THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Using Modeled Cyber-Physical Systems for Independent Review of Intrusion Detection Systems

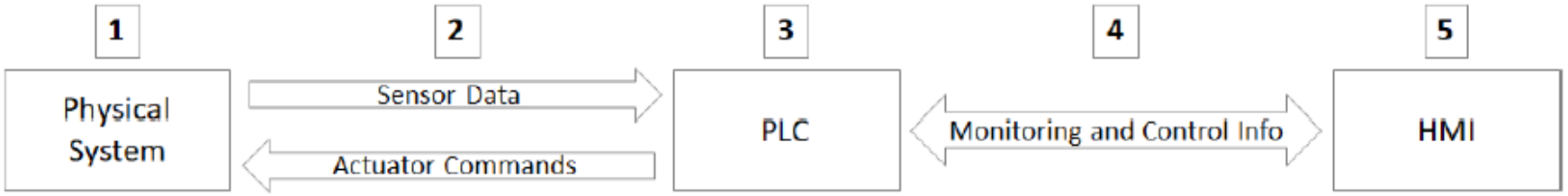
Sue Griffith
Research Engineer
UAH Center for Cybersecurity Research and Education

The Idea

- Create a virtual testbed of a cyber-physical system
- Create sample attacks
- Use standardized comparison metric
- Perform independent review of intrusion detection and prevention systems

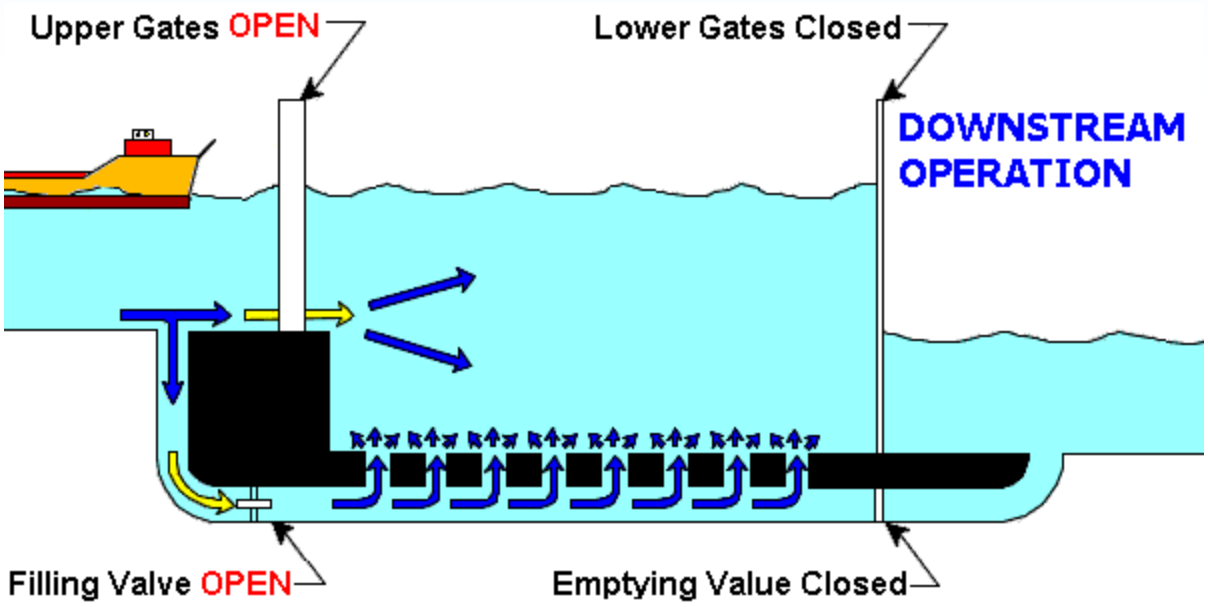
Introduction – CPSs

- Cyber Physical System (CPS)
  - Physical system controlled by digital device(s)
  - Manufacturing, utilities, etc.
- Broken into five distinct parts (see below)
- Safer to test on model than actual
- Modeled system is a navigational lock



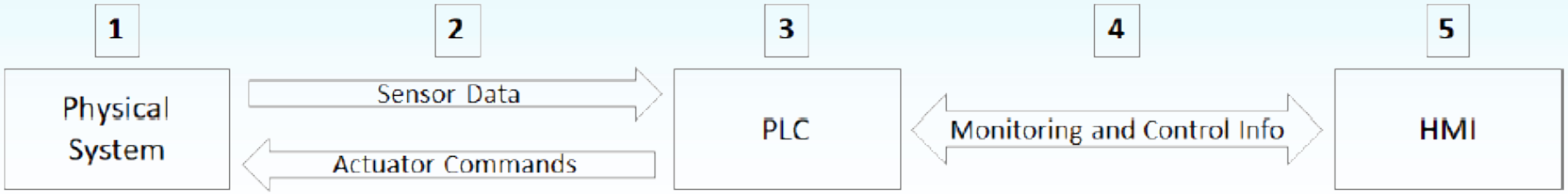
Dams 101 – Navigational Locks

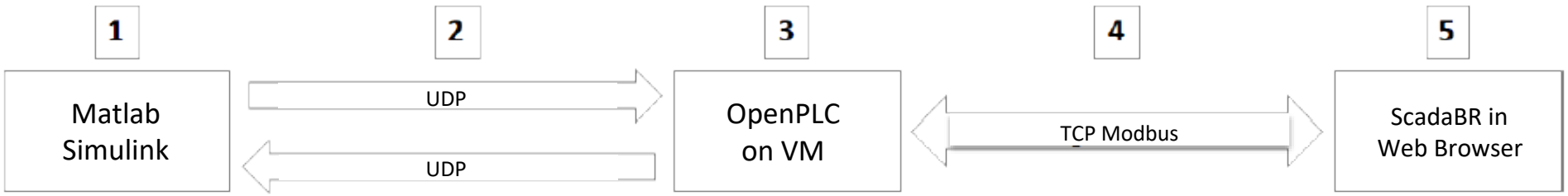
- Used to raise and lower ships at dams
- Gates and valves operated remotely
- Shipping relies on smooth operation



https://www.lre.usace.army.mil/Missions/Recreation/Soo-Locks-Visitor-Center/Soo-Locks-Animation/

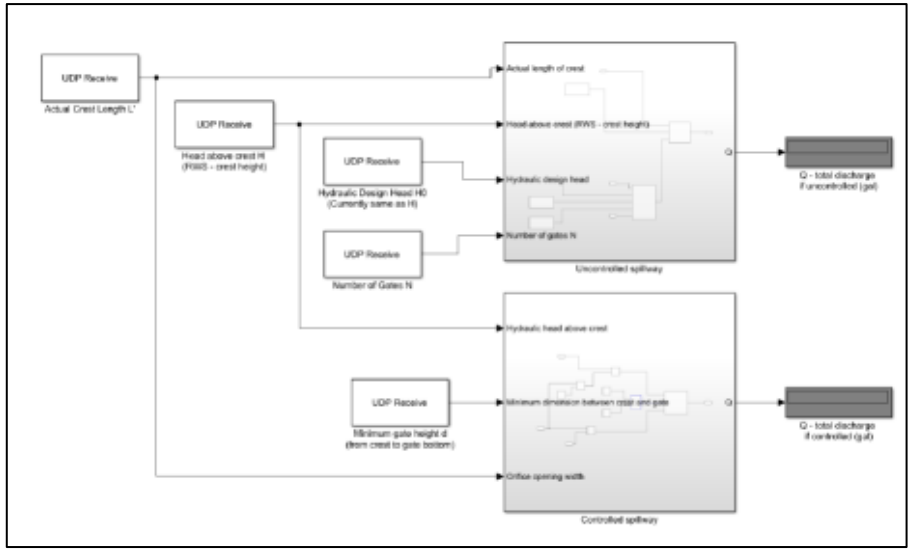
Virtual Testbed

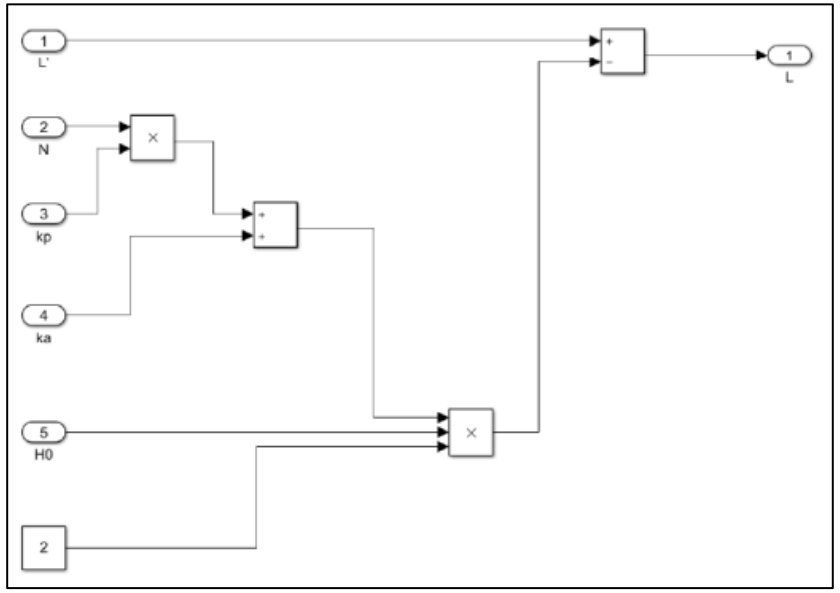




Testbed – Physical System

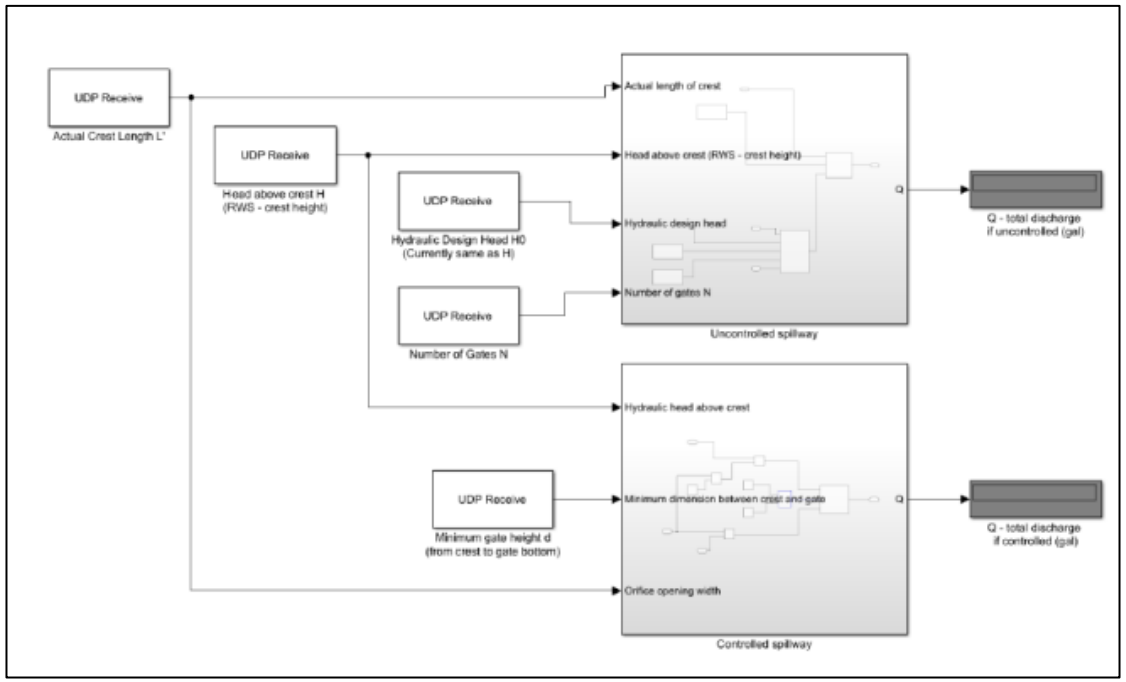
- Physical system includes real, moving parts
  - Gates and valves
- Modeled in Matlab Simulink
- Output via UDP connection





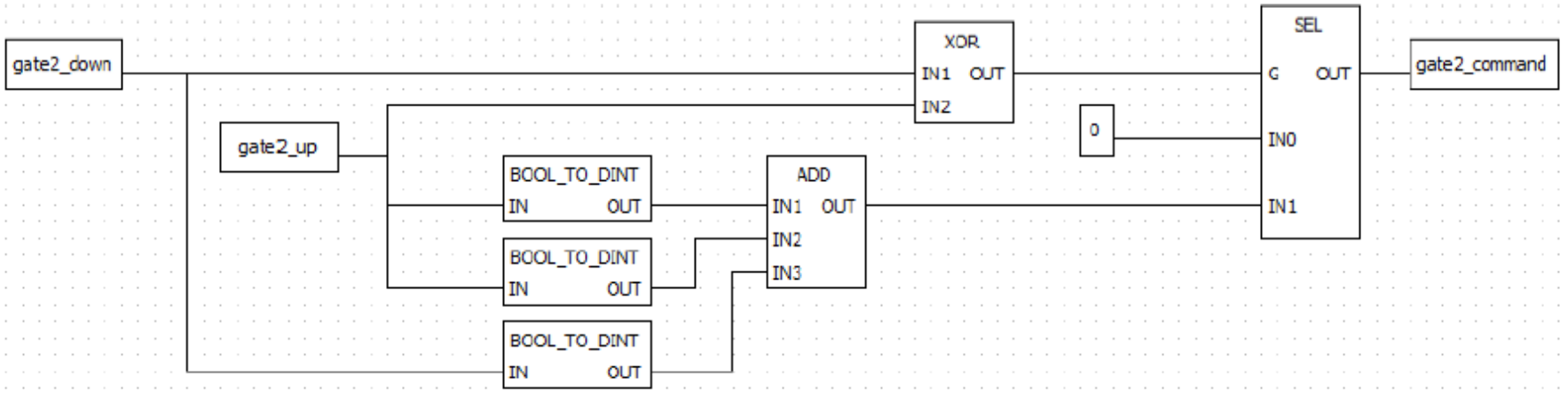
Testbed – UDP Connection

- Data sent between physical system and PLC via UDP
- Emulating a wired connection
  - UDP send and forget
- UDP send/receive built into Simulink
- PLC's virtual machine has interface to convert protocol



Testbed – Controller

- PLC (Programmable Logic Controller)
  - Used to read sensor data and control actuators
  - Receives commands from operators
  - Runs code written in ladder logic
  - Usually have limited memory and processing
- Will use OpenPLC running on virtual machine



Testbed – Modbus

- Data sent between PLC and HMI over Modbus
- Standard, open protocol
- Can be sent over TCP (called “TCP Modbus”)
- Simple to read and therefore manipulate
  - Device address
  - Function code
  - Payload (address to read, etc.)

Testbed – Human-Machine Interface

- HMI (Human Machine Interface)
- Used by operator to monitor and control physical parts
- Can be physical control panel or GUI
- Creating in ScadaBR
  - Free and open-source
  - Runs on server on host computer
  - Access via web browser

What to use it for? Testing IDS/IPSs

- Intrusion Detection and Prevention System (IDS/IPS)
  - Installed on host or network device
  - Monitors for potentially malicious data
- Have been studied for use on CPS controllers
- No set approach to testing effectiveness
- Need variety of attacks to test

Designing Attacks

- Three types chosen by frequency in literature
  - Reconnaissance
  - Man-in-the-Middle (MitM)
  - Denial of Service (DoS)
- To be sent in baseline, generic traffic

Designing Attacks

- Reconnaissance
  - No system change
  - Eavesdropping on network
  - Scanning addresses

Designing Attacks

- Man-in-the-Middle (MitM)
  - Use network access to interfere
  - Injection – send commands or data
  - Replay – record and send back
  - Alteration – intercept, change, resend

Designing Attacks

- Denial of Service (DoS)
  - Make device unreachable
  - Overwhelm system with packets
  - Intercept and drop all data (DoS/MitM)

Attacks

#	Category	Attack Name	Description
1	Recon	Query 1	Query all addresses to find which are in use
2	Recon	Query 2	Query select addresses to find which are in use
3	Injection (MitM)	Com. Inj. 1	Inject random commands
4	Injection (MitM)	Com. Inj. 2	Inject sensical commands chosen by researcher
5	Injection (MitM)	Resp. Inj. 1	Inject random response values
6	Injection (MitM)	Resp. Inj. 2	Inject sensical response values
7	Injection (MitM)	Resp. Inj. 3	Inject out of bounds response values
8	Replay (MitM)	MitM Replay 1	Record and re-send sensor readings
9	Replay (MitM)	MitM Replay 2	Record and re-send commands from HMI
10	Alteration (MitM)	MitM Alt. 1	Record, change payload value randomly, re-send
11	Alteration (MitM)	MitM Alt. 2	Record, change payload value set amount, re-send
12	Alteration (MitM)	MitM Alt. 3	Record, change command randomly, re-send
13	Alteration (MitM)	MitM Alt. 4	Record, change to chosen command, re-send
14	DoS	DoS Flood 1	Flood with nonsensical packets
15	DoS	DoS Flood 2	Flood with valid packets
16	DoS/MitM	DoS/MitM	Intercept and drop all packets

Comparison Criteria

- IDS/IPS effectiveness will be determined by set criteria
  - Detected attacks
  - False positives – flag safe traffic as malicious
  - False negatives – flag malicious traffic as safe
  - Speed with which attack detected
  - Storage size of IDS/IPS
  - System functionality post-attack
- As with set of attacks, future users can easily add on

Running the Tests

- Must recreate these IDS/IPSs as best possible
  - Try to reproduce using publications
  - Contacting authors when possible
- Use previously discussed criteria to compare
- Publish results, improve field, etc.

Questions?

s.griffith@uah.edu
Booth 220
uah.edu/ccre