SAFETY REQUIREMENT SPECIFICATION

ENGINEERING TECHNICAL STANDARDS & PROCEDURES

PT KILANG PERTAMINA INTERNASIONAL

DIREKTORAT PROYEK INFRASTRUKTUR

00	Issued For Record	04/25	ASY	JMS	ASR	RMD	AG
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*
9 / 7.5	02/25	*Update*: - Add voting logic for the transmitter used for SIL 3 classified SIF - Add PST for On/Off Valve used for SIL 3 classified SIF	ASY
1-22	04/25	Revisi dokumen ini kembali ke Rev.00 dikarenakan *update* format penomoran dari RP-ETS-INS-GS-0030-01 menjadi KPI-ETS-INS-GS-0030	WHE

TABLE OF CONTENTS
DAFTAR ISI

1. INTRODUCTION

1.1 The purpose of this Safety Requirement Specification (SRS) document is to specify the functional and integrity requirements for each SIF implemented in the SIS for needs of the Project.

Both the functional and integrity requirements have been provided in order to achieve the required functional safety complying with IEC 61511, Clause 10.3.1 as well as project standard.

In the General Sections, the requirements which are common to SIS and all the SIFs havebeen identified. In the SIF Specific Section, those requirements which are specific to a SIF have been identified. The SIF Specific Section has been organized in a Microsoft Excel spreadsheet.

1. PENGANTAR

1.1 Tujuan dokumen *Safety Requirement Specification* (SRS) adalah untuk menetapkan persyaratan fungsional dan integritas untuk setiap implementasi SIF dalam SIS untuk memenuhi kebutuhan Proyek.

Persyaratan fungsional dan integritas telah disediakan untuk mencapai keselamatan fungsional yang disyaratkan sesuai dengan IEC 61511, *Clause* 10.3.1 serta standar proyek.

Pada bagian umum, persyaratan umum untuk SIS dan seluruh SIF telah diidentifikasi. Pada bagian spesifik SIF, persyaratan yang khusus untuk SIF telah diidentifikasi, dan telah tersedia dalam bentuk *Microsoft Excel spreadsheet.*

2. SCOPE

2.1 This specification, together with its attachments, defines the requirements of all the Safety Instrumented Functions (SIF) pertaining to the Project

The requirements have been furnished in the following sections:

a. General Safety Instrumented System (SIS) Section

b. General Safety Instrumented Function (SIF) Section

c. Safety Instrumented Function (SIF) Specific Section

2. LINGKUP

2.1 Spesifikasi ini, bersama dengan lampirannya, mendefinisikan persyaratan dari semua *SafetyInstrumented Functions* (SIF) yang berkaitan untuk Proyek

Persyaratan telah dilengkapi di bagian berikut:

a. Bagian umum *Safety Instrumented System* (SIS)

b. Bagian umum *Safety Instrumented Function* (SIF)

c. Bagian spesifikasi *Safety Instrumented Function* (SIF)

3. CONFLICTS AND DEVIATIONS

3.1 Any conflicts between this standard and other applicable Engineering Technical Standards & Procedures (ETSP), or OWNER standard, codes, and forms shall

3. KONFLIK DAN DEVIASI

3.1 Apabila terdapat konflik antara standar ini dengan *Engineering Technical Standards & Procedures* (ETSP) yang berlaku lainnya, atau standar PEMILIK, *codes* dan formulir, maka harus diselesaikan secara tertulis oleh

be resolved in writing by OWNER.

3.2 All direct requests to deviate from this standard (ETSP) in writing to OWNER, who shall follow internal OWNER procedure and forward such requests to OWNER for approval.

4. ABBREVIATIONS

4.1 Abbreviations used for this specification shall have the following definitions:

ISA	International Society of Automation
LOPA	Layer of Protection Analysis
MOC	Management of Change
SIF	Safety Interlock Functions
SIL	Safety Integrity Level
SIR	Safety Interlock Review
SIS	Safety Instrumented System
SRS	Safety Requirements Specification

5. DEFINITIONS

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

OWNER	Owner of the Plant is defined as PT Kilang Pertamina Internasional
CONTRACTOR/ CONSULTANT	Defined as the Organization to which PT Kilang Pertamina Internasional assign the work
shall	Indicates that the statement is

PEMILIK.

3.2 Semua permintaan penggunaan standar yang berbeda dari standar ini (ETSP), harus diajukan kepada PEMILIK secara tertulis dengan mengikuti prosedur *internal* PEMILIK untuk mendapatkan persetujuan.

4. SINGKATAN

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

ISA	*International Society of Automation*
LOPA	*Layer of Protection Analysis*
MOC	*Management of Change*
SIF	*Safety Interlock Functions*
SIL	*Safety Integrity Level*
SIR	*Safety Interlock Review*
SIS	*Safety Instrumented System*
SRS	*Safety Requirements Specification*

5. DEFINISI

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

PEMILIK	Pemilik Kilang didefinisikan sebagai PT Kilang Pertamina Internasional
KONTRAKTOR/ KONSULTAN	Didefinisikan sebagai Organisasi yang ditunjuk oleh PT Kilang Pertamina Internasional untuk melakukan suatu pekerjaan
shall	Menunjukkan bahwa

	mandatory		pernyataan itu wajib
should	Indicates a recommendation	*should*	Menunjukkan rekomendasi
VENDOR	Defined as the company selected to supply the equipment and service detailed in this specification.	*VENDOR*	Didefinisikan sebagai perusahaan yang dipilih untuk memasok peralatan dan *service* yang dirinci dalam spesifikasi ini.
SUB CONTRACTOR	Any person or persons, firm, partnership, corporation or combination thereof engaged by Contractor for supplying services to Contractor for the performance of services.	SUB KONTRAKTOR	Setiap orang atau beberapa orang, firma, kemitraan, korporasi atau kombinasi daripadanya yang dipekerjakan oleh Kontraktor untuk memasok servis kepada Kontraktor untuk pelaksanaan servis.
SUB VENDOR	Any supplier of equipment and support services for a particular piece of equipment/package to a VENDOR.	SUB *VENDOR*	Setiap pemasok peralatan dan servis penyangga untuk peralatan/ paket tertentu ke *VENDOR*.
May	The word ‘may’ is to be understood as indicating a possible course of action.	Mungkin	Kata 'mungkin' harus dipahami sebagai indikasi kemungkinan tindakan.

6. CODES AND STANDARDS

The following Codes, Standard and Specifications apply to this specification. When an edition date is not indicated for a code or standard or any update in codes and standards in this specification document, the latest edition and addendum in force at the time of purchase shall apply. Material & equipment shall be as a specification or an equal approved by OWNER.

6. *CODE* DAN STANDAR

Code, standar, dan spesifikasi berikut berlaku untuk spesifikasi ini. *Code* dan standar harus menggunakan edisi yang terbaru atau edisi yang berlaku pada saat pembelian. *Material* & peralatan harus sesuai spesifikasi atau setara dengan yang disetujui oleh PEMILIK.

6.1 International Electrotechnical Commission (IEC)

IEC 61508	Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related systems
IEC 61511	Functional Safety – Safety Instrumented Systems for the Process Industry Sector

6.2 Reference Documents

RP-ETS-HSE-DP-0008	Emergency Isolation Valve
RP-ETS-HSE-DP-0009	Pressure Relieving and Emergency Depressurizing System
RP-ETS-HSE-DP-0010	Emergency Shutdown System
RP-ETS-HSE-DP-0011	Active Fire Protection
RP-ETS-HSE-DP-0014	Fire & Gas Detection System
RP-ETS-INS-DP-0033	Alarm Management System Philosophy

7. GENERAL SIS REQUIREMENTS

7.1 All field devices installed outdoors shall meet the following environmental requirements:

Area Classification:	Refer to the hazardous area classification drawings
Ambient Temperature:	Maxmimum 37 °C
	Minimum 23 °C
Humidity:	Maxmimum 99%
	Minimum 83%

6.1 *International Electrotechnical Commission* (IEC)

IEC 61508	*Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related systems*
IEC 61511	*Functional Safety – Safety Instrumented Systems for the Process Industry Sector*

6.2 Dokumen Referensi

RP-ETS-HSE-DP-0008	*Emergency Isolation Valve*
RP-ETS-HSE-DP-0009	*Pressure Relieving and Emergency Depressurizing System*
RP-ETS-HSE-DP-0010	*Emergency Shutdown System*
RP-ETS-HSE-DP-0011	*Active Fire Protection*
RP-ETS-HSE-DP-0014	*Fire & Gas Detection System*
RP-ETS-INS-DP-0033	*Alarm Management System Philosophy*

7. PERSYARATAN UMUM SIS

7.1 Semua perangkat *field* (lapangan) yang dipasang di luar ruangan harus memenuhi persyaratan lingkungan berikut:

Klasifikasi *area*:	Lihat gambar klasifikasi *area hazardous*
Suhu *ambient*:	Maksimum 37 °C
	Minimum 23 °C
Kelembaban:	Maksimum 99%
	Minimum 83%

Field instruments are specified and installed in line with project specifications, detailed technical datasheets, and installation details.

7.2 The SIS devices located in a building shall meet the following requirements:

Ambient Temperature:	Maxmimum 37 °C
	Minimum 23 °C
Humidity:	Maxmimum 99%
	Minimum 83%
Grounding:	The ground wiring design for this project should include normal precautions that are aligned with industry best practices.
EMI/RFI:	The electrical design for this project should include the normal precautions against radio interferences.

SIS components located in a building will be in an indoor air conditioned “HVAC controlled” environment. The system control components shall be designed to operate in a temperature range of 15 Degree C to 35 Degrees C and a humidity range of 5% to 95% non-condensing. The system shall continue to operate after HVAC failure in temperatures up to 50 Degrees C for short periods of time (i.e., 60 minutes). Indoor cabinets shall comply with IP31 as a minimum.

As a minimum, all indoor SIS system cabinets are furnished with common trouble alarms to include high temperature alarms.

Mechanical, EMC conditions, Environmental limitations of Logic Solver systems installed in plant buildings are

Instrumen *field* (lapangan) ditetapkan dan dipasang sesuai dengan spesifikasi proyek, *data sheet* teknis *detail*, dan *detail* instalasi.

7.2 Perangkat SIS yang terletak di bangunan harus memenuhi persyaratan berikut:

Suhu *ambient*:	Maksimum 37 °C
	Minimum 23 °C
Kelembaban:	Maksimum 99%
	Minimum 83%
Grounding:	Desain *ground wiring* untuk proyek ini harus termasuk tindakan pencegahan normal yang selaras dengan praktik terbaik industri.
EMI/ RFI:	Desain kelistrikan untuk proyek ini harus mencakup tindakan pencegahan *normal* terhadap interferensi *radio.*

Komponen SIS yang terletak di sebuah bangunan akan berada di lingkungan “terkendali HVAC” ber-AC dalam ruangan (*indoor*). Komponen kontrol sistem harus didesain untuk beroperasi dalam kisaran suhu 15 °C hingga 35 °C dan kisaran kelembaban 5% hingga 95% tanpa kondensasi. Sistem harus terus tetap beroperasi setelah kegagalan HVAC pada suhu hingga 50 °C untuk periode waktu yang singkat (yaitu, 60 menit). *Indoor cabinet minimum* harus memenuhi IP31.

Minimum, semua *cabinet* sistem SIS dalam ruangan (*indoor)* dilengkapi dengan *common trouble alarm* termasuk *alarm* suhu tinggi.

Mekanis, kondisi EMC, keterbatasan lingkungan dari sistem *logic solver* yang dipasang di bangunan kilang ditentukan

specified in the safety manual of each system (section 3.13). Caution Notices shall be placed on SIS system cabinets against use of radio equipment.

7.3 Logic solvers for the SIS are having a claim limit SIL 3. The logic solver design is a Hardware Fault Tolerance (HFT) 0 as a minimum, redundant type with separated processor module. Safety manual requirements for installation, start-up/ restarting, normal operation, and testing shall be followed strictly.

7.4 Safety manual requirements for installation, start-up/ restarting, normal operation, and testing will be followed strictly.

7.5 Plant Operations

- Operation Modes (refer to each project specification the Project of the Directorate of Infrastructure Project (PT KPI).
- SIS is active in all operation modes. No additional SIFs are required for normal or abnormal modes for the plant as a whole or individual plant procedures (maintenance or calibration)
- SIFs that have startup bypasses are designated in each SIF
- SIFs with SIL 3 classification as per SIL assessment shall use 2oo3 voting logic for the initiating devices (transmitters) as a minimum unless otherwise recommended by the licensor.
- On/Off Valves to be applied for SIFs with SIL 3 classification shall be completed with smart Partial Stroke Test (PST) devices in the Actuator.

Sequential operational requirements will be specified either in procedures or control narratives where they apply.

dalam *manual* keselamatan setiap sistem (bagian 3.13). *Caution Notice* harus ditempatkan pada *cabinet* sistem SIS terhadap penggunaan peralatan *radio.*

7.3 *Logic solver* untuk SIS memiliki batas klaim SIL 3. Desain *logic solver* adalah *Hardware Fault Tolerance* (HFT) 0 *minimum*, tipe *redundant* dengan modul *processor* terpisah. Persyaratan *manual* keselamatan untuk instalasi, *start-up/ restart*, operasi *normal*, dan pengujian harus diikuti dengan ketat.

7.4 Persyaratan *manual* keselamatan untuk instalasi, *start-up/ restart*, operasi *normal*, dan pengujian akan diikuti secara ketat.

7.5 Operasi Kilang

- Mode operasi (merujuk pada spesifikasi proyek masing-masing Proyek di Direktorat Proyek Infrastruktur PT. KPI.International (PT KPI)
- SIS aktif di semua mode operasi. Tidak ada SIF tambahan yang diperlukan untuk mode *normal* atau *abnormal* untuk kilang secara keseluruhan atau prosedur kilang individu (pemeliharaan atau kalibrasi)
- Setiap SIF yang memiliki *bypass startup* ditunjuk di setiap SIF
- Setiap SIF yang berkualifikasi SIL 3 sesuai SIL assessment harus minimal menggunakan voting 2oo3 pada transmitternya, kecuali jika Licensor merekomendasikan yang lain.
- Setiap On/Off Valve yang digunakan pada SIF dengan klasifikasi SIL 3 harus dilengkapi dengan smart Partial Stroke Test (PST) pada aktuatornya.

Persyaratan operasional berurutan akan ditentukan baik dalam prosedur atau narasi kontrol di mana digunakan.

7.6 Hardware fault tolerance shall be as per IEC 61511, Table 5 (Programmable Electronic logic solvers) and Table 6 (field devices, final elements and non-programmable electric logic solvers) unless otherwise noted in the interlock list.

7.7 The SIS chassis has a key switch that can be placed in either Run, Program, Stop, or Remote. The below describes each mode:

RUN – Application program being executed with read only capability. This is the normal mode of operation for the logic solver. SIF testing is carried out in this mode.

PROGRAM – For program loading and checkout

STOP – Stops reading inputs, forces non-retentive analog and discrete outputs to '0' and stops the application program. Retentive outputs hold the last value seen by the logic solver.

REMOTE – Allows writes to program variables by the engineering station and external hosts. Modification of program logic is not allowed.

To prevent unauthorized use, the key switch shall be removed with the position in RUN mode.

7.6 Toleransi kesalahan perangkat keras harus sesuai dengan IEC 61511, Tabel 5 (*Logic solver* elektronik yang dapat diprogram) dan Tabel 6 (perangkat *field*, elemen akhir dan non-*logic solver* listrik yang dapat diprogram) kecuali dinyatakan lain dalam daftar *interlock.*

7.7 SIS *chassis* memiliki *key switch* yang dapat ditempatkan di jalankan (*run*), *program*, *stop*, atau *remote*. Di bawah ini menjelaskan setiap mode:

RUN – Program aplikasi dijalankan dengan kemampuan hanya baca. Ini adalah mode operasi *normal* untuk *logic solver*. Pengujian SIF dilakukan dalam mode ini.

PROGRAM – Untuk *loading* dan *checkout program*

STOP – Menghentikan pembacaan *input*, memaksa *output analog* dan diskrit non-retentif ke '0' serta menghentikan (*stop*) *program* aplikasi. *Output* retentif menyimpan nilai terakhir yang dilihat oleh *logic solver*.

REMOTE – Memungkinkan penulisan ke variabel *program* oleh *engineering station* dan *host* eksternal. Modifikasi *program logic* tidak diperbolehkan.

Untuk mencegah penggunaan yang tidak dikehendaki, *key switch* harus dilepas dengan posisi dalam mode *RUN*.

7.8 SIS interface

7.8 SIS *Interface*

INTERFACE	PARAMETERS	COMMUNICATION PHYSICAL/ PROTOCAL	REDUNDANT
BPCS	Resets / Bypasses / Loop Control Action (MANUAL MODE)	Ethernet / Modbus TCP/IP	YES
BPCS HMI	Indication Only	Ethernet / Modbus TCP/IP	YES
Logic Solver Engineering/Maintenance Console	Configuration Parameters and System Settings	Ethernet / Internal Communications	YES

7.9 Common cause failures shall be minimized to the greatest extent possible. The following shall be actively considered in the design:

- Using diversity for redundancy where feasible.
- Providing redundant taps for the pressure transmitters.
- Providing separate lines for the redundant vent valves.
- Segregating BPCS and SIS to the maximum extent.
- Independent air supply regulators complete with isolation valves for the SIF valves.
- Independent power supply circuits for redundant SIF devices.
- Addressing human factors with regard to configuration, calibration, testing by different personnel.
- Development, checking and approval of application software for BPCS and SIS by different personnel.
- Segregation of SIS I/O's for redundant field devices shall be observed i.e.

7.9 Penyebab umum kegagalan harus diusahakan seminimal mungkin. Berikut ini harus secara aktif dipertimbangkan dalam desain:

- Menggunakan keragaman untuk *redundant* jika memungkinkan.
- Menyediakan *redundant tap* untuk *transmitter* tekanan.
- Menyediakan saluran terpisah untuk *redundant vent valve.*
- Memisahkan BPCS dan SIS semaksimal mungkin.
- Regulator suplai udara independen lengkap dengan *isolation valve* untuk *valve* SIF.
- *Power supply circuit* independen untuk perangkat *redundant* SIF.
- Mengatasi faktor manusia sehubungan dengan konfigurasi, kalibrasi, pengujian oleh personel yang berbeda.
- Pengembangan, pemeriksaan dan persetujuan perangkat lunak aplikasi untuk BPCS dan SIS oleh personel yang berbeda.
- Pemisahan I/ O SIS untuk perangkat *redundant field* harus diperhatikan yaitu

redundant devices shall be allocated to separate I/O cards to avoid common mode failures leading to plant shutdowns.

perangkat *redundant* harus dialokasikan ke *card* I/ O terpisah untuk menghindari kegagalan mode umum yang mengarah ke *plant shutdown.*

Specific designs to prevent identified common environmental causes include:

Desain khusus untuk mencegah penyebab umum kegagalan yang teridentifikasi meliputi:

No	Identified Common Cause Failure (Kegagalan Penyebab Umum yang Diidentifikasi)	Design Requirements (Persyaratan Desain)
1	Electric Power Failure Kegagalan *power* listrik	Redundant power supply (UPS and essential power). *Redundant power supply* (UPS dan *essential power*).
2	PLC Malfunction/failure Kegagalan/ kerusakan PLC	1. The PLC shall be redundant with a separated processor module. 2. For common faults caused external to PLC, (a) The routing of redundant power supply cables and redundant signal cables shall be separate, (b) the PLC surroundings shall have vibrations within allowable level. 1. PLC harus memiliki *redundant* dengan modul *processor* terpisah 2. Untuk gangguan umum yang disebabkan eksternal ke PLC, (a) *Routing* kabel *power supply* dari *redundant* PLC dan kabel sinyal *redundant* harus terpisah, (b) PLC yang disekitarnya harus memiliki vibrasi di *level* yang diperbolehkan.
3	Fire at Cable Room *Fire* pada *cable room*	All wire and cable shall be fire retarding with self-extinguishing, non-propagating characteristics and shall not release harmful quantities of toxic gasses or dense smoke. Semua *wire* dan kabel harus tahan api dengan *self-extinguishing,* karakteristik *non-propagating* dan harus tidak boleh melepaskan gas racun atau asap *dense* dalam jumlah yang membahayakan.

No	Identified Common Cause Failure (Kegagalan Penyebab Umum yang Diidentifikasi)	Design Requirements (Persyaratan Desain)
4	Flooding of Cable room *Flooding* (Banjir) dari *cable room*	Drainage shall be provided. Saluran *drain* harus disediakan
5	High Temperature and Humidity Suhu dan kelembaban tinggi	Air Conditioned Control Room and proper installation of sun-sheds. *Air Conditioned Control Room* dan instalasi *sun-shed* yang baik.

8. GENERAL SIF REQUIREMENTS

8.1 Unless otherwise indicated, all the SIFs are operating in a low demand mode of operation. Low demand is defined as the condition that two or more proof tests will be performed before a demand could be expected.

8.2 The SIS standards allow for field devices to be either certified by a qualified third party for use in SIS e.g. TUV certified or for them to be proven-in-use.

IEC 61511 Clause 11.5.2.1 states that “components and subsystems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with 11.4 and 11.5.3 to 11.5.6, as appropriate.”

Where SIL certified equipment is available, certified field devices should be used.

All SIF components shall be selected suitable for the stated application taking due consideration for process compatibility, technology and response

8. PERSYARATAN UMUM SIF

8.1 Kecuali dinyatakan lain, semua SIF beroperasi dalam mode operasi permintaan rendah. Permintaan rendah didefinisikan sebagai kondisi bahwa dua atau lebih uji pembuktian akan dilakukan sebelum permintaan pengaktifan SIF.

8.2 Standar SIS memungkinkan perangkat *field* (lapangan) disertifikasi oleh pihak ketiga yang memenuhi syarat untuk digunakan di SIS, misalnya bersertifikat TUV atau untuk yang terbukti dapat digunakan.

IEC 61511 *Clause* 11.5.2.1 menyatakan bahwa “komponen dan subsistem yang dipilih untuk digunakan sebagai bagian dari sistem instrumentasi keselamatan untuk aplikasi SIL 1 hingga SIL 3 harus sesuai dengan IEC 61508-2 dan IEC 61508-3, jika sesuai, atau harus sesuai dengan 11.4 dan 11.5.3 hingga 11.5.6, sebagaimana mestinya.”

Jika peralatan bersertifikat SIL tersedia, perangkat *field* bersertifikat harus digunakan.

Semua komponen SIF harus dipilih yang sesuai untuk aplikasi yang disebutkan dengan mempertimbangkan kompatibilitas proses, teknologi, dan

time requirements.

8.3 Spurious trip rate (STR) for any SIF should be better than 10 years.

8.4 The total response time for all devices in a SIF including the application software logic processing in the logic solver shall be less process safety time to prevent the hazard. As a guideline, the SIF response time should be one half the process safety time (PST).

8.5 Process safety time is defined as the time elapsed between detection of the hazard and when the consequence of the hazard occurs. Process Safety Times and Interlock Response times are listed in the SIF Specific Section (Interlock List).

8.6 Unless stated separately for a specific SIF in the SIF list, the protection principle for any safety instrumented function should be “de-energize to trip” (DTT). If the protection principle for a specific SIF is “energize to action” or “energize to trip” (ETT), electrical circuits shall apply a method to ensure circuit and power integrity, such as an end-of-the-line monitor where a pilot current is continuously monitored and where the pilot current is small enough to avoid affecting the proper operation of the circuit.

8.7 All sensors associated with a SIF shall be transmitters and no switches shall be used.

8.8 Transmitters shall be checked and configured for line monitoring and shall initiate trip state on bad input/ faults and also be announced in the BPCS HMI.

8.9 Trip alarms are generated in the SIS. Pre-trip alarms that the operator may respond to in order to keep the process from

persyaratan waktu respons.

8.3 *Spurious Trip Rate* (STR) untuk setiap SIF harus lebih baik dari 10 tahun.

8.4 Total waktu respons untuk semua perangkat dalam SIF termasuk pemrosesan *software logic* aplikasi dalam *logic solver* harus lebih sedikit dari *Process Safety Time* (PST) untuk mencegah bahaya. Sebagai pedoman, waktu respons SIF harus setengah dari *Process Safety Time* (PST).

8.5 *Process Safety Time* (PST) didefinisikan sebagai waktu yang berlalu antara deteksi bahaya dan saat konsekuensi bahaya terjadi. *Process Safety Time* (PST) dan *Interlock Response Time* tercantum dalam bagian spesifik SIF (Daftar *Interlock*).

8.6 Kecuali dinyatakan secara terpisah untuk SIF spesifik dalam daftar SIF, prinsip proteksi untuk setiap fungsi yang dilengkapi instrumen keselamatan harus “*de-energize to trip*” (DTT). Jika prinsip proteksi untuk SIF spesifik adalah "*energize to action*" atau "*energize to trip*" (ETT), *circuit* listrik harus menerapkan metode untuk memastikan bahwa *circuit* dan integritas daya, seperti *monitor end-of-the-line* yang me*monitor* arus *pilot* terus menerus dan arus *pilot* cukup kecil agar tidak mempengaruhi operasi *circuit* yang sudah berjalan baik.

8.7 Semua *sensor* yang terkait dengan SIF harus berupa *transmitter* dan tidak boleh ada *switch* yang digunakan.

8.8 *Transmitter* harus diperiksa dan dikonfigurasi untuk *line monitoring* dan harus menginisiasikan status *trip* akibat *bad input/* kegagalan dan juga menampilkan status *trip* tersebut ke dalam BPCS HMI.

8.9 *Trip alarm* dihasilkan di SIS. *Pre-trip alarm* yang dapat segera direspons oleh *operator* agar proses tidak *shutting down*

shutting down the systems should be assigned the highest priority. Pre-trip alarms are generated in the BPCS. The alarms active in the SIS or BPCS will be displayed on the BPCS HMI process graphics and alarm page.

8.10 Fail Safe Positions for the SIF components

- Logic solvers shall be programmed to detect over-range and under-range failures of analog SIF components. The Logic Solver shall be configured as follows:
  - Under-range – instrument signal less than 3.75 mA
  - Over-range – instrument signal greater than 21 mA
- Analog SIF components shall be configured to enable the logic solver to detect a failure of the transmitter by failing the signal to the safe direction. Transmitters shall be configured to fail in the same direction of the trip setting per the following settings:
  - Low trip = Under-range
  - High trip = Over-range
- All the final elements shall go to their fail safe state on loss of energy as identified in the P&ID.
  - Isolation valve = Close
  - Vent valve = Open
  - Motor = Stop (open contacts)
- Logic Solver output is de-energized to bring the final element to its safe state.
- Logic Solver input is de-energized to initiate the trip.
- The fail position for a transmitter will fail in the direction of the alarm. Example: if a critical alarm is a high alarm, then the

sistem harus diberi prioritas tertinggi. *Pre-trip alarm* dihasilkan di BPCS. *Alarm* yang aktif di SIS atau BPCS akan ditampilkan pada grafik proses HMI BPCS dan halaman *alarm.*

8.10 Posisi *fail-safe* untuk komponen SIF

- *Logic solver* harus diprogram untuk mendeteksi kegagalan *over-range* dan *under-range* komponen SIF *analog. Logic solver* harus dikonfigurasi sebagai berikut:
  - *Under-range* – sinyal instrumen kurang dari 3.75 mA
  - *Over-range* – sinyal instrumen lebih besar dari 21 mA
- Komponen SIF *analog* harus dikonfigurasi untuk memungkinkan *logic solver* mendeteksi kegagalan *transmitter* dengan melewatkan sinyal ke arah yang aman. *Transmitter* harus dikonfigurasi untuk gagal dalam arah yang sama dari pengaturan *trip* dengan pengaturan berikut:
  - *Trip* rendah = *Under-range*
  - *Trip* tinggi = *Over-range*
- Semua elemen akhir harus menjadi ke *state fail-safe* saat kehilangan energi seperti yang diidentifikasi dalam P&ID.
  - *Isolation valve = Close*
  - *Vent valve = Open*
  - *Motor = Stop (open contact)*
- *Logic solver output* di *de-energized* untuk merubah elemen terakhir ke status amannya.
- *Logic solver input* di *de-energized* untuk memulai *trip.*
- Posisi gagal untuk *transmitter* akan gagal ke arah *alarm*. Contoh: jika alarm kritikal adalah *high alarm*, maka

transmitter needs to fail high so that the failure generates the alarm. On bad status detection, the SIS will treat this signal as a vote to trip.

transmitter harus *fail high* sehingga kegagalan menghasilkan *alarm*. Pada deteksi status *bad*, SIS akan memperlakukan sinyal ini sebagai perintah untuk *trip.*

8.11 Automatic SIS response to detection of detected dangerous faults:

- Unless stated separately for a specific SIF in the SIF list, the SIS shall treat a detected fault in a SIF with 1oo1 architecture as a vote to trip, place the process in a safe state, and notify the operator that the trip is based on a transmitter fault.

8.11 Respons SIS otomatis untuk mendeteksi kesalahan berbahaya yang terdeteksi:

- Daftar SIF, SIS akan memperlakukan kesalahan yang terdeteksi dalam SIF dengan arsitektur 1oo1 sebagai *vote to trip*, menempatkan proses dalam keadaan aman, dan memberitahu *operator* bahwa *trip* didasarkan pada kesalahan *transmitter*.

Table 8.11.1: 1-out-of-2 Voting

Voting Condition	Transmitter Status		Shutdown Status
2 Healthy Sensors	OK	OK	OK
	OK	SHUTDOWN	SHUTDOWN
	SHUTDOWN	SHUTDOWN	SHUTDOWN
Bypass Conditions 1oo1 Voting	BYPASS	OK	OK
	BYPASS	SHUTDOWN	SHUTDOWN
	BYPASS	REJECT**	OK
Bad PV	BAD PV	OK	SHUTDOWN

* Determination of whether BAD PV shall be alarmed only or is a vote to trip shall be defined by the process engineer and documented in the SRS.

** REJECT – The SIS logic solver will automatically reject an attempt to activate a BYPASS of the last sensor.

Table 8.11.2: 2-out-of-3 Voting

Voting Condition	Transmitter Status			Shutdown Status
3 Healthy Sensors	OK	OK	SHUTDOWN	OK
	OK	SHUTDOWN	SHUTDOWN	SHUTDOWN
	SHUTDOWN	SHUTDOWN	SHUTDOWN	SHUTDOWN
1 Bad PV 1oo2 Voting	BAD PV	OK	OK	OK
	BAD PV	SHUTDOWN	OK	SHUTDOWN
	BAD PV	SHUTDOWN	SHUTDOWN	SHUTDOWN
2 Bad PV 1oo1 Voting	BAD PV	BAD PV	OK	SHUTDOWN
	BAD PV	BAD PV	SHUTDOWN	SHUTDOWN
3 Bad PV	BAD PV	BAD PV	BAD PV	SHUTDOWN

8.12 Undetected dangerous failure modes include:

8.12 Mode kegagalan berbahaya yang tidak terdeteksi meliputi:

No	Equipment (Peralatan)	Failure Mode (Mode Kegagalan)
1	Sensor *Sensor*	Drift away from setpoint, fail mid range, bad calibration, etc. *Drift away* dari *setpoint,* gagal *mid range*, kalibrasi buruk, dll
2	SIS I/O SIS I/ O	Non-responsive (channel failure, etc.) Non-responsif (kegagalan saluran, dll)
3	SIS CPU SIS CPU	Erratic operation due to address failure, CPU locked, etc. Operasi tidak menentu karena kegagalan alamat, CPU terkunci, dll
4	Positioner *Positioner*	High packing friction not being suitable, electronic issues, etc. *Packing friction* yang tinggi tidak sesuai, masalah elektronik, dll
5	Actuator *Actuator*	Loss of instrument air, jammed shaft, leaking seat, etc. Kehilangan *instrument air, jammed shaft, leaking seat,* dll
6	Solenoid *Solenoid*	Coil burnout, contact frozen, etc. *Coil burnout, contact frozen,* dll

a. If the SIF final elements do not reach their safe states after activation, operator shall take appropriate actions by other means such as:

   1. Informing Control Engineer to bring SIF to safe state by manual isolation as required.

   2. Control by BPCS to bring the plant to a safe state.

a. Jika elemen akhir SIF tidak mencapai status amannya setelah aktivasi, *operator* harus mengambil tindakan yang sesuai dengan cara lain seperti:

   1. Menginformasikan *Control Engineer* untuk membawa SIF ke keadaan aman dengan isolasi *manual* sesuai kebutuhan.

   2. Dikontrol oleh BPCS untuk membawa kilang ke kondisi aman.

8.13 Resets

Following a trip, SIFs can be reset manually by the operator or by a supervisor. SIFs with resets will remain tripped even after the trip condition has cleared until an operator instructs the SIS to reset by selecting a soft reset button on the SIS graphics. Solenoids having manual reset switches in the field will require operator action in the field to reset the latch after BPCS reset.

8.14 Bypasses:

Maintenance bypasses:

Hardware Maintenance Override Switches (MOS, provided in SIS) are provided to bypass the trip initiators on SIS transmitters except for 2 out of 3 voting transmitters; the process alarm is not bypassed.

The maintenance bypass hardware-switches are operated by maintenance engineers with a key switch.

When a transmitter is bypassed, an alarm is generated and reflected in the SIS bypass graphic. The alarm shall be reactivated every 4 hours until returned to normal. Operator will initiate the bypass (Bypass ON) and clear it (Bypass-OFF) from the same graphic.

Administrative controls shall be conducted according to the operation guidelines. All field devices shall degrade due to a fault from 2oo3 to 1oo2 if applicable.

In case of loss of communication between SIS and DCS, the maintenance bypass softswitches keep last state and all active SIS bypasses remain. Maintenance or Engineering will have authorization to clear each bypass directly on the SIS if communications is lost for an extended

8.13 Pengaturan Ulang

Setelah *trip*, SIF dapat diatur ulang secara *manual* oleh *operator* atau *supervisor*. SIF dengan pengaturan ulang akan tetap *trip* bahkan setelah kondisi *trip* telah teratasi hingga *operator* menginstruksikan SIS untuk pengaturan ulang dengan memilih *soft reset button* pada grafik SIS. *Solenoid* yang memiliki *manual reset switch* di *field* (lapangan) akan membutuhkan tindakan *operator* di *field* (lapangan) untuk pengaturan ulang *latch* setelah pengaturan ulang BPCS.

8.14 *Bypass*:

Bypass untuk pemeliharaan:

Perangkat *Maintenance Override Switches* (MOS, disediakan dalam SIS) disediakan untuk mem-*bypass* penyebab *trip* pada *transmitter* SIS kecuali untuk 2 dari 3 *transmitter voting*; *alarm* proses tidak di *bypass*.

Maintenance bypass hardware-switch dioperasikan oleh *engineer* pemeliharaan dengan *key switch.*

Ketika *transmitter* di-*bypass*, *alarm* di-*generated* dan direfleksikan dalam grafik *bypass* SIS. *Alarm* harus diaktifkan kembali setiap 4 jam sampai kembali *normal. Operator* akan memulai *bypass (Bypass ON)* dan menghapusnya *(Bypass-OFF)* dari grafik yang sama.

Kontrol administratif harus dilakukan sesuai pedoman operasi. Semua perangkat *field* (lapangan) akan dimatikan karena kesalahan dari 2oo3 ke 1oo2 jika berlaku.

Dalam kasus kehilangan komunikasi antara SIS dan DCS, *maintenance bypass softswitch* mempertahankan status terakhir dan semua *bypass* SIS yang aktif tetap ada. Pemeliharaan atau *Engineering* akan mendapatkan otorisasi untuk menghapus setiap *bypass* secara

	period.	langsung pada SIS jika komunikasi terputus untuk waktu yang lama.
	Refer to the Interlock List for the applicable maintenance bypass switches for each SIF.	Merujuk daftar *interlock* untuk *maintenance bypass switch* yang berlaku untuk setiap SIF.
	Start-up bypasses:	*Start-up bypass:*
	Hardware start-up bypasses (Process Override Switches, POS) are provided as part of the interlock (in SIS) for those initiators which need to be bypassed during start-up for operational reasons.	*Hardware start-up bypass* (*Process Override Switches, POS*) disediakan sebagai bagian dari *interlock* (dalam SIS) untuk *initiator/* penyebab yang perlu di *bypass* selama *start-up* untuk alasan operasional.
8.15	All SIF elements are powered from a UPS which will provide a minimum of 30 minutes backup for all the components of the SIFs in the event of power supply failure. Refer to 4.25 for additional requirements.	8.15 Semua elemen *SIF* diberi *power* dari UPS yang akan menyediakan *backup minimum* 30 menit untuk semua komponen SIF jika terjadi kegagalan catu daya. Lihat 4.25 untuk persyaratan tambahan.
8.16	Instrument air supply: Air receiver tanks are sized to provide instrument air supply to the final elements for a minimum of 30 minutes in the event of failure of instrument air compressors. Volume tanks are provided for valves as identified in the P&ID. The volume tanks are sized for two full stroke operations in the event of loss of air supply.	8.16 Suplai *instrument air*: *Air receiver tank* dengan ukuran yang telah ditentukan untuk menyediakan suplai *instrument air* ke elemen akhir selama *minimum* 30 menit jika terjadi kegagalan *instrument air compressor*. *Volume* tangki disediakan untuk semua *valve* seperti yang diidentifikasi dalam P&ID. *Volume* tangki diperhitungkan untuk dua langkah operasi penuh (t*wo full stroke operation*) jika terjadi kehilangan *air supply.*
8.17	Where transmitters are installed for BPCS and SIS for the same service shall be checked and generate deviation alarms.	8.17 Apabila *transmitter* dipasang untuk BPCS dan SIS untuk servis yang sama harus diperiksa dan di-*generate alarm* ketika ada deviasi.
8.18	Proof tests procedures have been provided to allow the system to be restored to its design functionality. Proof test coverage factor of 1 has been considered in the SIL verification calculations.	8.18 Prosedur *proof test* telah disediakan untuk memungkinkan sistem dikembalikan ke fungsionalitas desainnya. Faktor cakupan *proof test* 1 telah dipertimbangkan dalam perhitungan verifikasi SIL.
8.19	Proof test intervals: Consider turnaround time for the units in determining the proof test interval.	8.19 *Interval proof test*: Pertimbangkan waktu penyelesaian untuk *unit* dalam menentukan *interval proof test*.

Proof test interval for the Logic Solver of 4 years shall be the basis of standard of design (Based on a 4-year plant turnaround). The SIS logic solver should not exceed 8 years without a full proof test performed.

If the integrity (PFD avg) cannot be achieved with the above proof test interval and a reduced proof test interval is required, then consider providing online testing facility/ redundancy as required.

Interval *proof test* untuk *logic solver* 4 tahun harus menjadi dasar standar desain (Berdasarkan *turnaround* kilang 4 tahun). *Logic solver* SIS tidak boleh melebihi 8 tahun tanpa dilakukan *proof test* penuh.

Jika integritas (rata-rata PFD) tidak dapat dicapai dengan *interval proof test* di atas dan *interval proof test* yang dikurangi diperlukan, maka pertimbangkan untuk menyediakan fasilitas/ *redundant* pengujian *online* sebagaimana diperlukan.

8.20 The design of all SIF's is based on the Mean Time To Restore (MTTR) of 72 hours for all the SIF elements taking into consideration spare inventory and maintenance capability.

8.20 Desain semua SIF didasarkan pada *Mean Time To Restore* (MTTR) 72 jam untuk semua elemen SIF dengan mempertimbangkan persediaan cadangan dan kemampuan pemeliharaan.

8.21 There are no special requirements, beyond what is identified in the Project Specifications and listed below, for the SIS to survive or be operational for a given time due to a major event such as a fire or major damage to the facility.

- UPS backup shall be designed to provide a minimum 30-60 minutes of power.
- Diverse routing for redundant fiber optic communications for SIS.
- Power supply diversity to the SIS.

8.21 Tidak ada persyaratan khusus, di luar apa yang diidentifikasi dalam spesifikasi proyek dan tercantum di bawah ini, agar SIS dapat bertahan atau beroperasi untuk waktu tertentu karena peristiwa besar seperti kebakaran atau kerusakan besar pada fasilitas.

- *Backup* UPS harus didesain untuk menyediakan *power minimum* 30-60 menit.
- *Routing* yang beragam untuk komunikasi *redundant fiber optic* untuk SIS.
- Keragaman *power supply* ke SIS.

8.22 Instruments (sensors and final elements) that are not safety certified and form part of a SIF having a SIL 1 rating or higher are considered "Proven in Use".

The instrumentation used in the safety application are from an "Approved Manufacturer List / Approved Brand List" and are considered as "Proven in Use" based on their use in past projects and

8.22 Instrumen (*sensor* dan elemen akhir) yang tidak bersertifikat keselamatan dan merupakan bagian dari SIF yang memiliki *rating* SIL 1 atau lebih tinggi dianggap "Terbukti Digunakan".

Instrumentasi yang digunakan dalam aplikasi keselamatan berasal dari "*Approved Manufacturer List* / *Approved Brand List*" dan dianggap sebagai "Terbukti Digunakan" berdasarkan

formal review of the manufacturer's quality design, fabrication, and MOC practices.

penggunaannya dalam proyek sebelumnya dan *review formal* terhadap desain kualitas pembuat, fabrikasi, dan praktik MOC.

Through monitoring of previous projects, there are processes to verify vendors and their sub-suppliers. This includes lessons learned and supplier quality surveillance to determine the level of competence/rating for continuing to use a particular vendor.

Melalui *monitoring* proyek sebelumnya, ada proses untuk memverifikasi *vendor* dan sub-pemasoknya. Ini termasuk pembelajaran dan pengawasan kualitas pemasok untuk menentukan *level* kompetensi/ *rating* untuk terus menggunakan *vendor* tertentu.

The performance of the instruments shall be confirmed through periodic functional testing. Where the actual performance does not meet the design requirements, the failure shall be investigated and corrected.

Kinerja instrumen harus dikonfirmasi melalui pengujian fungsional berkala. Jika kinerja aktual tidak memenuhi persyaratan desain, kegagalan harus diselidiki dan diperbaiki.

To represent the closest approximation to true operating conditions from an industry database, OREDA data was employed for final elements such as valves. ISA data tables are also utilized for sensors/transmitters and other final elements.

Untuk mewakili perkiraan terdekat dengan kondisi operasi sebenarnya dari *database* industri, data OREDA digunakan untuk elemen akhir seperti *valve*. Tabel data ISA juga digunakan untuk *sensor/ transmitter* dan elemen akhir lainnya.

8.23 Alarm priorities and set points are defined in the Alarm Objective Analysis (TBD).

8.23 Prioritas alarm dan *set point* ditentukan dalam Analisis Objektif *Alarm* (TBD)

9. SPECIFIC SIF REQUIREMENTS

The specific performance requirements of each SIF design shall be found in the following locations.

9.1 Description of SIF and final element output actions - Found in the interlock listing under "Interlock_Description".

9.2 SIF definition of process safe state/ success criteria- Found in Interlock list under "process safe state".

9.3 Sources of demand.

9.4 Associated safeguards - Found in the interlock listing under "Existing Safeguards" Target SIL - Found in the

9. PERSYARATAN KHUSUS SIF

Persyaratan kinerja spesifik dari setiap desain SIF harus ditemukan di lokasi berikut.

9.1 Deskripsi SIF dan tindakan keluaran elemen akhir - Ditemukan dalam daftar *interlock* di bawah "*Interlock_Description*".

9.2 Definisi SIF tentang status aman proses/ kriteria keberhasilan- Ditemukan dalam daftar *interlock* di bawah "status aman proses".

9.3 Sumber permintaan.

9.4 *Safeguard* terkait – Ditemukan dalam daftar *interlock* di bawah "*Existing Safeguard*" Target SIL - Ditemukan dalam

interlock listing under “SIR Target SIL”.

9.5 Process safety time and overall SIF reaction time - Found in the interlock listing under “Process Safety Time (PST)” and “SIF Response Time (sec)”.

9.6 Final element leakage - Found in interlock listing under “PD Seat_Leak”.

9.7 HMI (soft) and field (manual) Resets - Found in interlock listing under “DCS Reset HS” and “Manual Reset”.

9.8 Automatic start-up bypass - Found in interlock listing under “Startup bypass”.

9.9 Special SIF design requirements.

- Potentially dangerous SIF output combinations
- Unique environmental conditions due to process-side application or local placement beside equipment (i.e. vibration, heat, etc.)
- Compensating measures when testing
- Additional survivability requirements
- Other known, exceptional requirements.

10. PES HARDWARE COMMUNICATION AND GENERAL FAILURES

10.1 TBD based on SIS vendor selection.

daftar *interlock* di bawah "SIR *Target* SIL".

9.5 *Process Safety Time* (PST) dan waktu reaksi SIF keseluruhan - Ditemukan dalam daftar *interlock* di bawah “*Process Safety Time* (PST)” “SIF *Response Time* (detik)”.

9.6 Kebocoran elemen akhir - Ditemukan dalam daftar *interlock* di bawah “PD *Seat_Leak*”.

9.7 Pengaturan ulang HMI (*soft*) dan *field (manual)* - Ditemukan dalam daftar *interlock* di bawah "DCS *Reset* HS" dan “*Manual Reset”*.

9.8 *Bypass start-up* otomatis - Ditemukan dalam daftar *interlock* di bawah “*Startup bypass”.*

9.9 Persyaratan khusus desain SIF

- Potensi kombinasi keluaran SIF yang berbahaya
- Kondisi lingkungan yang unik karena aplikasi sisi proses atau penempatan lokal di samping peralatan (yaitu getaran, panas, dll)
- Langkah-langkah kompensasi saat pengujian
- Persyaratan *survivability* tambahan
- Persyaratan luar biasa lainnya yang diketahui

10. KOMUNIKASI PES *HARDWARE* DAN KEGAGALAN UMUM

10.1 Akan didiskusikan lebih lanjut dengan *vendor* SIS yang terpilih.