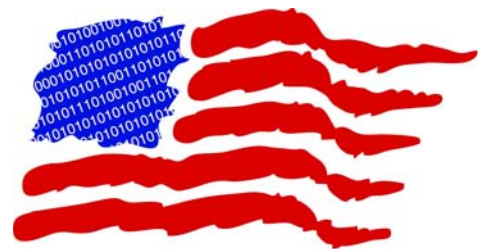


010010101001010101010100110010101010100001010101010101010100010100100

Modeling Control System Failures and Attacks – The Waterloo Campaign to Oil Pipelines

J. Butts, M. Rice, S. Shenoii
University of Tulsa
Tulsa, Oklahoma

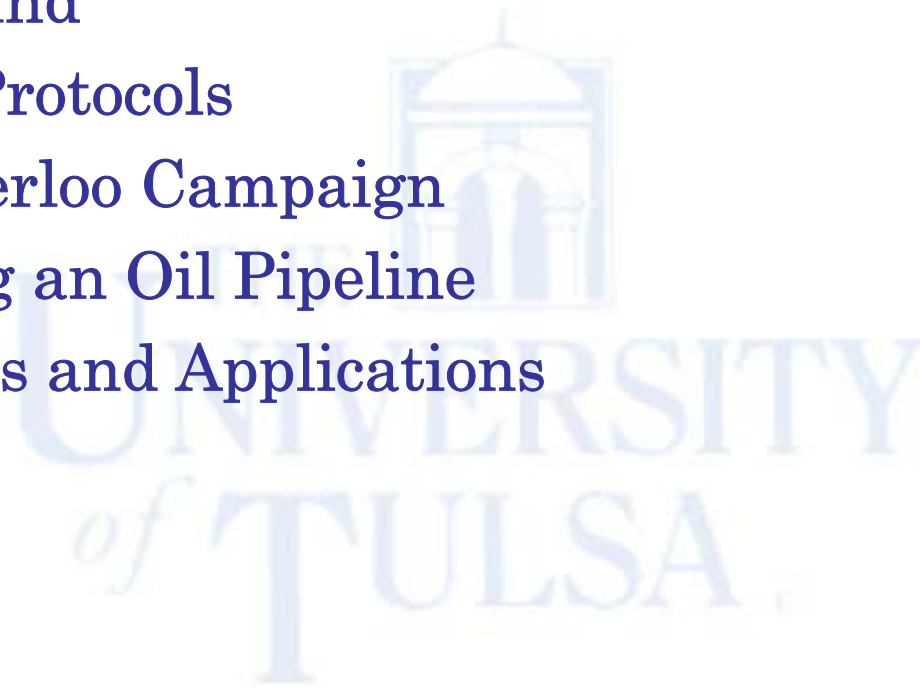


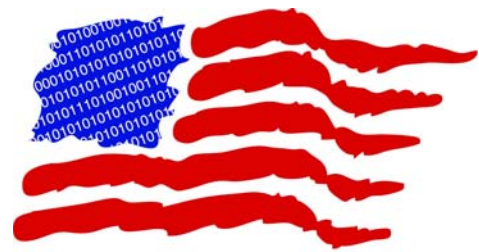
Outline



0100101010010101010101001100101010101000010101010101010100010100100

- Background
- Control Protocols
- The Waterloo Campaign
- Attacking an Oil Pipeline
- Attributes and Applications

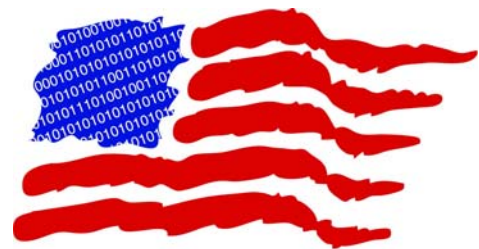




Control Systems

010010101001010101010100110010101010100001010101010101010100010100100—●

- **Backbone of nation's critical infrastructure**
 - Power grid, transportation, oil & gas, public works
- **Foreign countries and potential adversaries**
 - Rely on similar systems and technologies
- **Historically considered “kinetic targets”**
 - Evolution of technologies is altering warfare
 - Must understand vulnerabilities to defend systems from attack
 - Ability to exploit enemy will likely prove critical in future conflicts

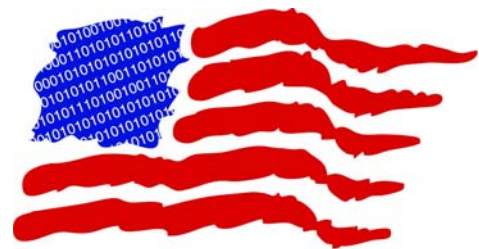


Control Systems

010010101001010101010100110010101010100001010101010101010100010100100—●

- Today's landscape
 - Cyber attacks on control systems are hindered by operational fog
 - Intelligence requirements
 - Effectiveness and assurance
 - Understanding of capabilities
 - No “endgame theory” or structured analysis
- Need for comprehensive understanding of control system failures and attacks

Formal methods are required to derive predictability and assurances similar to “kinetic” methods currently employed

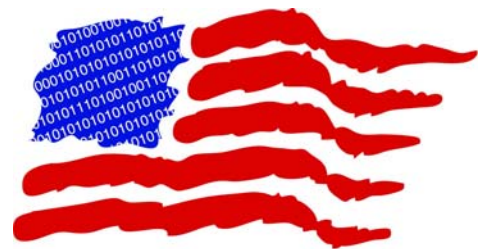


Control Protocols



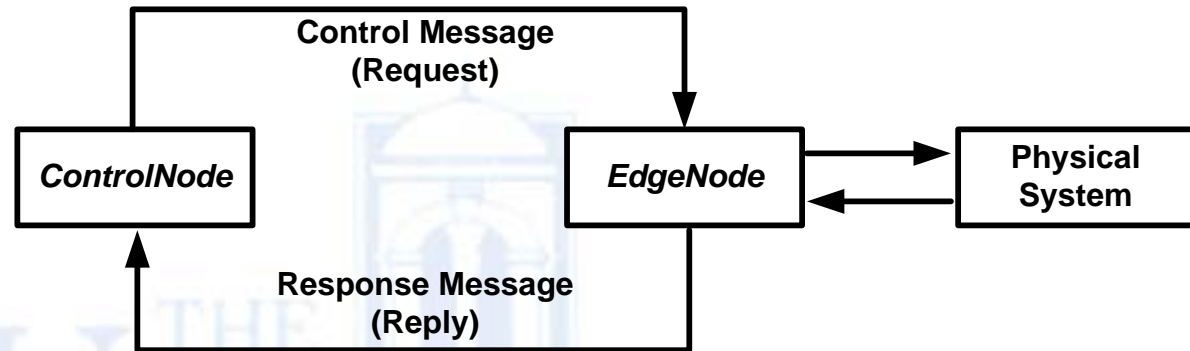
010010101001010101010100110010101010100001010101010101010100010100100

- Control is vital to any battle plan
 - Commander maintains situational awareness
 - Uses control techniques to maneuver forces
 - Battles won and lost because of control successes and failures
- Control “system” attributes
 - Messages direct actions and provide feedback
 - Device roles determine hierarchical structure
 - Message generation occurs based on conditional or scheduled events
 - A determined sequence of messages form a predictable stream
 - There may be multiple, concurrent message streams

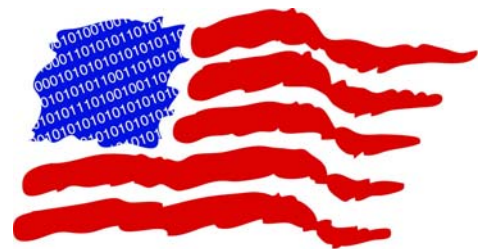


Control Protocols

0100101010010101010101001100101010101000010101010101010100010100100 —●



- **Primitive message types**
 - Request: Specify control actions and obtain data
 - Reply: Provide feedback and updates
- **Protocols**
 - Derived from primitive message types
 - Unicast, broadcast, unsolicited reply



Model Language

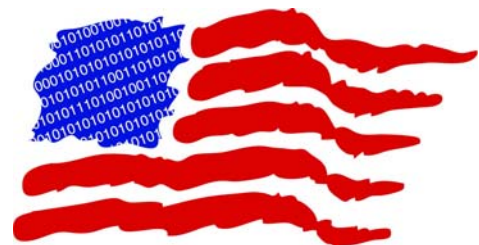


010010101001010101010100110010101010100001010101010101010100010100100—●

- Control System Components
 - Control device, Edge device, Communication paths
- Message transaction

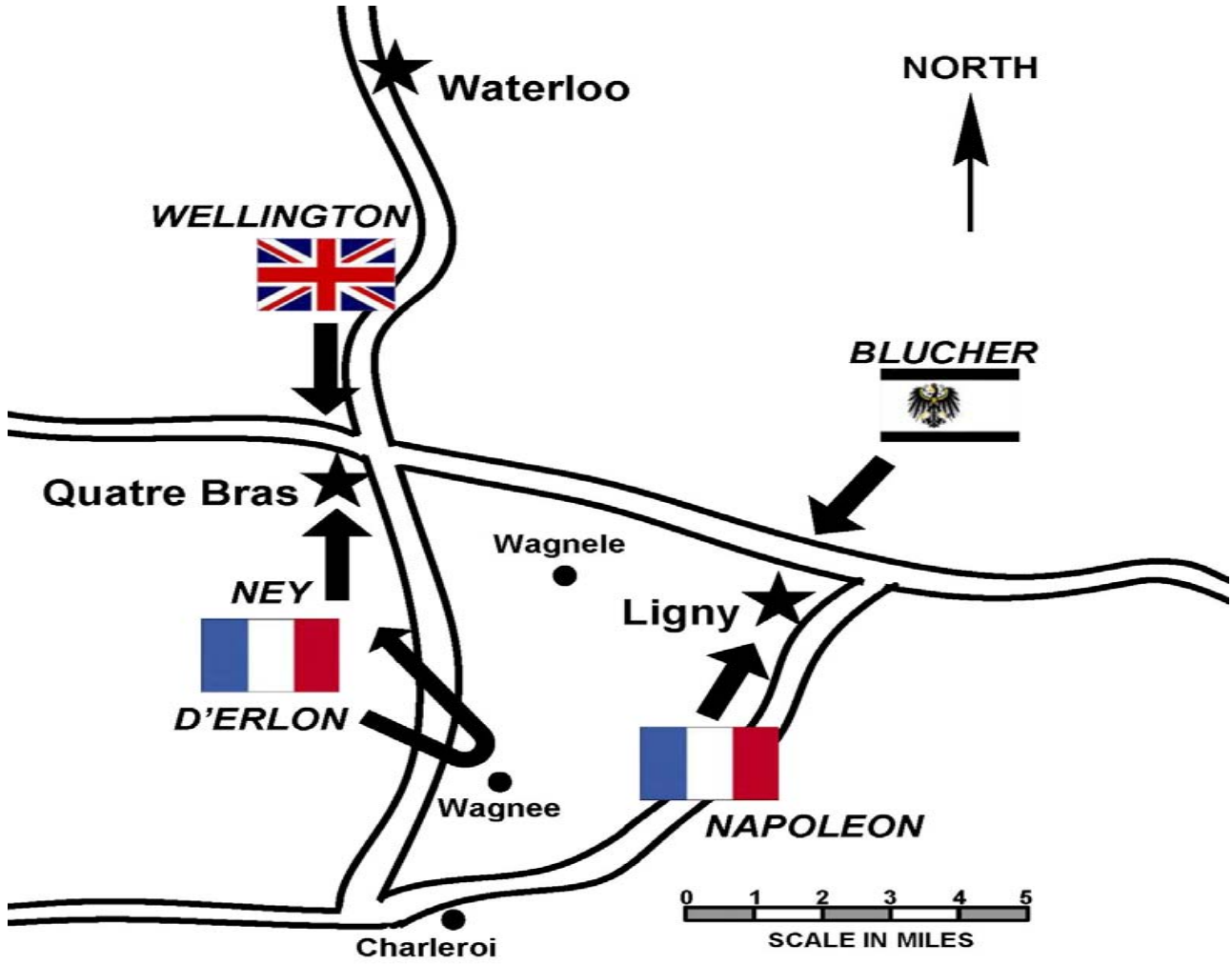
$$MsgSource \xrightarrow[MsgTypes]{CommPaths} MsgDest[Payload]$$

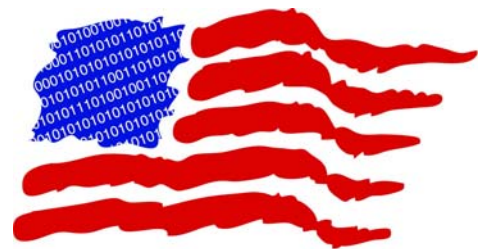
- Processes
 - Determined sequence of messages
- Attacker Capabilities
 - Fabricate (+) and Block (¬)
- States
 - Devices change state based on received message or change in physical parameters of system



Waterloo Campaign

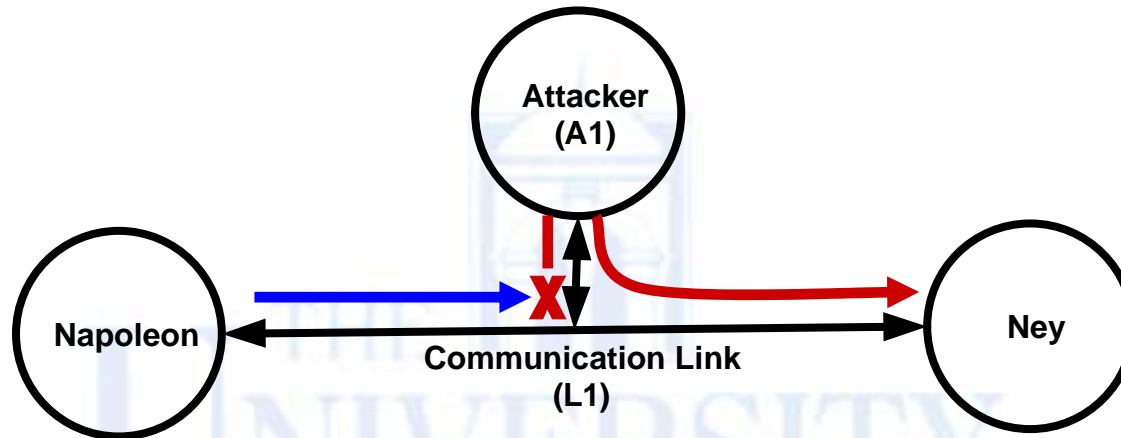
010010101001010101010100110010101010100001010101010101010100010100100



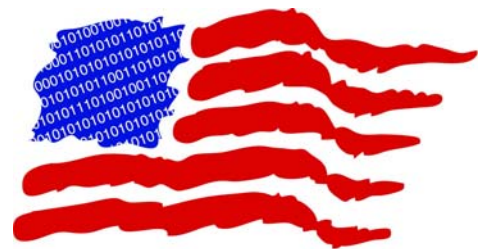


Waterloo Campaign

010010101001010101010100110010101010100001010101010101010100010100100



- **Control Failure 1 (Delay in Attacking Quatre Bras)**
 - Attacker blocks message from Napoleon to Ney ordering to attack
 - Attacker fabricates message to Ney ordering to attack



Waterloo Campaign

010010101001010101010100110010101010100001010101010101010100010100100

System

SystemNodes = {Napoleon, Ney}

CommPaths = {L1}

L1 = (Napoleon, Ney)

MsgTypes = {Request}

Attacker Capabilities

L1 = {¬, +}

Initial Node States

Ney := Ney⁰

Napoleon := Ney⁰

Possible Node States

Ney := Ney⁰ | Ney¹

Ney⁰ ≡ Attack on Quatre Bras is FALSE

Ney¹ ≡ Attack on Quatre Bras is TRUE

Napoleon := Ney⁰ | Ney¹

Control Failure 1

1. Napoleon $\xrightarrow[\neg Request]{L1}$ Ney[Attack]

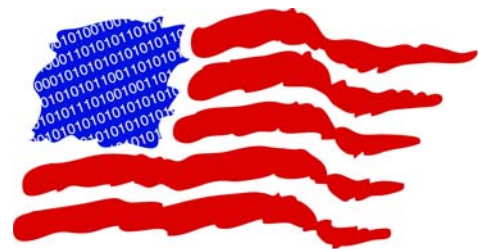
Ney := Ney⁰

Napoleon := Ney¹

2. Napoleon $\xrightarrow[+ Request]{L1}$ Ney[Attack]

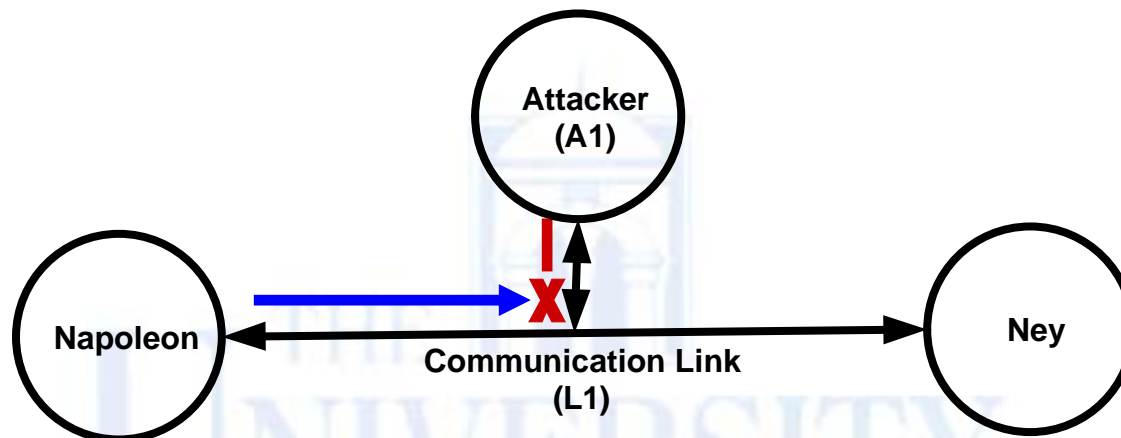
Ney := Ney¹

Napoleon := Ney¹

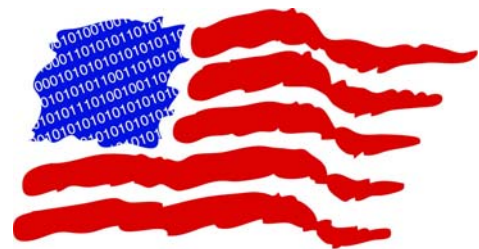


Waterloo Campaign

010010101001010101010100110010101010100001010101010101010100010100100

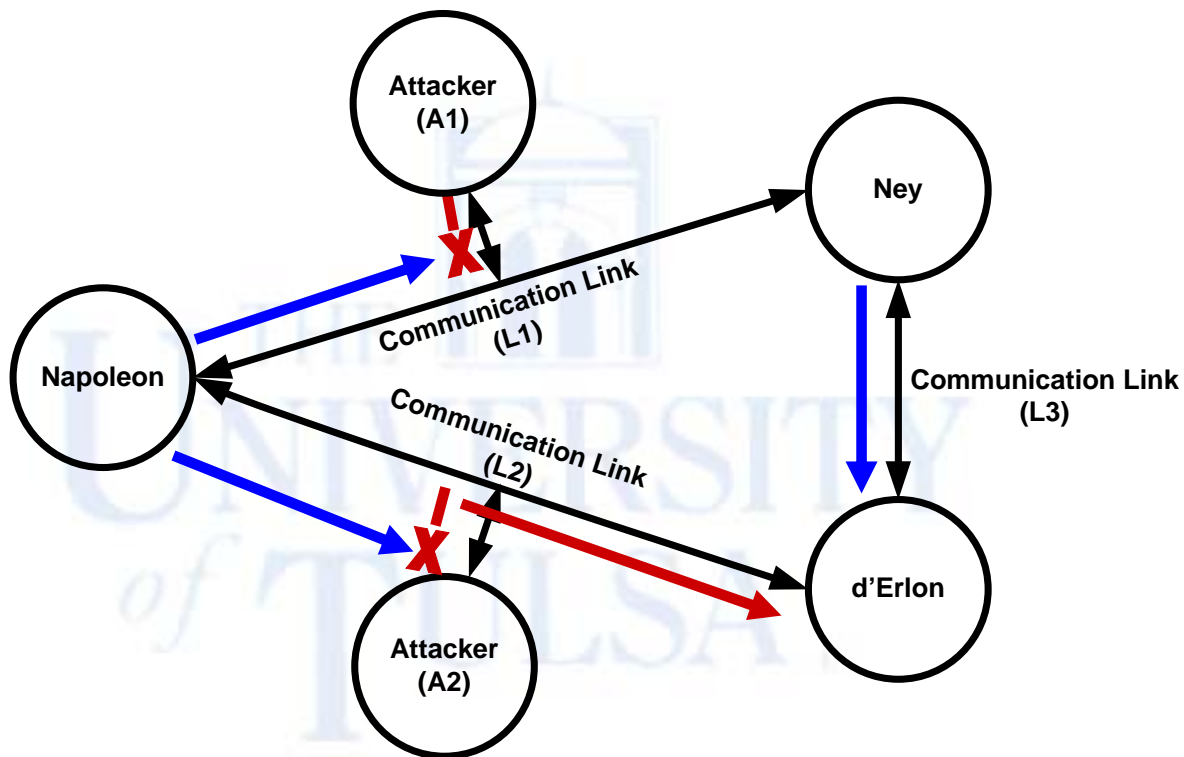


- **Control Failure 2 (Failure to Mobilize a Blocking Force)**
 - Attacker blocks message from Napoleon to Ney ordering to attack

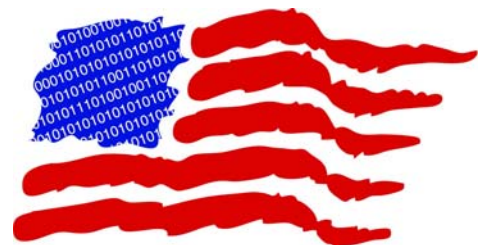


Waterloo Campaign

01001010100101010101010100110010101010100001010101010101010100010100100

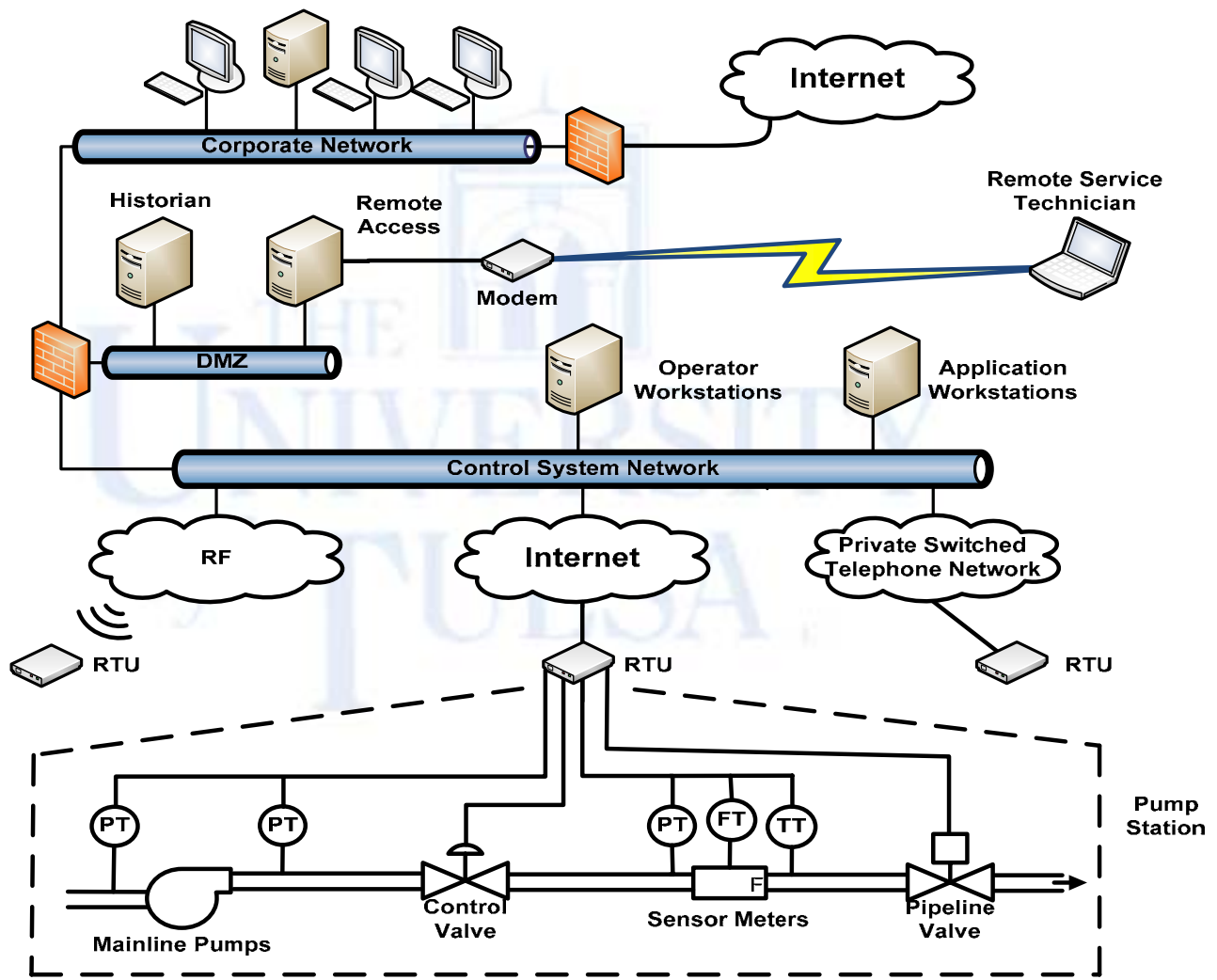


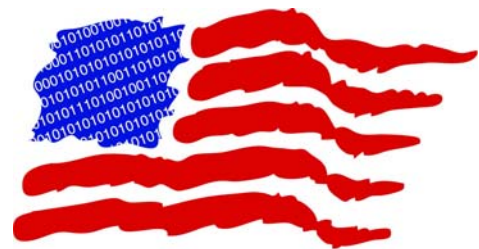
- Control Failure 3 (Failure to Engage Reserve Force)



SCADA Network Example

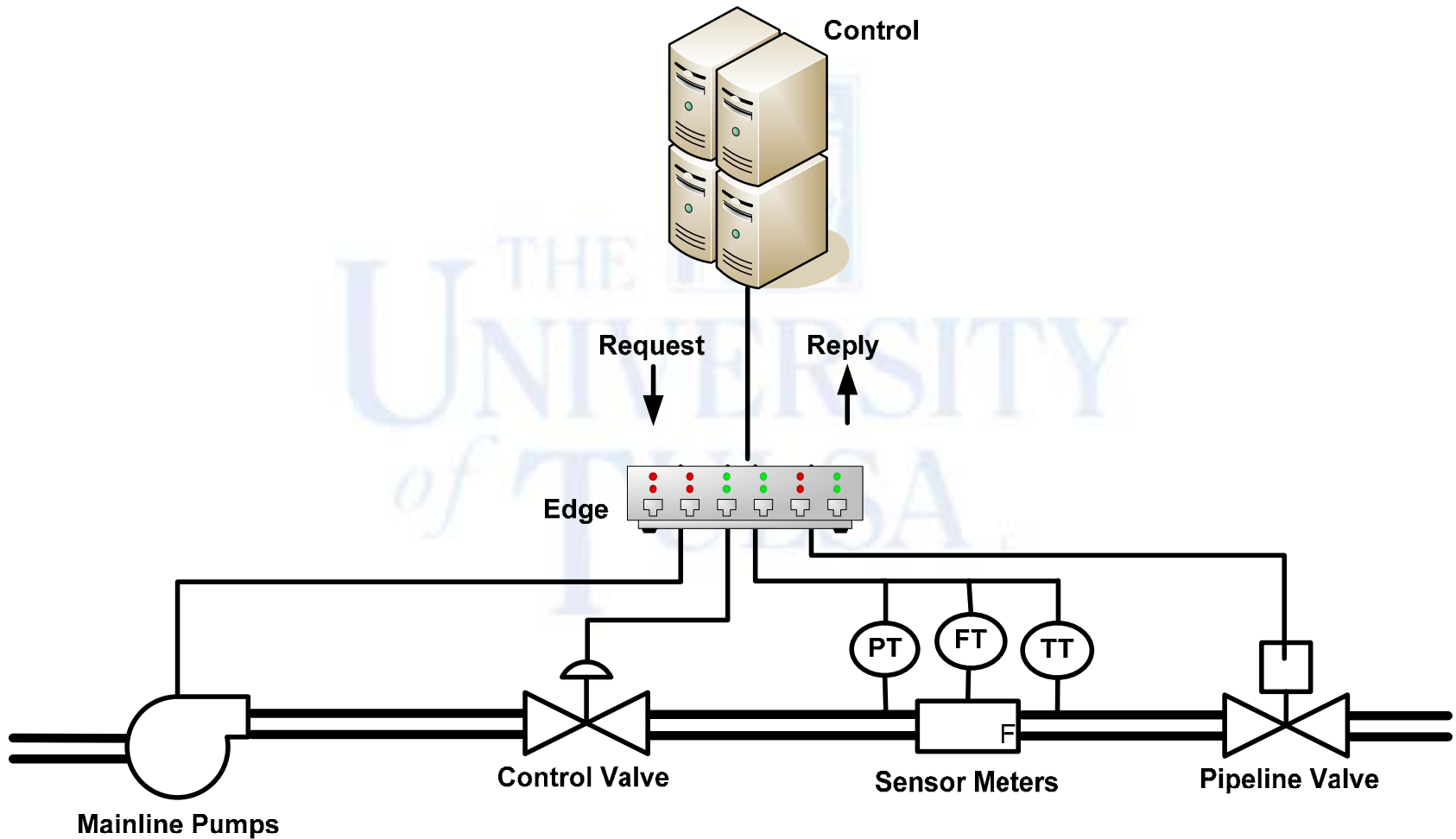
010010101001010101010100110010101010100001010101010101010100010100100

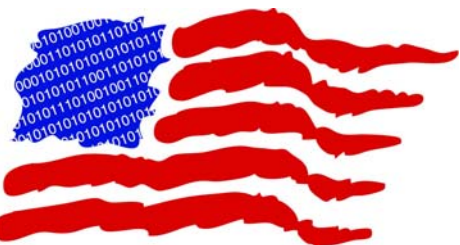




Control System Messaging

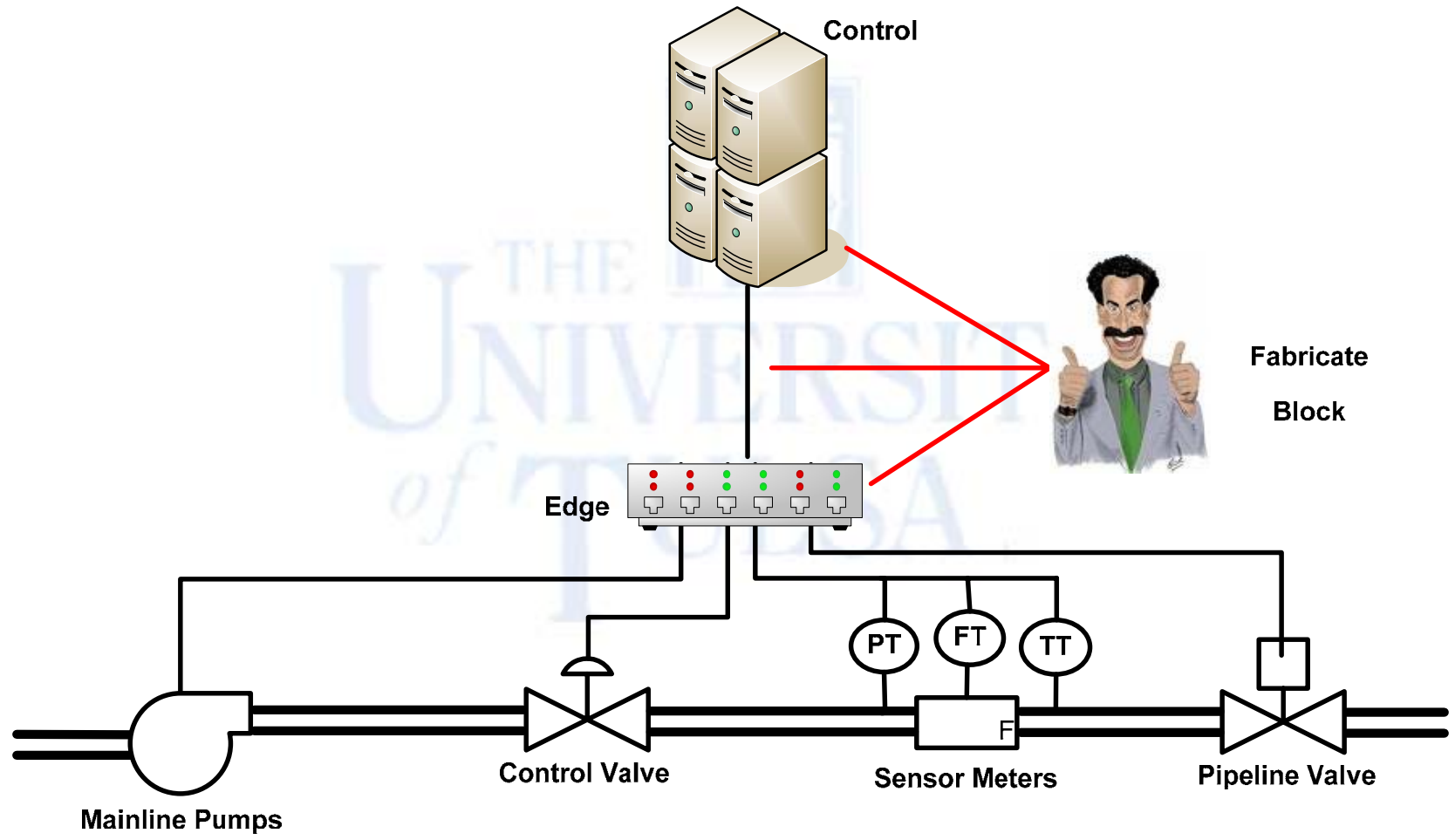
0100101010010101010101001100101010101000010101010101010100010100100—●

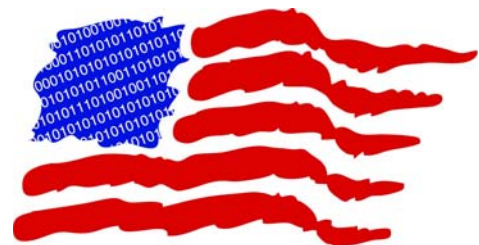




Attacker Capabilities

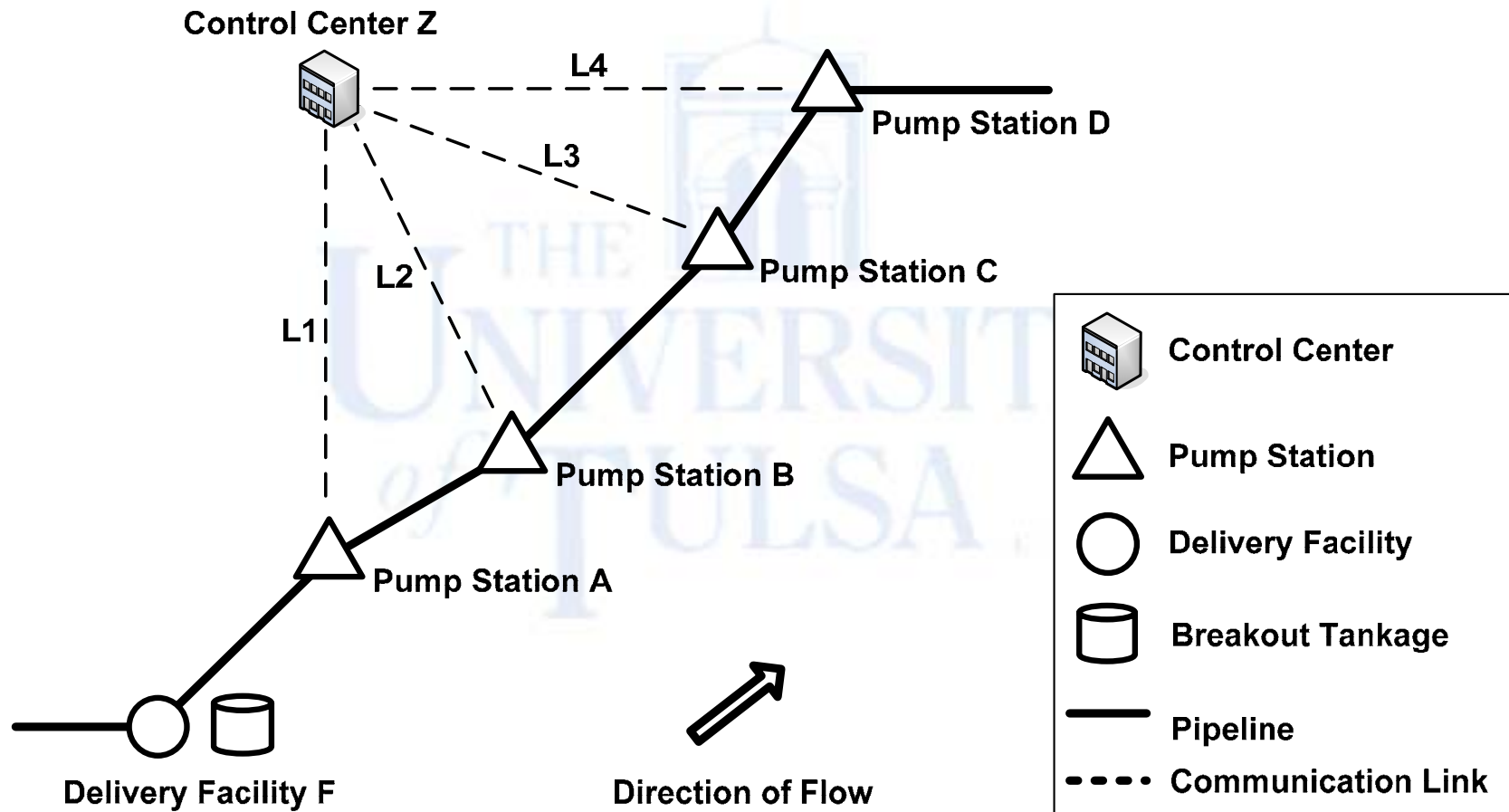
0100101010010101010101001100101010101000010101010101010100010100100

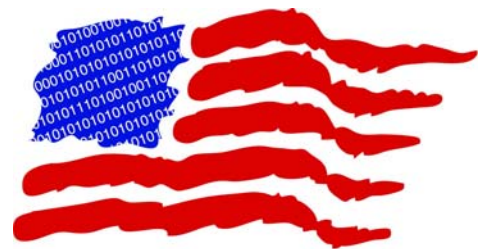




Attacking an Oil Pipeline

0100101010010101010101001100101010101000010101010101010100010100100



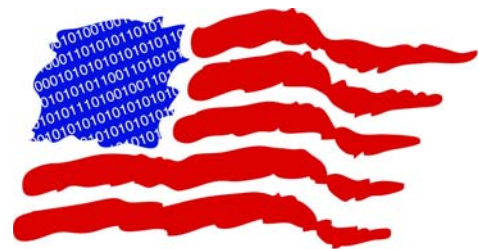


Modeling Control Failures



010010101001010101010100110010101010100001010101010101010100010100100100—●

- Control Failure 1 (Increase in Pumping Capacity)
 - Fabricate Control Message and Block Reply
- Control Failure 2 (Failure to Start Second Pump)
 - Block Control Message and Fabricate Reply
- Control Failure 3 (Stoppage of Active Pump)
 - Fabricate Control Message and Block Reply
- Control Failure 4 (Failure of Alert Notifications)
 - Block Polling Messages and Fabricate Reply

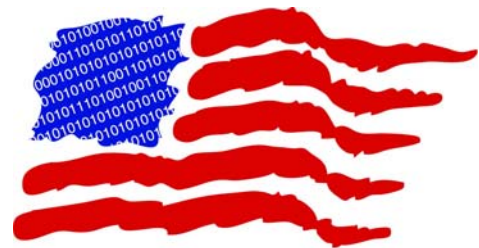


System States

U CYBER CORPS
Defending America's Cyberspace

010010101001010101010100110010101010100001010101010101010100010100100—●

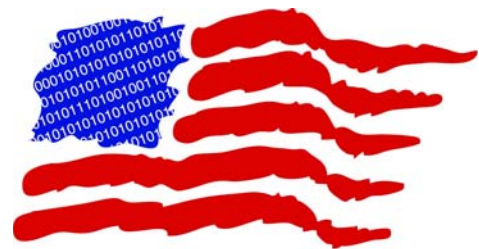
State	Pump #1	Pump #2	Pump #3	Pressure	Alarm
A ⁰	On	Off	Off	Acceptable	F
A ¹	On	On	Off	Acceptable	F
A ²	*	*	*	*	T
B ⁰	On	Off	Off	Acceptable	F
B ¹	On	On	Off	Acceptable	F
B ²	*	*	*	*	T
C ⁰	On	Off	Off	Acceptable	F
C ¹	On	Off	On	Acceptable	F
C ²	Off	Off	On	Acceptable	F
C ³	*	*	*	*	T
D ⁰	On	Off	Off	Acceptable	F
D ¹	Off	Off	On	Acceptable	F
D ²	Off	Off	Off	*	*
D ³	*	Off	On	Acceptable	F



Modeling Control Failures

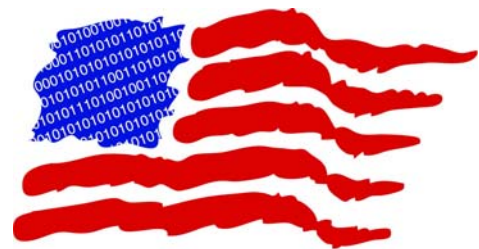
010010101001010101010100110010101010100001010101010101010100010100100—●

<p><u>Process 1</u> $\psi = 1$ 1. Z $\xrightarrow{L1}$ A[Start Pump #2] $Z + Request$ $A := A^1$ $Z := (A^0, B^0, C^0, D^0)$ 2. A $\xrightarrow{L1}$ Z[ACK] $Z \neg Reply$ $A := A^1$ $Z := (A^0, B^0, C^0, D^0)$ 3. Z $\xrightarrow{L2}$ B[Start Pump #2] $Z + Request$ $B := B^1$ $Z := (A^0, B^0, C^0, D^0)$ 4. B $\xrightarrow{L2}$ Z[ACK] $Z \neg Reply$ $B := B^1$ $Z := (A^0, B^0, C^0, D^0)$ 5. Z $\xrightarrow{L3}$ C[Start Pump #3] $Z + Request$ $C := C^1$ $Z := (A^0, B^0, C^0, D^0)$ 6. C $\xrightarrow{L3}$ Z[ACK] $Z \neg Reply$ $C := C^1$ $Z := (A^0, B^0, C^0, D^0)$ 7. Z $\xrightarrow{L3}$ C[Stop Pump #1] $Z + Request$ $C := C^2$ $Z := (A^0, B^0, C^0, D^0)$ 8. C $\xrightarrow{L3}$ Z[ACK] $Z \neg Reply$ $C := C^2$ $Z := (A^0, B^0, C^0, D^0)$</p>	<p><u>Process 2</u> $\psi = \infty$ CONDITIONAL: IF $(Z == (A^*, B^*, C^*, D^0)$ or $(A^*, B^*, C^*, D^2))$ 1. Z $\xrightarrow{L4}$ D[Start Pump #3] $Z \neg Request$ $D := D^*$ $Z := (A^0, B^0, C^0, D^3)$ 2. D $\xrightarrow{L4}$ Z[ACK] $Z + Reply$ $D := D^*$ $Z := (A^0, B^0, C^0, D^3)$</p> <p><u>Process 3</u> $\psi = 1$ 1. Z $\xrightarrow{L4}$ D[Stop Pump #1] $Z + Request$ $D := D^2$ $Z := (A^0, B^0, C^0, D^0)$ 2. D $\xrightarrow{L4}$ Z[ACK] $Z \neg Reply$ $D := D^2$ $Z := (A^0, B^0, C^0, D^0)$</p>
---	---



Control System Messaging

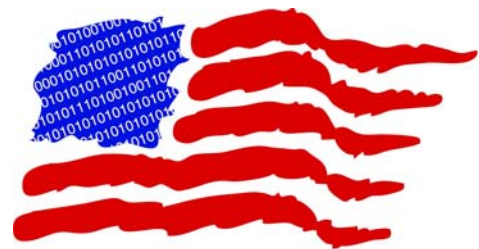
Modbus	DNP3	Profibus	Waterloo
Request/Reply	Request/Reply Unsolicited Reply	Request/Reply	Request
Unicast and Broadcast	Unicast and Broadcast	Unicast and Broadcast	Unicast only
No Guaranteed Integrity	No Guaranteed Integrity	No Guaranteed Integrity	No Guaranteed Integrity
Non-Repudiation Uncertain	Non-Repudiation Uncertain	Non-Repudiation Uncertain	Non-Repudiation Degree of Certainty
No Guaranteed Confidentiality	No Guaranteed Confidentiality	No Guaranteed Confidentiality	No Guaranteed Confidentiality



Attributes

010010101001010101010100110010101010100001010101010101010100010100100—●

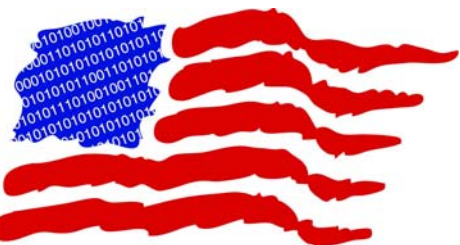
- Generality allows abstract characterizations
- Expressive for specific analysis
- Models temporal aspects and causal effects
- Attack-centered
- Provides holistic system view
 - Situational awareness represented through node states
- Expresses complex attacks using simple constructs
 - Primitive message types Request and Reply
 - Attack operators Fabricate and Block
 - Demonstrated delay, modify and DoS



Application

010010101001010101010100110010101010100001010101010101010100010100100—●

- **Conceptualize attacks**
 - Translate similar attacks to various protocols
 - Target specific protocol and system implementation
 - Examine feasibility of attack based on available information
 - Compare courses of action for attacking control systems
- **Comprehensive representation**
 - Facilitate risk analysis and risk management
 - Examine implementation of defensive posture
 - Derive common vulnerability classes and mitigation strategies
 - Aid in the design of robust control protocols



U CYBER CORPS
Defending America's Cyberspace

0100101010010101010101001100101010101000010101010101010100010100100



Questions?