

PETRONAS TECHNICAL STANDARDS

DESIGN AND ENGINEERING PRACTICE

TECHNICAL SPECIFICATION

INSTRUMENTED PROTECTIVE SYSTEMS

PTS 32.80.10.30

FEBRUARY 2011



2011 PETROLIAM NASIONAL BERHAD (PETRONAS)

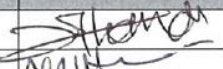
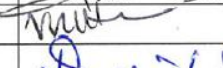
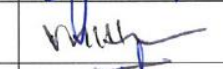
All rights reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the permission of the copyright owner.

PTS Circular 2011-18	PETRONAS 
PTS No:	32.80.10.30
Publication Title:	INSTRUMENTED PROTECTIVE SYSTEMS

This revision of PTS **32.80.10.30 – Instrumented Protective Systems** has been updated incorporating PETRONAS Lessons Learnt, Best Practice and new information issued by relevant industry code and standards.

The previous version of this PTS (**Release 13 December 1998**) will be removed from PTS binder/e-repository from herein onwards.

Document Approval

	Name	Designation	Date	Signature
Prepared	Zulkarnain Darus	Principal I&C	25/2/11	
Approved	V R Harindran	Custodian I&C	25/2/11	
Verified	Dzulkifli A Razak	Senior Manager, PAO Engineering - GTS	25/2/2011	
Verified	V R Harindran	for General Manager, Engineering - GTS	28/2/11	
Endorsed	Pau Kiew Huai	Senior General Manager, GTS	28.2.11	

Revision History

Date	Version	Description of Updates	Author

TABLE OF CONTENTS

1.	INTRODUCTION.....	1
1.1	SCOPE.....	1
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS.....	1
1.3	DEFINITIONS.....	1
1.4	ABBREVIATIONS.....	5
1.5	CROSS-REFERENCES.....	6
1.6	SUMMARY OF MAIN CHANGES.....	6
2.	SYSTEM REQUIREMENTS.....	7
2.1	FUNCTIONALITY.....	7
2.2	CERTIFICATION.....	7
2.3	INFORMATION SECURITY REQUIREMENTS.....	7
2.4	RESPONSE TIME.....	9
2.5	STRUCTURE.....	9
2.6	SPARE CAPACITY.....	15
2.7	SYSTEM HARDWARE.....	15
2.8	SYSTEM AND APPLICATION SOFTWARE.....	17
2.9	ALARM SIGNAL HANDLING.....	17
2.10	SEQUENCE OF EVENTS RECORDER.....	18
2.11	ASSET MANAGEMENT SYSTEM.....	19
3.	HARDWARE CONSTRUCTION REQUIREMENTS.....	20
3.1	CABINETS.....	20
3.2	CABLING.....	20
3.3	EARTHING.....	21
3.4	LABELLING.....	21
4.	POWER SUPPLY.....	22
4.1	POWER SUPPLY FACILITIES.....	22
4.2	POWER CONSUMPTION AND TOLERANCE.....	22
4.3	POWER DISTRIBUTION.....	22
4.4	BATTERIES.....	22
5.	ENVIRONMENTAL CONDITIONS.....	23
6.	FACTORY ACCEPTANCE TEST.....	24
6.1	GENERAL.....	24
6.2	FAT PHASE 1.....	24
6.3	FAT PHASE 2.....	25
7.	DRAWINGS AND DOCUMENTATION.....	26
7.1	GENERAL.....	26
7.2	PLANNING.....	26
7.3	DOCUMENTATION.....	26
7.4	APPROVAL OF DRAWINGS.....	28
8.	REFERENCES.....	29

1. INTRODUCTION

1.1 SCOPE

This PTS specifies requirements and gives recommendations for Instrumented Protective Systems (IPSS), including fire, gas and smoke detection and protection systems (FGSS). The PTS covers the system functional requirements, the hardware definition, power supply requirements, environmental conditions, factory acceptance tests and drawings and documentations necessary to design, manufacture, test and deliver IPSS, FGSS and the SER system.

The primary purpose of the IPS is to be the logic solver of an SIS, i.e. to be the logic solver for IPFs, the secondary purpose is to act as an SER.

The operator interface is entirely implemented through the PAS hence extensive communication with the PAS is specified.

The requirements stated in this PTS are closely related to the requirements in PTS 32.80.10.10 and PTS 32.80.10.12.

The IPF requirements specification PTS 32.80.10.12 typically refers to this PTS to specify general requirements for the logic solver.

Excluded from the scope of this PTS are pneumatic or hydraulic types of IPSS and the installation and maintenance of the IPS.

This is a revision of the PTS of the same number dated July 1996.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by PETRONAS, the distribution of this PTS is confined to companies forming part of or managed by the PETRONAS Group, and to Contractors nominated by them.

This PTS is intended for use in oil refineries, chemical plants, gas plants, onshore and offshore exploration and production facilities, and supply/marketing installations.

If national and/or local regulations exist in which some of the requirements may be more stringent than in this PTS the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable as regards safety, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this PTS which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned with the object of obtaining agreement to follow this PTS as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party that manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party that initiates the project and ultimately pays for its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorised to act for and on behalf of the Principal.

The word **shall** indicates a requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

Basic Process Control System

The system that responds to input signals from the process and generates output signals to

maintain operation of the process in a desired state. The system shall not perform functions assessed as SIL 1 or higher.

Beta Factor

The number of Common Mode Failures (of robust Initiators or Final Elements), expressed as a fraction of all possible Failures.

Common Mode Failure

A Failure having the potential to affect all duplicated components in a robust configuration by virtue of common or shared characteristics.

Dangerous Failure

A Failure that has the potential to place the IPF in a state in which it will fail to perform its function. Dangerous Failures are usually only revealed when the system has to perform a certain action or through testing. Formerly known as unrevealed failure.

Dangerous Failure Rate

The number of Dangerous Failures per unit time.

Dangerous Failure Robustness

A configuration in which plant integrity is not jeopardised by the Dangerous Failure of a single IPF component. Formerly known as unrevealed failure robustness.

Demand

A process or equipment condition or event that requires an Instrumented Protective Function to take action to prevent a Hazardous Situation.

Demand Rate

The frequency at which a Demand occurs, i.e. the number of Demands per unit time.

Diagnostic Coverage Factor

The number of Dangerous Failures that diagnostic features are capable of detecting expressed as a fraction of all possible dangerous failures.

NOTE: Diagnostic features may only be recognised as such if they can trip the process to a safe state or maintain safety by different means.

Engineering Work Station (EWS)

An EWS is a workstation, which contains the software and / or the database required to prepare and download configuration changes into the safety system. It may also be used to interpret and diagnose the state of the logic of the safety system in a 'read-only' mode. For smaller sites the function of the EWS may be combined with an Operator Work Station.

Fail Safe

A concept that defines the failure direction of a component or system as a result of specific malfunctions. That failure direction is towards a safer or less hazardous condition.

Failure

An abnormal condition that may cause a reduction or loss of capability of the IPF to perform its intended function.

Fault Tolerance

Ability of a functional unit to continue to perform a required function in the presence of faults or errors.

Final Element

A device, or combination of devices, that manipulate a process variable or attract the attention of the operator to achieve risk reduction. The Final Element includes output cards or output relays, solenoid valves and cabling. Examples are valves, switchgear (rotating equipment stop circuits) and alarms.

Hazard or Hazardous Situation

A situation with the potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.

Hazard Rate

The frequency at which Hazardous Situations occur per unit time.

Hazard Rate = Demand rate x Probability of Failure on Demand.

Information Security

The protection of data and IT resources from accidental or malicious acts, usually by taking appropriate actions. These acts may be modification, destruction, access, disclosure, or acquisition, if not authorized. (ISO 2382-8)

Information security is quantified in terms of availability, integrity and confidentiality.

Sensor

A device (such as a load cell, thermocouple, accelerometer etc.) that detects the value of a physical quantity and converts the measurement into a useful input for another device.

Instrumented Protective Function

A function comprising one or more Sensors, a Logic Solver and one or more Final Elements whose purpose is to prevent or mitigate hazardous situations.

An IPF is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event.

In IEC 61508 and IEC 61511, an IPF is referred to as a Safety Instrumented Function (SIF).

Instrumented Protective System

The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment.

In IEC 61508 and IEC 61511, an IPS is referred to as a 'Logic Solver'.

Logic Solver

The portion of an Instrumented Protective Function that performs the application logic function. The Logic Solver excludes trip amplifiers, input cards and output cards. Examples are electromechanical relays, solid-state/magnetic-core logic and the Central Processing Unit (CPU) section of programmable electronic systems.

Logically Separated Networks:

Logical separation is a separation between different entities/groups that is enforced by configuration or administration and not by physical means i.e. VLAN, VPN tunnelling, etc. The Safety Bus and the Control Bus are both physically as well as logically separated networks.

Mitigation

The action of making a consequence less severe or relieving consequences.

PAS

Process Automation System; Incorporates DCS functionality and includes PES networks, RTUs, and other vendor/OEM equipment integrated via serial and/or hardwired interfaces. Also generally provides the primary HMI to IPS.

Permissive

The result of a check on whether or not a combination of conditions is healthy, to allow the Logic Solver to proceed with the next step.

Physically Separated Networks

Networks that use the same physical network (e.g cabling) however IP addressing, routing and network protocols separate the traffic of the various logical networks.

Probability of Failure on Demand

The probability (dimensionless) of the Instrumented Protective Function failing to respond to a Demand.

Process Control Access Domain (PCAD)

A firewall and associated systems that securely interconnect the Process Control Domain (PCD) to other network environments.

Process Control Domain (PCD)

The network environment to which Process Control systems are connected.

Programmable Electronics (PE)

Electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units.

NOTE: This term covers micro-electronic devices based on one or more central processing units (CPUs) together with associated memories, etc. Examples of process sector programmable electronics include:

- Smart sensors and final elements;
- Programmable electronic logic solvers including:
- Programmable controllers;
- Programmable logic controllers
- Process automation system (PAS);
- Loop controllers.

Programmable Electronic System (PES)

System for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices. As an example, an IPS could be a PES.

Process Safety Time

The period of time in which the process can be operated without protection and with a Demand present without entering a dangerous condition. The Process Safety Time determines the dynamic response requirements of the IPF.

Proof Test

A test carried out on IPF components against an approved procedure to confirm that all requirements of the IPF are met.

Proof Test Coverage Factor

The number of Dangerous Failures detected by the Proof Test expressed as a fraction of all possible dangerous failures.

Risk

The frequency at which a Hazardous Situation occurs multiplied by the consequence of the Hazardous Situation.

Safe Failure

A Failure whose occurrence does not have the potential to place an IPF in a dangerous state. Formerly known as revealed failure.

Safe Failure Rate

The number of Safe Failures per unit time.

Safe Failure Class

A class (N or F) derived from the cost benefit analysis of providing Safe Failure Robustness. Where robustness can be justified, the Safe Failure Class is F. where robustness cannot be justified; the safe failure class is N. Formerly known as Revealed Failure Class.

Note: N = Non fault tolerant design – safe failure robustness is not justified.

F = Fault tolerant design – safe failure robustness is justified.

Safe Failure Fraction

The fraction of all Failures that drive the sub-system (e.g. Initiator or Final Element) to the safe state.

$$\text{Safe Failure Fraction} = \frac{\lambda_{\text{safe}} + \lambda_{\text{dangerous}} * DCF}{\lambda_{\text{safe}} + \lambda_{\text{dangerous}}}$$

where:

λ_{safe} is the safe failure rate (year^{-1});
 $\lambda_{\text{dangerous}}$ is the dangerous failure rate (year^{-1});
 DCF is the diagnostic coverage factor.

Safe Fault Tolerance A configuration in which plant availability is not jeopardised by the safe failure of a single IPF component. Formerly known as Revealed Failure Robustness.

Safety Integrity Level (SIL)

Dangerous failure class 1, 2, 3 or 4, derived from the consequences of failure on demand and the Demand Rate. Formerly known as IPF Class.

The IEC 61511 definition is: Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions (IPF) to be allocated to the safety instrumented systems (trip systems). Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

Safety Instrumented System (SIS)

Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s). (IEC 61511).

i.e. the collection of IPFs (including sensors and final elements) that together protect a process unit or major piece of equipment (furnace, compressor).

Trip

An Instrumented Protective Function action to bring the Final Element to a safe state.

1.4

ABBREVIATIONS

AC	Alternating Current
AK	Anforderungsklasse (requirement class)
AMS	Asset Management System
CPU	Central processing unit
DACA	Data Acquisition and Control Architecture
DC	Direct current
DCS	Distributed control system
DIN	Deutsche Industrie Norm (German Industrial Standard)
EPROM	Erasable programmable read-only memory
FGS	Fire gas and smoke detection and protection system
FAT	Factory acceptance test
FLD	Functional logic diagrams
GPS	Global Positioning System, includes a highly accurate time source
I/O	Input/output
IPF	Instrumented protective function
IPS	Instrumented protective system
MODBUS	Modicon Bus, a messaging protocol structure developed by Modicon
MOS	Maintenance override switch
NTFS	New Technology File System
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
PC	Personal computer
PAS	Process Automation System
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCN	Process Control Network
PES	Programmable Electronic System

RAM	Random access memory
RLL	Relay ladder logics
RTU	Remote transmission unit
SER	Sequence of events recorder
SFC	Sequential function charts
SIF	Safety Instrumented Function (IEC 61508 and IEC 61511 equivalent of IPF)
SIL	Safety integrity level
TCP/IP	Transmission Control Protocol/Internet Protocol
UZ	Tag numbering system to group protection functionality dedicated to specific process equipment or group of equipment. Note that an IPF may span several UZ 'blocks'.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1.5 CROSS-REFERENCES

Where cross-references to other parts of this PTS are made, the referenced section number is shown in brackets. Other documents referenced in this PTS are listed in (8.).

1.6 SUMMARY OF MAIN CHANGES

This PTS is a revision of the PTS of the same number dated July 1996. The main, non-editorial changes are as follows:

- The PTS has been revised to reflect developments in international standardisation, mainly the publication of IEC 61511, as well as to bring it in line with PTS 32.80.10.10;
- The PTS has been converted from requisition format to technical specification for IPS;
- A new section 2.3 has been added on Information Security Requirements;
- Selection between physically or logically separated networks for the IPS-IPS (safety communication) and the EWS has been included;
- Possible IPS technologies have been included.

2. SYSTEM REQUIREMENTS

2.1 FUNCTIONALITY

The IPS shall be normally energised except for lamp outputs. A "1" logic signal is considered to be the normal state, and a "0" logic signal the abnormal (trip or failure) state. Output signals should go to a "0" (de-energised) state on power failure or on component failure.

NOTE: Inputs and outputs which are energised to trip, such as in some cases emergency depressurising and FGS outputs, shall have line monitoring and earth fault detection for each input and output channel

For commissioning purposes it shall be possible to force I/O signals to certain states via the engineering workstation. Forcing shall be seen as a configuration change and shall be according to the site change control procedure. This forcing feature shall be controlled by a configure enable switch, and forcing shall be ineffective when the switch is not enabled. For details on the implementation of this mechanism see (2.3).

Loss of data communication with the PAS or in the SER and maintenance and engineering network shall not result in trips or status changes of the IPS communication points. Recovery of communication shall be automatic.

The operator shall be continuously informed of the system status by means of system alarms. As these are Supplier-specific, they are not included in the I/O listing provided by the Principal, but shall be included in the scope. As minimum the below shall be configured:

- The position of configure enable switch;
- Common cabinet utility alarm and a common system alarm;
- Total IPS failure via hardwired signal (i.e. not via serial links);
- IPS system alarms and IPS utility alarms.

Diagnostic information from field devices may be collected using HART multiplexers which are connected to the AMS.

In all cases writeable parameters shall only be configurable from the EWS, and shall require a change of configuration mode to enable a change.

2.2 CERTIFICATION

Where "reputable certifying authority" is specified in this PTS, this shall be in accordance with IEC 61508.

Disagreements between this PTS and the constraints of the IEC 61508 SIL 3 certification approval report shall be highlighted and further discussed.

All conditions regarding application of the IPS listed in the IEC 61508 SIL 3 certification report and in the IPS safety manual shall be met.

IEC 61508 SIL 3 certification shall include, but not limited to:

- The IPS hardware including I/O cards, manual-switches like configuration and force enable switches and network switches;
- All input and output cards, which shall be fail safe except for those outputs driving SIL <1 outputs (not safety related), unless specified by principal, and those driving hardwired alarm lamps;
- IPS-to-IPS communication over the Safety Bus;
- Application software;
- Interface cards.

2.3 INFORMATION SECURITY REQUIREMENTS

This section is not applicable to electromechanical relays and solid-state/magnetic-core