

Changes shown by ↗

SCOPE

- I ↗ 1.1 This practice covers the **design, installation, and documentation** of protective systems.
- I ↗ 1.2 Mechanical devices used to implement protective functions such as mechanical overspeed trips or relief valves are not covered in this practice.
- I ↗ 1.3 Protective systems for **electrical generation and distribution systems** are not covered by this practice.
- I 1.4 **Power supply** to the protective system **from an external source** (e.g., electrical power, instrument air) is not covered in this practice.
- I 1.5 **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 the vendor or contractor.

SUMMARY OF ADDITIONAL REQUIREMENTS

- I ↗ 2.1 **Table 1** lists the practices and standards which shall be used with this practice. The Design Specification shall indicate which standards are applicable.

TABLE 1

PRACTICES			
IP 3-6-1	Piping for Instruments	IP 15-6-3	Programmable Logic Controllers
IP 3-6-2	Piping at Control and Protective System Valve Stations	IP 15-7-1	Electrical Circuit Design for Instruments
IP 3-12-1	Valve Selection	IP 15-7-3	Alarm Systems
IP 7-2-1	Industrial Boilers	IP 15-9-1	Control Valves
IP 14-3-1	Fireproofing	IP 15-9-2	Motor Actuators for Valves
IP 15-1-1	Instrumentation for Fired Heaters	IP 15-10-1	Field Wiring of Thermocouples and Instruments
IP 15-1-2	Instrumentation for Compressors and Drivers	IP 15-12-1	Instrument Wire and Cable
IP 15-2-1	Temperature Instruments	IP 16-1-1	Area Classification and Related Electrical Design for Flammable Liquids, Gases, or Vapors
IP 15-3-1	Pressure Instruments	IP 16-3-1	Wiring Methods and Material Selection
IP 15-4-1	Flow Instruments	IP 16-8-1	Instrument Power Supply
IP 15-5-1	Level Instruments		
IP 15-6-1	Electronic and Pneumatic Instruments		
IP 15-6-2	Environmental Protection for Instrumentation		
STANDARDS AND SPECIFICATION			
ISA Standards		IEC	
S5.2	Binary Logic Diagrams for Process Operations	812	Procedure for Failure Mode and Effects Analysis
ANSI / ISA		1075	Fault Tree Analysis
S84.01	Application of Safety Instrumented Systems for the Process Industries	1078	Reliability Block Diagram Method
ANSI / NEMA		1131-3	Programmable Controllers - Programming Languages
MG 1	Motors and Generators	61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - All Parts
ICS 6	Enclosures for Industrial Controls and Systems	ISO	
MIL Specification		9000-3	Guidelines for the Application of ISO9001 to the Development, Supply and Maintenance of Software
MIL-HDBK-217	Reliability Assessment of Electronic Components	9001	Model for Quality Assurance in Design/Development, Production, Installation, and Servicing
ANSI / FCI			
70.2	Quality Control Standard for Control Valve Seat Leakage		

DEFINITIONS

- I 3.1 **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.
- I 3.2 **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.
- I 3.3 **Diagnostic Coverage.** The percentage of faults that are detected by built-in test functions or a suitable test program.



IP 15-7-2		Protective Systems	
Page 2 of 9			
Rev. 1	June 1999		

- I 3.4 **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.
- I 3.5 **Electrical protective device.** A fuse or circuit breaker.
- I 3.6 **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.
- I 3.7 **Ground fault.** Any unintentional connection to ground of 6000 ohms or less.
- I 3.8 **Hazard.** A potential source of serious harm to people, property or the environment.
- I 3.9 **Initiator.** A device, such as a sensor or pushbutton, which causes the protective system to bring the process to its safe state.
- I 3.10 **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:
 - ♦ a. **Pneumatic logic.** (e.g., pneumatic relays)
 - b. **Electrical logic.** (e.g., electromechanical relays)
 - c. **Electronic logic.** (e.g., solid-state devices)
 - d. **Programmable electronic logic.** (e.g., Programmable Logic Controllers)
- I 3.11 **Manual initiator.** A manually actuated pushbutton or switch which causes the protective system to bring the process to its safe state.
- I 3.12 **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.
- I 3.13 **Power Supply.** A device that is internal to the protective system and converts one level of power to another.
- I 3.14 **Process demand.** A process condition or event which requires the protective system to bring the process to its safe state.
- I 3.15 **Process safe state.** The state of the process when the hazard no longer exists.
- I 3.16 **Proof Testing.** The process of periodic validation that the protective system is able to respond to a process demand and bring the process to its safe state. Proof testing is performed from initiating sensor to final element. Preventive maintenance is not considered proof testing. The time between proof tests is called the **proof test interval.**
- I 3.17 **Protective system.** A component, group of components, or system that reduces risk by preventing, or mitigating the consequences of hazardous incidents. A protective system responds to a process demand, and brings the process to its safe state. Systems may be either manually or automatically initiated. These systems are also described as Safety Instrumented Systems (SIS). Systems are designated as Protective Systems by Safety or Process specialists.
- I ♦ 3.18 **Protective system failure action.** The resulting action of the protective system upon loss of energy (e.g., electrical power, instrument air), or failure of M-out-of-N voting redundant components. There are two possible protective system failure actions:
 - a. **Fail-Action** (fail-safe or de-energize to trip). Failure or loss of energy or loss of circuit continuity to any protective system or component causing the protective system to take a predetermined protective action and move the process to its safe state. A circuit which is energized and uses closed contacts during normal operation is fail-action.
 - b. **Fail-No-Action** (energize to trip). Failure or loss of energy or loss of circuit continuity to any protective system or component does not initiate any protective action. The protective system may not be able to respond to subsequent process hazards. A circuit which is de-energized and uses open contacts during normal operation is fail-no-action.

- I 3.19 **Qualified Personnel.** Persons who have the specialized knowledge, experience and training to ensure the safe, environmentally sound execution of a project, task or activity.
- I 3.20 **Risk.** The possibility of injury, loss, or environmental incident created by a hazard. The magnitude of risk is a function of the probability of an unwanted incident and the severity of its consequences.
- I 3.21 **Safety Integrity.** The probability of a protective system satisfactorily performing the required protective functions under all stated conditions within a stated period of time.
- I 3.22 **Safety Lifecycle.** The necessary activities involved in the implementation of protective systems, occurring during a period of time that starts at the conceptual phase of a project and finishes when the protective system is no longer available for use.
- I 3.23 **Sensor.** A device that converts physical information such as flow, temperature, level, or pressure, to an electrical or pneumatic signal for input to protective system logic.
- I 3.24 **Validation.** The process of testing the protective system, after installation and integration with field and other devices, to ensure that it meets the Safety Requirements Specification.
- I 3.25 **Verification.** The process of evaluating the protective system design and testing the individual components to ensure that the design requirements are met prior to integration with plant facilities.
- I 3.26 **Voting Redundancy.** A process for making a logical decision based on the output of more than one sensor, actuator, or logic element. **M-out-of-N voting redundancy** (M-o-o-N) requires at least M of the N channels to agree before the protective system can take an action.
- I 3.27 **Watchdog Timer.** A component that causes a programmable electronic device to go to a predetermined state if it is idle or looping endlessly. Watchdog Timers can be **internal** or **external** to the programmable electronic device.

DOCUMENTATION

- I 4.1 **Design documentation** shall include:
 - a. Written description of the system and its operation.
 - b. Block diagram of the system configuration.
 - c. Logic diagrams shall show initiators, final elements and the relationship between them; test and maintenance facilities; operator interface facilities; and interfaces to external devices.
 - d. Listing of the application program, including comment statements (programmable logic only).
 - e. List of input and output connections with tag name and physical address.
 - f. Connection, and interconnection (wiring or pneumatic tubing) diagrams for trouble shooting and maintenance. System components shall be identified by Owner's instrument tag names.
 - g. Hookup installation drawings for sensors and final elements.
 - h. Total equipment list and bill of materials with component vendors and model numbers.
 - i. Vendor's standard documentation, including (but not limited to): specifications, site planning, installation, implementation and operating manuals.
 - j. Recommended spare parts list for 2 years continuous operation.
- I 4.2 **Verification and validation documentation** shall include:
 - a. Verification test procedure(s) and test report(s) (e.g., Factory Acceptance Tests)
 - b. Validation test procedure and test report (e.g., Site Acceptance Test)
 - c. On-line proof testing, and preventative and corrective maintenance procedures
- I * 4.3 The design of all protective systems, including a detailed logic description showing the functions of the system, shall be reviewed and approved by the Owner's Engineer prior to the start of application logic implementation.

BASIC DESIGN

- S ♦ 5.1 The **failure action** of protective systems shall be Fail-Action, unless specified otherwise in the application-specific practices listed in [Table 1](#). Exceptions shall be approved by the Owner's Engineer.
- S,O ♦ * 5.2 Each protective system shall protect a **single piece of process equipment** (e.g., fired heater). Proposals to combine protective system functions for multiple pieces of process equipment in a single protective system are allowed when individual systems are part of a single process unit. These shall be approved by the Owner's Engineer.