



# Digital I&C Cyber Research Test-bed at CAER: NRC Cyber Security Workshop 5/29/2013

Carl Elks, University of Virginia  
Department of Electrical and Computer Engineering  
[cre4g@virginia.edu](mailto:cre4g@virginia.edu)

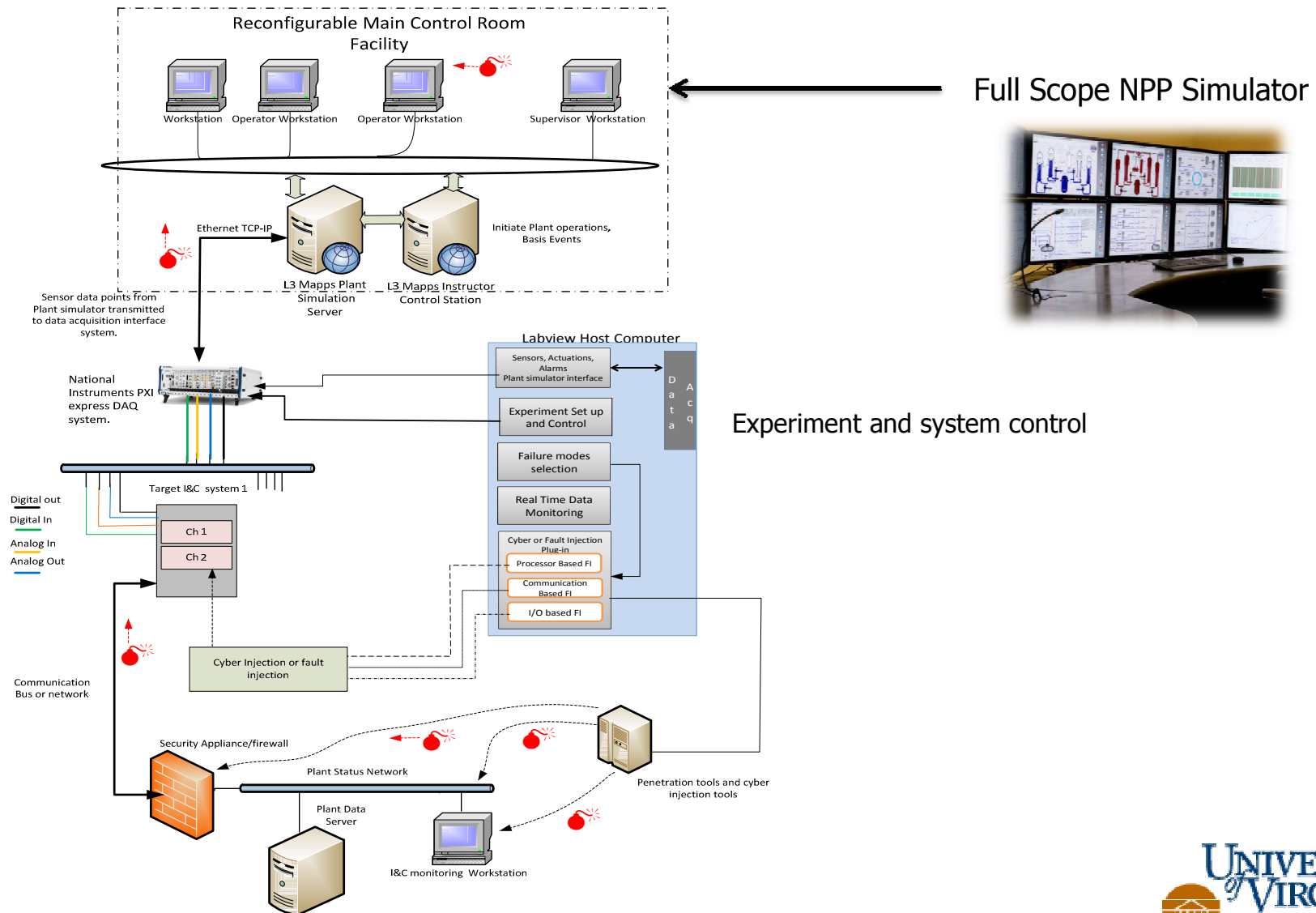
# Purpose of the CAER/UVA I&C Test-Bed Facility



- ▶ To promote better understanding of comprehensive security practices of highly integrated I&C systems.
- ▶ Obtain deep knowledge about integrated plant and I&C Interactions in the presence of cyber events and anomalies.
- ▶ A test bed for conducting applied research with respect to compliance of NRC cyber security regulations and standards.
- ▶ Explore emerging integrated safety and security methods for building resilient I&C systems.



# Architectural Layout of DI&C Lab at CAER



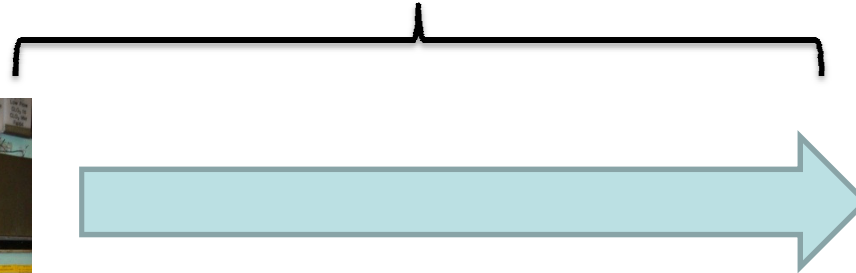
# Evolution of I&C at NPP

## Hardwired Control



- Analog and Relays
- Push Buttons
- Single Loop Controls
- Stand Alone
- No Networks
- No inter-communication between systems

80% of current operating systems



## First Generation Digital



- Serial bus connections between systems
- Industrial based PC's...
- Proprietary OS
- Mimic Hardwired control systems

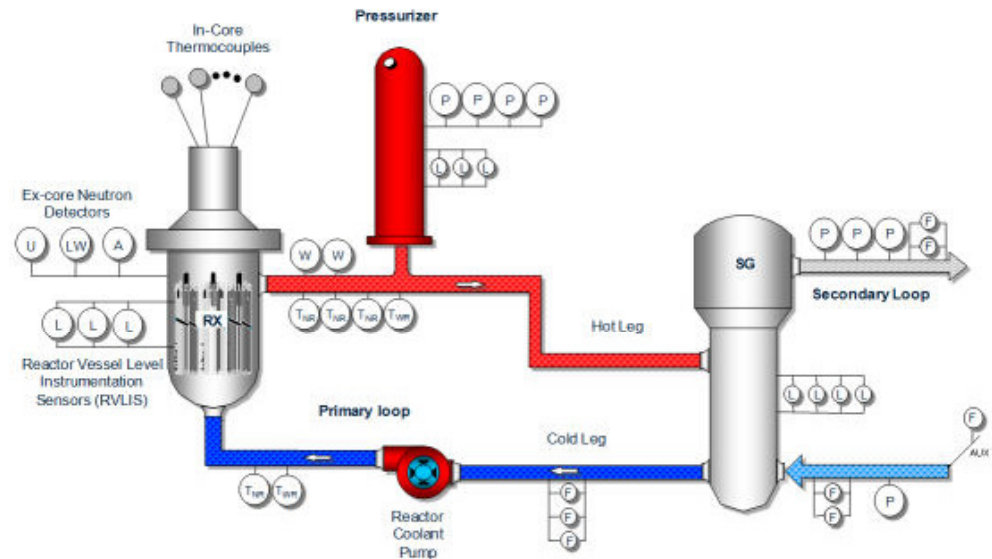
## Modern I&C



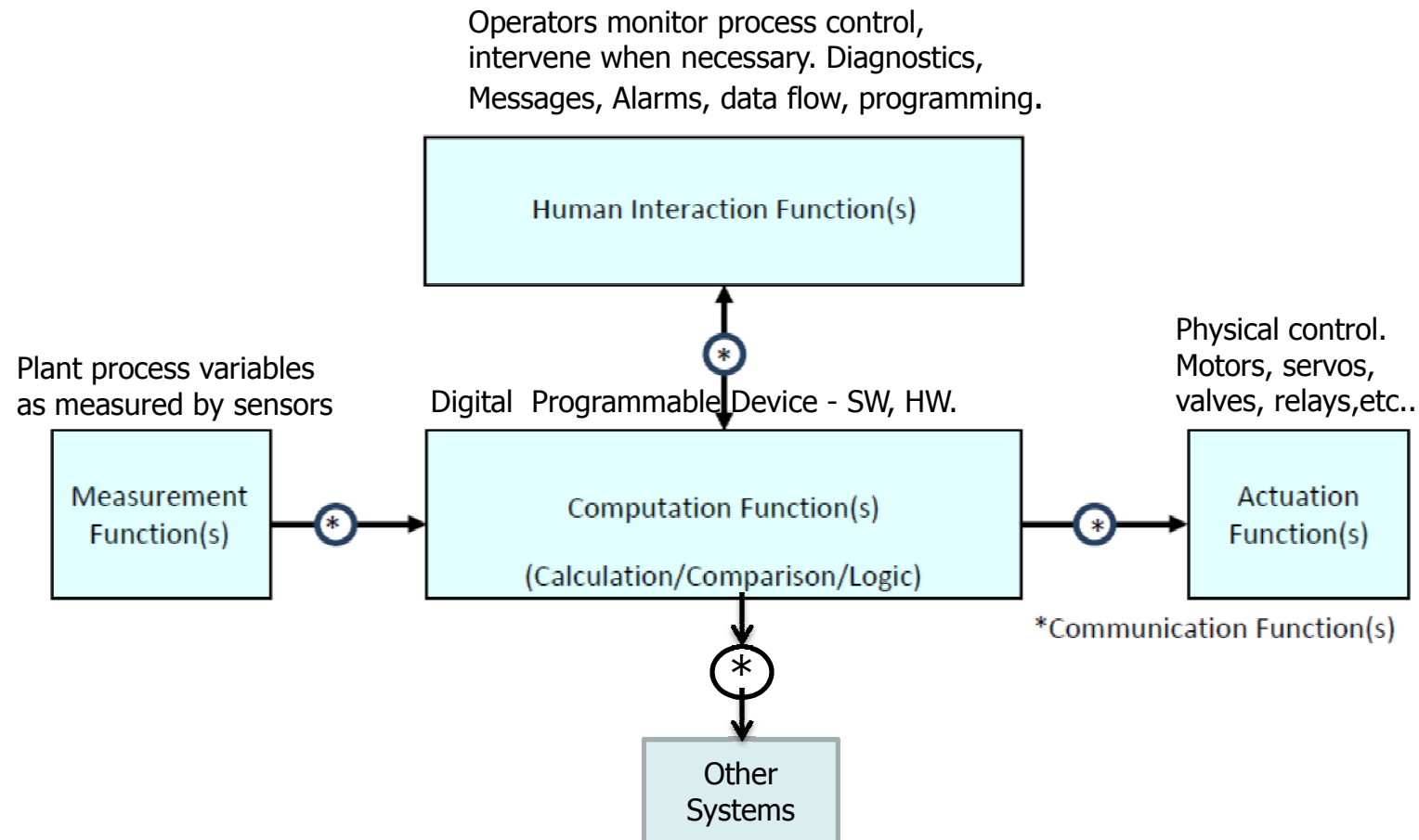
- I/O – Industry Process control networks – Profibus, Modbus...
- Intra system communications - Ethernet
- A mix of proprietary and commercial system software
- Configurable to specific plant layouts
- Computer display based Human Machine Interface
- Highly integrated control room functions

# Instrumentation and Control Systems (I&C)

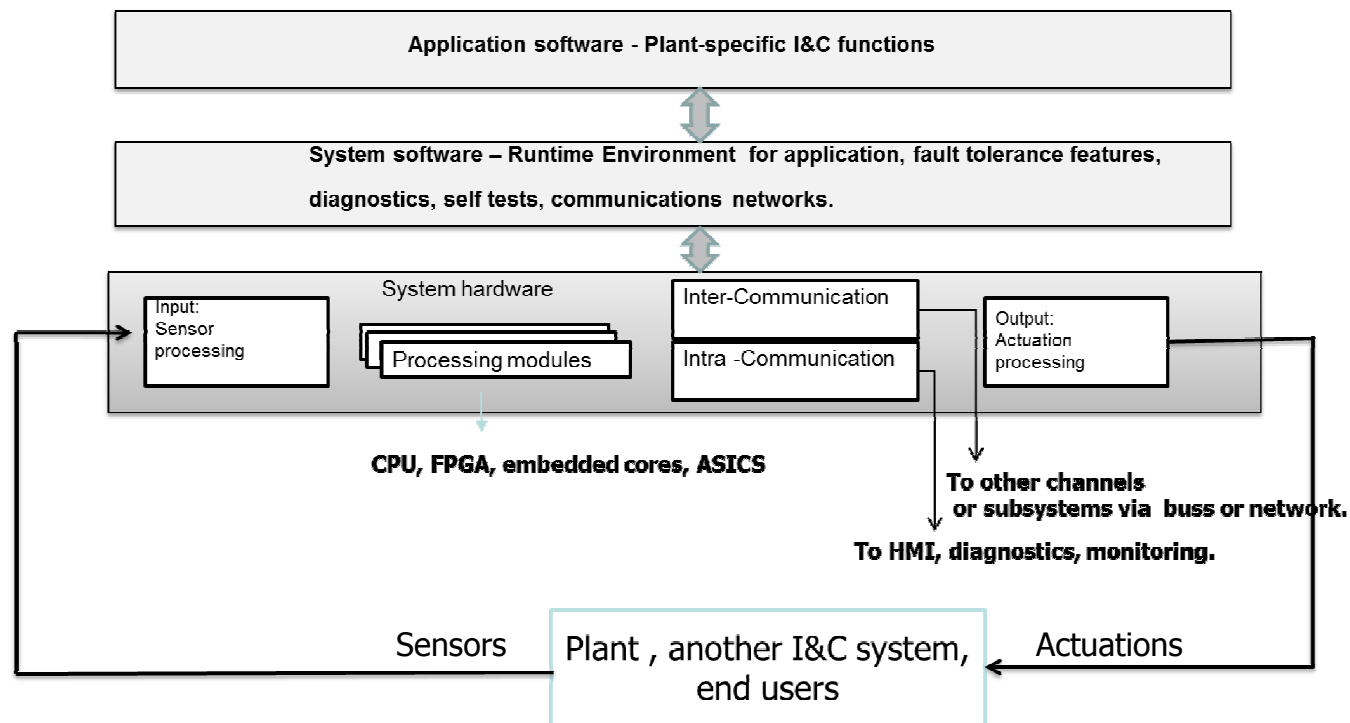
- Among the thousands systems and sub-systems that comprise a nuclear power plant, the system class relied upon most for protection, control, monitoring, and supervision is Instrumentation and Control (I&C) system.
- Behind the reactor, probably the most important system in the plant.
- I&C versus Supervisory Control and Data Acquisition (SCADA)
- Nuclear I&C is distinguished by demanding safety and reliability requirements. *Regulatory driven technology.*



# Simple I&C Functional Representation



# Modern Digital I&C Platform Architecture



# I&C, SCADA, and DCS: Differences and Similarities

- We often hear terms I&C, SCADA, and DCS used interchangeably.
- The difference between SCADA, I&C and DCS are blurring rapidly with advanced process control technology, but some subtle points to help distinguish.
- **I&C** is usually distinguished by very high reliability, availability, or safety requirements which tend to drive the architectures toward enhanced fault tolerance operations, modular redundancy, and diversity. Single level control - One control function one I&C system. Nuclear, Plant Process Automation.
- **SCADA** systems consist of a network of either hardwired or wireless RTUs, PLC's which perform subordinate control functions to a supervisory control system located at control room. Data is transmitted in real-time to the central location. Supervisory control functions are enabled at the central station. Multi-level control. Also, it is common to have large geographical separation between supervisory controller and subordinate controller – Power grid, oil and gas...
- **DCS** – Very similar to SCADA, Multi-level control, networked controllers. High level controllers send high level commands to low level controllers over a network. More interactions between controllers. Redundant systems, High Reliability, Safety. Avionics, Flight Control systems, advanced process control plants.

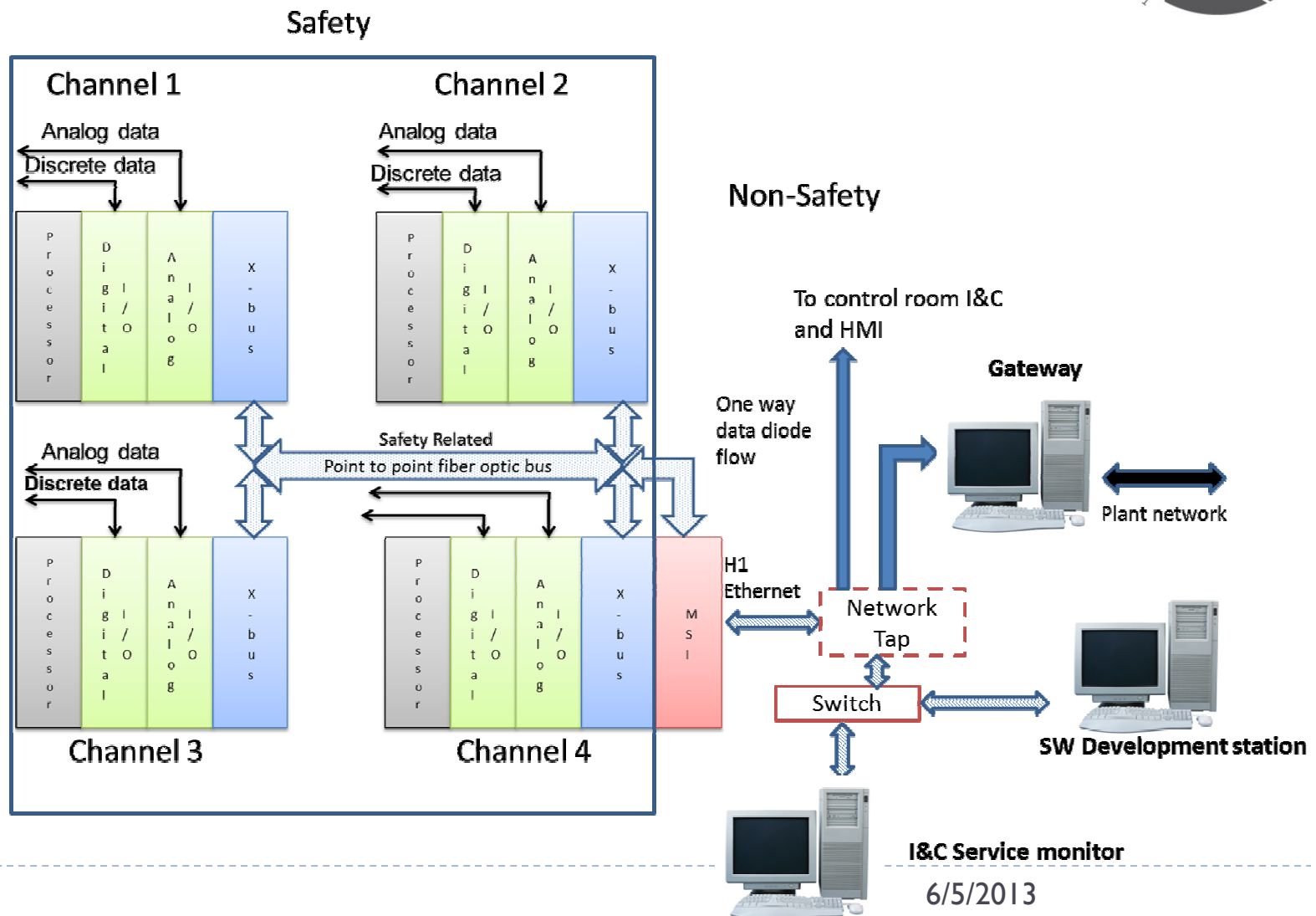


# Introduction to the CAER Safety Grade I&C Benchmark System

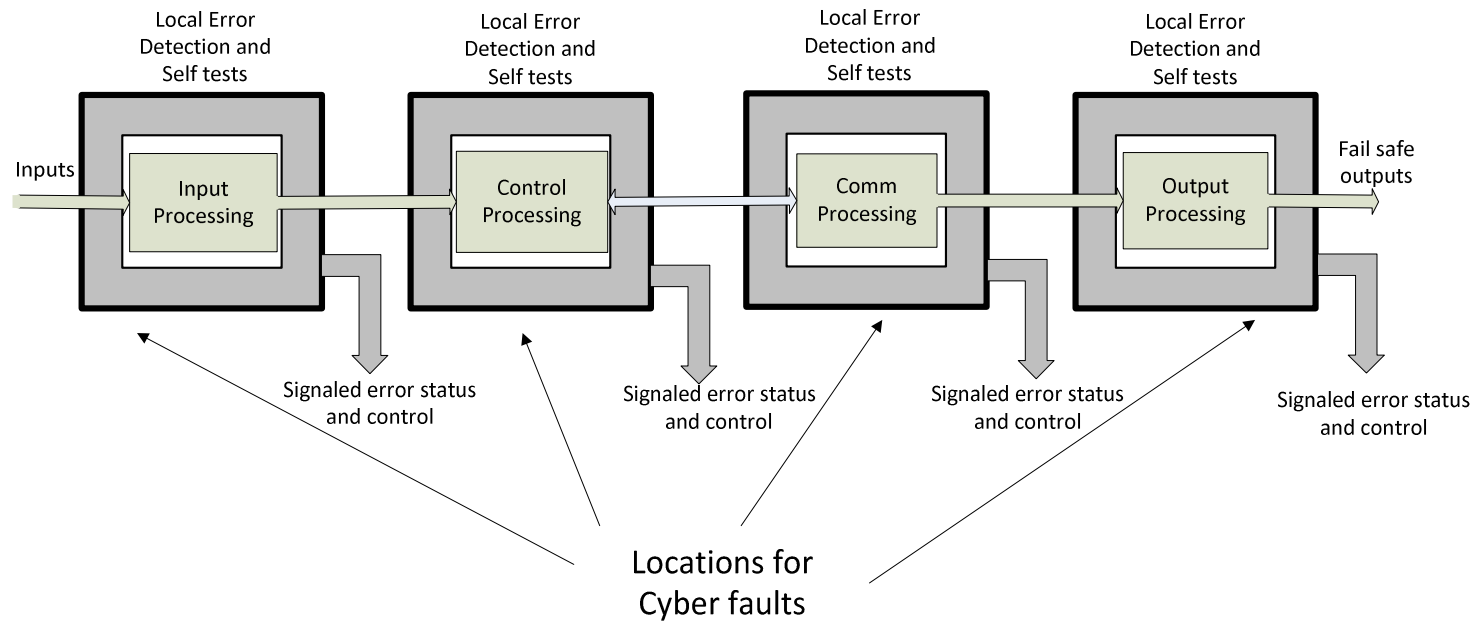


- ▶ **Key Features:**
  - ▶ A safety critical I&C architecture.
  - ▶ Processing and communication redundancy to improve fault tolerance to faults/failures.
  - ▶ Voting architecture provides ability to sustain operations in the presence of faults.
  - ▶ Extensive self-diagnostics to detect latent faults.
  - ▶ Real time deterministic processing.
  - ▶ Configured to emulate a 2-out-of-4 voting scheme –Typical of Reactor Protection Systems.
  - ▶ Can be configured for other applications.
  - ▶ Donated by NRC to CAER for I&C research.

# Basic Architecture of Benchmark I&C System

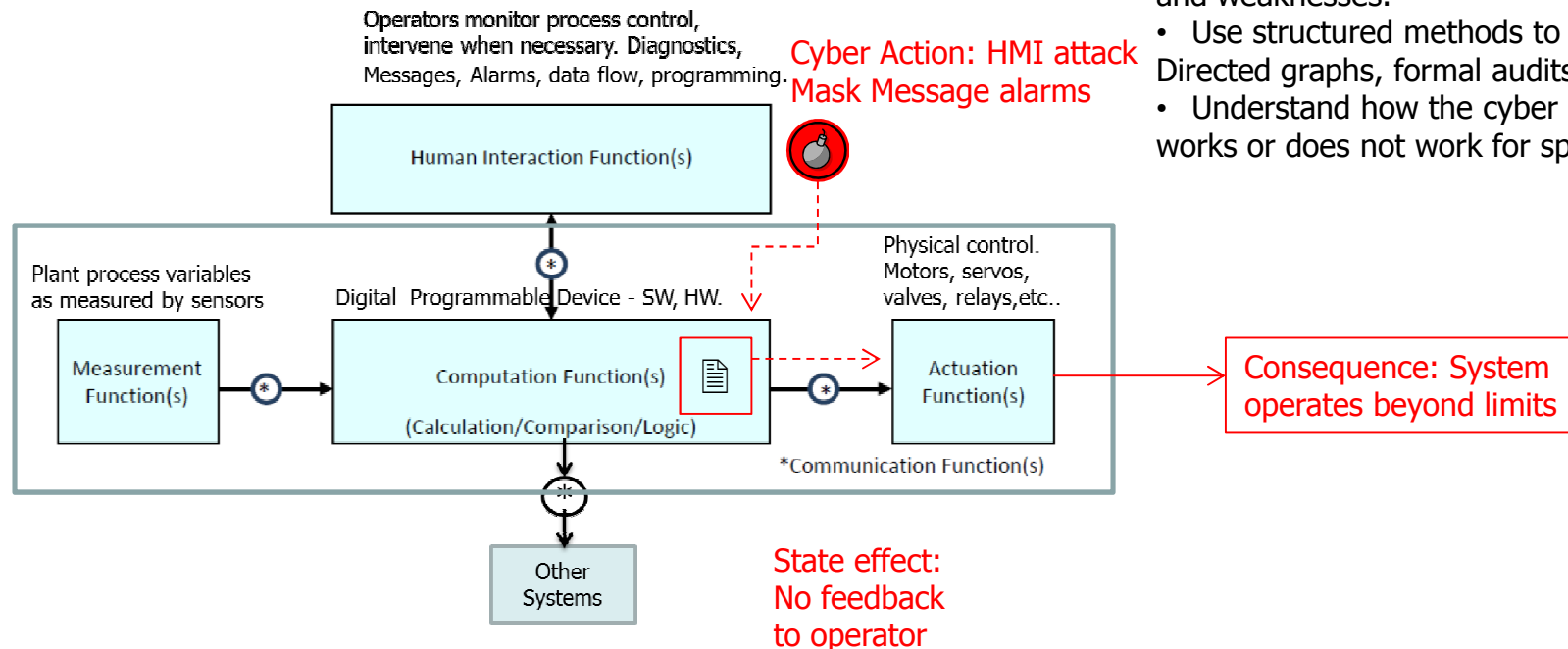


# 1 Channel of Processing



# Looking at the system with cyber-security glasses

- Understand the importance of system interactions both implicit and explicit.
- Use simple diagrams to understand how functions relate.
- Reason about vulnerabilities and weaknesses.
- Use structured methods to access: attack trees, Directed graphs, formal audits, experts, etc..
- Understand how the cyber perimeter works or does not work for special cases.

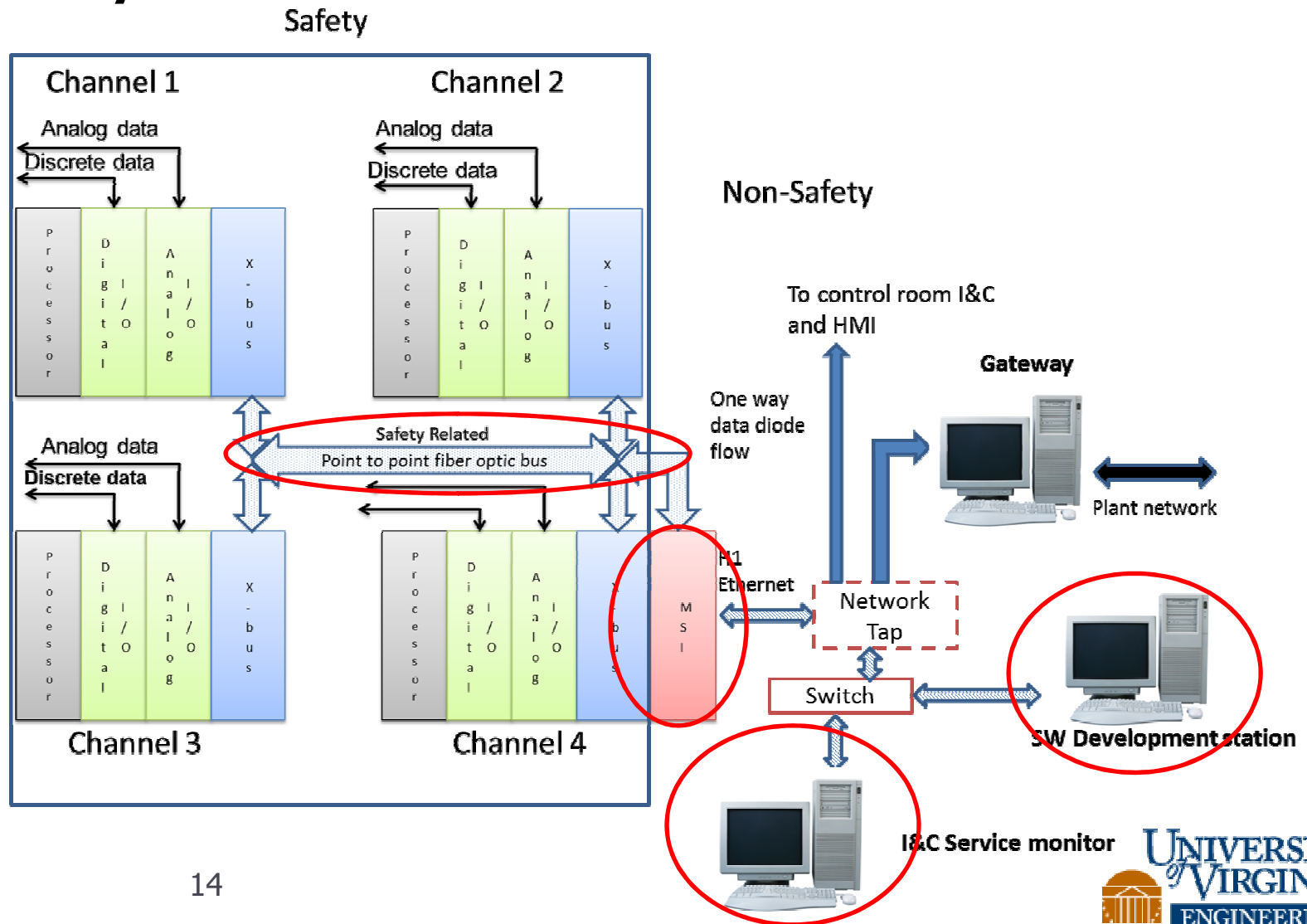


**Existence of Vulnerabilities->Pathway Exploit->System State Effects->Consequences**

# Looking at the system with cyber-security glasses (2)

- Let's examine how critical components outside the safety barrier and inside the safety barrier should be viewed for vulnerabilities.
- **The Service Unit** – (Outside) Compromised SU can provide misinformation about the health of the system. Potentially allow corrupted commands to flow back into the system. SV runs typical Linux system SW, SUSE, X-windows, etc..
- **The SW development station** – (Outside) Compromised SW development station can allow “infected” code to be uploaded on the I&C system. SW development tools run under Linux as well.
- **MSI** – (Outside) Responsible for processing outgoing messages and incoming commands. Signaling Messages are important for situational awareness.
- **Profibus Communication Network** – (Inside) Provides interconnection data path for critical process control measurements and variables between channels. If compromised, data integrity may be lost, network functionality could be lost, real time behavior may be altered.

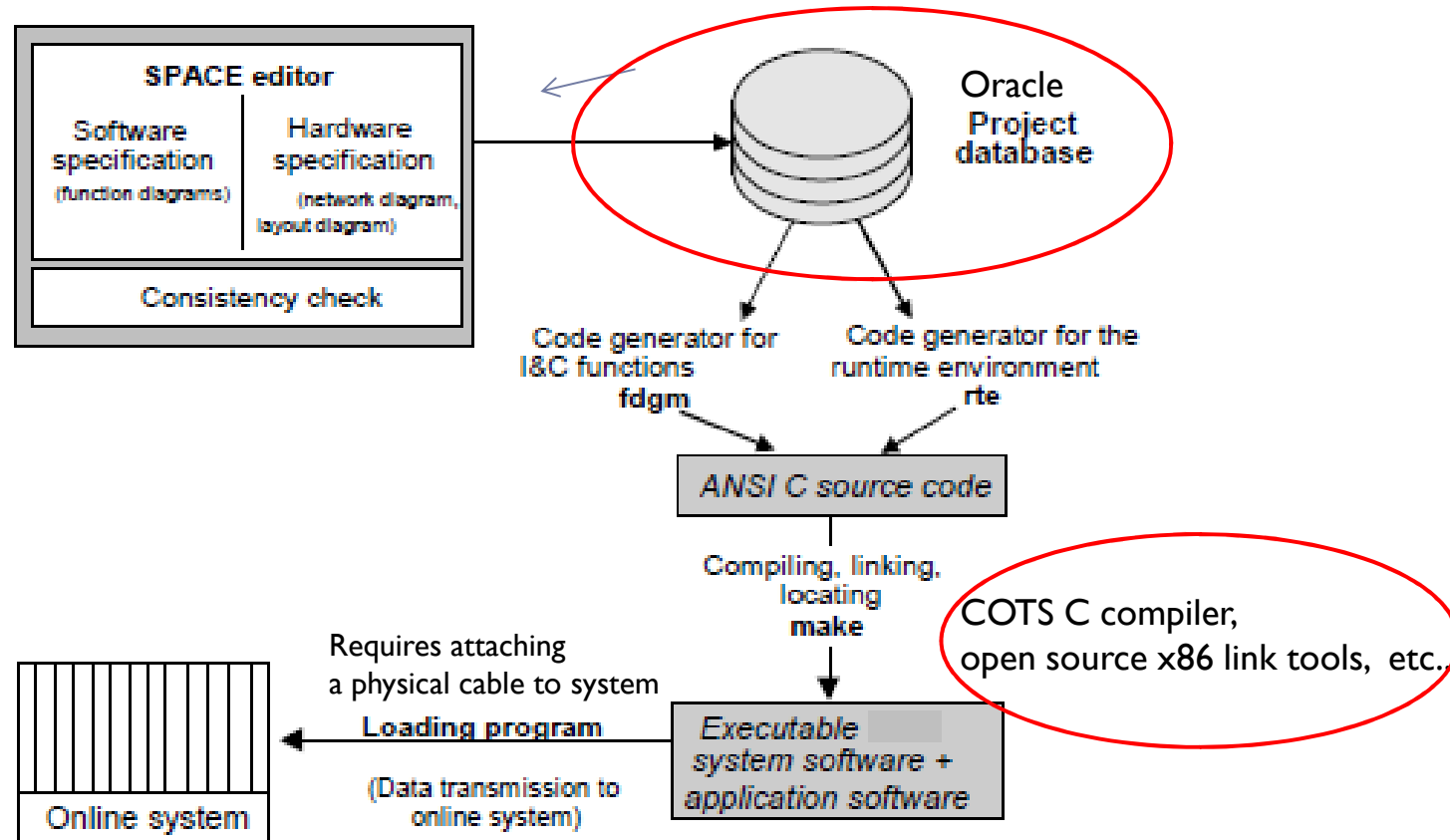
# Basic Architecture of Benchmark I&C System



# I&C Software Development Station



## Library Function Blocks



# SW development and Service Unit

- Service Unit
  - Linux box. Runs SUSE a variant of Linux.
  - Most of the tools to build code, configure system, monitor system, and maintain system configuration are here.
- Oracle database on the Service Unit.
  - Contains lots of sensitive information about the system – SW and HW configurations, parameters, settings, etc..
  - The Oracle Database requires significant effort to maintain security.
  - Protected by passwords of varying strength.
  - Breaking the password opens the door for stealing information, at the very least.



# SW development and Service Unit

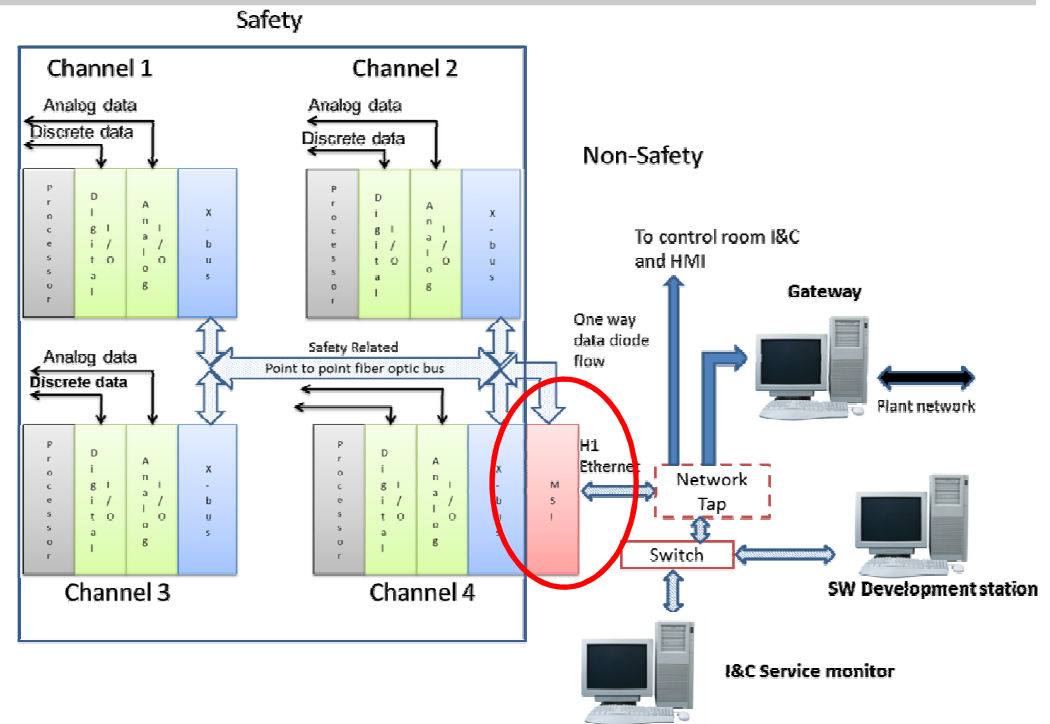
- Password cracking of the Oracle database.
  - A number of efficient password brute forcing programs exist for Oracle(s)
  - Speed is at least 10 million passwords per second for desktop/laptop
  - Speed is around 500 million passwords per second for specialized hardware (FGPA/GPU)
  - Takes about 2 days on laptop for 8 length pwd, and 2 hours on specialized hardware.
  - Only the username and hash are required. Both are easy to get – once inside the service unit.
- Oracle Database password algorithm published Oracle 11g – hash changed to SHA-1
  - Hash is unique to the username, but common across all versions and platforms of the Oracle database SYSTEM/MANAGER is always D4DF7931AB130E37 in every database in the world
  - Getting into the service unit from the outside may be challenging, but not impossible or even infeasible.

# SW development and Service Unit

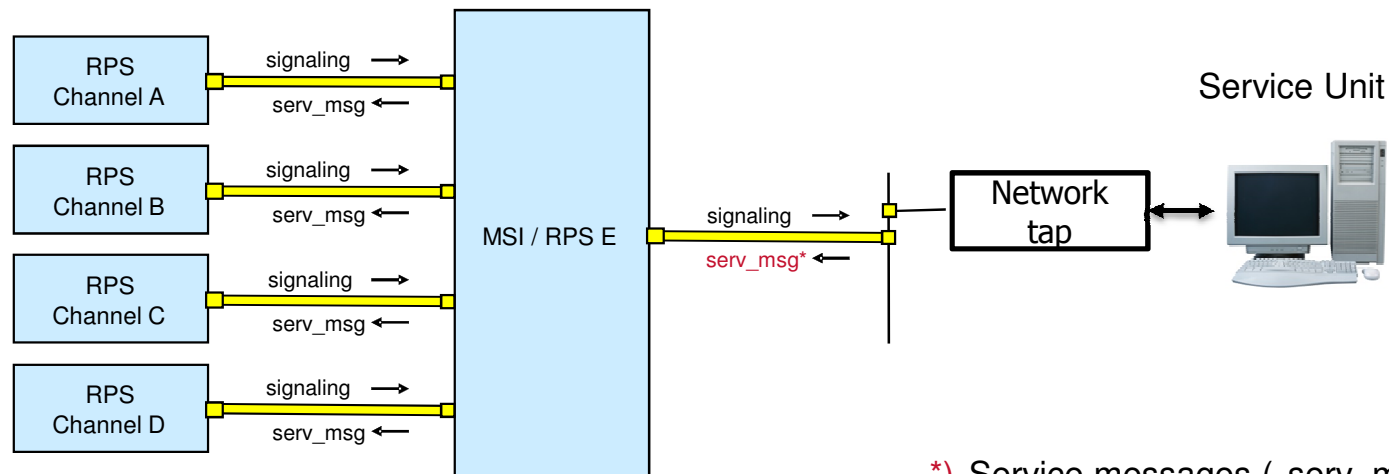
- Most I&C SW development environments use a combination of open source SW tools, compilers, COTS products, proprietary tools.
- This is blessing and curse. Blessing is that environment is supportable and sustainable. Curse is the “black hats” know how to exploit these open source tools too.
- One reason why security is not static fixed process, but evolving to changes.

# Role of MSI Computer

- Acts as a concentrator and preprocessor of signaling information
- Collects and processes analog and binary plant status information received from the protection channels
- Prepares MSI annunciation and indication information suitable for
  - Output to indicator panels in the control room and to the plant information system / process computer



# Message Transfers



signaling = Signaling messages from I&C computers to the Service unit  
serv\_msg = Service messages from Service unit to I&C computers

\*) Service messages ( serv\_msg) from the Service Unit are sent only on request (activities at the Service Unit). All other messages are sent cyclically

## Message transfer from and to the Service Unit

# Service Unit – HMI Graphic Service Monitor

- Overview on CPUs of the I&C I&C system
  - Operating mode
  - Signalization, alarms
- Allows the operator or I&C staff to graphical visualize processing operations
  - Parametrization
  - etc.
- Menu-guided service actions
  - Acknowledging
  - Tracing signals
  - Performing tests

Spoofer Attack can alter this information – mislead the operator

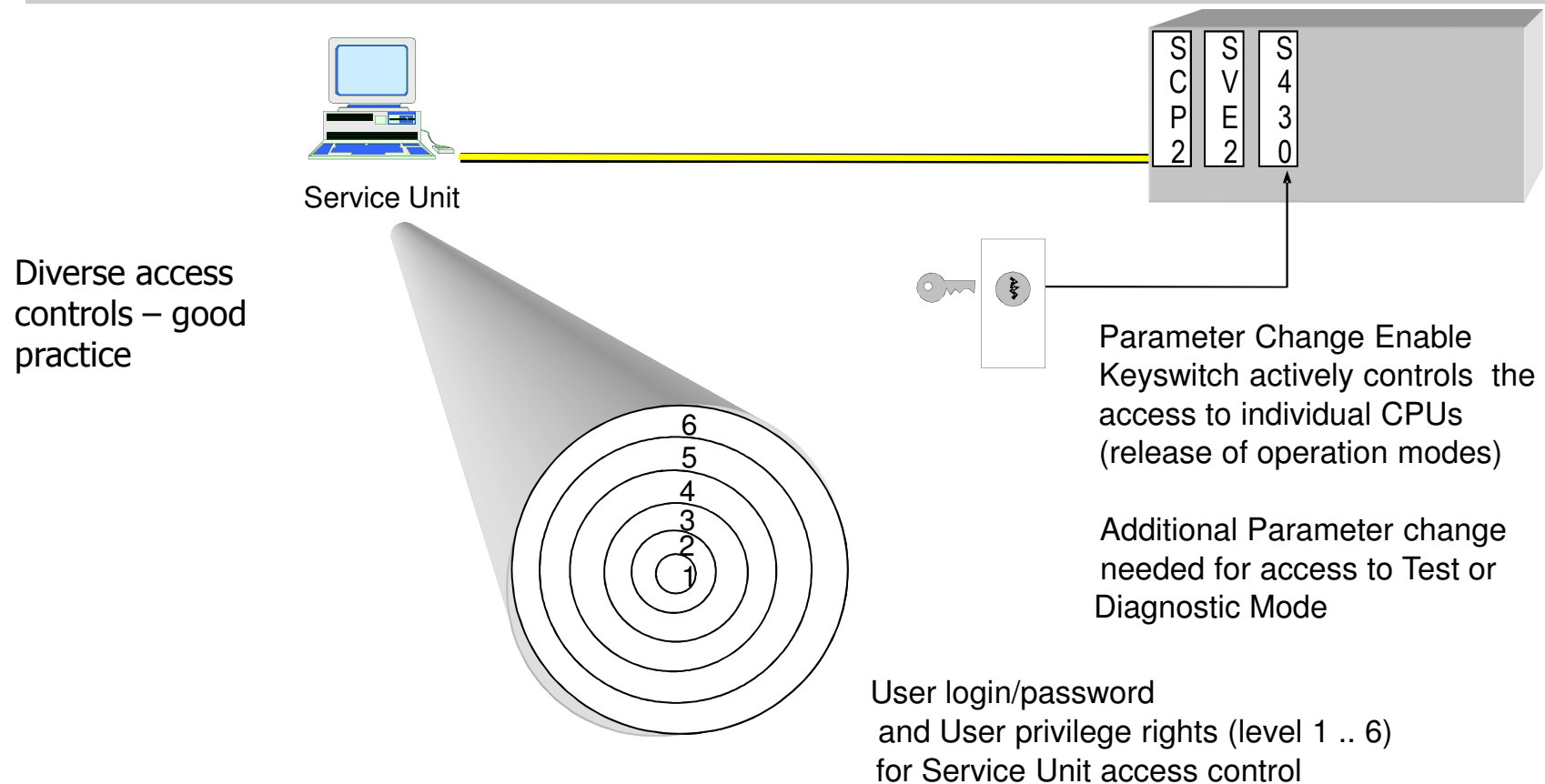
CPU	Role	Location	Mode	Permission	Flag	Redundancy	Train
501	SU		operation	op para...	no_flag	0	0
111	Single	+ER-VA.AB001	operation	op para...	no_flag	0	0
122	Single	+ER-VA.EB003	operation	op para...	no_flag	0	0
132	VO_M	+VO.JB003	operation	op para...	no_flag	0	0
134	VO_C	+VO.JB043	operation	op para...	no_flag	0	0
112	Single	+ER-VA.JB003	operation	op para...	no_flag	0	0
113	Single	+ER-VA.JB091	operation	op para...	no_flag	0	0
131	Single	+ER-VA.AB003	operation	op para...	no_flag	0	0

SMT server 1.06 / 2000-07-06  
Database kh  
User waedt Privilege diag  
Client ID 2 2000-07-11 10:15:09

Exec. Errors 0  
State OK

Name	Changed	Size
A1.sm	2000-03-23 12:59:10	3114
A2.sm	2000-03-21 19:13:33	3088
A3.sm	2000-03-21 19:13:36	3088
A4.sm	2000-03-21 19:13:41	3088
B1.sm	2000-03-21 19:14:15	3088

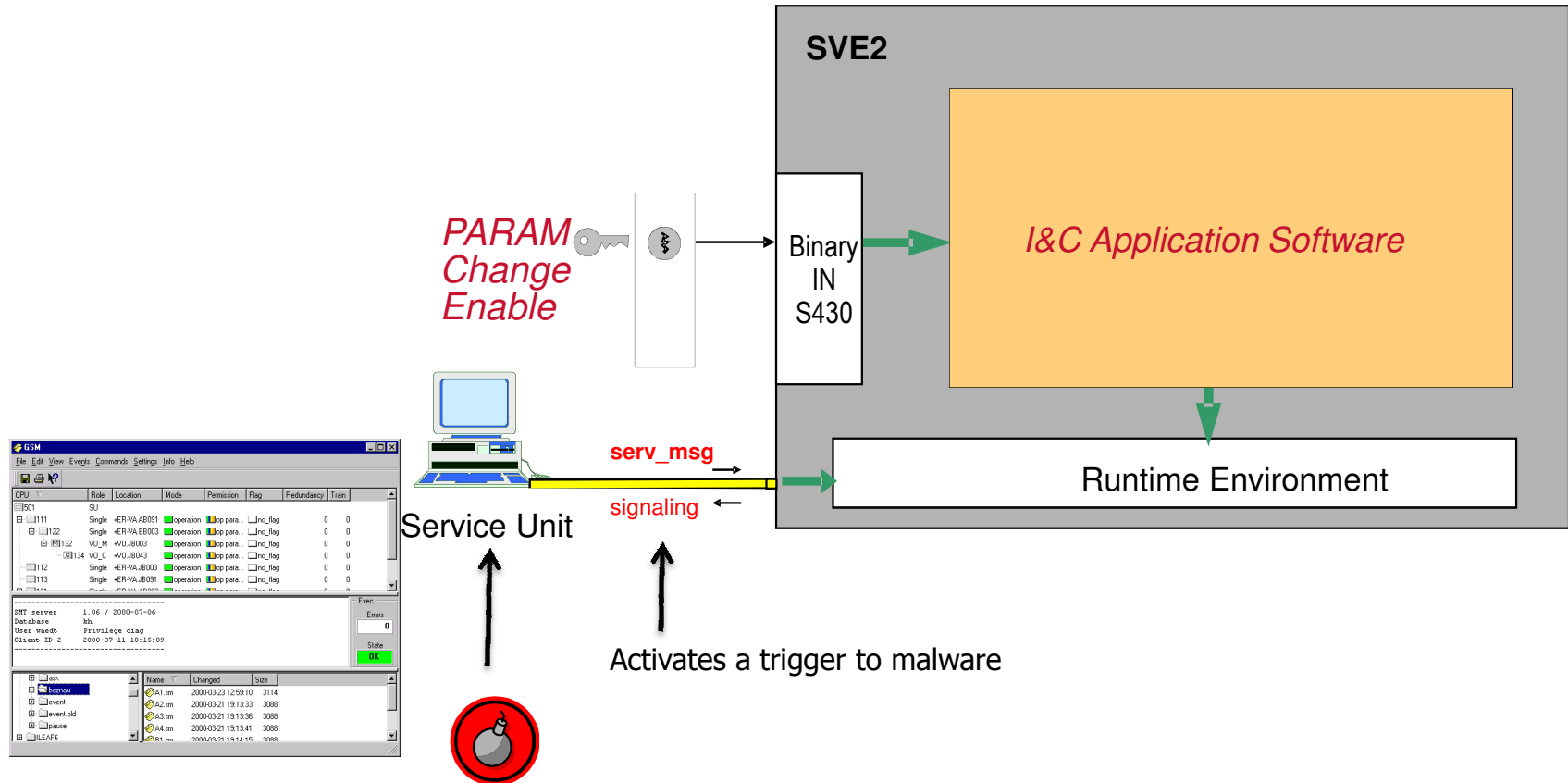
# Access Control



# Service Unit – Parameter Attack

- **Parameter Attack on the Service Unit** – Control Parameters are sometimes modified during operation to compensate for the changes in the certain plant dynamics.
- Diverse access controls to prevent unauthorized access of system operational modes are good practice, but are not bullet proof.
- An attack here would be a “bait and switch” attack. That is, once the key is switched to “change mode”, malware on the Service Unit computer would be activated to record the parameter change, substitute in alternate parameters of its choosing, but playback the correct values to the SRO for verification.
- The malware could lay dormant for a long time waiting for key state change.
- This type of attack is feasible, but requires substantial level of detailed system operational knowledge to achieve success – but post “stuxnet” has taught us the improbable does not imply infeasible.

# Possible Parameter Change Exploit

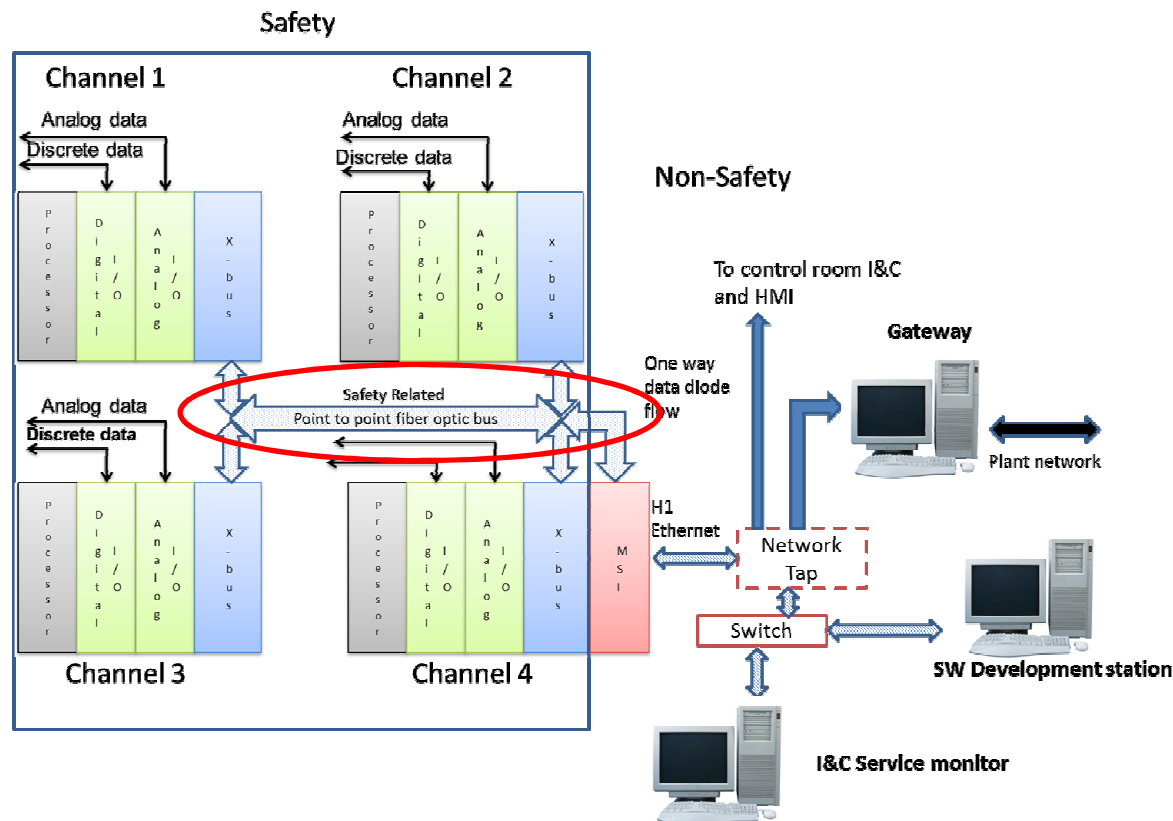




# Inside the Perimeter Vulnerabilities and Exploits

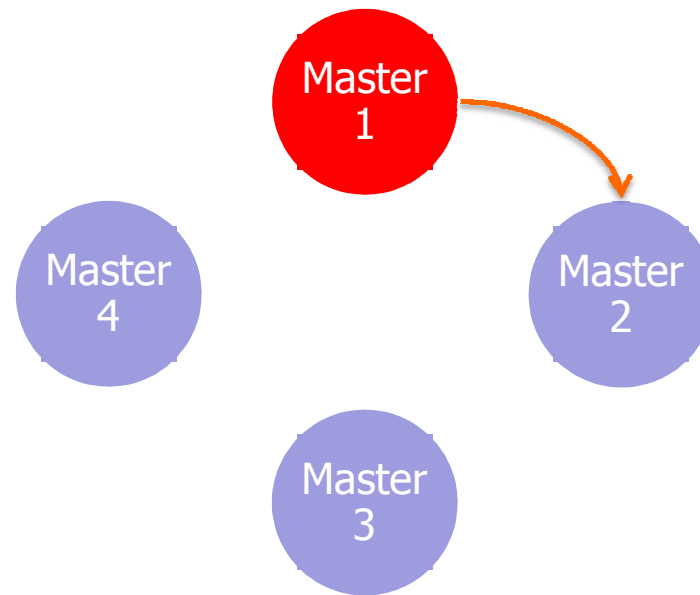
- Until now we discussed possible exploits that attack perimeter systems (SV, Oracle, SW development).
- Things can happen inside the perimeter as well. Much more difficult to detect because very little if any detection security exists inside the perimeter.
- Let's look at one known vulnerability: Profibus interchannel communication network.
  - Profibus is a IEC standard for Process control bus protocols.
  - Rotating token bus protocol to ensure each controller has fair access to send and receive data FOR EACH CHANNEL.
- At present, at least 30 or so vulnerabilities and exploits have been published in the open literature for Profibus. Some have been addressed, many have not.
- UVA published about 15 vulnerabilities in 2005 thru 2009.

# Profibus Communications

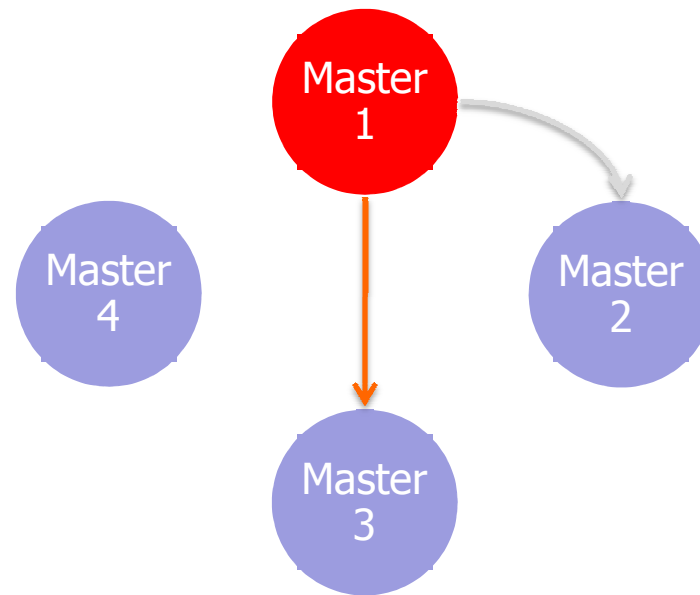


# Example: Malicious Profibus Master Controller Behavior

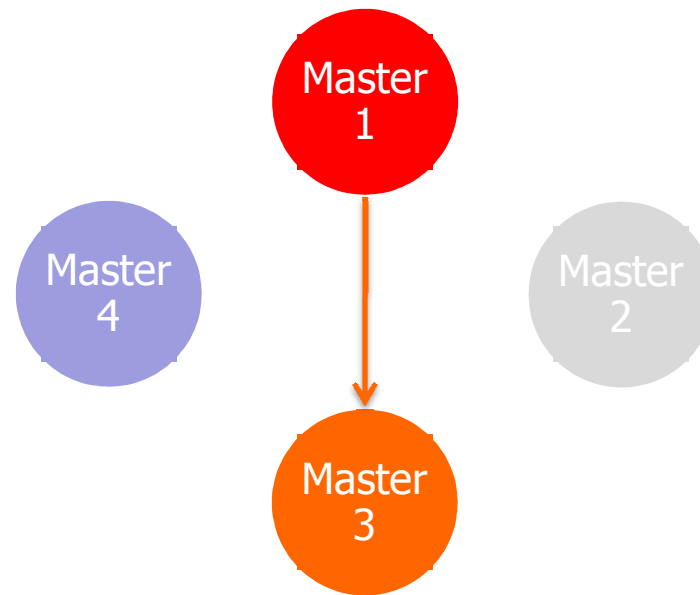
- Situation: A Faulty Master Profibus Controller removes good Master controller from the logical ring.
- The “faultiness” is due to well crafted attack on the protocol controller.
- In Profibus, a Removed Master controller has to be reinserted by at least one good master in the logical ring.
  - As side, this takes a long time - becomes part of the exploit.
- Scenario on the next slides



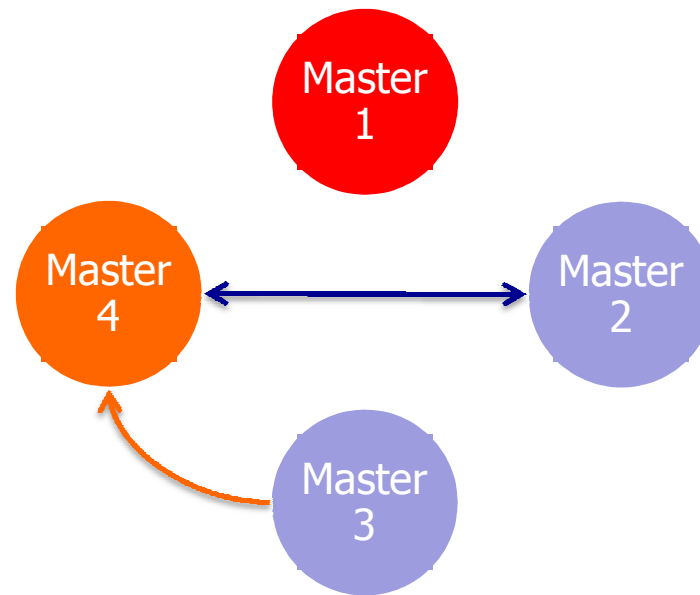
- Profibus Master 1 tries to pass the Token to Master 2
  - Address 00000010



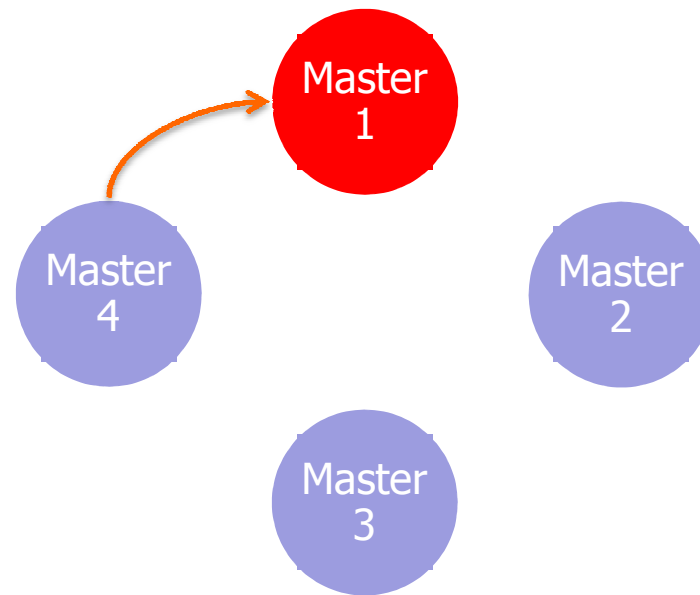
- Master 1 tries to pass the Token to Master 2
  - Address 00000010
    - But it has “altered” bits at the most and least significant bit due to the cyber inject.
      - So it will be sending to 10000011
      - Which is the address to Master 3, because the leading 1 does not count
      - Parity is preserved, so everything seems to be working correctly wrt master 1



- Because Master 1 passed the Token to Master 3 (and it was correctly received by Master 3), Master 2 is removed from the logical ring – it did not respond during its token time slot.
  - Master 3 now has possession of the Token
  - Master 2 cannot “talk” on the network, just “listen”
    - Needs to be reinserted

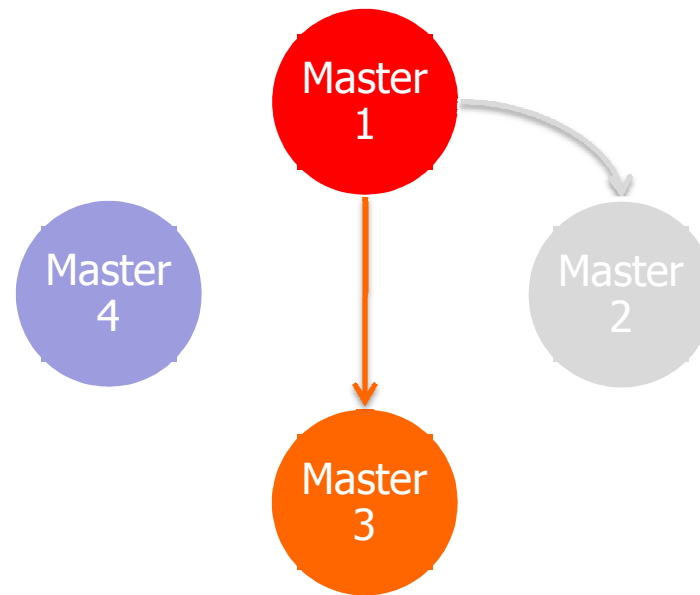


- Master 3 correctly passes the Token to Master 4
  - Master 4 might have enough time to reinsert 2 into the ring
  - Depends on the message traffic load. The more load on the network, the less time for a reinsertion action.



- Master 4 correctly passes the Token to Master 1 (the misbehaving one)
  - Master 1 tries to pass the token to Master 2 (as at the beginning), but can't because of altered address.





- But because Master 1 has stuck bits that point to address 3 instead of 2, it will bypass Master 2 again
  - Hence removing it from logical ring once again
  - In this scenario Master 2 will never get to send out its critical information

# Misbehaving Master Results

- Misbehaving profibus master can take out correctly working profibus master from the logical ring
  - Effectively making it only a receiving station
  - In the previous scenario, we showed that profibus master 2 will never get to send out data
- It would be very hard to detect the origin of the attack and problem.
  - Manifests as a long string of error messages then a “out of service controller message”.
  - System thinks profibus master 2 is faulty when in fact it is not.
  - Error messages will direct operator attention to profibus master 2 - away from the cyber attack infection site.
- The attack could move from one profibus controller to another, if so designed. End result could be temporary loss of channel communications in the system which results in temporary loss of system. Would eventually trip the reactor.
  - Redundant profibus controllers don't help, they can be infected too.
- In reality, this attack would be difficult to “vector” into the system, requires malware to run on the profibus controller. However, this and other vulnerabilities DO EXIST with the protocol.

# Summary

- Cyber Security of I&C systems is about:
  - Acknowledgement of Vulnerabilities.
  - Perform Penetration Tests to demonstrate system can resist real world challenges
  - Management and mitigation of risk associated with Vulnerabilities.
  - Awareness that cyber threats are non-stationary.
  - Enhancing system safety, availability.