or dangerous faults, then a split of 50% shall be used.

Diagnostic coverage for a non-Smart device is 0% (none available), for a smart device a value of 60% shall be assumed. This is the minimum value of DC for a smart device according to IEC 61508.

IEC61508 was revised and reissued in 2010; the following examples demonstrate the differences in architectural constraints due to the two different methods for calculating Safe Failure Fraction. IEC61508:2010 methodology give more conservative results and may result in redundant hardware for application above SIL 1, especially for shutdown/ emergency isolation valves.

dalam Kegagalan dalam Waktu (FIT), ini adalah kesalahan per miliar jam atau 1 FIT = 1E-09 jam. Atau, tingkat kegagalan dalam jam dikutip, misalnya 200 FIT = 200E-09 = 2.0E-07 jam.

Jika tidak ada laporan FMEDA atau data lapangan umum yang tersedia maka *Mean Time to Fail (MTTF)* dapat digunakan, dan dibuat asumsi sebagai berikut. Misalnya, dari informasi vendor perangkat memiliki MTTF 40 tahun; λ_T = 1 / MTTF, maka total tingkat kegagalan per jam adalah 1/40/365/24 = 2.85E-06 jam. Jika tidak ada rasio yang disediakan untuk kesalahan yang aman atau berbahaya, maka pembagian 50% harus digunakan.

Cakupan diagnostik untuk perangkat non-Smart adalah 0% (tidak tersedia), untuk perangkat *smart* nilai 60% harus diasumsikan. Ini adalah nilai minimum DC untuk perangkat pintar menurut IEC 61508.

IEC61508 sudah direvisi dan diterbitkan kembali pada tahun 2010; contoh berikut menunjukkan perbedaan batasan arsitektur karena dua metode berbeda untuk menghitung Fraksi Kegagalan Aman. Metodologi IEC61508:2010 memberikan hasil yang lebih konservatif dan dapat mengakibatkan adanya redundan perangkat keras untuk aplikasi di atas SIL 1, terutama untuk *shutdown valve / valve* isolasi darurat.

9.10 Consideration for Systematic Capability

Where a device has been certified to IEC 61508:2010 it will have a stated Systematic Capability, e.g. SC 3 “(SIL 3 Capable)”. This is determined by an independent SIL assessment to ensure there is sufficient integrity against systematic errors during the design and manufacturing processes by the

9.10 Pertimbangan untuk Kemampuan Sistematis

Jika perangkat telah disertifikasi untuk IEC 61508:2010, perangkat tersebut akan dinyatakan memiliki Kemampuan Sistematis, misalnya SC 3 “(Mampu SIL 3)”. Ini ditentukan oleh penilaian SIL independen untuk memastikan ada integritas yang cukup terhadap kegagalan sistematis selama proses desain dan

manufacturer. Based on the results of the assessment a SC level is awarded and declared on the SIL certificate. Where IEC 61508 systematic capability is considered during SIL verification this may be the limiting factor for the achieved safety integrity level where a high SIL is required. For example, considering a device certified to SC 2 where used in a voted configuration of 1oo2 or 2oo3 may meet SIL 3 in terms of PFDavg and hardware fault tolerance, but the SIF will be limited to a maximum of SIL 2. When a device is certified to SC 2/3 the systematic capability is limited to 2 for a simple 1oo1 device but increases to SC 3 with an HFT = 1 for voted architecture such as 1oo2 or 2oo3.

manufaktur oleh pabrikan. Berdasarkan hasil penilaian, tingkatan SC diberikan dan dinyatakan pada sertifikat SIL. Kemampuan sistematis IEC 61508 dipertimbangkan selama verifikasi SIL, karena ini mungkin bisa menjadi faktor penghambat untuk mencapai tingkat integritas keselamatan saat SIL tinggi diperlukan. Misalnya, mempertimbangkan perangkat yang disertifikasi SC 2 yang digunakan dalam konfigurasi voting 1oo2 atau 2oo3 dapat memenuhi SIL 3 dalam hal PFDavg dan toleransi kesalahan perangkat keras, tetapi SIF akan dibatasi hingga maksimum SIL 2. Saat perangkat disertifikasi untuk SC 2/3 kemampuan sistematis terbatas pada 2 untuk perangkat 1oo1 sederhana tetapi meningkat menjadi SC 3 dengan HFT = 1 untuk arsitektur terpilih seperti 1oo2 atau 2oo3.

IEC 61511:2016 does not mandate the use of devices certified with a systematic capability but refers to a qualitative approach with justification provided by the user. The preference is to perform SIL verification with systematic capability justified to IEC 61508 wherever possible.

IEC 61511:2016 tidak mengamanatkan penggunaan perangkat yang disertifikasi dengan kemampuan sistematis tetapi mengacu pada pendekatan kualitatif dengan pembenaran yang diberikan oleh pengguna. Preferensinya adalah melakukan verifikasi SIL dengan kemampuan sistematis yang sesuai dengan IEC 61508 jika memungkinkan.

In cases where this is not possible it is recommended that SINTEF PDS data handbook failure reliability data is used since this includes all failures including dangerous undetected failure due to systematic faults.

Dalam kasus di mana hal ini tidak memungkinkan, disarankan agar data yang ada pada buku pegangan SINTEF PDS data handbook failure reliability digunakan karena ini mencakup semua kegagalan termasuk kegagalan berbahaya yang tidak terdeteksi karena kesalahan sistematis.

9.11 Partial Stroke Testing

Partial Stroke Testing is a technique used to detect dangerous undiagnosed failures within the final element sub-system, in this case a shutdown/ emergency isolation valve. The method typically involves moving the SIS valve 10-20% and back in

9.11 Pengujian Partial Stroke

Partial Stroke Testing adalah teknik yang digunakan untuk mendeteksi kegagalan berbahaya yang tidak terdiagnosis dalam sub-sistem elemen akhir, dalam hal ini *shutdown valve / valve* isolasi darurat. Metode ini biasanya berupa aktivitas

a short period of time. From this test, diagnostic information is gathered that can help determine the suitability of the valve for continued SIS service.

menggerakkan valve SIS 10-20% dan kembali dalam waktu singkat. Dari pengujian ini, informasi diagnostik yang dikumpulkan dapat membantu menentukan kesesuaian valve untuk layanan SIS lanjutan.

PST does however increase the spurious trip rate due to the potential for the valve to fully close during the test. The spurious failures due to PST are not normally included in the MTTFS figures.

Meskipun demikian PST akan meningkatkan laju sinyal trip palsu yang berpotensi menyebabkan *valve* menutup penuh selama pengujian. Kegagalan palsu karena PST biasanya tidak termasuk dalam angka MTTFS.

Manufacturers tend to claim very high figures for DC some as high as 99% and use this as an argument for reduction in Hardware Fault Tolerance (HFT). Since PST only provides diagnostics to reveal failure during the PST (DCPST) it is not continuous and shall not be used to affect the SFF, and subsequently make any reduction in HFT.

Produsen cenderung mengklaim angka yang sangat tinggi untuk DC ada yang memberi angka 99% dan menggunakan ini sebagai argumen untuk pengurangan Toleransi Kesalahan Perangkat Keras (HFT). Karena PST hanya menyediakan diagnostik untuk mengungkapkan kegagalan selama PST (DCPST), maka PST tidak berkelanjutan dan tidak boleh digunakan untuk mempengaruhi SFF dan membuat pengurangan HFT

Diagnostic coverage for partial stroke testing varies from a pessimistic 30% to 70%, while a figure of around 60% for DCPST is quoted by OREDA. The DCPST from Exida's Safety Equipment database may be used for SIL verification when PST is implemented by selecting the "Use Equipment Data" option.

Cakupan diagnostik untuk pengujian stroke parsial bervariasi dari pesimistis 30% hingga 70%, sementara angka sekitar 60% untuk DCPST ditentukan oleh OREDA. DCPST dari database Peralatan Keselamatan Exida dapat digunakan untuk verifikasi SIL saat PST diterapkan dengan memilih opsi "Gunakan Data Peralatan".

On a critical application where the safety function relies upon the valve shut-off with leakage class to ANSI CLASS VI the diagnostic coverage will be less since the PST test cannot verify the leakage rate. In an application where a valve has a very short stroke time PST in some cases may be considered unsuitable, for example a HIPPS where the valve closure time is less than or equal to 2 seconds for full stroke.

Pada aplikasi kritis di mana fungsi keselamatan bergantung pada *shut-off valve* dengan kelas kebocoran ke ANSI KELAS VI, cakupan diagnostik akan lebih sedikit karena uji PST tidak dapat memverifikasi tingkat kebocoran. Dalam aplikasi di mana *valve* memiliki waktu langkah yang sangat singkat PST dalam beberapa kasus dapat dianggap tidak sesuai, misalnya HIPPS dimana waktu penutupan *valve* kurang dari atau sama

The provision of PST will reduce the achieved PFDavg for the SIF but should only be accounted for in the PFD calculation if it has been confirmed that the device will be provided.

9.12 Compare Achieved SIL against the Target SIL

When comparing the Achieved Safety Integrity Level against the Target Safety Integrity Level, PFDavg, architectural constraints and systematic capability must be met.

If the architectural constraints are not met, redundancy adequate for the required hardware fault tolerance shall be recommended.

If the PFDavg does not meet the required target, risk reduction factors should be explored in the following order:

a) If the architectural constraints SIL does not meet the target SIL and redundant devices were recommended, check if the new achieved PFDavg with additional redundancy meets the required SIL.

b) Identify if any other SIS Sensor or Final Element is available that can also return the process to a safe state. Increased redundancy (e.g. 1oo2 configuration) can reduce the achieved PFDavg.

c) Reduce the Proof Test Intervals – the interval should not be unreasonably short, (e.g. 1 month).

d) If the sub-system which is driving the PFDavg up into the next range is a valve, perform a sensitivity check to establish if partial stroke testing can improve the achieved PFDavg.

dengan 2 detik untuk full stroke

Penyediaan PST akan mengurangi PFDavg yang dicapai untuk SIF tetapi hanya diperhitungkan dalam perhitungan PFD jika telah dikonfirmasi bahwa perangkat akan disediakan

9.12 Membandingkan Pencapaian SIL dengan Target SIL

Saat membandingkan Tingkat Integritas Keselamatan yang Dicapai dengan Tingkat Integritas Keselamatan Target, PFDavg, batasan arsitektur, dan kemampuan sistematis harus dipenuhi.

Jika kendala arsitektur tidak terpenuhi, redundansi yang memadai untuk toleransi kesalahan perangkat keras yang diperlukan harus direkomendasikan.

Jika PFDavg tidak memenuhi target yang disyaratkan, faktor pengurangan risiko harus dieksplorasi dalam urutan berikut:

a) Jika kendala arsitektur SIL tidak memenuhi target SIL dan perangkat redundan direkomendasikan, periksa apakah PFDavg baru yang dicapai dengan redundansi tambahan memenuhi SIL yang diperlukan.

b) Identifikasi apakah ada Sensor SIS atau Elemen Akhir lain yang tersedia yang juga dapat mengembalikan proses ke status aman. Peningkatan redundansi (misalnya konfigurasi 1oo2) dapat mengurangi PFDavg yang dicapai.

c) Kurangi Interval *Proof Test,* akan tetapi interval tidak boleh terlalu pendek, (misalnya 1 bulan)

d) Jika sub-sistem yang mendorong PFDavg ke kisaran berikutnya adalah *valve,* lakukan pemeriksaan sensitivitas untuk menentukan apakah pengujian *partial stroke* dapat meningkatkan

e) Perform a sensitivity check to establish if additional redundancy in sensors or final elements improves the achieved PFDavg so that the target SIL may be met.

f) Consider replacing the “guilty” device with a device that has a lower probability of failure on demand.

These may be employed in combination if necessary.

9.13 Record Recommendatios

Recommendations should be clearly listed within the body of the SIL Verification Report, linked to the correct SIF, and contain the relevant device tag numbers.

Each SIF verification calculation record should identify assumptions that are in reality “recommendations” (i.e. not yet implemented) to avoid confusion. If possible, the improvements gained through the adoption of recommendations may be reported separately as “sensitivity checks”.

The typical recommendations include Proof Test Intervals that are shorter than the generally assumed values, requirement for an additional valve to be tripped as part of a SIF, provision of PST and the recommended interval, etc.

10. SOFTWARE

SIL calculations are typically verified using commercially purchased software. Widely used and proven software should be selected (Exida’s exSILentia or equivalent).

PFDavg yang ingin dicapai.

e) Lakukan pemeriksaan sensitivitas untuk menetapkan apakah redundansi tambahan pada sensor atau elemen akhir meningkatkan PFDavg yang ingin dicapai sehingga SIL target dapat terpenuhi.

f) Pertimbangkan untuk mengganti perangkat "bersalah" dengan perangkat yang memiliki kemungkinan kegagalan yang lebih rendah sesuai permintaan.

Ini dapat digunakan dalam kombinasi jika perlu

9.13Catatan Rekomendasi

Rekomendasi harus dicantumkan dengan jelas di dalam isi Laporan Verifikasi SIL, ditautkan ke SIF yang benar, dan berisi nomor *tag* perangkat yang relevan.

Setiap catatan perhitungan verifikasi SIF harus mengidentifikasi asumsi yang sebenarnya didalam “rekomendasi” (yaitu belum diterapkan) untuk menghindari kebingungan. Jika memungkinkan, peningkatan yang diperoleh melalui penerapan rekomendasi dapat dilaporkan secara terpisah sebagai “pemeriksaan sensitivitas”.

Rekomendasi tipikal termasuk interval *Proof Test* yang lebih pendek dari nilai yang diasumsikan secara umum, persyaratan untuk *valve* tambahan yang gagal sebagai bagian dari SIF, penyediaan PST dan interval yang direkomendasikan, dll.

10. PERANGKAT LUNAK

Perhitungan SIL biasanya diverifikasi menggunakan perangkat lunak yang dibeli secara komersial. Perangkat lunak yang banyak digunakan dan terbukti harus dipilih (exSILentia Exida atau yang setara).

The results should be validated to ensure they are giving correctly calculated values. Typical methods of checking include, but are not limited to, comparison of results against a known correct standard, either other software or hand-calculated. To minimize the required effort, this can be achieved initially by a typical approach, based on hardware architecture, i.e. single transmitter - single valve, 2oo3 transmitters - single valve, etc.

Hasilnya harus divalidasi untuk memastikan mereka memberikan nilai yang telah dihitung dengan benar. Metode pemeriksaan yang umum termasuk, tetapi tidak terbatas pada, perbandingan hasil terhadap standar yang diketahui benar, baik dengan perangkat lunak lain atau yang dihitung dengan tangan. Untuk meminimalkan upaya yang harus dilakukan, dapat dicapai dengan pendekatan tipikal, berdasarkan arsitektur perangkat keras, yaitu transmitter tunggal – valve tunggal, transmitter 2oo3 - dll.