

GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

Protective Systems

GP 15-07-02

Scope

- 1) [I] This Global Practice (GP) covers the design, installation, and documentation of protective systems.
- 2) [I] Mechanical devices used to implement protective functions such as mechanical overspeed trips or relief valves are not covered in this GP.
- 3) [I] Protective systems for electrical generation and distribution systems are not covered in this GP.
- 4) [I] Power supply to the protective system from an external source (e.g., electrical power, instrument air) is not covered in this GP.
- 5) [I] An asterisk (*) indicates that either a decision by the Owner's Engineer is required, that additional information is to be furnished by the Owner's Engineer, or that information for the Owner's Engineer approval is to be supplied by Vendor or Contractor.
- 6) * [I] Operating experience demonstrates that protective systems designed, assembled and tested to this GP should give acceptable performance for all typical services in our industry such as boilers, furnaces, compressors, etc. For systems where high levels of availability are required, the Owner's Engineer shall be consulted for design details.

Downstream, Chemical, Upstream, Downstream Imperial Oil	For ExxonMobil Use Only	Version 1.0.0
Page 1 of 23	©ExxonMobil Development Company	 Documents Document Sharing Hub

GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

Table of Contents

1. Required References	3
1.1. Global Practices–ExxonMobil Engineering Practices	3
1.2. FCI–Fluids Control Institute, Inc.	4
1.3. IEC–International Electrotechnical Commission	4
1.4. ISA–The Instrumentation, Systems, and Automation Society	5
1.5. ISO–International Organization for Standardization	5
1.6. MIL–Military Handbooks	5
1.7. NEMA–National Electrical Manufacturers Association	5
2. Definitions	5
3. Documentation	9
4. Basic Design	10
5. Logic	11
5.1. Pneumatic Logic	12
5.2. Electrical/Electronic Logic	12
5.3. Programmable Electronic Systems (PES)	12
6. Operator Interface	14
7. Power	15
8. Field Wiring	16
9. Sensors	16
10. Final Elements	17
11. Test and Maintenance Facilities	18
12. Inspection and Testing	20
Record of Change	22
Attachment: Purpose Codes Definitions	23

DNST, CHEM, UPST, DIOL	For ExxonMobil Use Only	Version 1.0.0
Page 2 of 23	©ExxonMobil Development Company	



GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

1. Required References

* [I] This Section lists Practices and Standards that are generically referenced and assumed to be a part of this document. Unless otherwise specified herein, use the latest edition. The Design Specification shall indicate which standards are applicable.

1.1. Global Practices–ExxonMobil Engineering Practices

GP 03-06-01	Piping for Instruments
GP 03-06-02	Piping at Control and Protective System Valve Stations
GP 03-12-01	Valve Selection
GP 07-02-01	Industrial Boilers
GP 14-03-01	Fireproofing
GP 15-01-01	Instrumentation for Fired Heaters
GP 15-01-02	Instrumentation for Compressors and Drivers
GP 15-02-01	Temperature Instruments
GP 15-03-01	Pressure Instruments
GP 15-04-01	Flow Instruments
GP 15-05-01	Level Instruments
GP 15-06-01	Electronic and Pneumatic Instruments
GP 15-06-02	Environmental Protection for Instrumentation
GP 15-06-03	Programmable Logic Controllers
GP 15-07-01	Electric Power Branch Circuit Design for Instrumentation
GP 15-07-03	Alarm Systems
GP 15-09-01	Control Valves
GP 15-09-02	Electric Motor Operators for Valves
GP 15-10-01	Instrument Transmission Systems
GP 15-12-01	Instrument Wire and Cable
GP 16-01-01	Area Classification and Related Electrical Design for Flammable Liquids, Gases or Vapors
GP 16-03-01	Wiring Methods and Material Selection
GP 16-08-01	Instrument and Essential Services Power Supplies

DNST, CHEM, UPST, DIOL	For ExxonMobil Use Only	Version 1.0.0
Page 3 of 23	©ExxonMobil Development Company	



GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

1.2. FCI–Fluids Control Institute, Inc.

FCI 70-2	Control Valve Seat Leakage
----------	----------------------------

1.3. IEC–International Electrotechnical Commission

IEC 60812	Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)
IEC 61025	Fault Tree Analysis (FTA)
IEC 61078	Analysis Techniques for Dependability - Reliability Block Diagram Method
IEC 61131-3	Programmable Controllers - Part 3: Programming Languages
IEC 61508-1	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 1: General Requirements
IEC 61508-2	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems
IEC 61508-3	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 3: Software Requirements
IEC 61508-4	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 4: Definitions and Abbreviations
IEC 61508-5	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 5: Examples of Methods for the Determination of Safety Integrity Levels
IEC 61508-6	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3
IEC 61508-7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 7: Overview of Techniques and Measures
IEC 61511-1 Ed. 1.0	(Pending) Functional Safety Instrumented Systems for the Process Industry Sector - Part 1: General Framework, Definitions System Software and Hardware Requirements
IEC 61511-2 Ed. 1.0	(Pending) Functional Safety Instrumented Systems for the Process Industry Part 2: Guidelines in the Application of Part 1
IEC 61511-3 Ed. 1.0	(Pending) Functional Safety: Safety Instrumented for the Process Industry Sector - Part 3: Guidance for the Determination of Safety Integrity Levels - Informative
IEC 61000-4-3	Electromagnetic Compatibility (EMC) - Part 4-3: Testing and Measurement Techniques - Radiated, Radio-Frequency, Electromagnetic Field Immunity Test

DNST, CHEM, UPST, DIOL	For ExxonMobil Use Only	Version 1.0.0
Page 4 of 23	©ExxonMobil Development Company	



GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

1.4. ISA–The Instrumentation, Systems, and Automation Society

ISA 5.2	Binary Logic Diagrams for Process Operations
ISA 84.01	Application of Safety Instrumented Systems for the Process Industries

1.5. ISO–International Organization for Standardization

ISO 9000-3	Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001: 1994 to the Development, Supply, Installation and Maintenance of Computer Software
ISO 9001	Quality Management Systems - Requirements

1.6. MIL–Military Handbooks

MIL-HDBK-217F CHG NOTICE 2	Reliability Prediction of Electronic Equipment
-------------------------------	--

1.7. NEMA–National Electrical Manufacturers Association

NEMA MG 1	Motors and Generators
NEMA ICS 6	Industrial Control and Systems Enclosures

2. Definitions

Term	[I] Description
Availability	The statistical probability that the protective system is operational and can properly respond to a process demand at some instant in time. Availability = 1-PFD.
Certifying Authority	An agency such as TÜV (Technischer Überwachungs-Verein (German for Technical Supervisory Association)), that performs safety and inspection testing on equipment that includes safety systems.
Component	Sensors, alarms, cabling, power supplies, discrete solid-state device(s), programmable electronic device(s), relays, current switches, or final elements used in a protective system.
Common cause fault	A single source that causes a failure in multiple elements of a system. The single source may be either internal or external to the system. A common cause failure is the result of a common cause fault.

DNST, CHEM, UPST, DIOL	For ExxonMobil Use Only	Version 1.0.0
Page 5 of 23	©ExxonMobil Development Company	



GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

Term	[I] Description
Control system	A component, group of components or system that controls the process under normal operating conditions. Normal operating conditions can include startup, operation, and shutdown. The control system can perform basic regulatory control, sequential control, batch control, or advanced control.
Diagnostic coverage	The percentage of faults that are detected by built-in test functions or a suitable test program.
Diversity	The existence of different means of performing a function, for example: different technologies, different vendors, independent systems, or independent design teams. The intent of diversity is to eliminate common cause failures.
Electrical protective device	A fuse or circuit breaker.
Final element	A device, such as a valve or motor, used to bring the process to its safe state in response to a signal from the protective system logic. The final element may have devices associated with it, such as solenoid valves, pneumatic components, and actuators.
Ground fault	Any unintentional connection to ground of 6000 ohms or less.
Hazard	A potential source of harm to people, property or the environment.
Initiator	A device, such as a sensor or pushbutton, which causes the protective system to bring the process to its safe state.

DNST, CHEM, UPST, DIOL	For ExxonMobil Use Only	Version 1.0.0
Page 6 of 23	©ExxonMobil Development Company	



Documents

Document Sharing Hub

GP 15-07-02	Protective Systems	January 2002
-------------	--------------------	--------------

Term	[I] Description
Logic	A component or group of components that receives inputs from sensors, performs a predetermined decision-making function, causes final elements to assume a protective position, and provides alarms. Technologies used to implement logic include: - Pneumatic logic (e.g., pneumatic relays). - Electrical logic (e.g., electromechanical relays). - Electronic logic (e.g., solid-state devices). - Programmable Electronic Systems (PES) (e.g., Microprocessor based devices such as Programmable Logic Controllers (PLCs)). Two PES logic configurations are typically used in ExxonMobil for protective systems: 1-o-o-2D redundant.: This uses a dual processor with diagnostics to achieve fault tolerance. Either processor channel can initiate a trip however a diagnosed failure of one processor channel allows the other channel to continue to protect the process for a period of time until the faulty channel is repaired. The required availability and the safety certification of the system set the length of this period. If the faulty channel is not repaired and this period elapses the system initiates a trip. - Triple Modular Redundant (TMR): The TMR system uses three parallel processors to achieve fault tolerance and to execute a 2-o-o-3 function on the output states. Similar considerations apply to the TMR system when it degrades to 1-o-o-2 operation as apply to the 1-o-o-2D redundant system.
Manual initiator	A manually actuated pushbutton or switch which causes the protective system to bring the process to its safe state
Power source	A source of power that is external to the protective system. Examples of power sources are instrument air (pneumatic), hydraulic supply, or electrical power.
Power supply	A device that is internal to the protective system and converts one level of power to another.
Process demand	A process condition or event which requires the protective system to bring the process to its safe state.
Process safe state	The state of the process when the hazard no longer exists.
Probability of Failure on Demand (PFD)	A value that indicates the probability of a protective system failing to respond to a process demand.

DNST, CHEM, UPST, DIOL	For ExxonMobil Use Only	Version 1.0.0
Page 7 of 23	©ExxonMobil Development Company	



Documents

Document Sharing Hub