An Approach for Evaluating the Consequence of Cyber Attacks on Nuclear Power Plants

Athi Varuttamaseni[1], Robert A. Bari[1], Robert Youngblood[2]

Presented at the 2017 ANS PSA Conference

Pittsburgh, PA

September 24-28, 2017

[1]Brookhaven National Laboratory , [2]Idaho National Laboratory

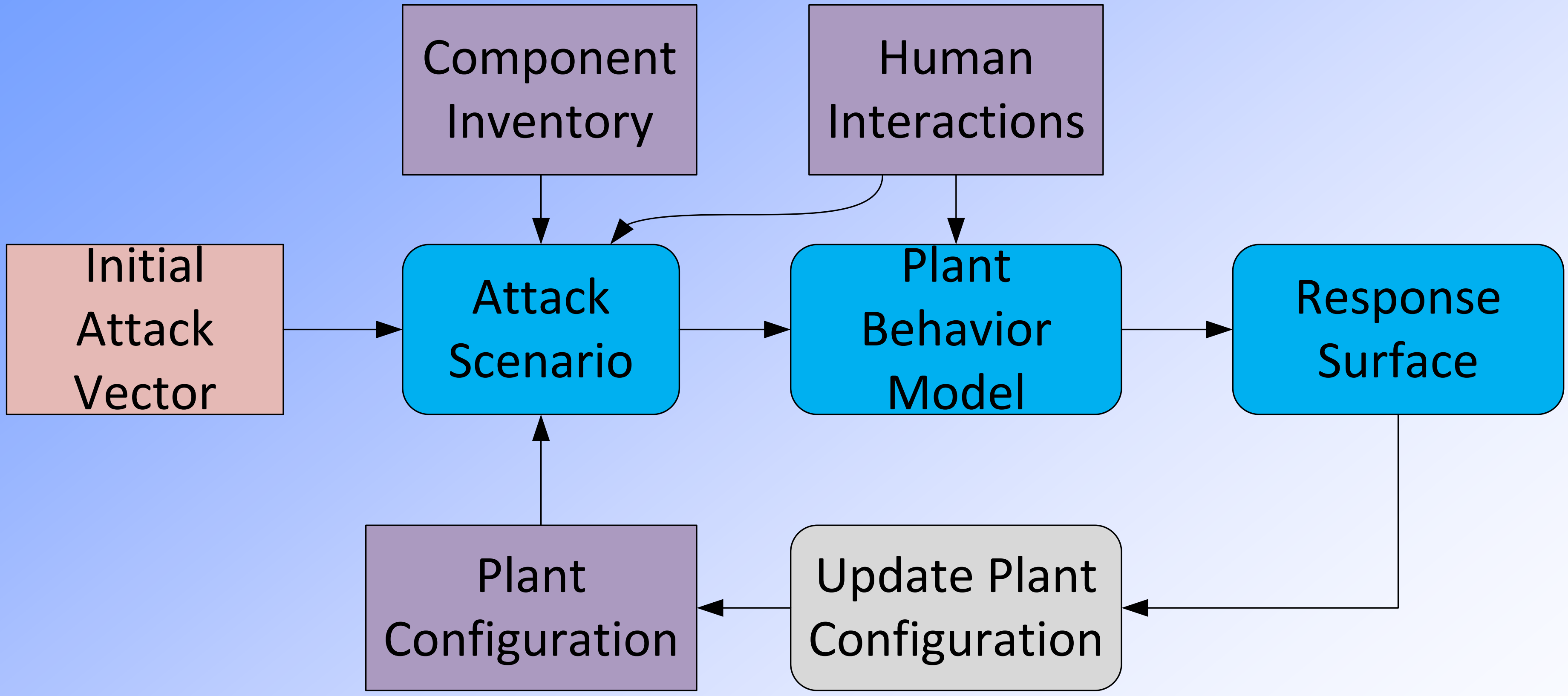
Objectives

- Evaluate the “consequence” of cyber-attacks on nuclear power plants. “Consequence” includes
  - safety,
  - availability (e.g., recovery time),
  - reliability (e.g., spurious actuation),
  - equipment damage,
  - loss of public confidence.

- Questions we want answered include:
  - What plant systems are susceptible (what are the possible attack scenarios)?
  - How will the plant behave when these systems are attacked (what is the system response)?
  - What preventive and mitigation measures can be implemented?

- Difference from traditional risk assessment:
  - inter-dependencies of digital systems (trust relationships).
  - non-binary behaviors of compromised components.
  - intelligent adversary.

Overall Approach for Consequence Evaluations



Scenario Development

- Similar components are analyzed as a group instead of individually.
  - Vulnerability is more dependent on a small number of attributes (e.g., user updatable firmware) than on the function of the component in the system.
  - Example: Compromise of a network interface leads to the same impact regardless of device type.
- Software configuration (e.g., trust settings) and initial privilege of the attacker are important factors in determining the degree of information (e.g., command) propagation.

Some Propagation Evaluation Methods

- Logic tree analysis
  - Uses logical operators to enumerate conditions needed to reach a target event (e.g., compromised component).
  - Examples include fault trees and attack trees.
- Simulation
  - Uses attacker, defender, and system models to simulate attack scenarios.
- Markov modeling
  - Tracks system states and state transitions.
- Game theory
  - Models adversarial interactions between the attacker and defender.

Classes of Impacts from Cyber Attacks

Impact of cyber attacks on control systems may be classified into several groups:

- Reconnaissance
- Deny manual or automatic control of system functions
- Deny operator awareness of system status
- Disable security features
- Enable control of the system by the attacker

Impact Type	Attack Type
Reconnaissance	Network sniffing
Loss of awareness	Man-in-the-middle (network traffic spoofing)
Full attacker control	Buffer overflow in control codes
Degradation of control	Induce Latency

Methods to Induce Latency

- Introducing latency into the system can degrade the performance of control and safety systems.
  - Delay action of safety functions, leading to a reduction in safety margins
  - Spurious actuation of safety function (e.g., delay of critical input signals)
  - Delay operator awareness of system state

- Common latency types include network latency and processing latency.

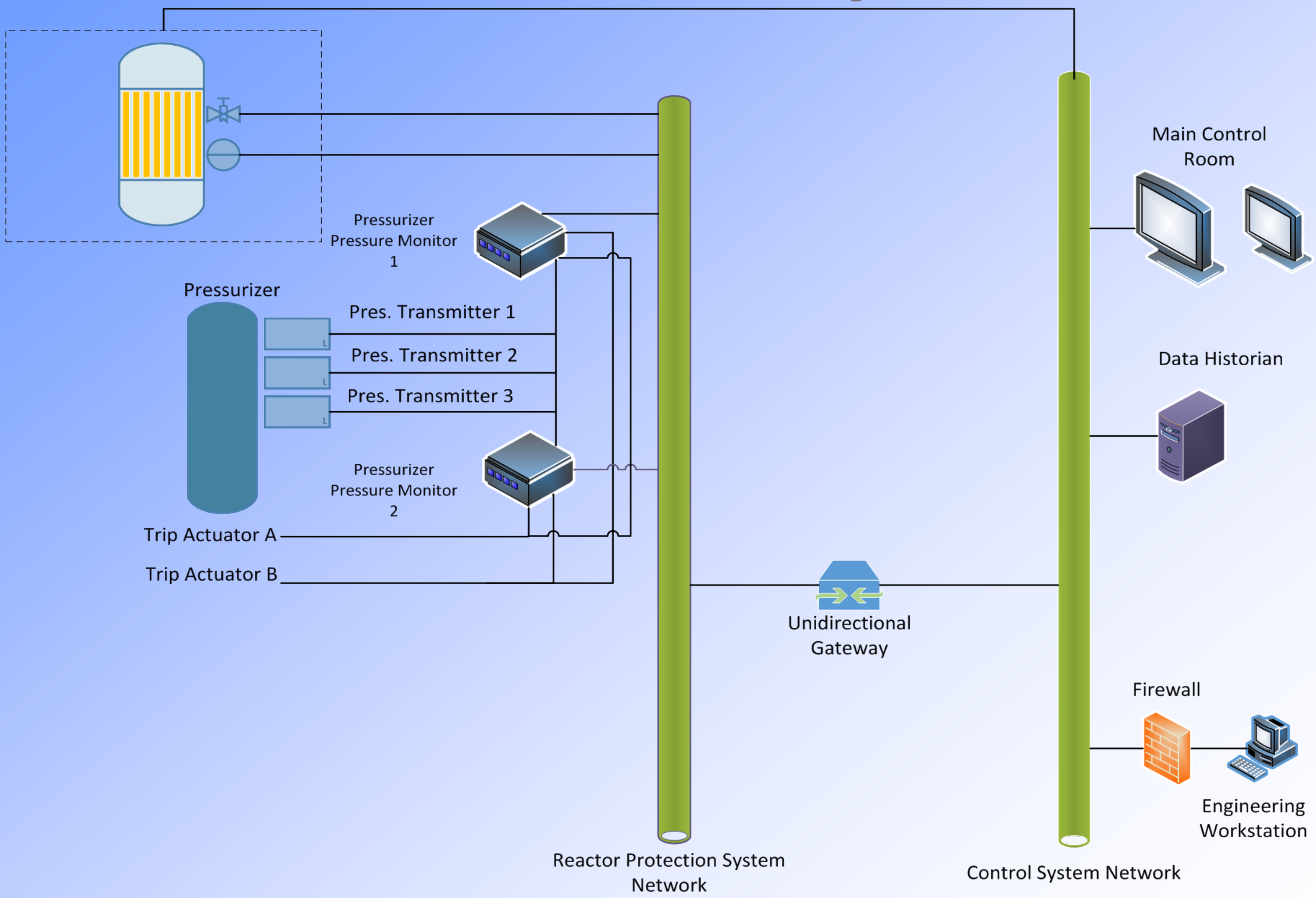
Action	Implementation
Exhaust CPU cycle	Put CPU in an infinite loop
Exhaust network bandwidth	Increase network queue length
Exhaust memory or storage space	Write random data to memory or storage

Example: Pressurizer Pressure Trip Function

- Are there scenarios where the pressurizer pressure trip function can be impacted?
- How can an attacker gain access to the system?
- If successful, what is the impact of the attack (e.g., effect on safety margins)?

Consider a low pressurizer pressure trip function in a simplified pressurizer pressure protection system.

Simplified Pressurizer Pressure Protection System



Analyzing the Component Vulnerabilities

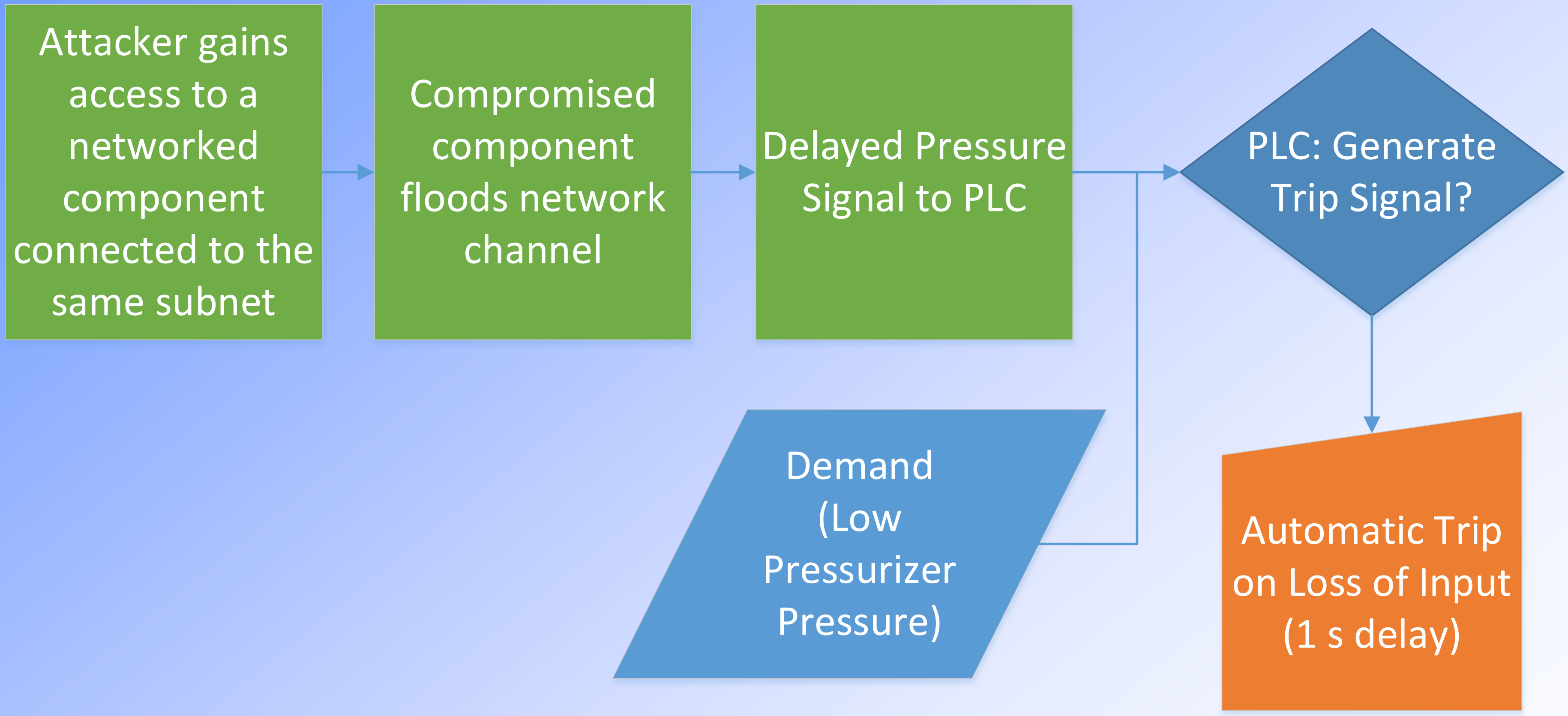
What components in the pressurizer pressure protection system are potentially vulnerable?

ID	Component Name
1	Digital Pressure Transmitter
2	Programmable Logic Controller (PLC)
3	Voting Logic
4	Trip breaker

ID	Potential Vulnerability Points
1	Network Interface
2	Program Logic, Setpoint, Memory corruption
3	Analog
4	-

Attribute	Enabled Capability (possible behavior if compromised)
Network Interface	Denial of service (flood network traffic)
	Man-in-the-middle attack (e.g., ARP cache poisoning)
	Data collection (traffic sniffing)
	Data egress (send data to new hosts)

An Example Attack Scenario



Attacker gains access to a networked component connected to the same subnet

Compromised component floods network channel

Delayed Pressure Signal to PLC

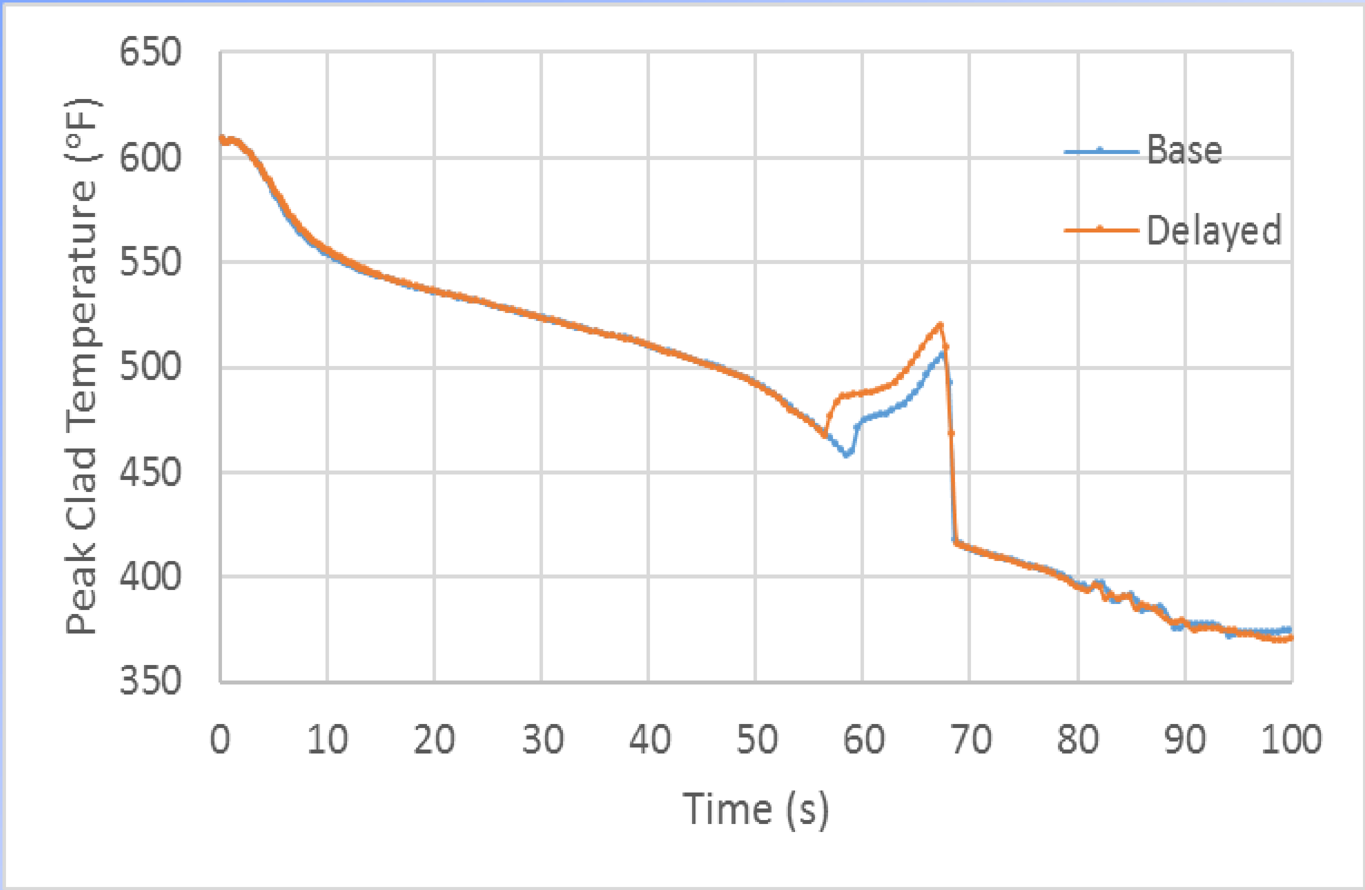
PLC: Generate Trip Signal?

Demand (Low Pressurizer Pressure)

Automatic Trip on Loss of Input (1 s delay)

System Response (1)

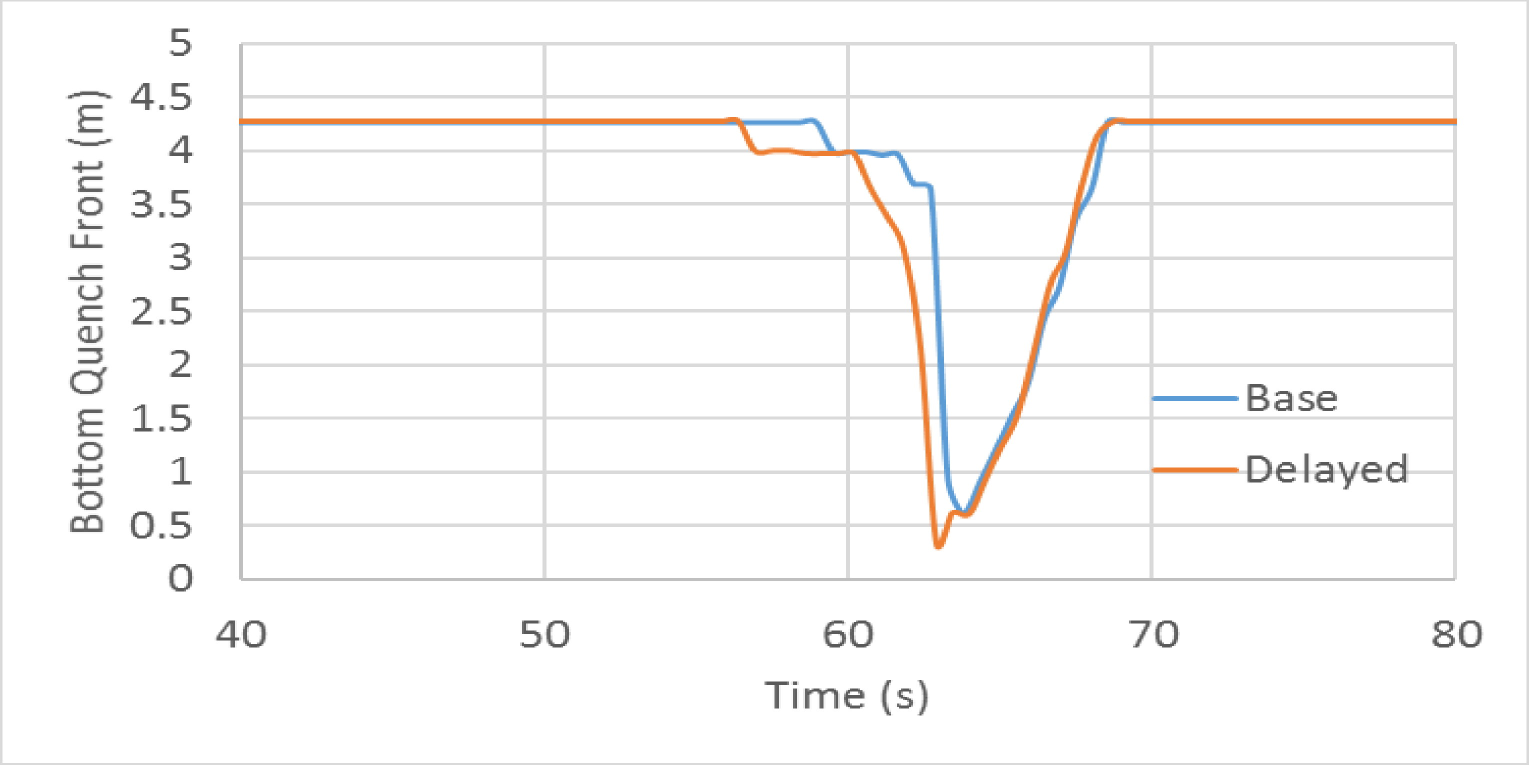
What is the impact on peak clad temperature?



Peak clad temperature is about 20 ^{o}F higher than the base case.

System Response (2)

What is the impact on bottom quench front?



Summary

We have presented an approach to evaluate the system response to various cyber attack scenarios.

1. Use information on component properties, system design, and network topology to generate plausible attack scenarios.
2. Use system model to evaluate plant response under the scenario being analyzed.
3. Identify preventive and mitigative measures to prevent undesirable outcomes.

Next Steps:

- Develop scalable interface between attack scenarios and system response models.
- Integration with PRA