Process-Aware Cyberattacks for Thermal Desalination Plants

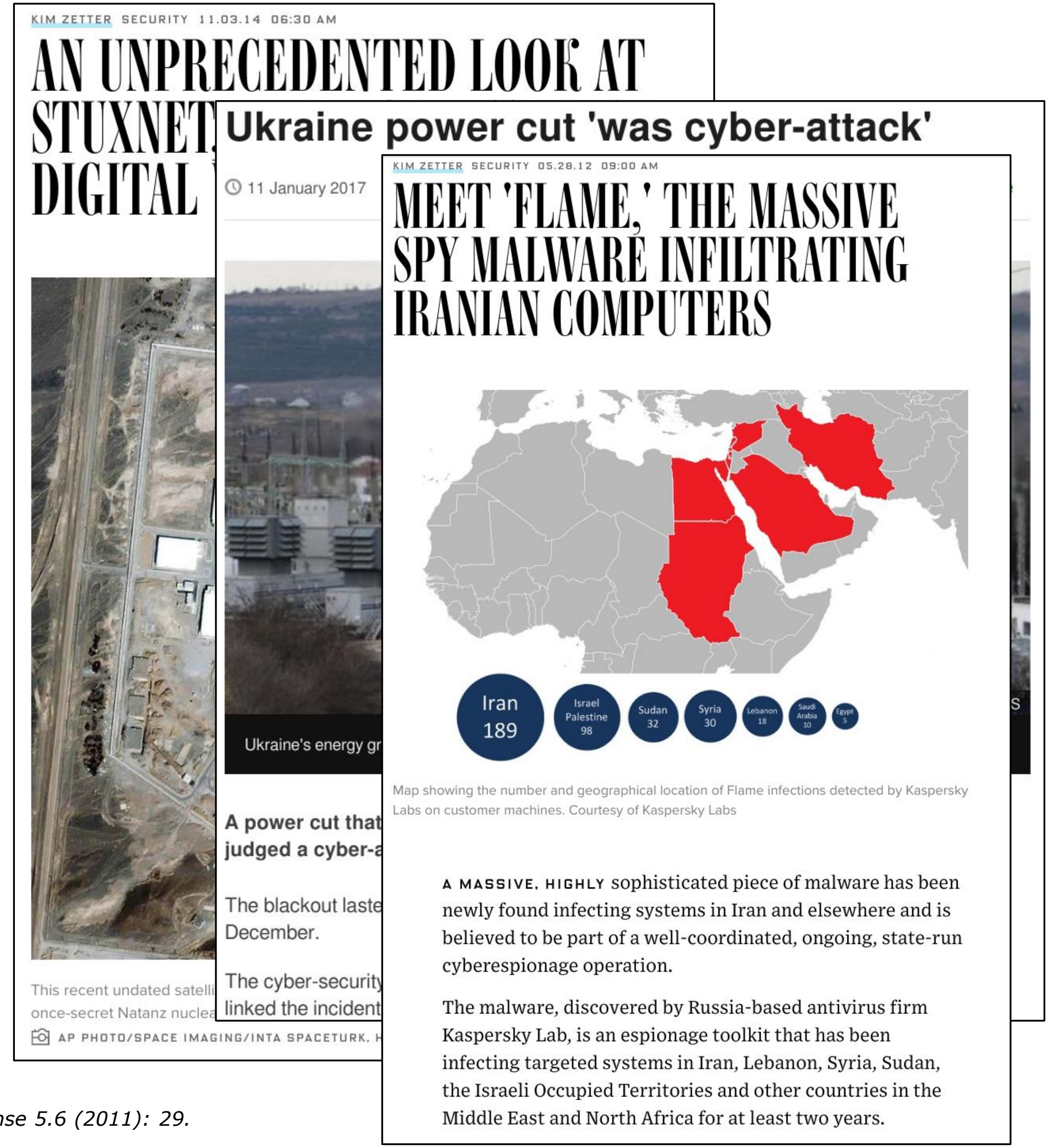
ACM ASIACCS 2019

Prashant Rajput, Pankaj Rajput, Marios Sazos, Michail Maniatakos

New York University

Attacks on Critical Infrastructures

- Stuxnet[1] **[Process-Aware attack]**
  - Infected Step 7 project files
  - Iran
    - 984 centrifuges
    - Reduced efficiency 30%
  - Indonesia, India, USA, etc
- Ukrainian Power Grid
- Shamoon malware[2] **[IT attack]**
  - Deleted files on Aramco computers
  - Overwrote master boot record → machines unusable
  - 35,000 workstations
- Flame malware



[1] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5.6 (2011): 29.
[2] Bronk, Christopher, and Eneken Tikk-Ringas. "The cyber attack on Saudi Aramco." Survival 55.2 (2013): 81-96.

Process-Aware Attacks

- Assumption: Adversary has prior knowledge
  - Control algorithm
  - Operational range
  - PID controllers, Actuators, Sensors, etc.

- Limitations
  - Cannot generalize to other plants
  - Requires prior knowledge

- Contributions
  - First cybersecurity study for desalination plants
  - Performance & Mechanical damage analyzed
  - Quantified mechanical damage

MSF Desalination Process[3]

- Heats up the recycle brine → Feed brine
- Uses input steam

- Feed brine is then sent to stages
- Same process continues again

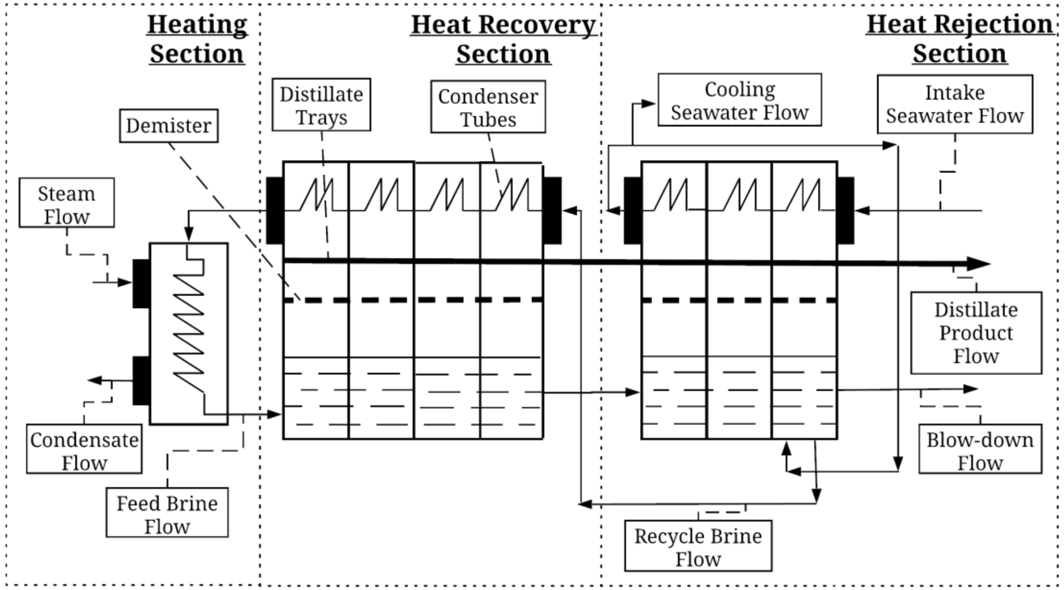


Figure 1: A typical Multi-Stage Flash desalination process.

- Input sea water absorbs latent heat of condensation → increases temperature
- Mixed with feed brine
- Some part rejected as blow-down → to control salinity
- Remaining is sent to next stage as recycle brine

- Feed brine flows inside chambers → looses heat
- Recycle brine absorbs latent heat of condensation → produces distillate
- Distillate collected on distillate tray

[3] Imad Alatiqi, Hisham Ettouney, and Hisham El-Dessouky. 1999. Process control in water desalination industry: an overview. European Conference on Desalination and the Environment 126, 1 (1999), 15 – 32

Attack Tree

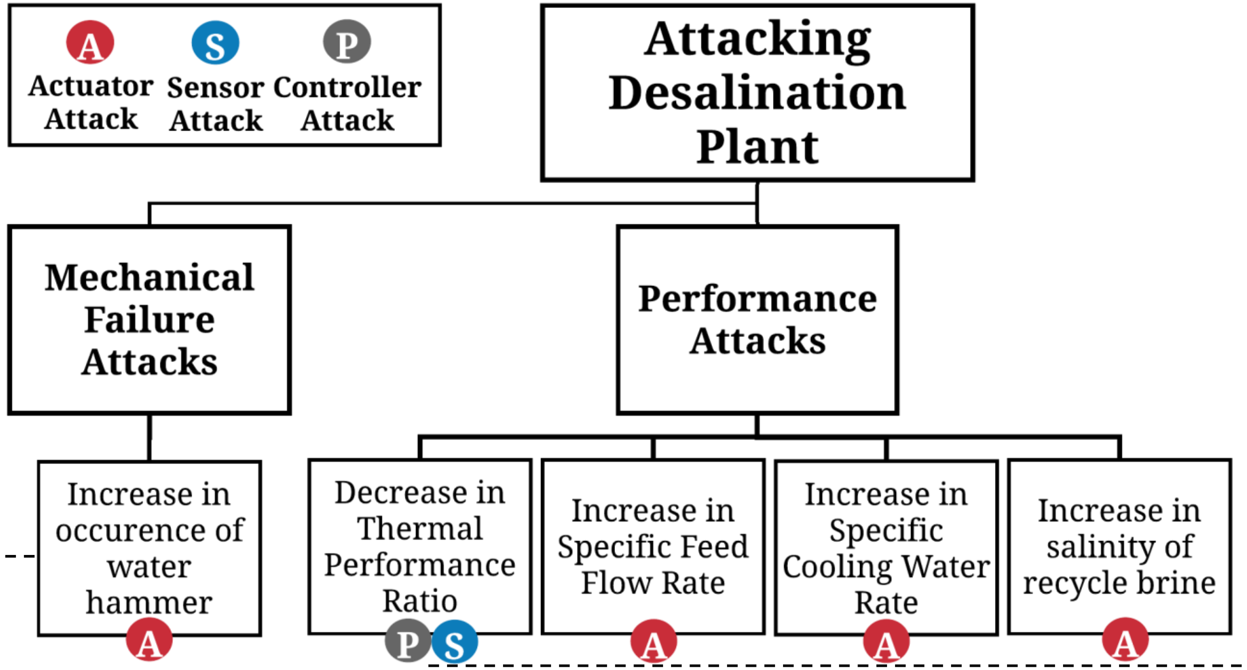


Figure 2: Attack tree for thermal desalination plants.

$$\frac{dP}{dt} = \rho a \frac{dv}{dt}$$

- $\frac{dv}{dt} \uparrow$, $\frac{dP}{dt} \uparrow$
- Adversary intends to induce water hammer

$$TPR = \frac{Distillate\ Output}{Steam\ Supplied}$$

- TPR ↑ , Distillate ↑ and Steam ↓
- Adversary intends to decrease TPR

Experimental Setup[8]

- MATLAB Simulink model
- Khubar II MSF plant in Saudi Arabia
- 22 stages → 3 Heat Rejection Sections and 19 Heat Recovery Sections
- 11 sensors, 11 valves and 3 PI Controllers

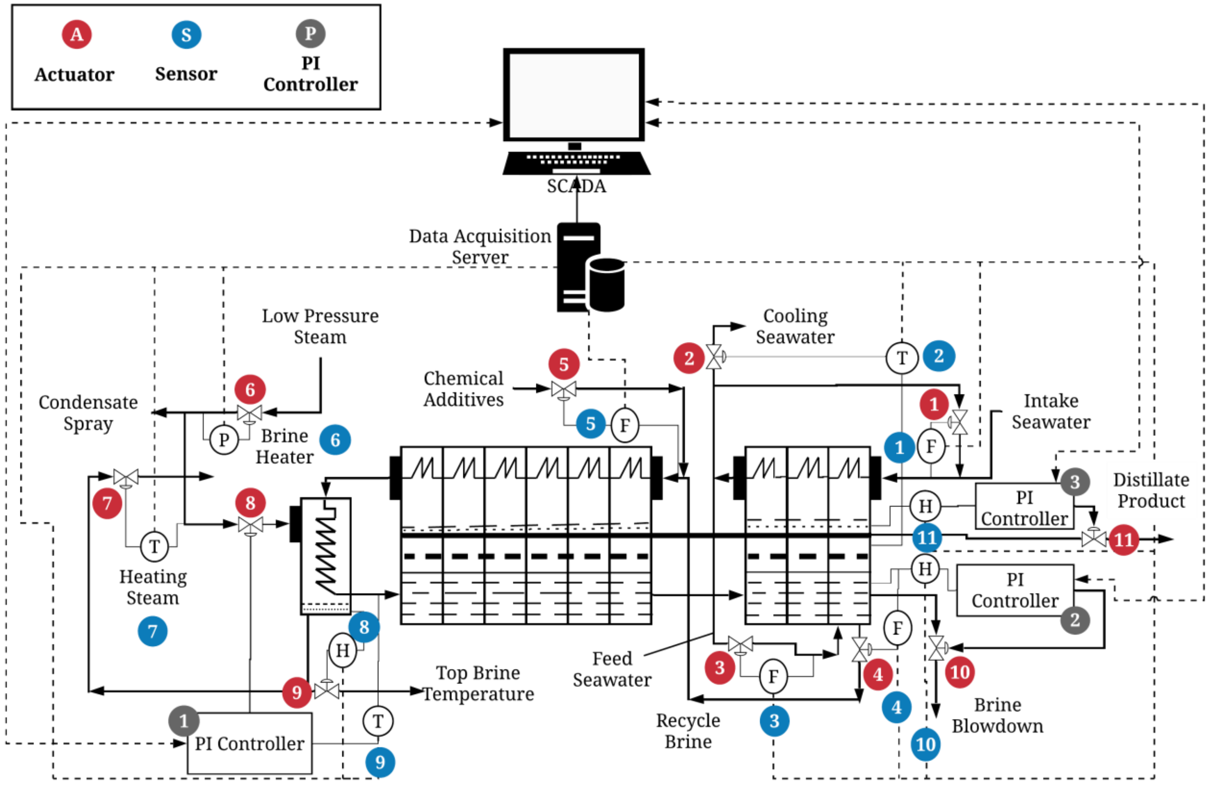


Figure 3: A MSF desalination Schematic.

Control Loop Example

- Sensor 9 → feed brine temperature
- PI Controller 1 reads this
- Actuator 8 (valve) is opened/closed to maintain the temperature
- In our simulation feed brine temperature was maintained at 93 C

Impact of Performance Attacks

Decrease in Thermal Performance Ratio

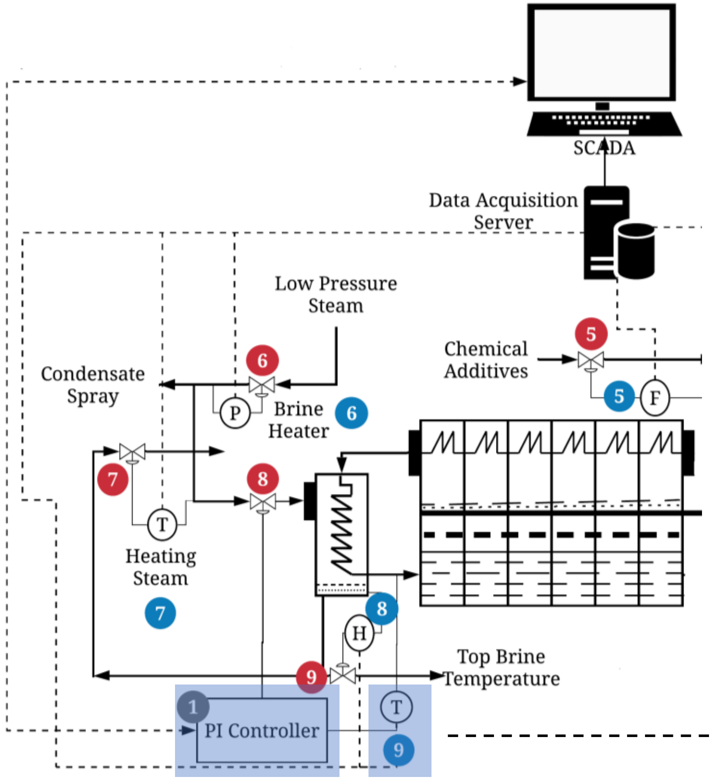


Figure 4: Plant Schematic for TPR Attack.

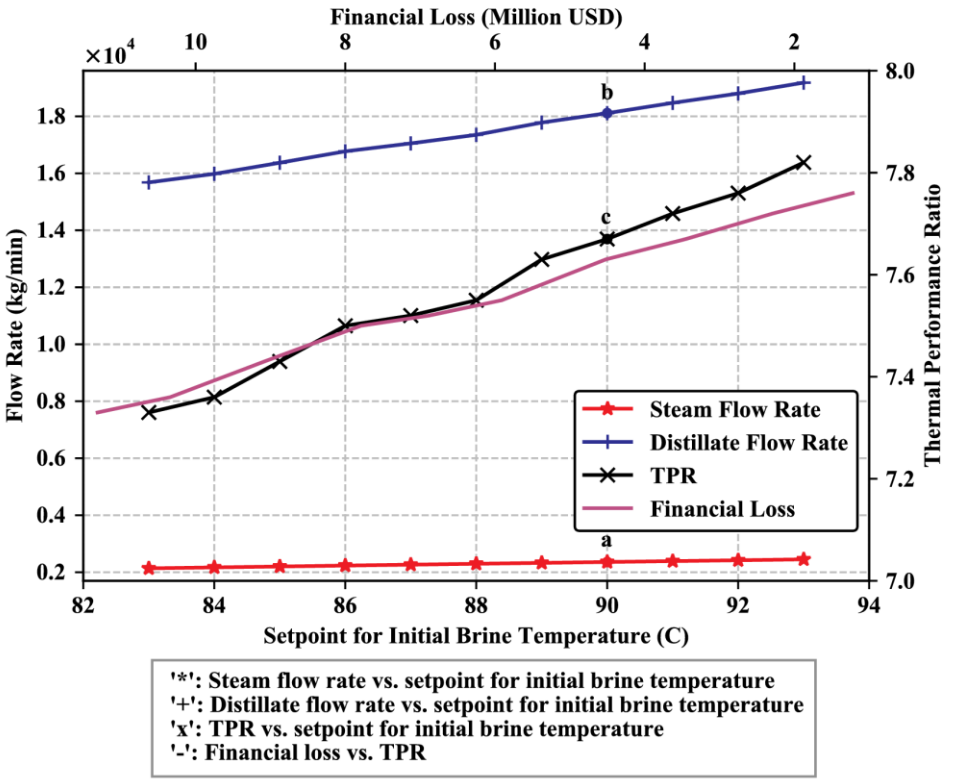


Figure 5: Change in distillate flow during attack to TPR.

- Setpoint: 93C → 90C
- 1.07 ton/min ↓ distillate produced
- Loss of $3 million

- I: 0.001 → 1
- 0.04 ton/min ↓ distillate produced
- Loss of $130K

- Sensor 9 measures initial brine temperature
- Temperature: 93C → 94C
- ↓ steam flow to 1000kg/min
- ↓ distillate production to 4.57 ton/min
- Remain undetected → spoof sensor data for fixed repeating intervals

Impact of Mechanical Failure Attacks

Increase in Occurrence of Water Hammer

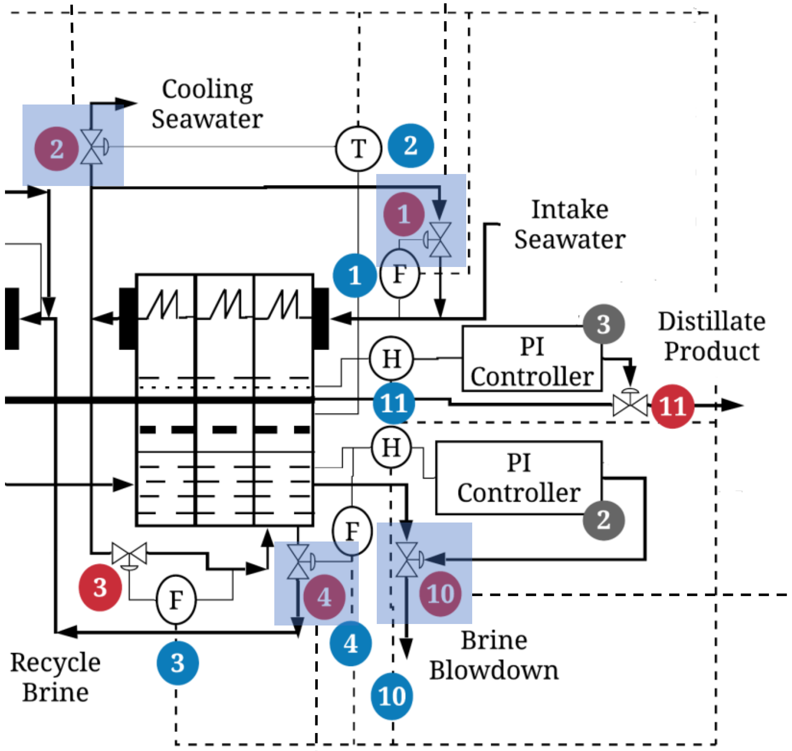


Figure 6: Plant Schematic for Water Hammer Attack.

- Actuator 2 → Reject flow rate
- Actuator 1 → Cooling sea water
- Close Actuator 2 and open Actuator 1

- Actuator 10 → Blowdown flow rate
- Adversary closes this valve suddenly to induce water hammer
  - Mechanical damage
  - Combine with corrosion

- Actuator 4 controls the recycle brine
- Close Actuator 4
- ↑ brine in stage 22
- ↑ salinity

Mechanical Attack Experimental Setup

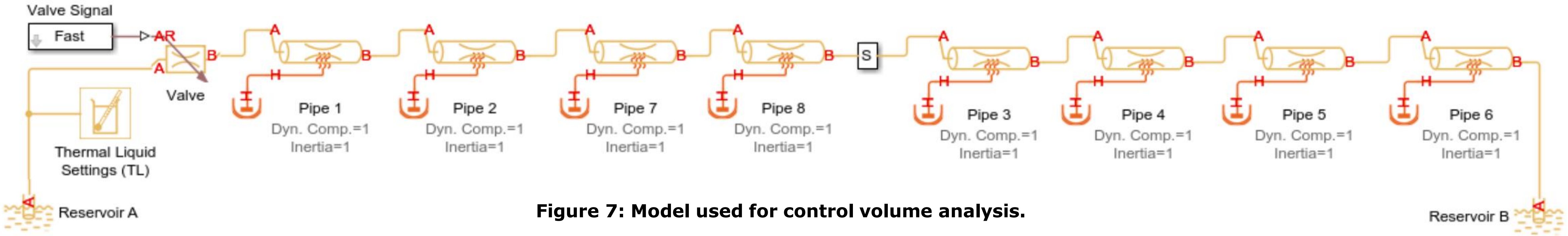


Figure 7: Model used for control volume analysis.

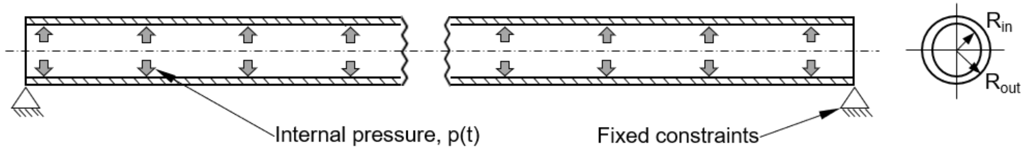


Figure 8: Schematic of the pipeline with boundary conditions used for finite element analysis.

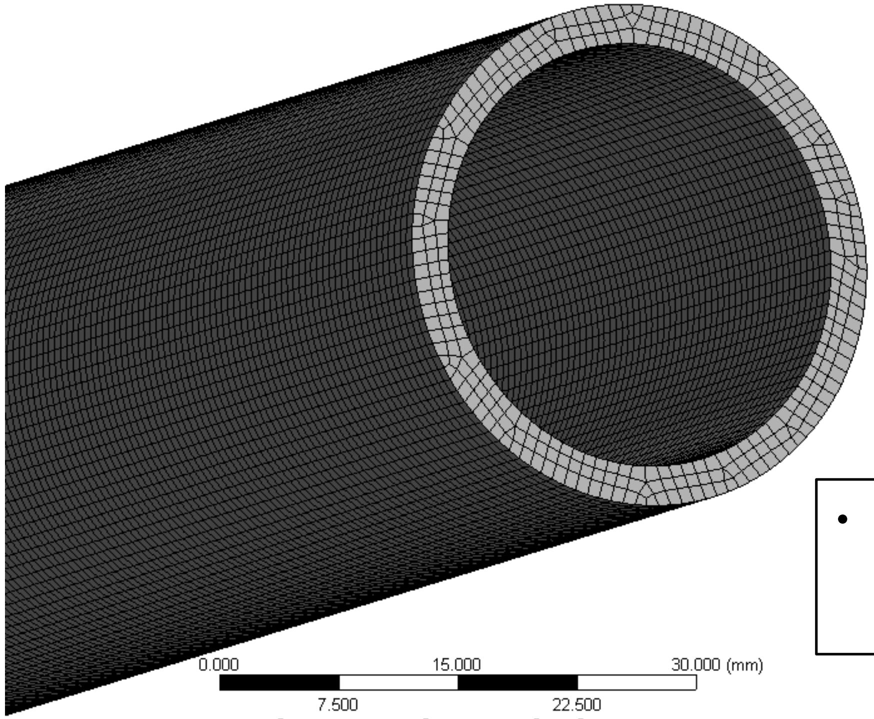


Figure 9: Pipe model in ANSYS.

- FEA: Structural problems modeled with discrete interconnected elements

Inner radius	0.0134 m
Wall Thickness	0.0025 m
Pipe Length	2.5 m
Nodes	540, 883

Impact of Mechanical Failure Attacks

Increase in Occurrence of Water Hammer

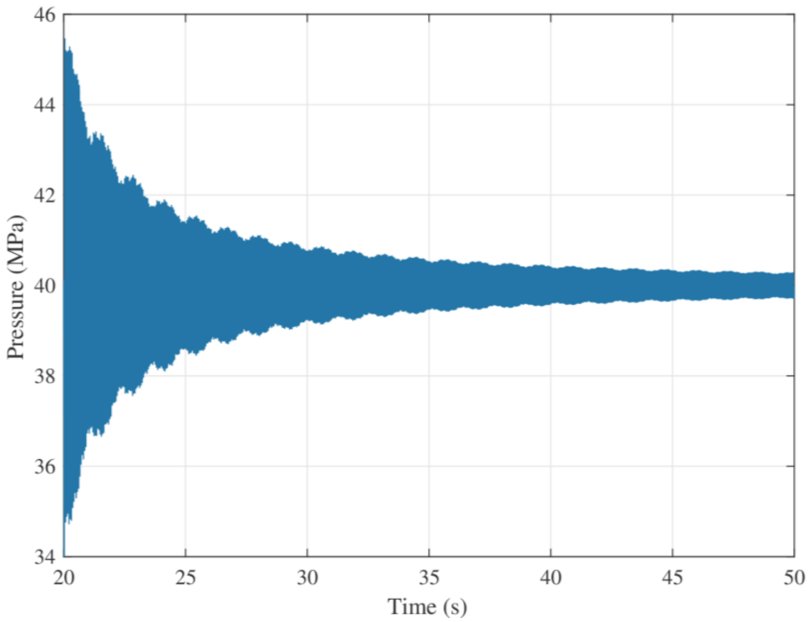


Figure 10: Pressure surge in the pipe.

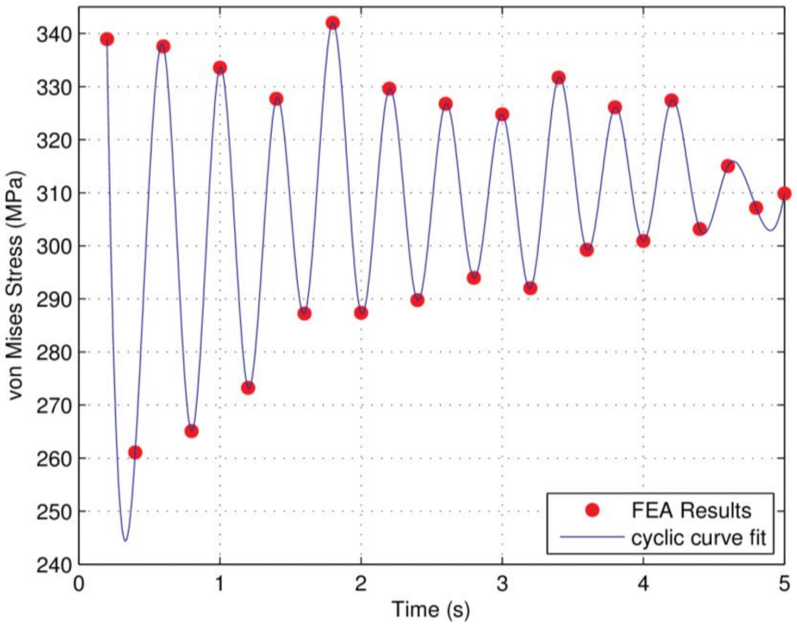


Figure 11: Von Mises Stress in the pipe.

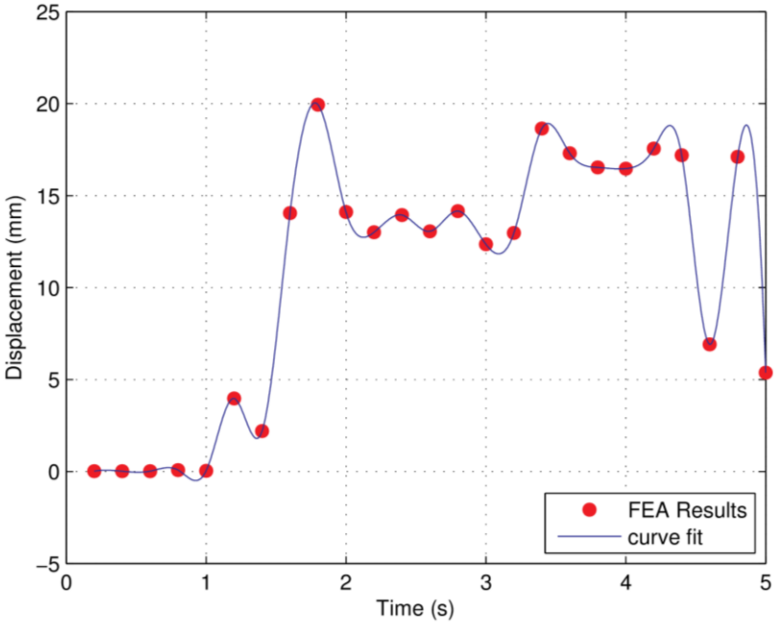


Figure 12: Displacement in the pipe.

- Pressure fluctuations just after water hammer
- Maximum Pressure Increase → 5MPa

- Stress follows pressure variations
- Maximum stress → 340MPa
- Yield Strength → 215 MPa

- Displacement in the pipe as a result of stresses induced
- Maximum displacement 19.9 mm
- Adversary exploited access to actuators 1, 2, 4 and 10

Discussion

- Maximizing Impact
  - TPR: Actuator 8 vs. PI Controller 2
  - Actuator 8 → steam inflow in the heater

- Remaining Within Operational Limit
  - Optimum product flow rate → 19.3 ton/min, Variation → 15 to 28 ton/min

- Future Work
  - Extend desalination simulation to include mechanical results
  - Opensource

Thank You