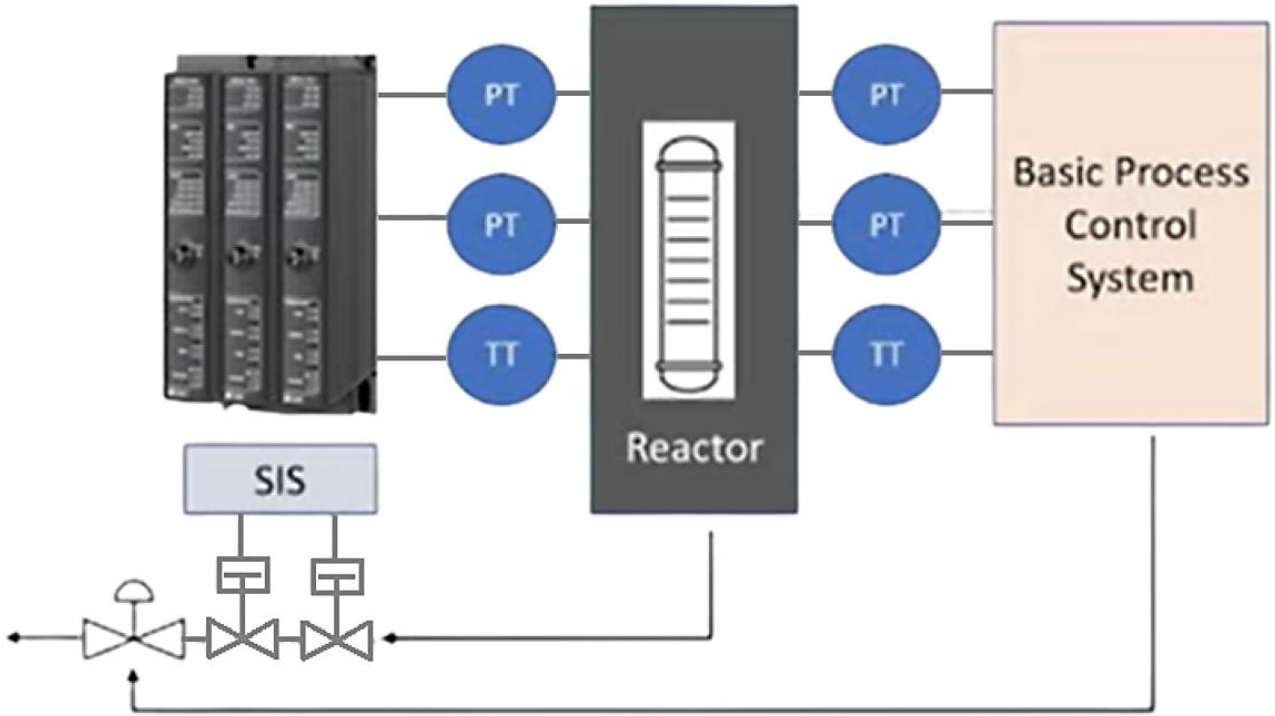
PROJECT
ENG
PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

Safety Instrumented Systems (SIS) Overview

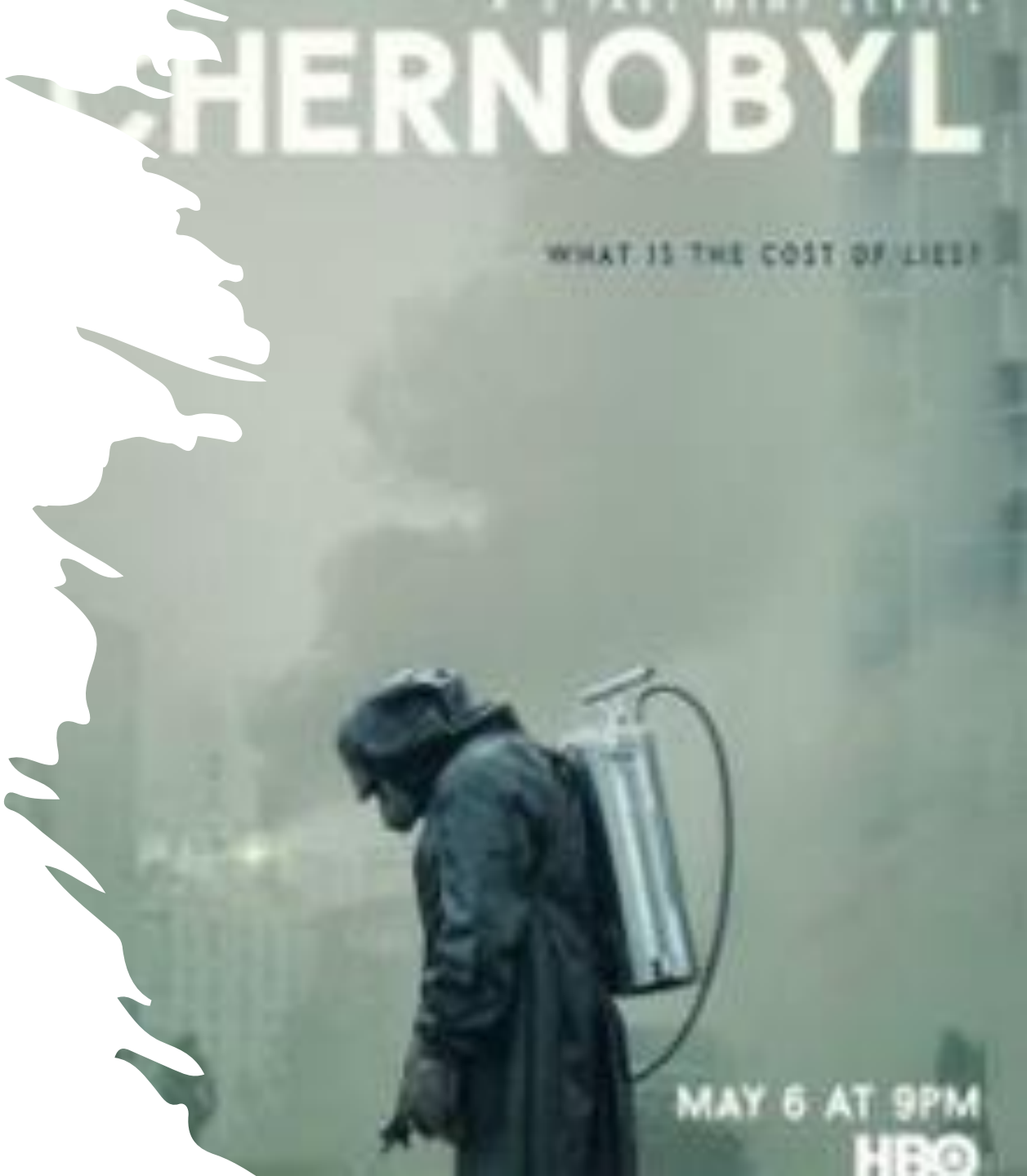


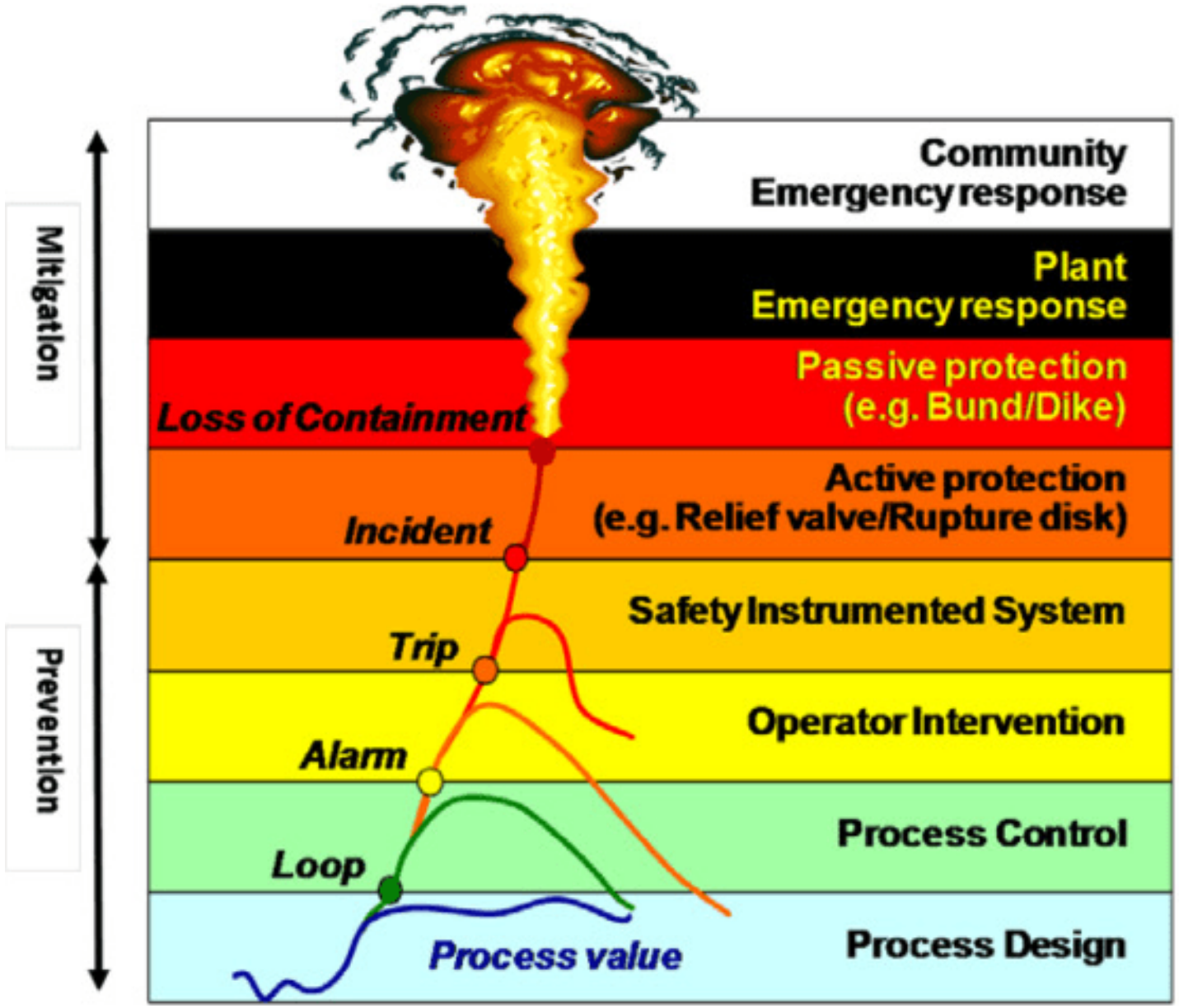
What is SIS? SIS stands for Safety Instrumented System. These systems are the unsung heroes of industrial safety, designed to reduce the likelihood or consequences of hazardous situations by bringing the system to a safe state when needed.

Why are SIS Necessary?

In industries like oil and gas or chemical production, there are critical processes and systems that, if something goes wrong, can result in catastrophic consequences. Think of a sudden pressure surge in a chemical reactor or a leak in a high-pressure gas pipeline. In such situations, you need a fail-safe mechanism to step in and mitigate the risks.

Chernobyl



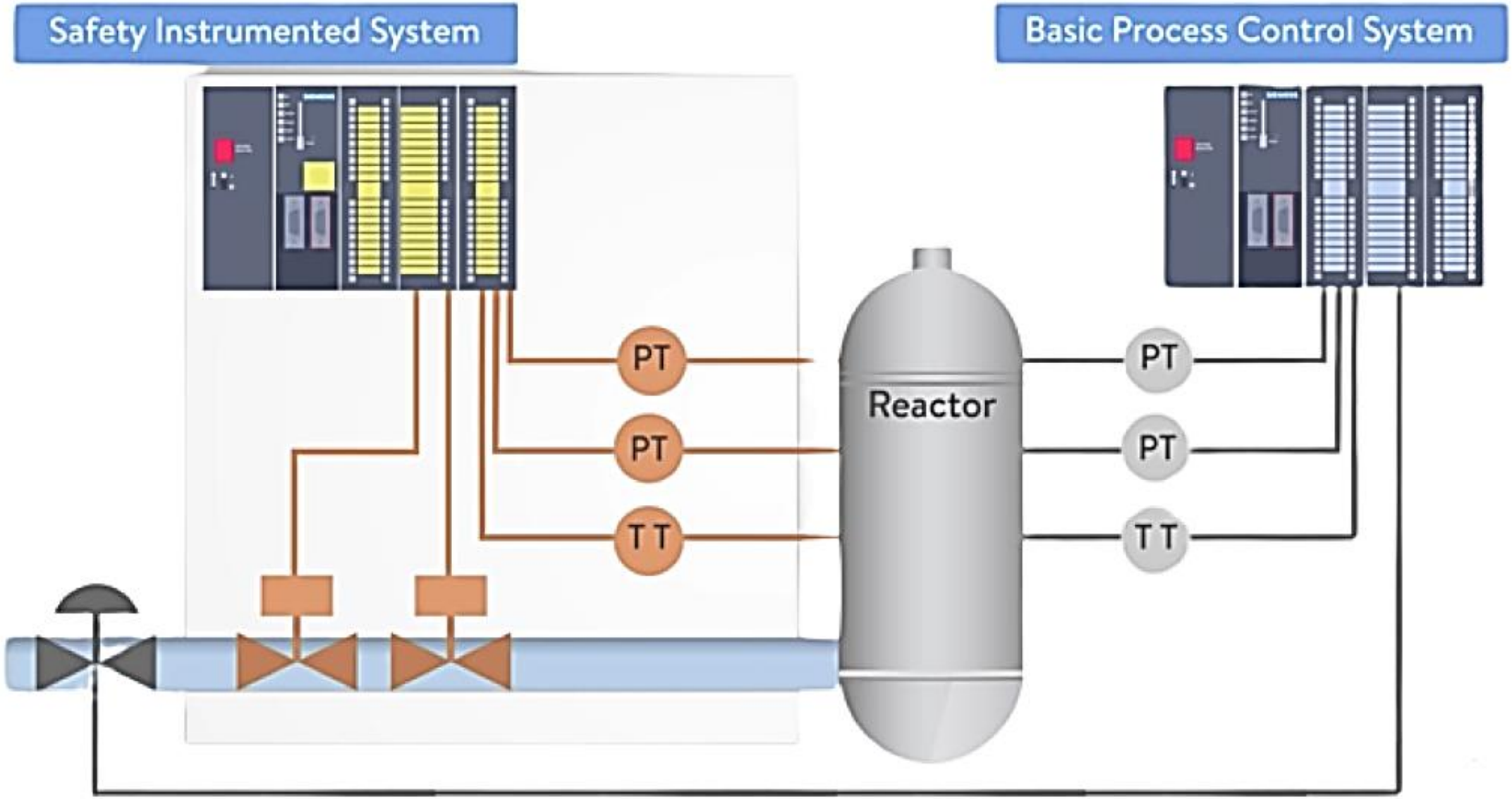


How SIS works

In order to minimize these risks, process control systems are installed to maintain a safe operation of the plant, assisted by a robust alarm detection and reporting system, and operated by trained, qualified personnel.

But often, these measures alone cannot reduce the risk of injury, fire, explosion, or other risks to a tolerable level.

Regardless of the types of risks, the process design itself, the basic process control system, alarms, and operator intervention, provide the first layers of protection for the process.

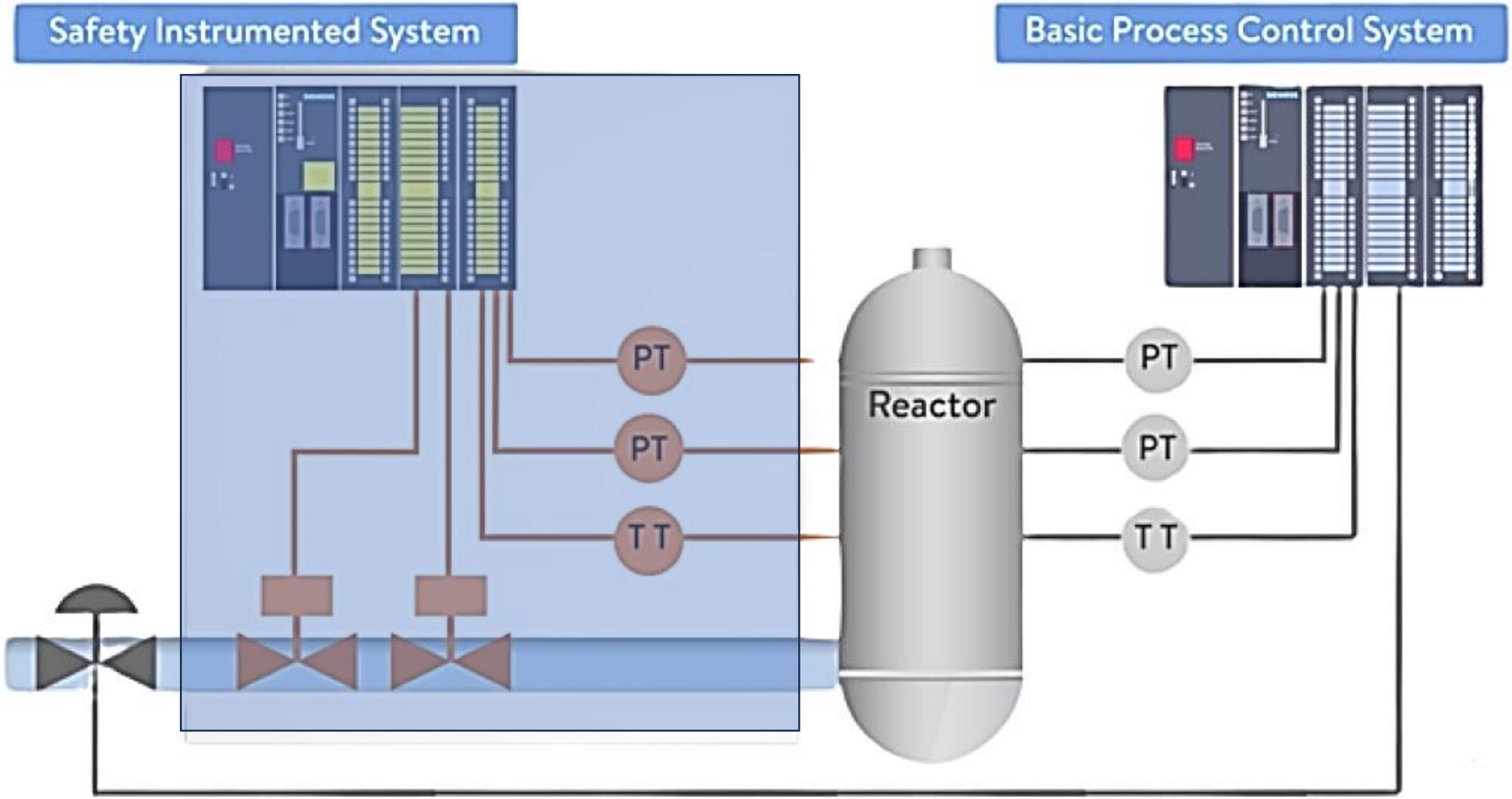


EMERSON

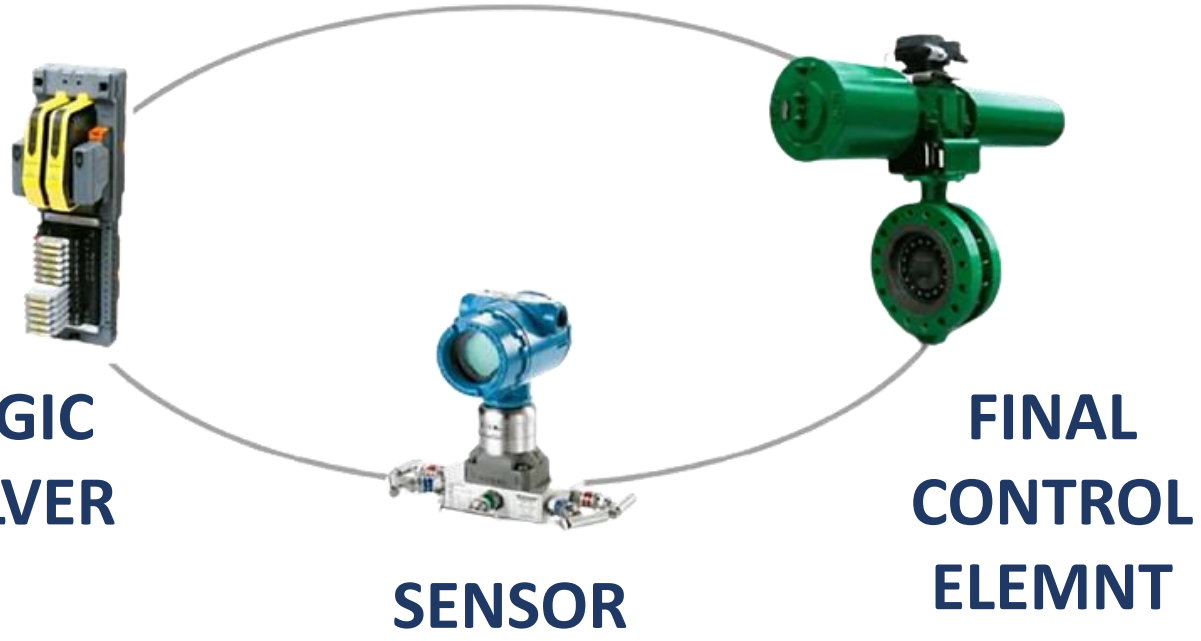
Schneider Electric

SIEMENS

Safety Instrumented Systems (SIS) Providers



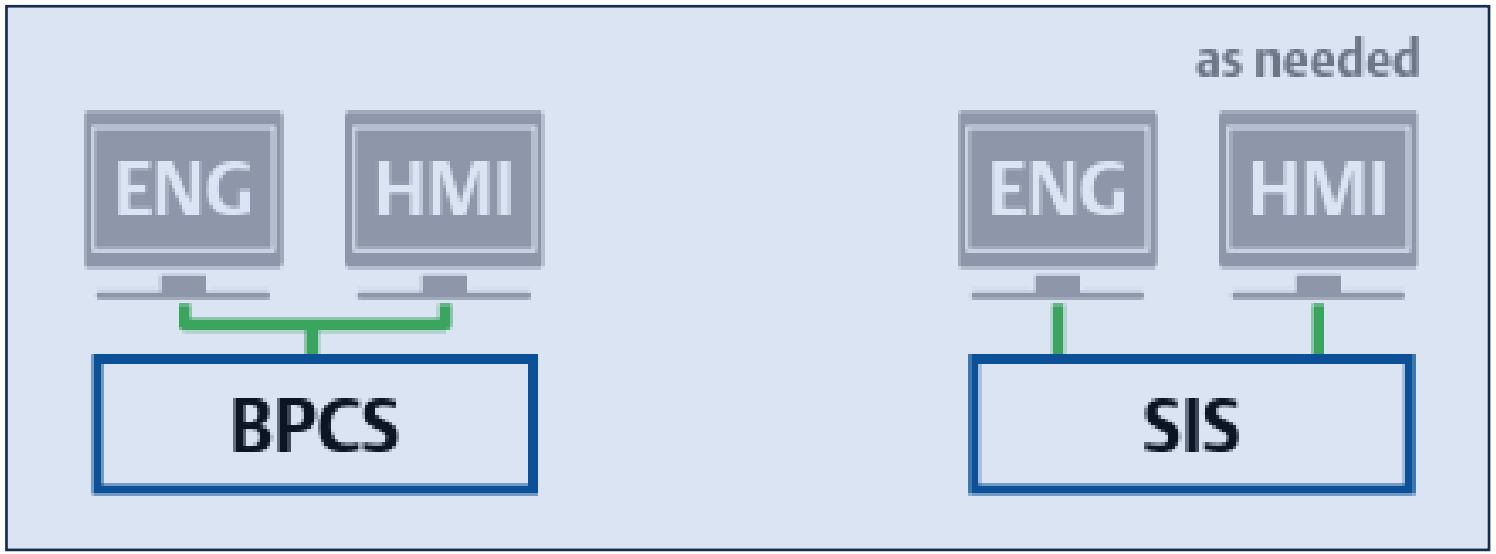
Components of an SIF

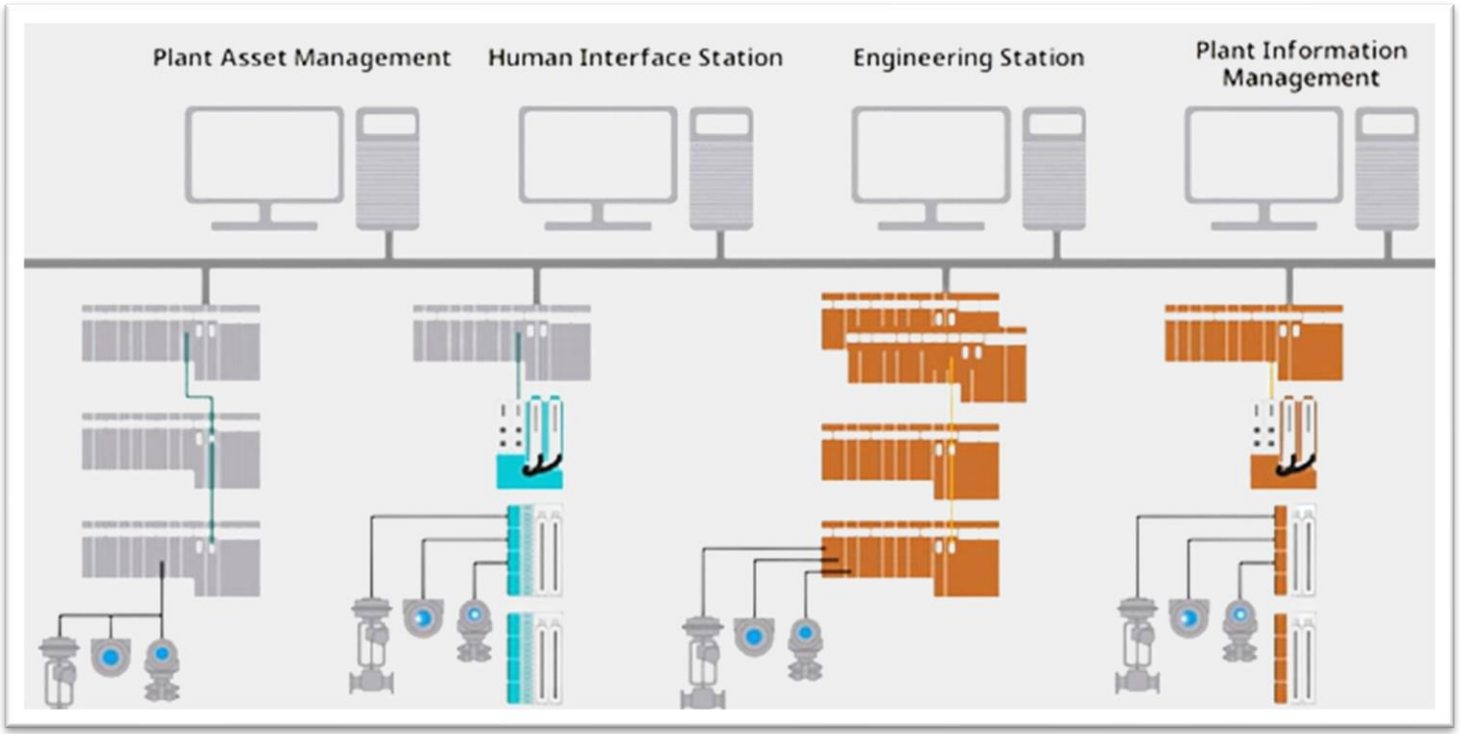


SIS Independence

Safety Instrumented Systems (SIS) are intentionally designed to be independent of the basic process control systems (BPCS) for several crucial reasons:

1.Isolation from BPCS Failures
2.Redundancy and Reliability
3.Different Purposes
4.Standards and Regulations



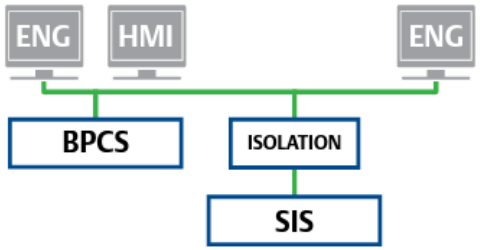


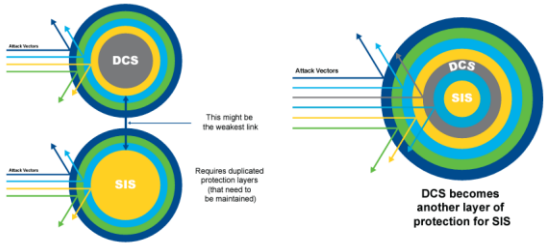
Air Gapping

Safety Instrumented Systems were often designed to operate independently and were physically and logically separated from the BPCS. Some facilities even implemented air gaps, which means there was no direct network communication between the SIS and BPCS. This separation was primarily for safety and security reasons, as it minimized the risk of unintended interactions or cyber threats compromising safety.

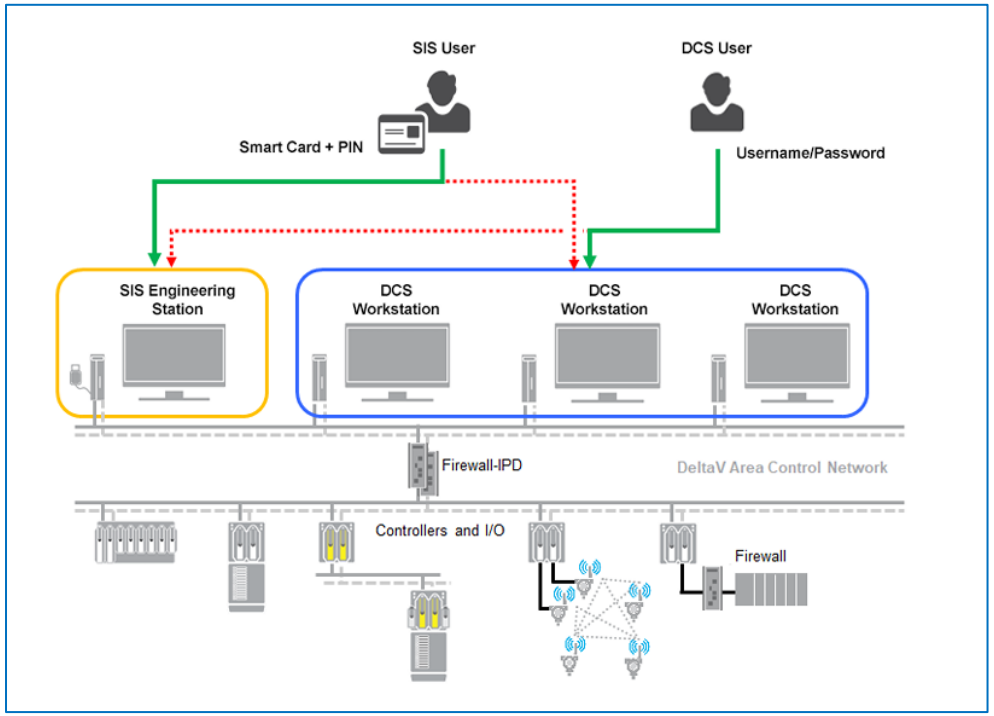
Integrated Control and Safety Systems (ICSS)

Modern Integrated Control and Safety Systems (ICSS): Integrated Control and Safety Systems (ICSS) represent a significant advancement in process control and safety technology. ICSS solutions, like the one offered by Emerson, combine the functionalities of both BPCS and SIS within a single integrated platform. Here are key features of ICSS:





SIS Systems Cybersecurity



Cybersecurity for SIS Systems:
Safeguarding Safety Instrumented Systems (SIS) is critical. These systems are prime targets for adversaries due to their importance. To protect SIS:

1.Assess Risks

2.Segmentation

3.Access Control

4.Patching

5.Network Security

6.Continuous Monitoring

7.Policies

8.Vendor Collaboration

9.Incident Response

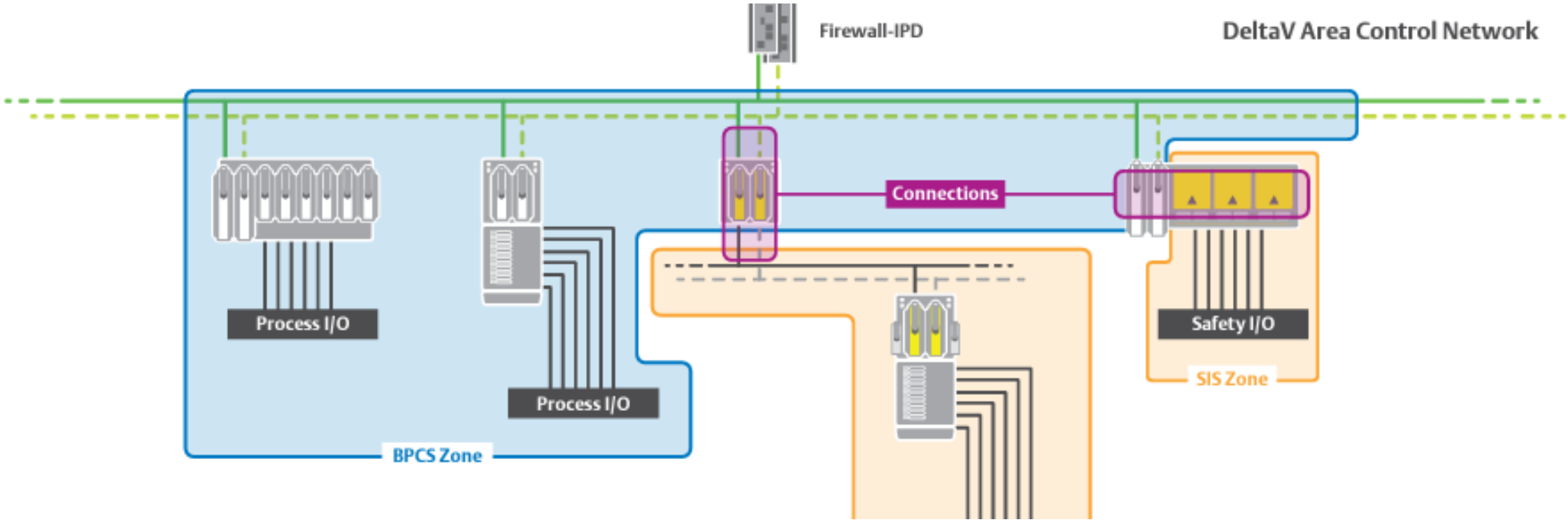
10.Compliance

11.Training

12.Redundancy

13.Anomaly Detection

14.Audits.



SIS Systems Cybersecurity

Cybersecurity for Safety Instrumented Systems (SIS), includes some important measures:

1.Air Gapping
2.Physical Access Controls
3.Vendor-Provided Cybersecurity Solutions
4.Cybersecurity Image Implementation
5.Log Collection for Non-Repudiation

Wrap Up