# DESIGN PHILOSOPHY



## EMERGENCY SHUTDOWN SYSTEM

## ENGINEERING TECHNICAL STANDARDS & PROCEDURES

## PT KILANG PERTAMINA INTERNASIONAL

## DIREKTORAT PROYEK INFRASTRUKTUR

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| 01 | Issued for Record | 04/2022 | LC/RD/SFA | VS | HY | RMD | BAP |
| 00 | Issued for Record | 11/2018 | KZH/TS | VS | DC | PH | IMS |
| Rev. | Description | Date | Prepared by | Checked by | Verified by | Validated by | Approved By |

## REVISION HISTORY
*RIWAYAT REVISI*

| Page / Section<br>*Hal. / Bagian* | Date<br>*Tanggal* | Description<br>*Deskripsi* | Revised by<br>*Direvisi oleh* |
|---|---|---|---|
| 2 – 21 | 04/2022 | Add: content translation in Bahasa<br>*Penambahan: penerjemahan konten dalam Bahasa* | LC/RD/SFA |
| 1 – 21 | 04/2022 | Change: format and document numbering related to restructuring of Pertamina<br>*Perubahan: format dan penomoran dokumen terkait restrukturisasi Pertamina* | LC/RD/SFA |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

*DAFTAR ISI*

## 1. INTRODUCTION

1.1 General

The function of the ESD is to provide an independent protection system (SIS) to place and maintain the plant processes in a safe state when the Basic Process Control System (BPCS) is unable to keep them within predetermined safe limits or in the case of fire or gas alarm or operator intervention (ESD Push Button). The required Safety Instrumented Functions (SIFs) comprising the ESD System shall be defined based on the hazard identification studies and associated risk assessment.

The ESD performs its Safety Instrumented Function (SIF) by sensing the abnormal conditions and actuating final elements to bring the process to a safe state. For example, safe state may be achieved by isolating sections of the plant via isolation valves, stopping rotating equipment machinery such as compressors and pumps and blowing down sections of plant. The ESD may provide signals to the BPCS which, though not required for ESD, may provide information or initiate actions and as such, the ESD and the BPCS systems should be aligned (compatible) to allow such communication where it is required.

In general application the ESD system shall initiate automatically, and/or enable the operators to perform, the quick shutdown of an equipment or unit or whole facility in an emergency condition to protect against explosion or fire hazards escalation which could result from accidental interruption to various services or operations (utility supply loss, human error, etc.), or loss of containment due to the loss of the

## 1. PENGANTAR

1.1 Umum

Salah satu tujuan ESD adalah menyediakan *independent protection system* (SIS) untuk menempatkan dan memelihara proses instalasi dalam keadaan aman ketika *Basic Process Control System* (BPCS) tidak dapat menjaganya dalam batas aman yang telah ditentukan atau jika terjadi kebakaran atau *alarm* gas atau intervensi *operator* (ESD *Push Button*). *Safety Instrumented Function* (SIF) yang diperlukan terdiri dari Sistem ESD yang harus ditentukan berdasarkan studi identifikasi bahaya dan penilaian risiko terkait.

ESD menjalankan *Safety Instrumented Function* (SIF) dengan mendeteksi kondisi *abnormal* dan menggerakkan *final element* untuk membawa proses ke keadaan aman. Misalnya, keadaan aman dapat dicapai dengan mengisolasi bagian *plant* melalui *isolation valve*, menghentikan mesin peralatan *rotating* seperti *compressor* dan pompa, dan *blowing down* bagian *plant*. ESD dapat memberikan sinyal ke BPCS yang, meskipun tidak diwajibkan untuk ESD, dapat memberikan informasi atau memulai tindakan, ESD dan sistem BPCS harus diselaraskan (kompatibel) untuk memungkinkan komunikasi jika diperlukan.

Dalam aplikasinya, sistem ESD harus dimulai secara otomatis, dan/ atau memungkinkan *operator* untuk melakukan *quick shutdown* pada peralatan atau *unit* atau seluruh fasilitas dalam kondisi darurat untuk melindungi dari ledakan atau eskalasi bahaya kebakaran yang dapat diakibatkan dari gangguan yang tidak disengaja ke berbagai layanan atau operasi (kehilangan pasokan utilitas,

structural integrity of the pipelines or critical equipment (corrosion, external impact, process run-out, etc.).

kesalahan manusia, dll), atau hilangnya *containment* karena hilangnya integritas struktural dari jaringan pipa atau peralatan penting lainnya (korosi, dampak eksternal, *process run-out*, dll).

1.2 Purpose

The purpose of this document is to provide information regarding the Emergency Shutdown System philosophy and design requirements for the Project of PT Kilang Pertamina Internasional (PT KPI).

1.2 Tujuan

Tujuan dari dokumen ini adalah untuk memberikan informasi mengenai filosofi *Emergency Shutdown System* dan persyaratan desain untuk Proyek dari PT Kilang Pertamina Internasional (PT KPI).

## 2. SCOPE

2.1 This Standard contains the minimum mandatory requirements for the design of ESD, including spacing requirements for ESDs and safe-location actuating buttons, for PT KPI Projects.

## 2. LINGKUP

2.1 Standar ini berisi persyaratan wajib *minimum* untuk desain ESD, termasuk persyaratan jarak untuk ESD dan tombol penggerak di lokasi aman, untuk Proyek PT KPI.

## 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 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.

## 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 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. ABBREVIATIONS

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

| | |
|---|---|
| API | American Petroleum Institute |
| BPCS | Basic Process Control System |

## 4. SINGKATAN

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

| | |
|---|---|
| API | *American Petroleum Institute* |
| BPCS | *Basic Process Control System* |

| | |
|---|---|
| CCF | Common Cause Failure |
| EDP | Emergency Depressuring |
| ESD | Emergency Shutdown |
| ETSP | Engineering Technical Standards & Procedures |
| FAR | Field Auxiliary Room |
| F&G | Fire and Gas |
| HAZOP | Hazard and Operability |
| HMI | Human Machine Interface |
| NFPA | National Fire Protection Association |
| RU | Refinery Unit |
| SIL | Safety Integrity Level |
| UPS | Uninterruptible Power Supply |

| | |
|---|---|
| CCF | *Common Cause Failure* |
| EDP | *Emergency Depressuring* |
| ESD | *Emergency Shutdown* |
| ETSP | *Engineering Technical Standards & Procedures* |
| FAR | *Field Auxiliary Room* |
| F&G | *Fire and Gas* |
| HAZOP | *Hazard and Operability* |
| HMI | *Human Machine Interface* |
| NFPA | *National Fire Protection Association* |
| RU | *Refinery Unit* |
| SIL | *Safety Integrity Level* |
| UPS | *Uninterruptible Power Supply* |

## 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 mandatory. |
| should | Indicates a recommendation. |

## 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 di PT Kilang Pertamina Internasional untuk melakukan suatu pekerjaan. |
| *shall* | Menunjukkan bahwa pernyataan itu wajib. |
| *should* | Menunjukkan rekomendasi. |

| | | | |
|---|---|---|---|
| Emergency Shutdown (ESD) System | Is a system of automatic safety devices that, when activated either automatically or by operator, initiates equipment shutdown. The ESD system can shut down a single piece of process equipment, an entire process unit, or an entire facility. | *Emergency Shutdown* (ESD) *System* | Adalah seperangkat sistem keamanan otomatis yang menginisiasi *shutdown* peralatan ketika diaktifkan baik secara otomatis atau oleh *operator*. Sistem ESD dapat membuat *shutdown* satu bagian peralatan proses, seluruh *unit* proses, atau seluruh fasilitas. |
| Local Actuating Button | A button mounted on or adjacent to the valve or equipment that, when pushed or pulled, initiates the closing of that valve or stopping of that equipment. A local ESD actuating button is a button mounted adjacent to a plant, equipment train, or process unit that, when pushed or pulled, initiates the ESD system. See Section 9 for guard and labeling requirements. | *Local Actuating Button* | Sebuah tombol yang dipasang atau berdekatan dengan *valve* atau peralatan yang, ketika didorong atau ditarik, menginisiasi penutupan *valve* atau menghentikan peralatan itu. *Local* ESD *actuating button* adalah tombol yang dipasang di dekat *plant*, rangkaian peralatan, atau *unit* proses yang akan menginisiasi sistem ESD saat didorong atau ditarik. Lihat Bagian 9 untuk persyaratan pelindung dan pelabelan. |
| Remote Actuating Button | An actuating button located a considerable distance from the valve or equipment being activated, usually located in a control room. A remote ESD actuating button | *Remote Actuating Button* | Tombol penggerak yang terletak cukup jauh dari *valve* atau peralatan yang sedang diaktifkan, biasanya terletak di *control room*. *Remote* ESD *actuating button* menginisiasi |

| | | | |
|---|---|---|---|
| | initiates the ESD system associated with a plant, equipment train, or process unit. | | sistem ESD yang terkait dengan *plant*, rangkaian peralatan, atau *unit* proses. |
| Safe-Location Actuating Button | An actuating button is located at grade and at least 15 m horizontally from any fire-hazardous equipment to isolate process equipment from a relatively safe location. | *Safe-Location Actuating Button* | Tombol penggerak yang terletak di *grade* dan setidaknya berjarak 15 m secara *horizontal* dari peralatan dengan bahaya kebakaran, berfungsi untuk mematikan dan/ atau mengisolasi peralatan proses dari lokasi yang relatif aman. |

## 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.

6.1 Reference Documents

| | |
|---|---|
| API RP 554 | Process Instrumentation and Control |
| API STD 2510 | Design and Construction of LPG Installations |
| IEC 61511 | Functional safety – Safety Instrumented Systems for the Process Industry Sector |

## 6. KODE DAN STANDAR

Kode, standar, dan spesifikasi berikut berlaku untuk spesifikasi ini. Kode 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 Dokumen Referensi

| | |
|---|---|
| API RP 554 | *Process Instrumentation and Control* |
| API STD 2510 | *Design and Construction of* LPG *Installations* |
| IEC 61511 | *Functional safety – Safety Instrumented Systems for the Process Industry Sector* |

| | | | |
|---|---|---|---|
| NFPA 85 | Boiler and Combustion Systems Hazards | NFPA 85 | *Boiler and Combustion Systems Hazards* |
| NFPA 86 | Ovens and Furnaces | NFPA 86 | *Ovens and Furnaces* |

## 7. DESIGN CONSIDERATIONS

### 7.1 General Design Requirements

The following criteria shall be considered for the functionality and configuration of the ESD System:

a) The ESD system shall be fully autonomous. This means that the ESD system must be independent and separated from any part/component of the BPCS to prevent/avoid Common Cause Failures (CCF) which may result in ESD unavailability under hazardous conditions caused by the BPCS component.

b) To assure the maximum reliability of signal transmission and data exchange the ESD System shall be capable of interfacing to a BPCS, Peer-to-Peer deterministic communications to other ESD nodes or subsystems within each Field Auxiliary Room (FAR). This shall not compromise the full independence of the ESD System in terms of its instrumentation or actions.

c) The ESD system shall communicate with the BPCS, which shall provide the primary operator interface. The ESD system-BPCS communication link and BPCS based Human Machine Interface (HMI) shall permit the operators to:

- View the current values and states of all ESD system inputs.

## 7. PERTIMBANGAN DESAIN

### 7.1 Persyaratan Desain Umum

Kriteria berikut harus dipertimbangkan untuk fungsionalitas dan konfigurasi Sistem ESD:

a) Sistem ESD harus sepenuhnya otonom. Ini berarti bahwa sistem ESD harus independen dan terpisah dari setiap bagian/ komponen BPCS untuk mencegah/ menghindari *Common Cause Failures* (CCF) yang dapat mengakibatkan ketidaktersediaan ESD dalam kondisi berbahaya yang disebabkan oleh komponen BPCS.

b) Untuk memastikan keandalan maksimum transmisi sinyal dan pertukaran data, Sistem ESD harus mampu *interfacing* ke BPCS, komunikasi deterministik *Peer-to-Peer* ke *node* atau subsistem ESD lain dalam setiap *Field Auxiliary Room* (FAR). Ini tidak akan mengganggu independensi penuh Sistem ESD dalam hal instrumentasi atau tindakannya.

c) Sistem ESD harus berkomunikasi dengan BPCS, yang akan menyediakan *interface operator* utama. Tautan komunikasi *system* ESD - BPCS dan BPCS berbasis *Human Machine Interface* (HMI) harus mengizinkan *operator* untuk:

- Melihat nilai dan status saat ini dari semua input sistem ESD.

- Effect start-up and maintenance overrides of ESD system I/O.
- Receive ESD system alarm notification.
- View ESD system status and effect reset commands.

d) The ESD system shall be considered as a part of the Instrumented Protective System (IPS) which also comprises the Fire & Gas system (F&G) and Emergency Depressurization (EDP) system. The EDP shall be incorporated in the ESD system whereas the F&G system is an independent system. The depressurization applications shall be designed as energized to depressurize (that is they are not fail open). Energize to depressurize outputs shall be provided with line monitoring and fault alarm notification. It should be a separate requirement introduced to the EDP system to maintain its functionality of the depressurization systems even in the event of main power failure.

e) The ESD System shall receive process inputs from field devices, use discrete logic language to perform logical operations, execute control of discrete safety shutdown field devices and communicate with external devices and other third party supplied systems such as control panels for compressors, boilers etc.

f) Each system shall function in a redundant format using appropriate voting to establish channel integrity. Each channel path shall be completely isolated and operate independently of each other. There shall be no single

- Efek *override* pada *start-up* dan pemeliharaan pada I/O sistem ESD.
- Menerima *alarm* pemberitahuan dari sistem ESD.
- Melihat status sistem ESD dan efek perintah *reset*

d) Sistem ESD harus dianggap sebagai bagian dari *Instrumented Protective System* (IPS) yang juga terdiri dari *Fire & Gas system* (F&G) dan sistem *Emergency Depressurization* (EDP). EDP harus dimasukkan ke dalam sistem ESD sedangkan sistem F&G adalah sistem independen. Aplikasi depresurisasi harus dirancang sebagai penyaluran energi untuk menurunkan tekanan (Sistem ESD tidak gagal untuk dibuka). Energi untuk menurunkan tekanan yang keluar harus dilengkapi dengan pemantauan jalur dan pemberitahuan alarm kesalahan. Harus ada persyaratan terpisah yang digunakan ke sistem EDP untuk mempertahankan fungsionalitasnya dari sistem depresurisasi bahkan jika terjadi kegagalan daya utama.

e) Sistem ESD akan menerima *input* proses dari perangkat lapangan, menggunakan bahasa logika diskrit untuk melakukan operasi logis, menjalankan kontrol dari perangkat lapangan *discrete safety shutdown* dan berkomunikasi dengan perangkat eksternal dan sistem yang disediakan pihak ketiga lainnya seperti panel kontrol untuk *compressor, boiler,* dll.

f) Setiap sistem akan berfungsi dalam *format redundant* dengan menggunakan *voting* yang sesuai untuk membangun integritas saluran. Setiap jalur saluran harus sepenuhnya diisolasi dan beroperasi secara

failure point that could affect more than one channel. Failure of a single component shall not cause a shutdown action. The failure shall be logged and control room operators informed and the ESD system shall remain available to provide process safety protection.

independen satu sama lain. Tidak boleh ada satu titik kegagalan yang dapat mempengaruhi lebih dari satu saluran. Kegagalan satu komponen tidak akan menyebabkan tindakan pemadaman. Kegagalan harus dicatat dan diinformasikan ke *control room operator* dan sistem ESD harus tetap tersedia untuk memberikan perlindungan keamanan proses.

g) Final elements should remain in their safe (shutdown) state after a trip until manually reset. They should be allowed to return to their normal state only if the trip initiators have returned to their normal operating conditions. Shutdown valves connected to the ESD systems shall be supplied complete with smart valve positioners to allow partial stroke testing without necessitating either a partial or full facility shutdown.

g) *Final element* harus tetap dalam status aman (*shutdown*) setelah *trip* hingga *reset* secara *manual*. Mereka harus diizinkan untuk kembali ke keadaan normal hanya jika *trip initiator* telah kembali ke kondisi pengoperasian normal mereka. *Shutdown valve* yang terhubung ke sistem ESD harus dilengkapi dengan pengatur posisi *smart valve* untuk memungkinkan pengujian langkah parsial tanpa memerlukan pemadaman sebagian atau seluruh fasilitas.

h) A ‘fail safe’ mode for ESD isolation valves shall be defined as ‘fail close’ in order to prevent the continued flow of fuel to the incident.

h) Mode ‘*fail safe’* untuk *isolation valve* ESD harus didefinisikan sebagai ‘*fail close*’ untuk mencegah aliran bahan bakar yang berkelanjutan ke insiden tersebut.

i) ESD System reliability shall conform to the outcomes from HAZOP and SIL Assessment studies.

i) Keandalan Sistem ESD harus sesuai dengan hasil dari studi *HAZOP* dan SIL *Assessment*.

j) ESD controls shall be provided with suitable guard to prevent an accidental operation.

j) Kontrol ESD harus dilengkapi dengan pelindung yang sesuai untuk mencegah operasi yang tidak disengaja.

### 7.2 ESD Manual Activation Points

The manual activation points for initiating the ESD system response shall be arranged in such a way that their optimum availability can be assured in order to provide adequate protection to the facility. The following guideline can be considered

### 7.2 Titik Aktivasi *Manual* ESD

Titik aktivasi *manual* untuk memulai respons sistem ESD harus diatur sedemikian rupa sehingga ketersediaan optimalnya dapat dijamin untuk memberikan perlindungan yang memadai ke fasilitas. Panduan berikut dapat

for the deployment of the ESD manual activation points:

a) Each activation point shall be labelled to area of coverage and provided with an identification as to which valves it operates or equipment it shutdowns.

b) The activation points shall be located a minimum of 8 meters away from a high process hazard location but no more than 5 minutes of walking distance from any location within the facility.

c) The location of the activation point should be preferably upwind from protected hazard, especially in proximity to the installations handling toxic gases.

d) The activation points shall be located in the path of normal and emergency evacuation routes from the affected area.

e) The activation points should be preferably located near to other emergency devices that may need immediate activation in an emergency, such as manual blowdown valves, fire monitors, etc.

f) Install the activation points at a high which is convenient to personnel.

g) Manned control rooms shall always be provided with hardwired ESD activation points located on the main control panel.

h) Remote (control room) ESD actuating buttons shall be readily accessible to operations personnel within an operator's console or in a strategic location inside the control room.

i) Local hard-wired ESD actuating buttons for emergency shutdown shall be located at the plant equipment,

dipertimbangkan untuk penerapan titik aktivasi *manual* ESD:

a) Setiap titik aktivasi harus diberi label ke area cakupan dan dilengkapi dengan identifikasi *valve* mana yang dioperasikan atau peralatan yang dimatikan.

b) Titik aktivasi harus ditempatkan *minimum* 8 meter dari lokasi proses bahaya tinggi tetapi tidak lebih dari 5 menit berjalan kaki dari lokasi manapun di dalam fasilitas.

c) Lokasi titik aktivasi sebaiknya berlawanan dengan arah angin dari bahaya yang dilindungi, terutama di dekat instalasi yang menangani gas beracun.

d) Titik aktivasi harus terletak di jalur normal dan jalur evakuasi darurat dari area yang terkena dampak.

e) Titik aktivasi sebaiknya terletak di dekat perangkat darurat lain yang mungkin memerlukan aktivasi segera dalam keadaan darurat, seperti *manual blowdown valve*, pemantau kebakaran, dll.

f) Pasang titik aktivasi di tempat yang nyaman bagi personel.

g) *Manned control room* harus selalu dilengkapi dengan titik aktivasi ESD terprogram yang terletak di *panel* kontrol utama.

h) *Remote (control room) ESD actuating button* harus mudah diakses oleh personel operasi di dalam konsol *operator* atau di lokasi yang strategis di dalam *control room*.

i) *Local hard-wired* ESD *actuating button* untuk pemadaman darurat harus ditempatkan di peralatan *plant*,

equipment train, process unit, or battery limit as required by Owner.

rangkaian peralatan, *unit* proses, atau *battery limit* seperti yang dipersyaratkan oleh Pemilik.

### 7.3 Levels of Shutdown

To reflect the severity of hazardous conditions in the ESD system response it is advised to consider incorporation of several levels of the ESD. The initiating events for each level and the action should be defined in line with the result of hazard identification and risk assessment studies. For instance low level risk hazard or small area of involvement may only require a shutdown of individual equipment whilst the major incident may require a whole facility shutdown (with or without depressurization).

Up to five (5) levels of shutdown might be considered for ESD systems design for RU V and Lawe-Lawe terminal. The following guideline may be applied by defining the functionality for each level:

7.3.1 Level 1: Total facility Shutdown (Catastrophic Accident) (ESD1)

A Level 1 shutdown should shut down the complete facility (RU). This should be only initiated manually from a dedicated control room by an emergency push button with a protective cover. This level of shutdown may include, but not limited to, the following executive action:

a) Total process shutdown including all Level 2 associated shutdown events.

b) Depressurize the process installations (it may be a staggered depressurization

### 7.3 *Level of Shutdown*

Untuk mencerminkan tingkat keparahan kondisi berbahaya dalam respons sistem ESD, disarankan untuk mempertimbangkan penggabungan beberapa *level* ESD. Inisiasi awal untuk setiap *level* dan tindakan harus didefinisikan sejalan dengan hasil identifikasi bahaya serta studi penilaian risiko. Misalnya bahaya risiko tingkat rendah atau *area* yang kecil yang terlibat mungkin hanya memerlukan pemadaman peralatan individu, sementara insiden besar mungkin memerlukan pemadaman seluruh fasilitas (dengan atau tanpa depresurisasi).

Terdapat lima (5) *level* pemadaman yang dapat dipertimbangkan untuk desain sistem ESD. Panduan berikut dapat diterapkan dengan menentukan fungsionalitas untuk setiap *level*:

7.3.1 *Level* 1: *Total facility Shutdown* (*Catastrophic Accident*) (ESD1)

*Shutdown Level* 1 harus menutup fasilitas secara keseluruhan. Ini hanya diinisiasi secara *manual* dari *control room* khusus dengan tombol tekan darurat dengan pelindung sebuah penutup. *Shutdown level* ini dapat mencakup, tetapi tidak terbatas pada, tindakan eksekutif berikut:

a) *Total process shutdown* termasuk semua kegiatan *shutdown level* 2 yang terkait.

b) Depresurisasi instalasi proses (berupa depresurisasi bertingkat yang diterapkan karena batasan

implemented due to flare system constraints).

c) Isolate/ shutdown all utilities except essential systems to maintain safe state and considered to be life critical.

d) Relay the signal to initiate the relevant emergency alarms and communications.

7.3.2 Level 2: Process Unit/Plant Shutdown (Confirmed Fire in Unit) (ESD2)

A Level 2 shutdown should be initiated by a protected cover emergency push button located in the dedicated control room or emergency activation point in the field, or by confirmed fire detection in process areas, or by confirmed flammable or toxic gas, or by loss of instrument air pressure, or by loss of electrical power. This level of shutdown may include, but not limited to, the following executive action:

a) Stop/ isolate all electrical and rotating equipment.

b) Activates deluge valves and starts the fire water pumps.

c) Relay the signal to initiate the relevant emergency alarms and communications.

d) Initiate Level 3 associated shutdown events.

pada sistem *flare*).

c) Isolasikan/ *shutdown* semua utilitas kecuali *system* yang esensial untuk mempertahankan status aman dan penting bagi kehidupan.

d) *Relay* sinyal untuk memulai *alarm* dan komunikasi darurat yang relevan.

7.3.2 Level 2: *Shutdown* Proses Unit/ *Plant* (Kebakaran yang Dikonfirmasi dalam *Unit*) (ESD2)

*Shutdown level* 2 harus dimulai dengan tombol tekan darurat yang tertutup yang terletak di *control room* khusus atau titik aktivasi darurat di lapangan, atau dengan deteksi kebakaran yang dikonfirmasi di *area* proses, atau dengan dipastikan adanya gas yang mudah terbakar atau beracun, atau karena hilangnya tekanan udara instrumen, atau karena hilangnya daya listrik. *Shutdown level* ini dapat mencakup, tetapi tidak terbatas pada, tindakan eksekutif berikut:

a) Hentikan/ pisahkan semua peralatan listrik dan peralatan rotating.

b) Mengaktifkan *deluge valve* dan menyalakan *fire water pump.*

c) *Relay* sinyal untuk memulai *alarm* dan komunikasi darurat yang relevan.

d) Mulai kegiatan *shutdown level* 3 yang terkait.

Activation of Level 2 shutdown shall not disrupt in any way the availability and operability of the following systems:

- Fire protection and suppression systems.
- Instrument air supply.
- Uninterruptible Power Supplies (UPS).
- Emergency power generation facilities.

7.3.3 Level 3: Process Shutdown (Major Process Upset) (ESD3)

A Level 3 shutdown should be initiated by a protected cover emergency push button located in the dedicated control room or major process trip. This level of shutdown may include, but not limited to, the following executive action:

a) Shutdown the entire process unit.

b) Shutdown any directly connected upstream supplies.

c) Shutdown any downstream export ESD isolation valves.

d) Initiate the closure of ESD valves to stop the flow of flammable fluids.

e) Stop the heat input to process heaters or boilers (where appropriate).

f) Stop/ isolate electrical and rotating equipment (except compressors) (where applicable).

Aktivasi *shutdown level* 2 tidak akan mengganggu ketersediaan dan pengoperasian sistem berikut ini:

- Sistem proteksi dan pemadaman kebakaran.
- Pasokan *instrument air*.
- *Uninterruptible Power Supplies* (UPS).
- Fasilitas pembangkit listrik darurat.

7.3.3 *Level* 3: *Shutdown Process* (*Major Process Upset*) (ESD3)

*Shutdown* Level 3 harus dimulai dengan tombol darurat yang terlindungi dengan penutup yang terletak di *control room* khusus atau pada jalur proses utama. Level *shutdown* ini dapat mencakup, tetapi tidak terbatas pada, tindakan eksekutif berikut:

a) *Shutdown* seluruh unit proses.

b) *Shutdown* semua suplai hulu yang terhubung langsung.

c) *Shutdown* ESD *isolation valve* ekspor hilir.

d) Inisiasi penutupan ESD *valve* untuk menghentikan aliran cairan yang mudah terbakar.

e) Hentikan pasokan panas yang digunakan untuk memproses *heater* atau *boiler* (jika sesuai).

f) Hentikan/ isolasikan peralatan listrik dan peralatan *rotating* (kecuali kompresor) (jika memungkinkan).

g) Switch compressors to recycle mode (where applicable).

h) Relay the signal to initiate the relevant emergency alarms and communications.

i) Initiate Level 4 associated shutdown events.

Activation of Level 3 shutdown shall not disrupt in any way the availability and operability of the following systems:

- Fire protection and suppression systems.
- Instrument air supply.
- Uninterruptible Power Supplies (UPS).
- Emergency power generation facilities.

7.3.4 Level 4: Package Shutdown (Local Process Upset) (ESD4)

A Level 4 shutdown should be initiated by a protected cover emergency push button located in the dedicated control room or in the field, or field instrument trip or package trip. This level of shutdown may include, but not limited to, the following executive action:

a) Shutdown the package.

b) Enable package depressurization via automatic initiation or manually.

c) Relay the signal to initiate the relevant emergency alarms and communications.

d) Initiate Level 5 associated shutdown events.

g) Alihkan kompresor ke mode *recycle* (jika memungkinkan).

h) *Relay* sinyal untuk memulai alarm dan komunikasi darurat yang relevan.

i) Inisiasi *shutdown level* 4 yang terkait.

Aktivasi *shutdown level* 3 tidak akan mengganggu ketersediaan dan pengoperasian sistem berikut ini:

- Sistem proteksi dan pemadaman kebakaran.
- Pasokan *instrument air*.
- *Uninterruptible Power Supplies* (UPS).
- Fasilitas pembangkit listrik darurat.

7.3.4 *Level* 4: *Shutdown Package* (*Local Process Upset*) (ESD4)

*Shutdown level* 4 harus dimulai dengan tombol darurat yang terlindungi penutup yang terletak di *control room* khusus atau di lapangan, atau pada *field instrument* atau *package trip. Level shutdown* ini mungkin termasuk, tetapi tidak terbatas pada, tindakan eksekutif berikut:

a) *Shutdown package*.

b) Aktifkan depresurisasi *package* melalui inisiasi otomatis atau manual.

c) *Relay* sinyal untuk memulai *alarm* dan komunikasi darurat yang relevan.

d) Inisiasi *shutdown level* 5 yang terkait.

7.3.5 Level 5: Local Equipment Shutdown (Equipment Failure) (ESD5)

A Level 5 shutdown should be initiated by a protected cover emergency field push button or field instrument trip. The executive actions are:

a) Trip outputs as per Cause and Effect Diagram.

b) Auto start of spare/redundant equipment.

c) Relay the signal to initiate the relevant emergency alarms and communications.

## 7.4 Critical Equipment Shutdown Requirements

7.4.1 Compressors

Typically, compressors are shutdown by either tripping the motor drive or closing the steam valve to the turbine drive. A protective system to accomplish the shutdown can be initiated if selected variables, such as level in a suction knockout drum, vibration, lubrication flow, seal fluid pressure, etc. exceed limits.

The criteria for compressor driver which requires ESD are:

a) Compressors driver over 200 HP (150 kW), ESD is actuated from the control room and locally.

b) On steam driven compressors that handle flammable materials, ESD is actuated from control room and local.

7.3.5 *Level* 5: *Shutdown* Peralatan Lokal (Kegagalan Peralatan) (ESD5)

*Shutdown level* 5 harus dimulai dengan tombol darurat lapangan yang dilindungi penutup atau *field instrument trip*. Tindakan eksekutifnya adalah:

a) Output *trip* sesuai *Cause* dan *Effect Diagram*.

b) Aktivasi otomatis peralatan cadangan/ *redundant.*

c) *Relay* sinyal untuk memulai *alarm* dan komunikasi darurat yang relevan.

## 7.4 Persyaratan *Shutdown* Peralatan Kritikal

7.4.1 Kompresor

Biasanya, kompresor dimatikan dengan cara menyetop *motor* penggerak atau menutup *steam valve* ke penggerak turbin. Sistem pelindung untuk melakukan *shutdown* dapat dimulai jika variabel yang dipilih, seperti *level* dalam *suction knockout drum*, *vibration, lubrication flow, seal fluid pressure*, dll, sudah melebihi batas

Kriteria *driver compressor* yang membutuhkan ESD adalah:

a) *Driver compressor* lebih dari 200 HP (150 kW), ESD digerakkan dari *control room* dan secara lokal.

b) Pada *compressor* yang digerakkan oleh uap yang menangani *material* yang mudah terbakar, ESD digerakkan dari *control room* dan lokal.

7.4.2 Combustion Gas Turbine

Combustion gas turbine (CGT) consisting of the manufacturer's shutdown devices.

7.4.3 Turbo-expanders

Turbo-expanders and associated equipment handling combustible fluids.

7.4.4 Pumps

a) Pumps with a rated capacity of over 45 m3/hr (200 US gpm) that handle flammable liquids or combustible liquids above or within 8°C (15°F) of their flash point temperatures.

b) Regardless of capacity, any pump handling a flammable liquid having a true vapor pressure equal to or greater than an absolute pressure of 200 kPa (29 psia) at 54°C (130°F) and taking suction from a system with a liquid inventory in excess of 8 m³ (50 barrels).

c) Pumps with a history of bearing failure or seal leakage.

d) Pumps with small piping subject to fatigue failure.

e) Pumps which handle potentially toxic material, have drivers larger than 7.5 kW (10 HP), and take suction from a system with a liquid inventory of more than 8 m³ (50 bbl).

7.4.2 *Combustion Gas Turbine*

*Combustion gas turbine* (CGT) terdiri dari perangkat *shutdown* pabrikan.

7.4.3 *Turbo-expander*

*Turbo-expander* dan peralatan terkait yang menangani cairan yang dapat terbakar.

7.4.4 Pompa

a) Pompa dengan *rated capacity* lebih dari 45 m3/jam (200 US gpm) yang menangani cairan yang mudah terbakar dan yang dapat terbakar di atas atau pada suhu 8°C (15°F) dari suhu *flash point*.

b) Terlepas dari kapasitasnya, setiap pompa yang menangani cairan yang mudah terbakar yang memiliki *true vapor pressure* yang sama atau lebih besar dari tekanan absolut 200 kPa (29 psia) pada 54°C (130 ° F) dan yang menyedot dari sistem dengan *inventory*/ persediaan cairan lebih dari 8 m³ (50 barel).

c) Pompa dengan riwayat kegagalan *bearing* atau kebocoran *seal.*

d) Pompa dengan perpipaan kecil yang dapat mengalami kegagalan *fatigue.*

e) Pompa yang menangani *material* yang berpotensi beracun, memiliki *driver* lebih besar dari 7.5 kW (10 HP), dan yang menyedot dari sistem dengan *inventory*/ persediaan cairan lebih dari 8 m³ (50 bbl).

7.4.5 Fired Heaters

The function of protective system for fired heaters is to shut off fuel to the furnace if selected variables exceed safe limits, such as:

a) Low fuel pressure shutoff when the fuel pressure becomes too low for stable burner operation (for main and pilot burners).

b) Low process flow shutoff of the fuel to prevent overheating the furnace tubes.

Remote fuel shutoff automated or manual shall be provided on all fired heaters or reboilers located in or adjacent to process units where there is possibility of vapor cloud forming as a result of serious spills or leaks. This remote shutoff shall be controlled from a safe location adjacent to the purge steam valve manifold, which shall be at least 15 m away from the furnace.

When the fired heater or reboiler is equipped with a remotely operated stack damper, the control switch or push button shall be located at least 15 m (50 ft) away from the furnace at the purge steam valve manifold.

7.4.5 *Fired Heater*

Fungsi sistem pelindung untuk *fired heater* adalah untuk mematikan bahan bakar ke *furnace* jika variabel yang dipilih melebihi batas aman, seperti:

a) Penutupan tekanan berbahan bakar rendah ketika tekanan bahan bakar menjadi terlalu rendah untuk operasi pembakar yang stabil (untuk pembakar utama dan *pilot*).

b) Penghentian aliran proses bahan bakar rendah untuk mencegah pemanasan berlebih pada *furnace tube.*

Penghentian bahan bakar jarak jauh otomatis atau manual harus disediakan pada semua *heater/* pemanas yang dibakar atau *reboiler* yang terletak di dalam atau berdekatan dengan unit proses di mana ada kemungkinan terbentuknya *vapor cloud* sebagai akibat dari tumpahan atau kebocoran yang serius. Penutupan jarak jauh ini harus dikontrol dari lokasi aman yang berdekatan dengan *purge steam valve manifold*, yang paling sedikit harus berjarak 15 m dari *furnace*.

Jika *heater* atau *reboiler* yang dibakar dilengkapi dengan *stack damper* yang dioperasikan dari jarak jauh, sakelar kontrol atau tombol tekan harus ditempatkan setidaknya 15 m (50 ft) dari *furnace* di *purge steam valve manifold*.

7.4.6 Boiler

The boiler shall be provided with a safeguarding/ interlock system (ESD) to avoid explosion and other hazardous situations.

The safeguarding/ interlock system (ESD) shall be designed to trip the boiler by the following reasons:

a) Loss of flame in operation and failure of ignition.

b) Forced Draft Fan (FDF) trip.

c) Extremely low water level.

d) Extremely low fuel pressure.

e) Manual push buttons for emergency trips.

7.4.7 Air Injection / Oxidizer Streams to Process

ESD actuated from the control room is required for an air injection or oxidizer stream to process where immediate shutoff is required to make the unit safe.

7.4.8 Sulphur Units

Combustion air, acid gas, sour water gas, and fuel gas (including pilot gas) to the thermal reactor, in-line burners (when installed), and incinerator shall be provided with ESD for the following upset conditions:

a) Combustion air failure.

b) Acid gas low flow.

c) High stack gas temperature.

d) Low water level in waste heat boiler.

7.4.6 *Boiler*

*Boiler* harus dilengkapi dengan sistem pengaman/ *interlock* (ESD) untuk menghindari ledakan dan situasi berbahaya lainnya.

Sistem pengaman/ *interlock* (ESD) harus dirancang untuk men-*trip*-kan *boiler* dengan alasan berikut:

a) Kehilangan api dalam operasi dan kegagalan penyalaan.

b) *Forced Draft Fan* (FDF) *Trip.*

c) Permukaan air sangat rendah.

d) Tekanan bahan bakar sangat rendah.

e) Tombol tekan *manual* untuk *emergency trip*.

7.4.7 Injeksi Udara/ *Oxidizer Stream* untuk *Unit* Proses

ESD yang digerakkan dari *control room* diperlukan untuk aliran injeksi udara atau *oxidizer* untuk memproses dimana pemadaman segera diperlukan untuk membuat unit aman.

7.4.8 *Unit* Belerang

Udara pembakaran, gas asam, gas air asam, dan gas bahan bakar (termasuk gas *pilot*) ke reaktor termal, pembakar *in-line* (bila dipasang), dan insinerator harus dilengkapi dengan ESD untuk kondisi gangguan berikut:

a) Kegagalan udara pembakaran.

b) Aliran rendah gas asam.

c) Suhu gas cerobong tinggi.

d) *Level* air rendah di *boiler* limbah panas

e) Incinerator flameout.

f) Low fuel gas pressure.

g) Sour water stripper off-gas low flow.

h) Thermal reactor flameout or high temperature.

7.4.9 Loading Arms

Loading arms at any berth handling flammable or combustible liquids or potentially toxic material.

e) Api insinerator padam.

f) Tekanan gas bahan bakar yang rendah.

g) Aliran gas yang keluar dari *sour water stripper* rendah.

h) Nyala api reaktor termal mati atau suhu tinggi.

7.4.9 *Loading Arm*

*Loading arm* di setiap *berth* mana pun yang menangani cairan yang mudah terbakar atau yang dapat terbakar atau bahan yang berpotensi beracun.