Operational Technology Cybersecurity in the Chemical Process Industries

Implications of Compromised Distributed Control Systems and Safety Instrumented Systems

Peyton C. Richmond and Helen Lou

Lamar University

2025 CySER Virtual Seminar, 1st April

Outline

- Hazards associated with CPI
  - Industrial incident in my community
- Traditional risk mitigation
  - Distributed control systems and safety instrumented systems
- Increasing cybersecurity risk
- Cybersecurity risk mitigation
- Promoting awareness of cybersecurity

Hazards Associated with CPI

- Refining and petrochemicals
- Hydrocarbons and chemicals
- Explosion, fire, and toxic release

Highsmith, Carol M, photographer.
An oil refinery in Groves, Texas, near Port Arthur.
Texas Groves United States, 2014. -02-27.
Photograph. https://www.loc.gov/item/2014630814/.

Hazards associated with CPI

- TPC Group Port Neches, TX, facility Wednesday, November 27, 2019
- Fractionator Loss of containment.
- Bottom level 6,000 gallons (30,000 pounds) escaped in less than one minute
- Vapor cloud explosion and fire
- Doors blown in and windows shattered

Just Close A Valve…

Vachon, John, photographer. Borger, Texas. Worker on night tour operating valve in Phillips refinery. Hutchinson County Borger United States Texas, 1942. Nov. Photograph. https://www.loc.gov/item/2017840482/.

Hazards associated with CPI

- Piping heavily damaged and some could not be isolated
- Two additional explosions resulting in four additional towers falling
- Four-mile radius evacuation order until 10:00am November 29th
- Fires burned for over a month
- Air quality issues

Hazards associated with CPI

- Loss of containment from process equipment
  - Vapor cloud explosion
  - Fire
  - Toxic release
- Equipment damage
  - Vessels
  - Compressors
  - Furnaces
- Unscheduled shutdowns

Traditional Risk Mitigation

- Control rooms consolidated and moved outside boundary limits
- Non-essential personnel moved outside boundary limits
- Adjacent land purchased by operators
- Flares located outside boundary limits

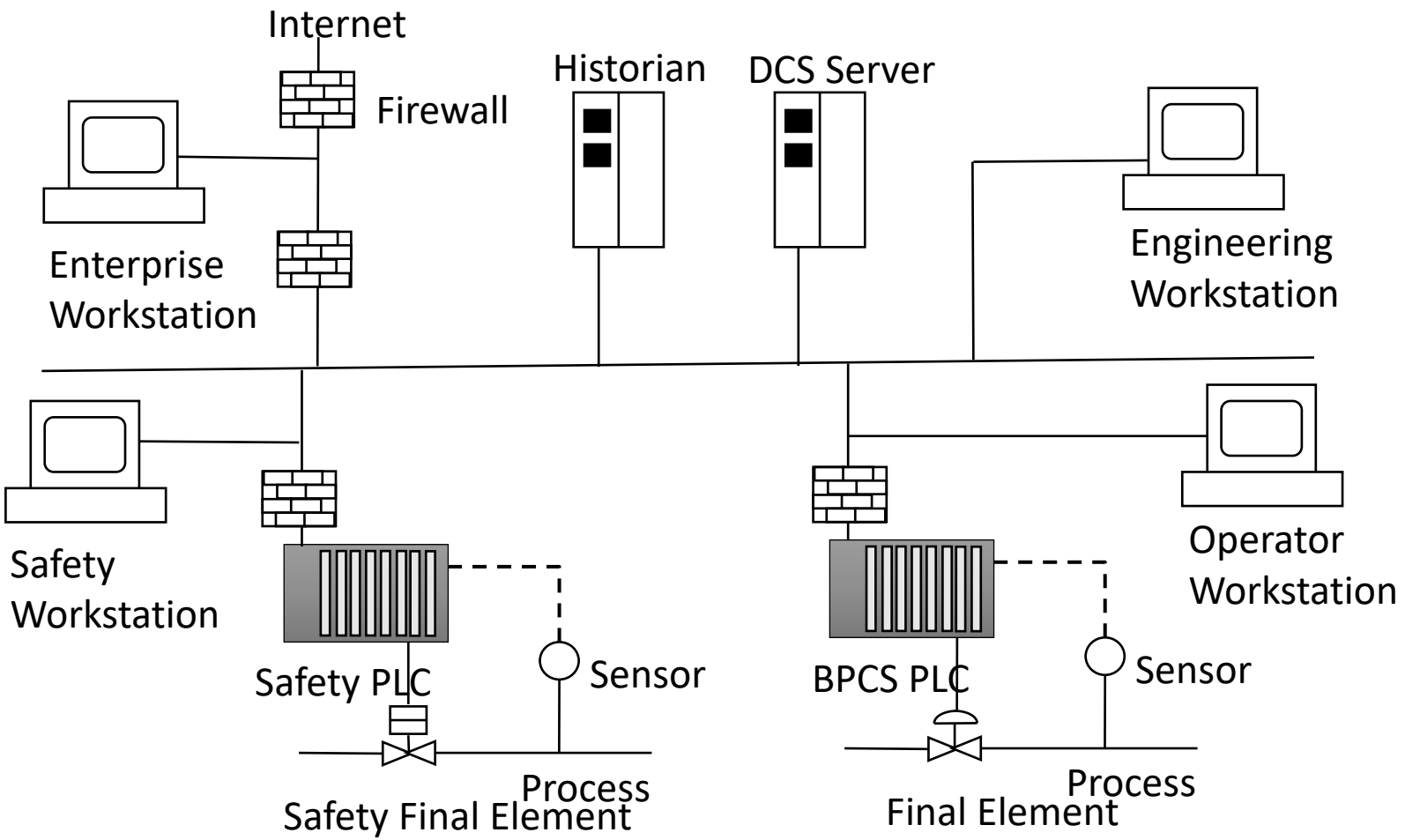
Traditional Risk Mitigation

- Process Safety Management
  - Regulations to manage highly hazardous chemicals
  - Process Hazard Analysis
- Hazard and Operability Study
  - Systematic method to identify and evaluate potential hazards and operability issues
- Layer of Protection Analysis
  - Technique to evaluate hazards and their mitigation

Traditional Risk Mitigation

- Basic Process Control System (BPCS)
  - Normal activity controlling process variables
  - Process alarms
- Safety Instrumented System
  - Safety shutdown systems
- Active protective systems
- Passive protective systems
- Disaster emergency response

Increasing Cybersecurity Risks



Increasing Cybersecurity Risks

- Modern operational technology uses Windows infrastructure
  - Corporate IT groups not suited for operational demands
  - Operators rely on control engineers for support
  - Control engineers with chemical engineering backgrounds
- Availability prioritized over security
  - DCS access required 24/7
  - SIS availability mandatory for safe operation

Increasing Cybersecurity Risks

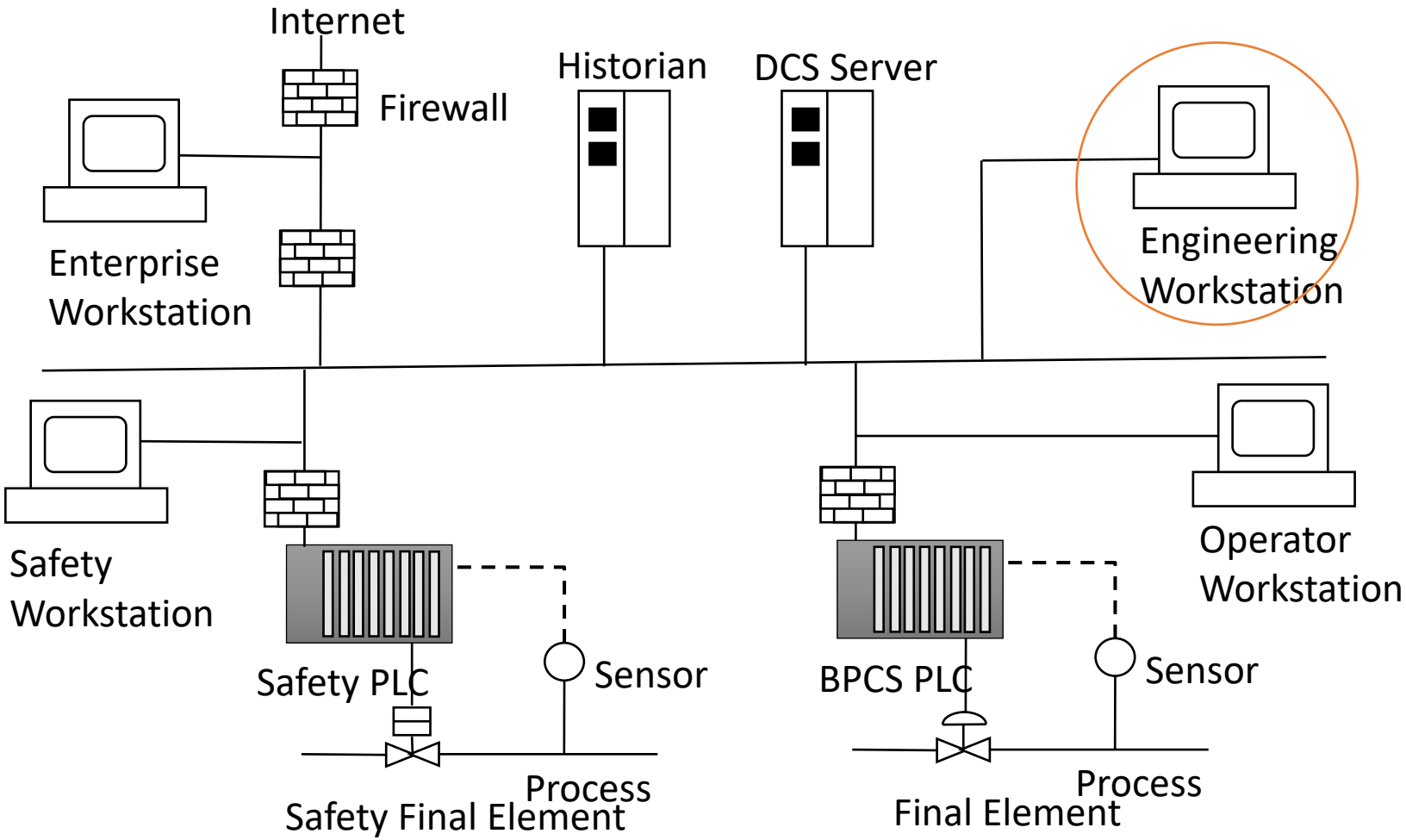
- Major cybersecurity incidents
  - Stuxnet, Triton, Colonial Pipeline Ransomware, Florida Water System
- Hacking tools for operational technology increasingly sophisticated
  - Windows zero-day vulnerability can be used to attack CPI OT systems.
  - Windows patches must be validated by DCS vendor

Cybersecurity Risk Mitigation

- Process Hazard Analysis (PHA)
- Process safety
  - Risk = Consequence x Frequency
- Cybersecurity
  - Risk = Consequence x Likelihood
  - Likelihood = Threat x Vulnerability x Value

Managing Cybersecurity in the Process Industries: A Risk-based Approach, CCPS (Center for Chemical Process Safety), April 2022

Cybersecurity Risk Mitigation



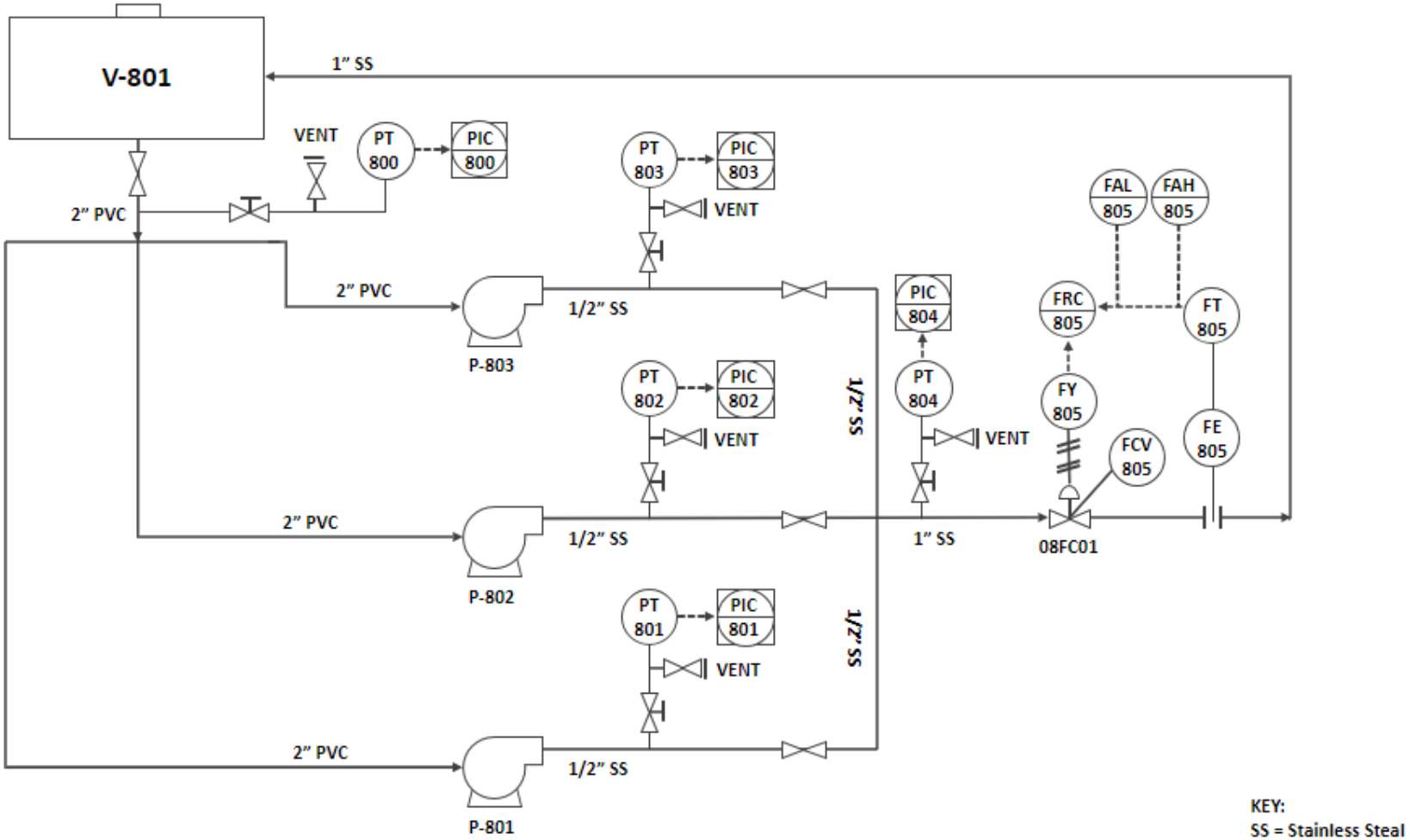
Cybersecurity Risk Mitigation

- Compromise engineering or safety workstation(s)
- Disrupt basic process control system (BPCS)
  - Cause operating deviations of critical control systems and/or interlocks
- Disable safety instrumented system (SIS)
  - Disable protective measures and cause initiating event
- Release, fire, explosion, or fatalities

Promoting Awareness

- Unit Operations Laboratory with Industrial DCS
- Operating groups perform normal process control lab activities (flow, level, temperature)
- Process Control group map control connections then simulate cyber attacks
- Demonstrates cybersecurity vulnerability in the context of chemical process operations

Pump Curve Experiment (Flow Control)

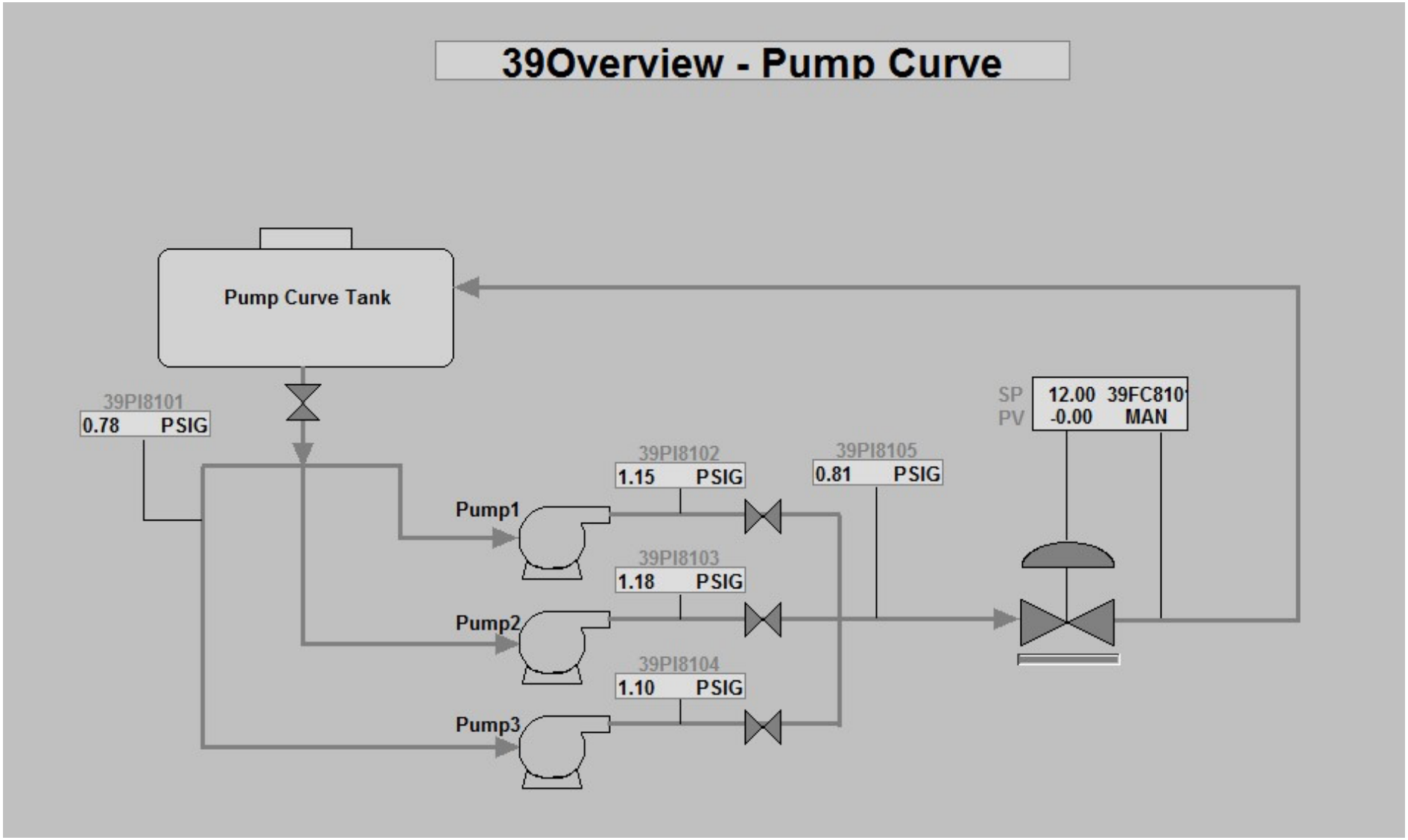


Pump Curve Experiment (Flow Control)

Pump Curve Experiment (Flow Control)

- Line-up and turn on appropriate pump
- Operate pumps with various impeller sizes and record flows and pressures
- Place PID loop in manual and manipulate valve while recording flows
- Place PID loop in automatic and tune flow control loop

Pump Curve Experiment (Flow Control)

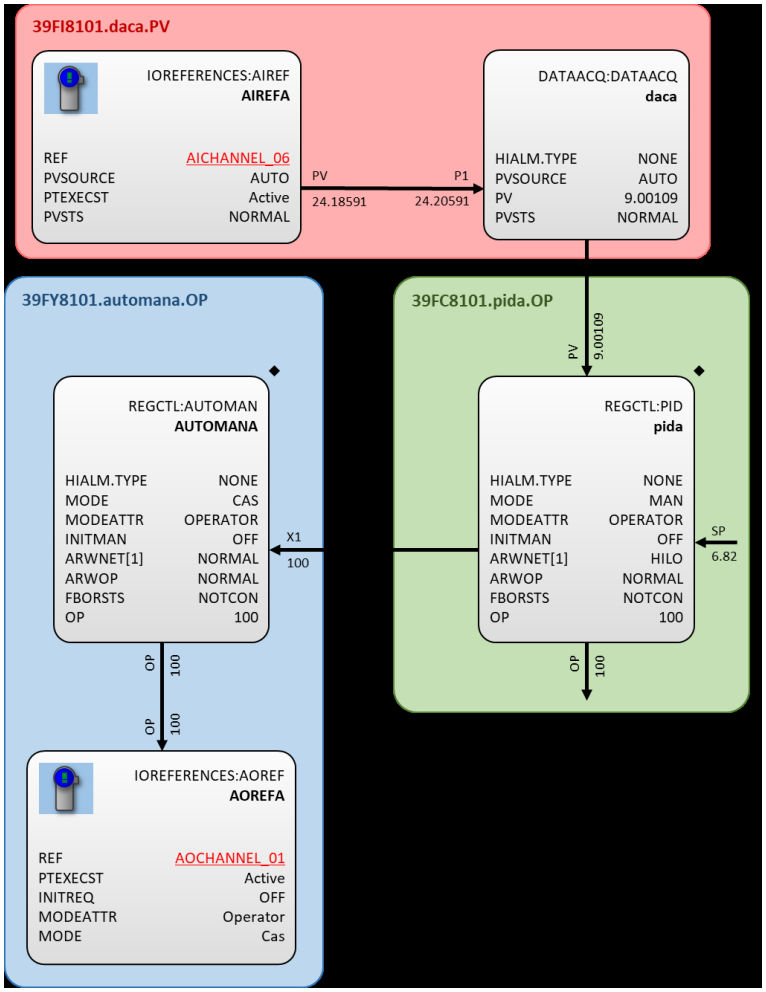


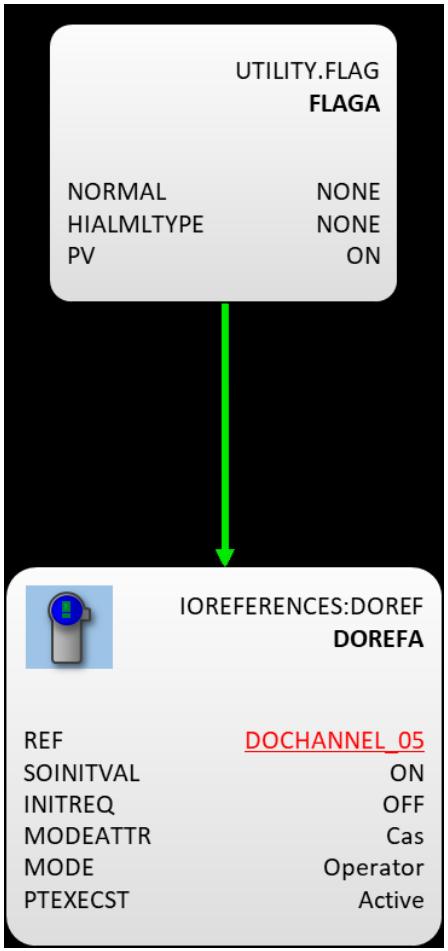
Process Control Group Activities

- Identify tags associated with experiments
- Diagram controls from control module diagrams
- Review additional parameters and modes accessible to process control engineers
- Simulate attacks forcing the operating group to detect and respond before continuing their work

Process Control Group Activities

Process Control Group Activities





Attack Scenarios

- Inactivate tags
- Place components in manual
- Misconfigure PID controllers
  - Change output limits
  - Change action (direct/reverse)
  - Change alarm settings
- Disable digital outputs
- Spoof inputs

Process Control Group Activities

- Shutdown a pump and the targeted team recognized that the action was beyond their control within seconds
- Manipulated a temperature reading and the affected team took more time to recognize the discrepancy
- Took away access to a level controller and, since the team was seated immediately behind us, they understand that they were being targeted relatively quickly
- Changed the temperature PID from direct acting to reverse acting causing the value to open 100% and not correct itself and the group was not able to determine the cause of this unusual control activity

Process Control Group Activities

- Access a pump interlock to falsely indicate a low level and turn of the pump. The targeted group did not see the alarm and it took them several minutes to notice the pump was turned off.
- Changed a pressure indicator to read much higher than its actual value and the targeted group did not notice it before the 3-minute deadline
- Changed the high limit output to 60% for the level controller
- Changed the temperature controller to manual and back to automatic repeatedly and it took the group significant time to realize their system was in manual control

Conclusions

- Hazards associated with CPI discussed
  - Explosion, fire, toxic release risks
- Traditional risk mitigation
  - Distributed control systems and safety instrumented systems
- Chemical processing cybersecurity risks increasing
  - Windows based modern manufacturing environment
  - Operational technology hacking tools increasingly sophisticated
- Cybersecurity risk mitigation
  - Cybersecurity in the context of Process Hazards Analysis
- Promote awareness with undergraduate process control laboratory module
  - Increased student awareness of cyber security risks

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 2321055.