Safety Instrumented Systems

Understanding SIS, SIL levels, and safety system security

OT Security Learning Series

Document 040 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Safety Instrumented Systems (SIS) are the last line of defense against catastrophic events in industrial processes. Unlike control systems that optimize production, safety systems exist solely to prevent harm to people, equipment, and the environment.

Safety systems operate independently from basic process control systems (BPCS) and are designed to bring a process to a safe state when dangerous conditions are detected. Understanding these systems is critical for OT security professionals because:

- Compromised safety systems can lead to **loss of life**
- They are explicitly targeted by sophisticated attackers (e.g., TRITON malware)
- Security measures must not compromise safety functionality

2 Safety vs Control Systems

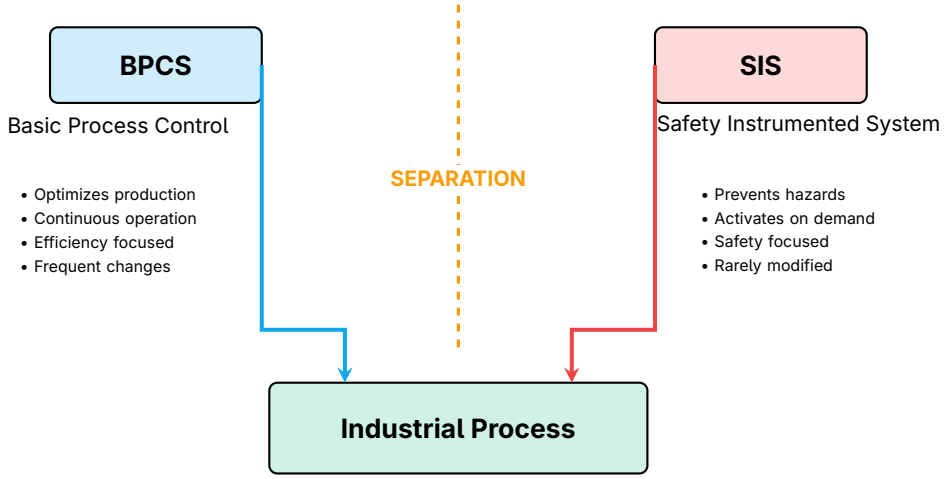

Figure 1: BPCS vs SIS: Separate Systems with Different Objectives

Key Principle: Independence

Safety systems must be **independent** from control systems. A failure in the BPCS should not affect the SIS, and vice versa. This separation extends to:

- Hardware (separate controllers, I/O, power supplies)
- Software (different logic solvers, no shared code)
- Networks (physically or logically separated)
- Personnel (different teams for engineering and maintenance)

3 SIS Components

A Safety Instrumented System consists of three main elements that form a Safety Instrumented Function (SIF):

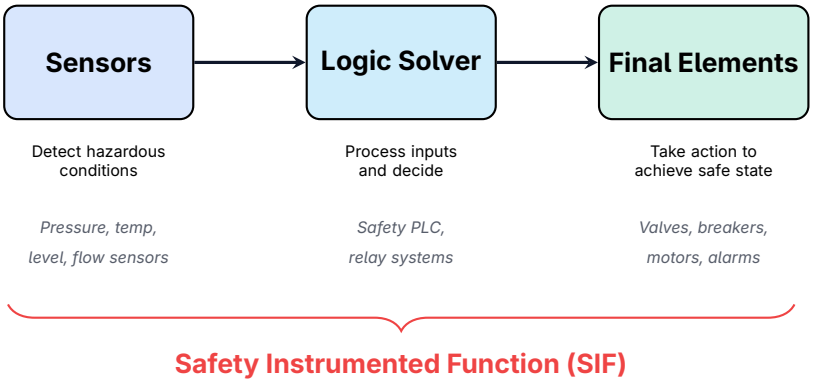

Figure 2: Components of a Safety Instrumented Function

3.1 Sensors

Safety sensors detect process variables that indicate hazardous conditions:

- High pressure, temperature, or level transmitters
- Gas detectors (toxic, combustible)
- Flame detectors, smoke detectors
- Emergency stop buttons (E-stops)

3.2 Logic Solver

The logic solver evaluates sensor inputs and determines when to activate final elements:

- **Safety PLCs** – Purpose-built controllers certified for safety applications
- **Relay systems** – Traditional hardwired logic (still used in simple applications)
- **Safety controllers** – Integrated systems from safety vendors

3.3 Final Elements

Final elements take physical action to achieve a safe state:

- Emergency shutdown valves (ESV)
- Motor trip relays
- Circuit breakers
- Audible/visual alarms

4 Safety Integrity Levels (SIL)

Critical

Safety Integrity Levels (SIL) define the required reliability of safety functions. Higher SIL levels require more rigorous design, testing, and maintenance to achieve lower probability of failure.

SIL	PFD Range	Risk Reduction	Typical Application
1	10^{-1} to 10^{-2}	10 to 100	Low-risk processes
2	10^{-2} to 10^{-3}	100 to 1,000	Standard chemical plants
3	10^{-3} to 10^{-4}	1,000 to 10,000	High-hazard processes
4	10^{-4} to 10^{-5}	10,000 to 100,000	Nuclear (rarely used)

Table 1: Safety Integrity Levels (PFD = Probability of Failure on Demand)

4.1 Achieving Higher SIL

Higher SIL levels are achieved through:

- **Redundancy** – Multiple sensors, logic solvers, or final elements (1oo2, 2oo3 voting)
- **Diversity** – Different technologies or manufacturers
- **Diagnostics** – Self-testing and fault detection
- **Proof testing** – Regular functional testing
- **Certified components** – Hardware/software certified to target SIL

5 Relevant Standards

Standard	Scope
IEC 61511	Process industry functional safety
IEC 61508	General functional safety (basis for sector standards)
IEC 62443	Industrial cybersecurity (includes SIS considerations)
ISA 84	US adoption of IEC 61511
NFPA 85	Boiler and combustion systems
API 556	Fired heaters in refineries

Table 2: Key Safety System Standards

6 Security Threats to Safety Systems

Warning

TRITON/TRISIS (2017): The first known malware specifically designed to attack safety instrumented systems. It targeted Schneider Electric Triconex safety controllers at a petrochemical facility, attempting to disable safety functions that could have enabled a catastrophic release.

6.1 Attack Scenarios

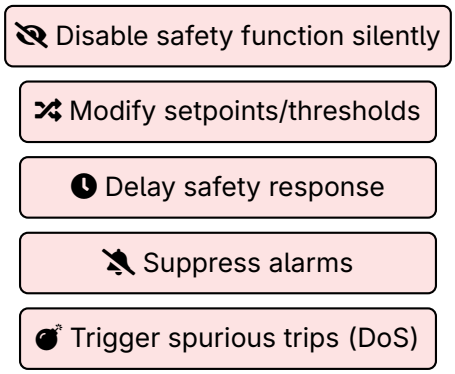

Figure 3: Potential Attack Scenarios Against Safety Systems

6.2 Why SIS is Targeted

- **Catastrophic impact** – Disabling safety enables physical destruction
- **Trusted status** – Safety systems are often less monitored
- **Rare changes** – Infrequent updates make anomalies harder to detect
- **Specialized knowledge** – Fewer defenders understand safety systems

7 Security Best Practices

Key Point

Defense in Depth for SIS:

- Maintain physical and logical separation from BPCS
- Implement strict access control (physical and logical)
- Monitor for unauthorized changes and anomalies
- Include SIS in security assessments and incident response plans
- Ensure security measures don't compromise safety functionality

7.1 Network Segmentation

- SIS should be on a **separate network** from BPCS
- Use firewalls with strict allowlists between zones
- Consider **data diodes** for one-way data flow out of SIS
- Disable unnecessary communication protocols

7.2 Access Control

- Restrict physical access to SIS cabinets and engineering stations
- Use key switches or hardware write-protect for logic changes
- Implement role-based access with strong authentication
- Log all access attempts and configuration changes

8 Summary

Key Takeaways

- **SIS protects lives** – Safety systems prevent catastrophic events
- **Independence is critical** – SIS must be separate from BPCS
- **SIL defines reliability** – Higher SIL = more rigorous requirements
- **TRITON proved the threat** – Nation-state actors target safety systems
- **Security supports safety** – Protection measures must not compromise safety
- **Defense in depth** – Layers of network, access, and change controls

9 Further Reading

Standards and Guidelines

- **IEC 61511** – Functional safety for process industries
  https://webstore.iec.ch/publication/5526
- **IEC 62443-4-2** – Technical security requirements for IACS components
  https://webstore.iec.ch/publication/34421

Resources

- **CISA – TRITON Malware Analysis**
  https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a

- **Dragos – TRISIS Analysis**
  https://www.dragos.com/resources/whitepaper/trisis-analyzing-safety-system-targeting-malware/

Books

- Gruhn, P. & Cheddie, H. – *Safety Instrumented Systems: Design, Analysis, and Justification* (ISA)
- Smith, D. & Simpson, K. – *Safety Critical Systems Handbook* (Elsevier)

Part of the OT Security Learning Series