Demonstrating separation and independence of automated systems

Angela E. Summers, PE, PhD
President
SIS-TECH Solutions, LP

Eloise Roche, CFSE
Senior SCAI Consultant
Eloise Roche
Senior SCAI Consultant
SIS-TECH Solutions

• 24 years Chemical Industry background, largely in automation and functional safety management

• Specializes in Safety Controls, Alarms, and Interlocks (SCAI)

• Member of ISA-84 committee and multiple working groups

• Subcommittee Member for revision of “Guidelines for Safe Automation of Chemical Processes”

• Certified Functional Safety Expert
Demonstrating separation and independence of automated systems

Angela E. Summers, PE, PhD  
President  
SIS-TECH Solutions, LP

Eloise Roche, CFSE  
Senior SCAI Consultant
Independence and Separation
Theoretical World

Control

Clear and understandable to everyone

Safety
Automation Network

[Figure 3.8 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Overall Control System

[Figure 4.1 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Independence

• Core attribute of a protection layer, in which the performance of the protection layer is not affected by the initiating cause of a loss event or by the failure of other protection layers.
  – CCPS, Guidelines for Initiating Events and Independent Protection Layers
Separation

- Use of physical and functional means to achieve independence.
  - Physical separation - uses dedicated equipment

2 clear and unambiguous zones
Separation

– Functional separation - uses engineered means and administrative controls to assure independent operation.
  • For example, a shared network results in both systems being managed as a single security zone.

![Diagram showing separation of control and safety systems with a firewall between them.](image)
Achieving independence

• Likelihood of ______ is sufficiently low compared to the performance requirements.
  – common mode, common cause, and dependent failures between layers
  – systematic errors throughout the lifecycle
Dependency Analysis

• Demand scenarios:
  – control failures
  – human error
  – cyber attacks
  – access security violations

• Dependencies:
  – common technologies, manufacturers, operating environment
  – common operations, maintenance, inspection or test activities
  – common proof test procedures and proof test times
Graphic Disclaimers

• Do not illustrate all possible combinations of architectures that are acceptable or unacceptable.

• Do not address field device sharing, although the principles described are still applicable.

• Do not address the design and management of wireless technology in safety applications as the process sector is still gathering prior use data in control and monitoring applications.

• Do not show the secure gateway (or firewall) necessary to protect Level 1 from Level 2 and higher attacks.
Air Gapped Systems

- No permanent digital connection between SCAI and rest of IACs network
  - No remote access capability to SCAI
- Most inherently secure SCAI zone architecture
  - Least convenient architecture for data acquisition or upgrade support
- Guard against mobile devices/mobile code and access to HMIs/workstations
  - Restrict hardwired communication to specific SIS I/O points and error check the incoming signal.

[Figure 3.10 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Interfaced Systems

- Permanent digital connection between the communication modules (e.g., serial or ethernet)
  - COM-COM links are usually very constrained in format and not capable of transmitting mobile code or instructions which could result in loss of SCAI controller
  - Restrict writes to SIS to specific I/O points and memory locations and error check the incoming signal.

- Loss of communication should not impact SCAI functionality.
  - Firewall should support point-to-point authentication, use controls, avert overloading the COM module, etc.

[Figure 3.12 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Integrated with Isolated Networks (2 zone)

- Permanent digital connection between network switches (COTS)
  - Vulnerability to the broad range of threats which can be made through network
- Network to network (Level 2) allows safety data to be accessed using common IT switch communication systems.
  - Strong controls are needed at switch and firewall to perform the broad range of countermeasures needed to secure SCAI portion of network
- Safety data should never be transmitted to SCAI logic solver via network.

[Figure 3.14 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Integrated with Shared Network
(1 zone)

- Single digital network shared between process control and SCAI
  - Can no longer sever network communications to SCAI controller without losing SCAI HMI (safety alarms)

- Network connection (Level 2) allows safety data to be accessed using common IT switch
  - Strong controls are needed at switch and firewall to support needed countermeasures
  - Safety data should never be transmitted to SCAI logic solver via network.

1 security zone

[Figure 3.16 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Shared PCN and I/O Bus (1 zone)

- Often the controllers in this architecture are of identical technology (vulnerable to identical attack) and may share engineering workstation.
- Can no longer sever network communications to SCAI controller without losing SCAI HMI and engineering workstation.
- Shared “safety” databus carries signals to and from the field devices.
  - Shared I/O network creates additional vulnerabilities for Safety Controls and Safety Interlocks, as well as Safety Alarms.
  - Restrict data flow from process control logic solver to SCAI logic solver using databus.

[Figure 3.17 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Combined System (1 zone)

- Systems are no longer independent and separate by design.
- Shared “safety logic solver” designed and managed as a safety system.
- Use physical means to limit ability to make process control and SCAI program changes from the network.

[Figure 3.19 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]
Understanding Dependence

• Challenges to independence are often underappreciated in the functional specification.

• As protection layers are collapsed through sharing or become more interconnected:
  – **Substantial complexity is added to:**
    • Assuring integrity and reliability
    • Assuring robust access security
    • Preventing human error propagation to multiple layers
    • Controlling changes and validating after change
    • Executing maintenance and testing
    • Maintaining audit trails
Design for Independence

• Use dedicated software and hardware
  – For equipment approved for both control and SCAI, functional separation should be sufficient that a failure of the control system does not cause a failure of the SCAI.

• Use secured connections

• Use separate databases

• Use separate configuration, engineering software tools, and engineering workstations
Design for Independence

• Use administrative controls and physical barriers to reduce cyber and other security vulnerabilities

• Use administrative controls and management of change to assure configuration and version management
Questions?

Thanks.