# Cyber-Physical Security Through Information Flow

**Bruce McMillin**

**Professor and Interim Chair, Department of Computer Science**

**2018-2020 Distinguished Visitor**

Missouri University of Science and Technology

325 Computer Science, 500 W. 15th St., Rolla, MO 65409

o/ (573) 341-6435 e/ ff@mst.edu

# Cyber-Physical Security Through Information Flow

**Bruce McMillin**

**Professor and Interim Chair, Department of Computer Science**

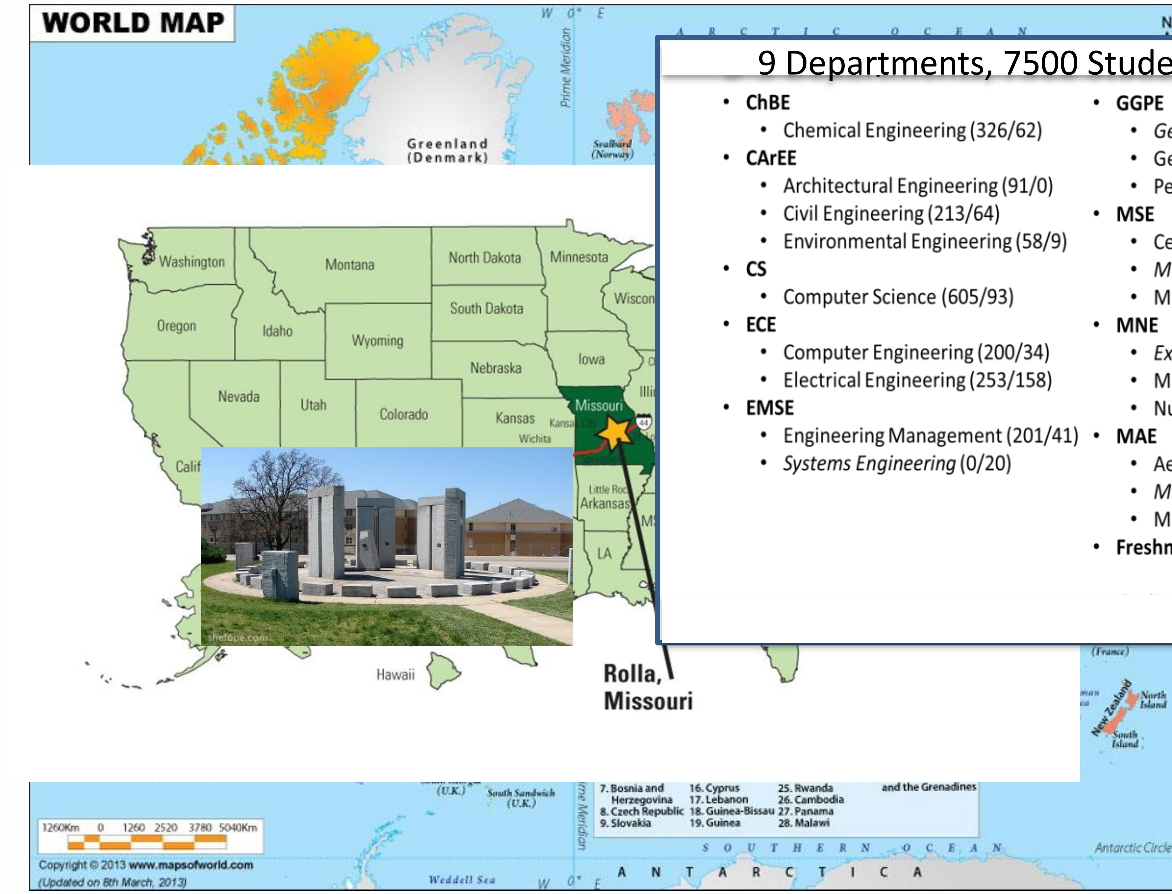
**2018-2020 Distinguished Visitor**

Missouri University of Science and Technology

325 Computer Science, 500 W. 15th St., Rolla, MO 65409

o/ (573) 341-6435 e/ ff@mst.edu

# Where is Missouri S&T

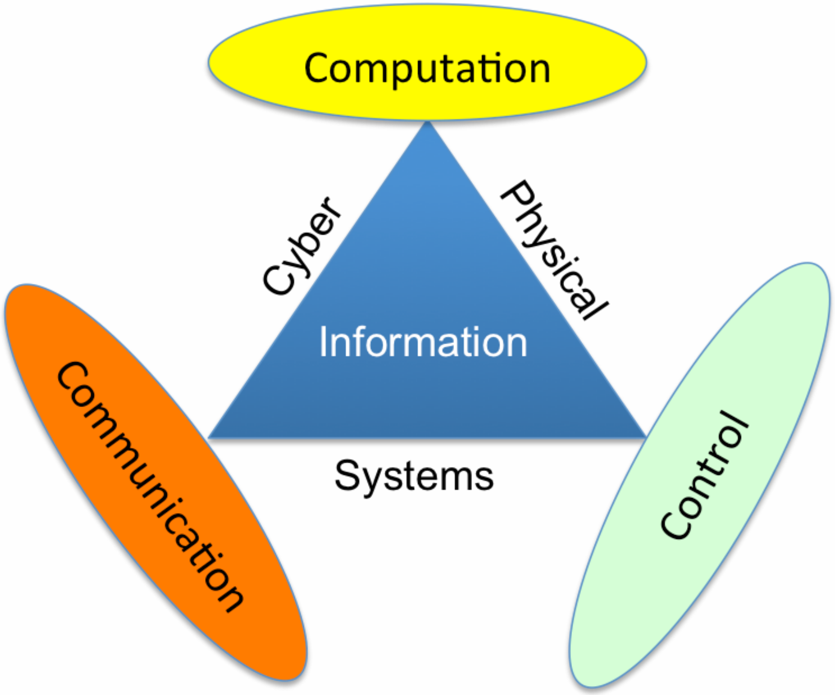



## 9 Departments, 7500 Students in Engineering

- **ChBE**
  - Chemical Engineering (326/62)
- **CArEE**
  - Architectural Engineering (91/0)
  - Civil Engineering (213/64)
  - Environmental Engineering (58/9)
- **CS**
  - Computer Science (605/93)
- **ECE**
  - Computer Engineering (200/34)
  - Electrical Engineering (253/158)
- **EMSE**
  - Engineering Management (201/41)
  - *Systems Engineering* (0/20)
- **GGPE**
  - *Geology and Geophysics* (86/50)
  - Geological Engineering (75/47)
  - Petroleum Engineering (169/84)
- **MSE**
  - Ceramic Engineering (103/9)
  - *Materials Science* (0/30)
  - Metallurgical Engineering (73/9)
- **MNE**
  - *Explosives Engineering* (0/9)
  - Mining Engineering (122/26)
  - Nuclear Engineering (99/45)
- **MAE**
  - Aerospace Engineering (215/42)
  - *Manufacturing Engineering* (0/16)
  - Mechanical Engineering (704/98)
- **Freshmen Engineering** (2126/0)

# CPS

- **Cyber-Physical Systems** (CPS) are physical systems that are controlled and monitored through computer-based systems.
- Critical infrastructures of a nation are CPS
  - Water treatment plant
  - Smart grid
  - Manufacturing plant
  - Autonomous Vehicle
  - Airspace Management

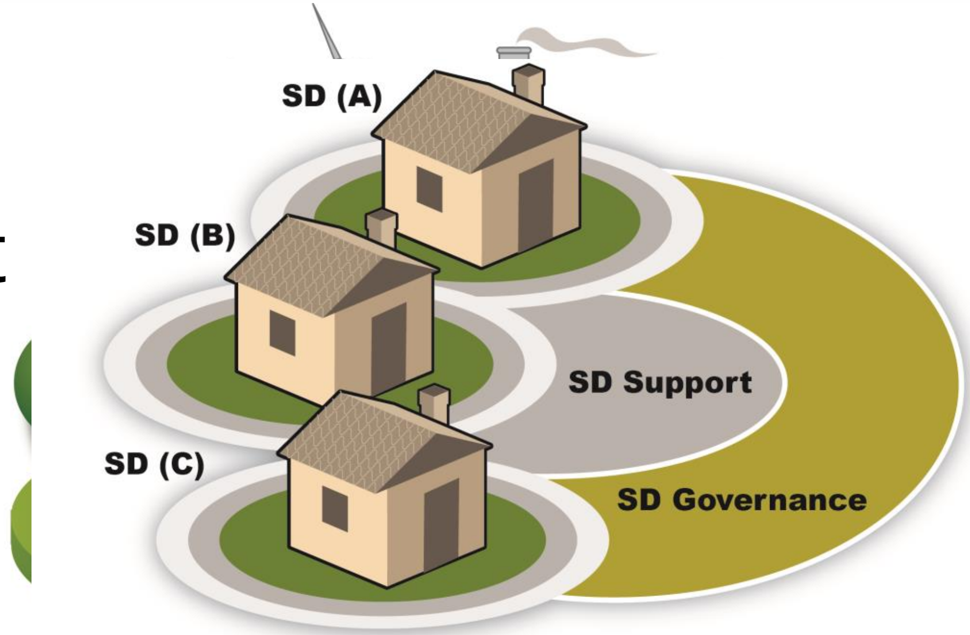


# A modern Cyber-Physical System

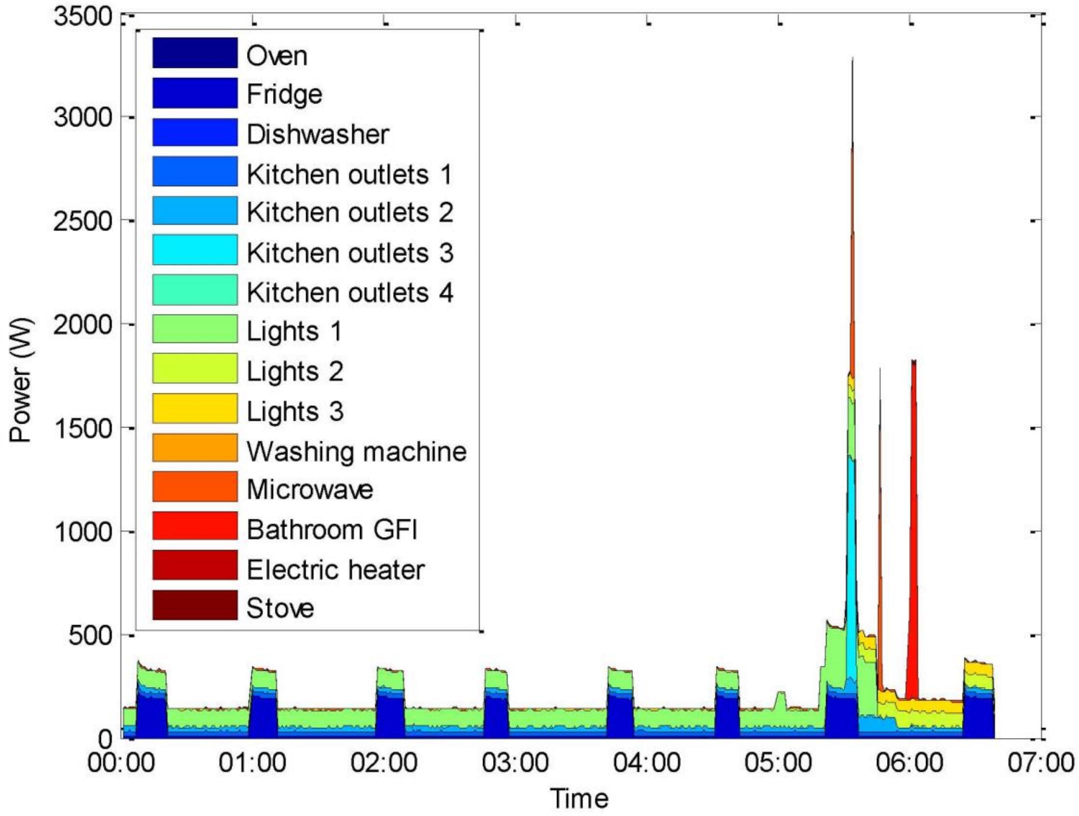
- Community
- Local Management
- Locally Sourced

# Modern Security Domains

- Community
- Local Management
- Locally Sourced
- Secure
- Privacy Preserving

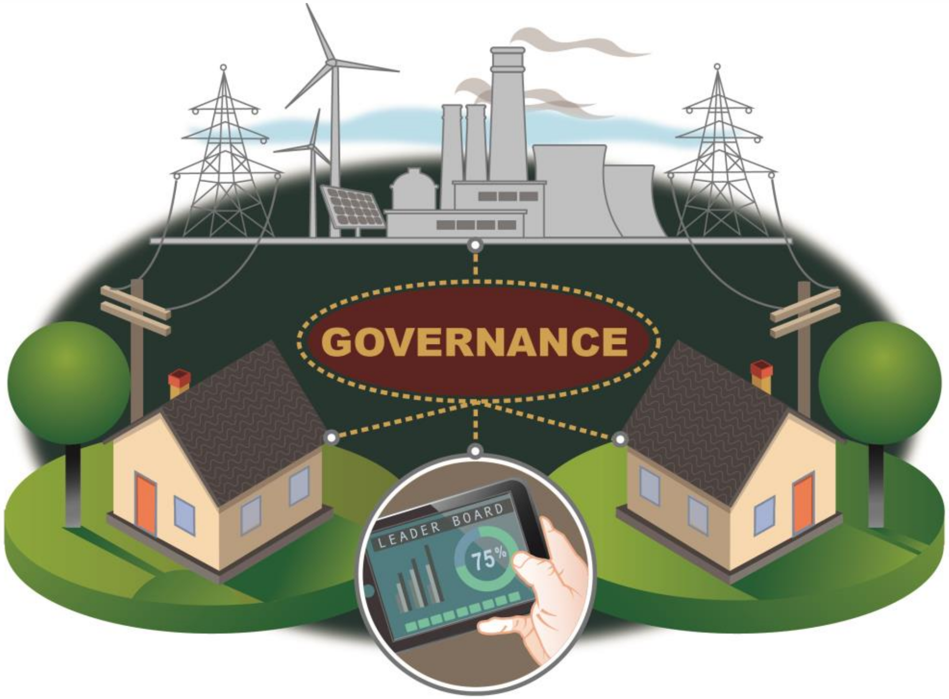


# Non-Intrusive Load Monitoring

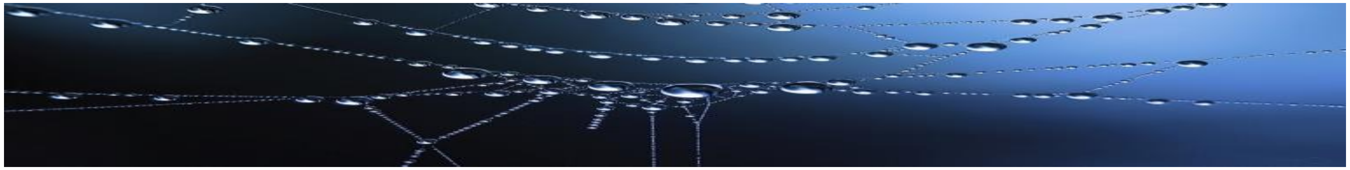


# Management and Governance

- Utility?
  - NISTIR 7628
- Cloud?
  - NERC CIP
  - Timing
- Fog?
  - IoT
  - Locally Managed
  - Locally Protected

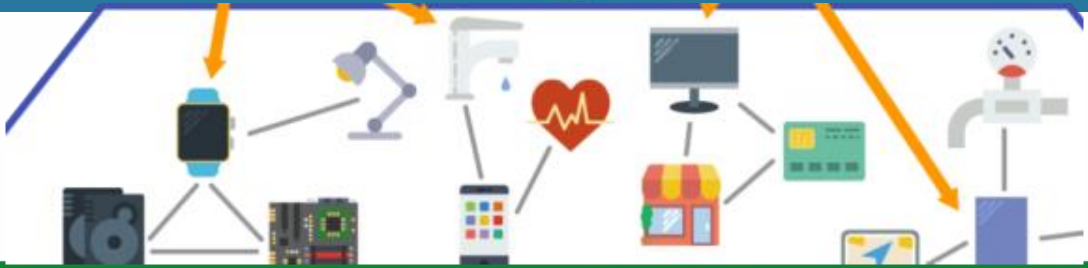


# Cloud



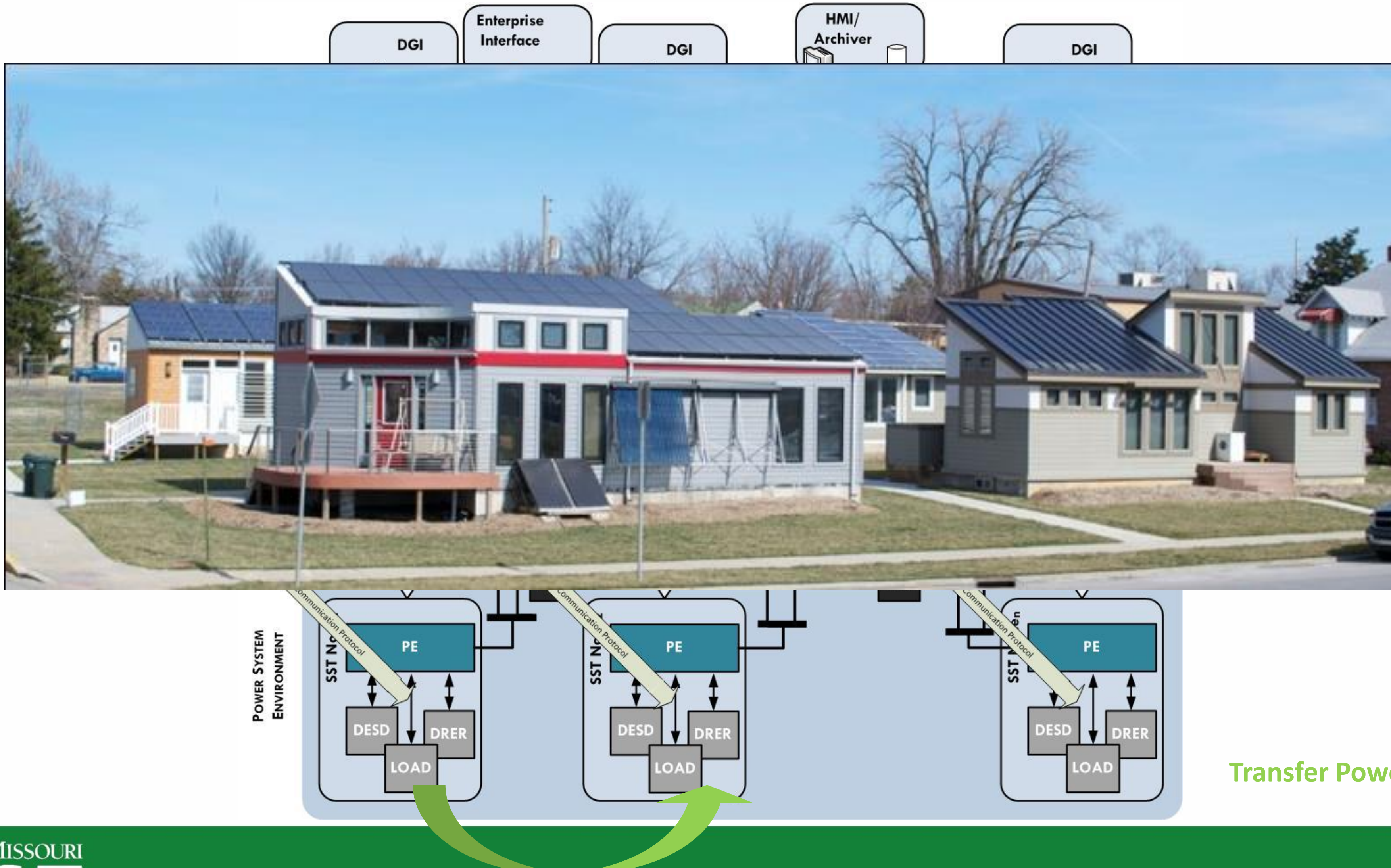
# Dew


# Fog

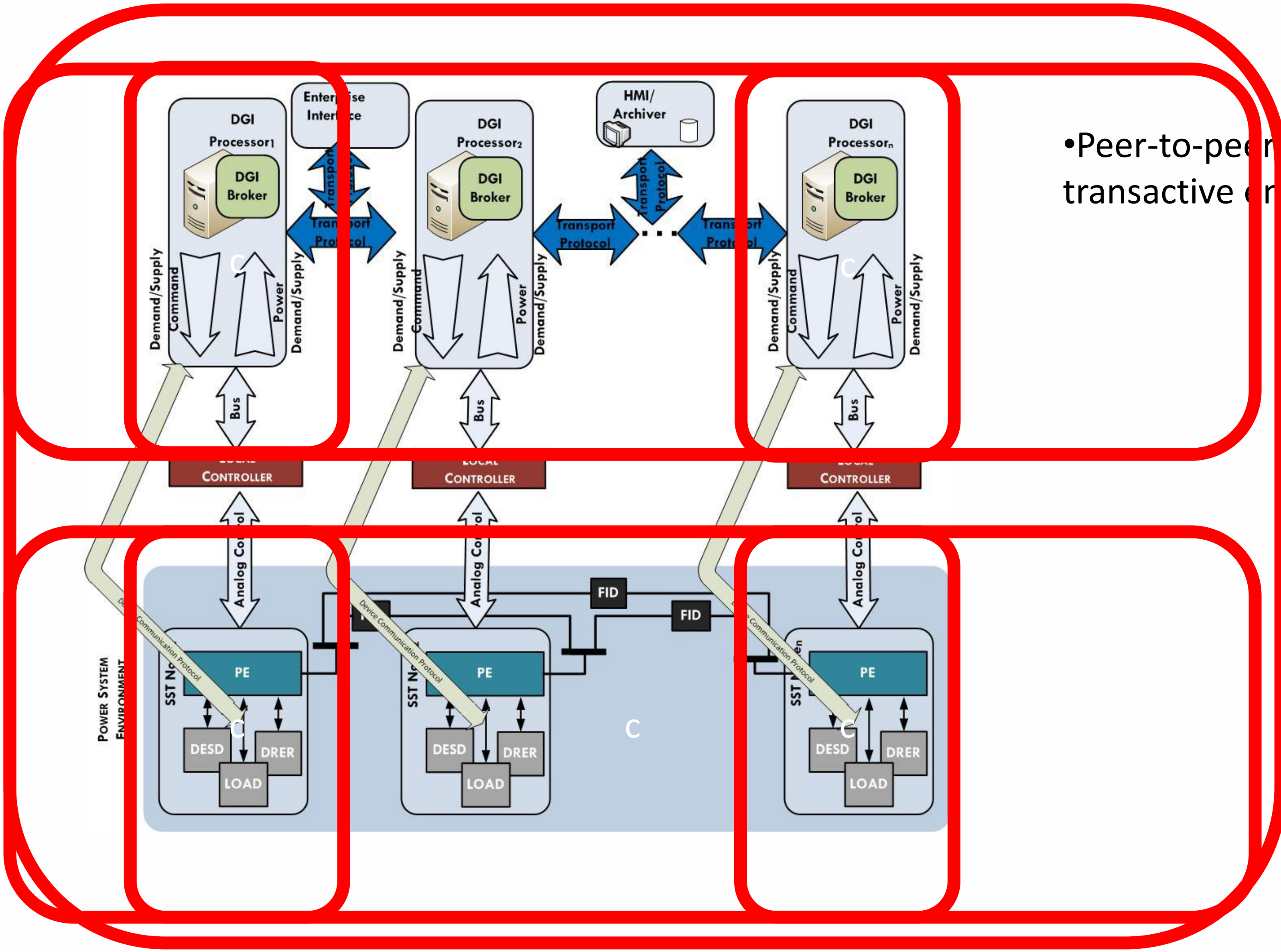


# Mist

# Transactive Energy Management



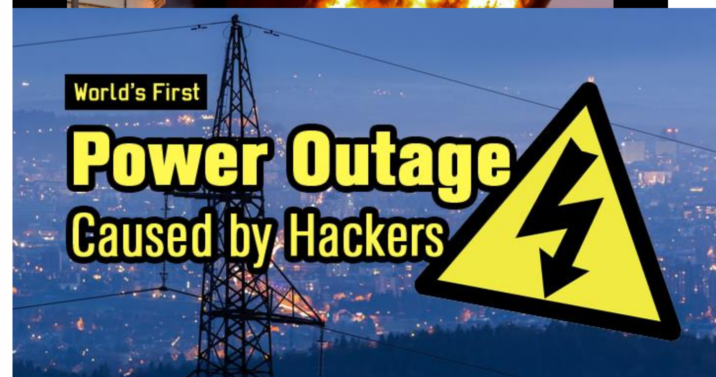

Transfer Power




•Peer-to-peer transactive energy

# Threats

- Physical
- Cyber
- Cyber-enabled Physical
- Physically-enabled Cyber




Stealing Plant Secrets

# Firewalls

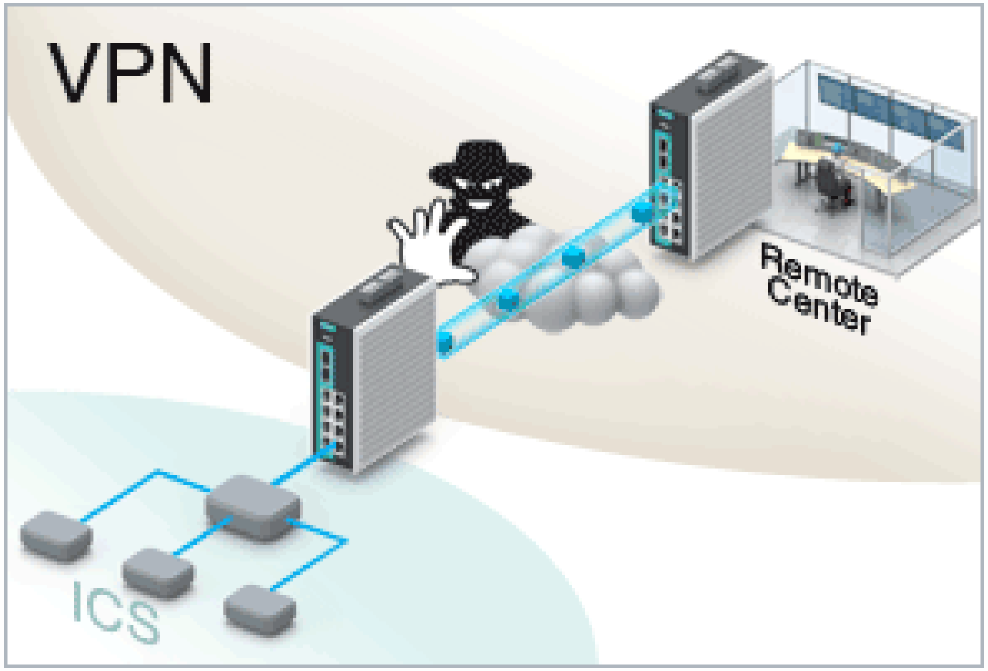
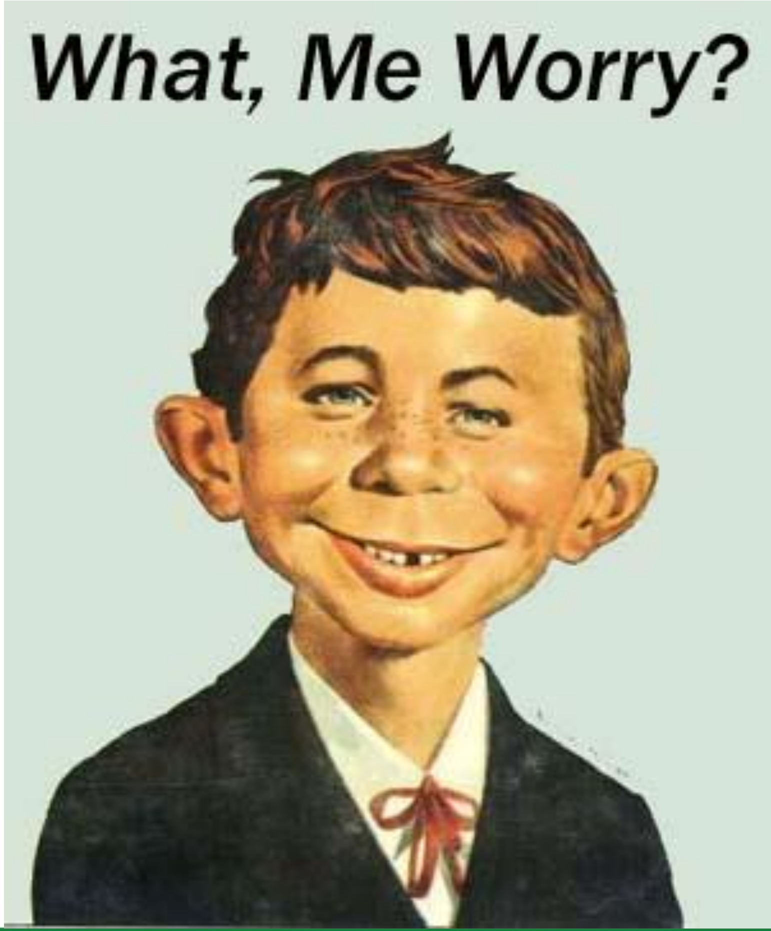
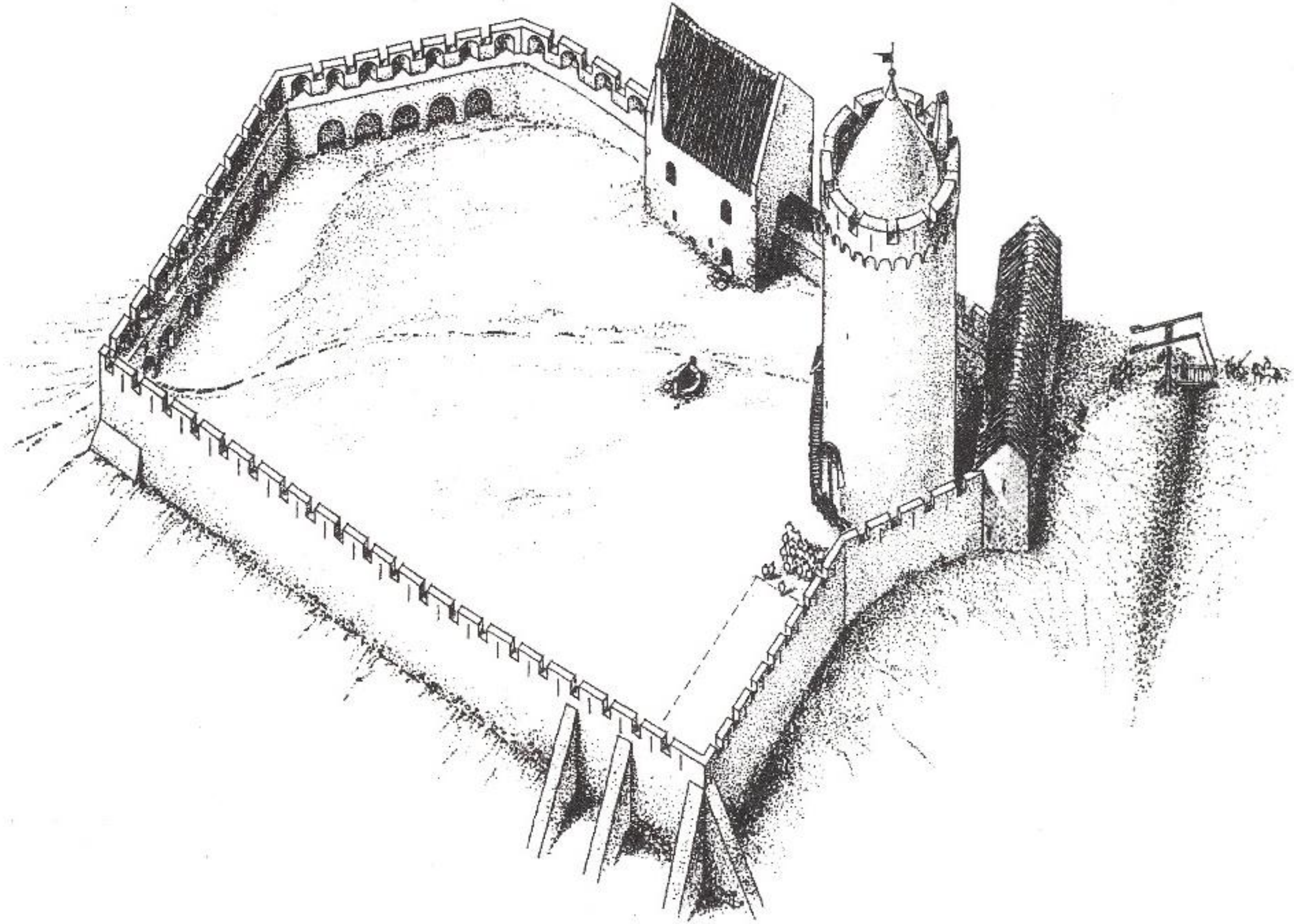


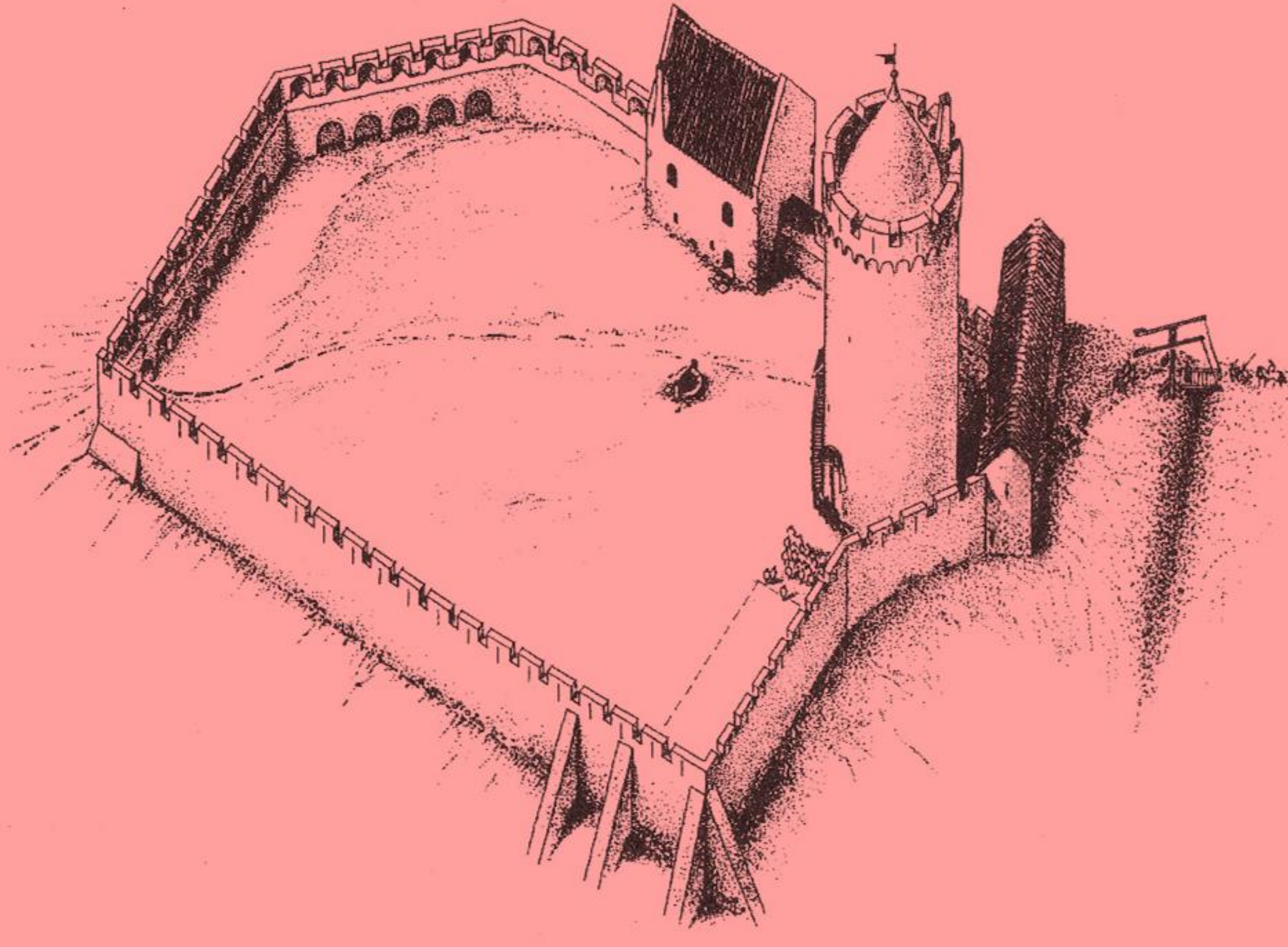

Figure Source, Manufacturers Automation, Inc.

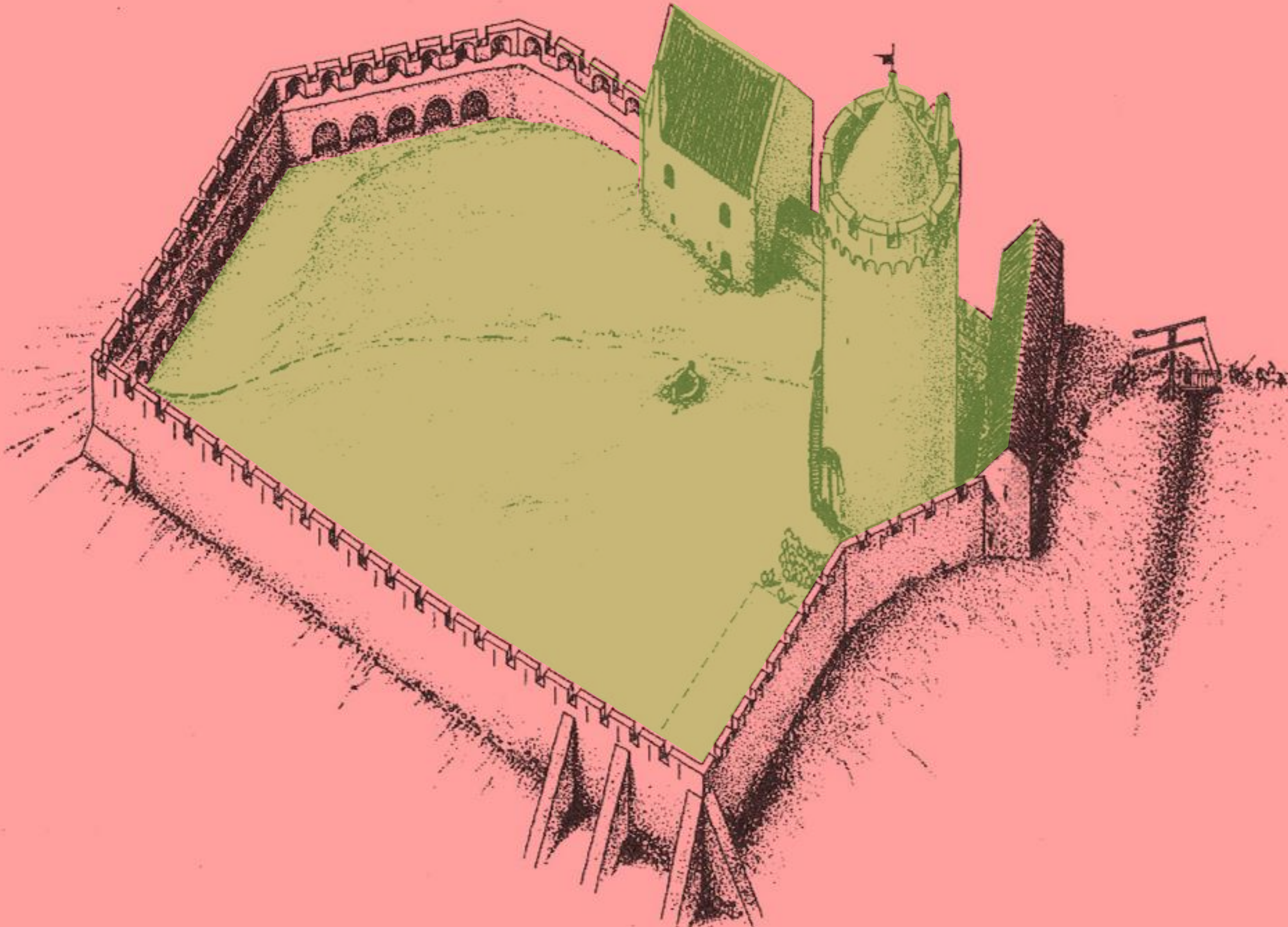
# Seems Simple, What could go wrong?

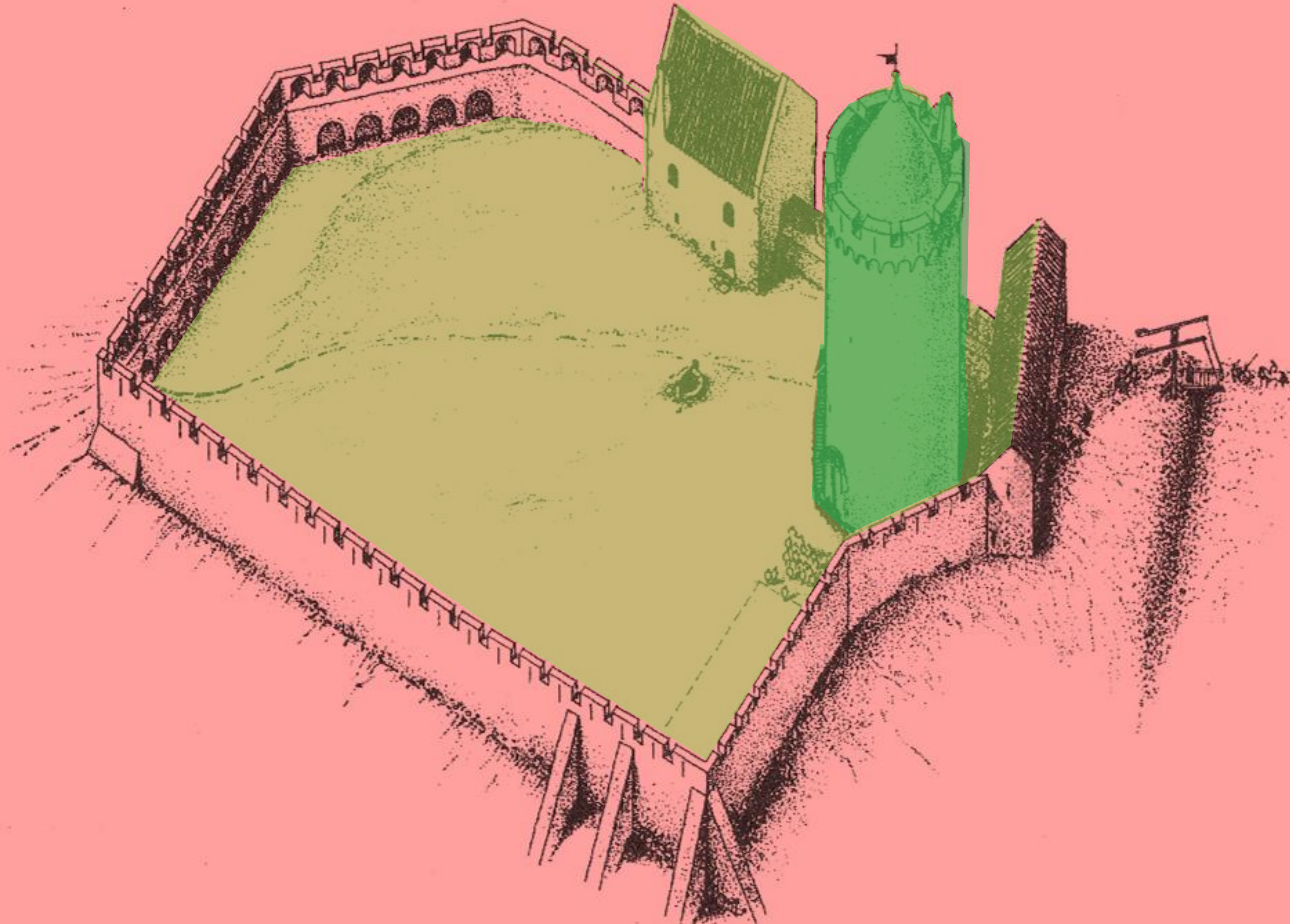


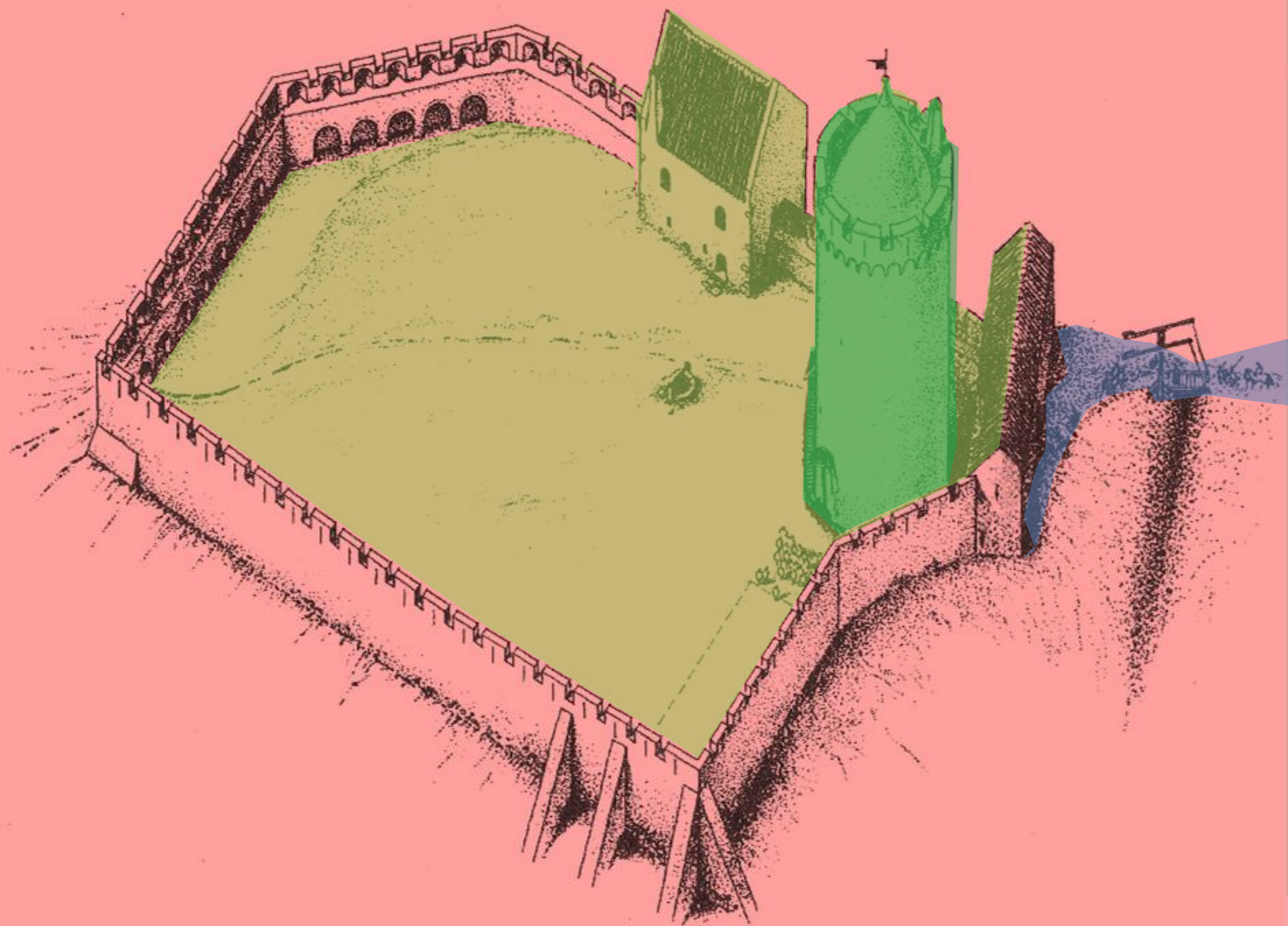

- Physical
- Cyber
- Cyber-enabled Physical
- Physically-enabled Cyber

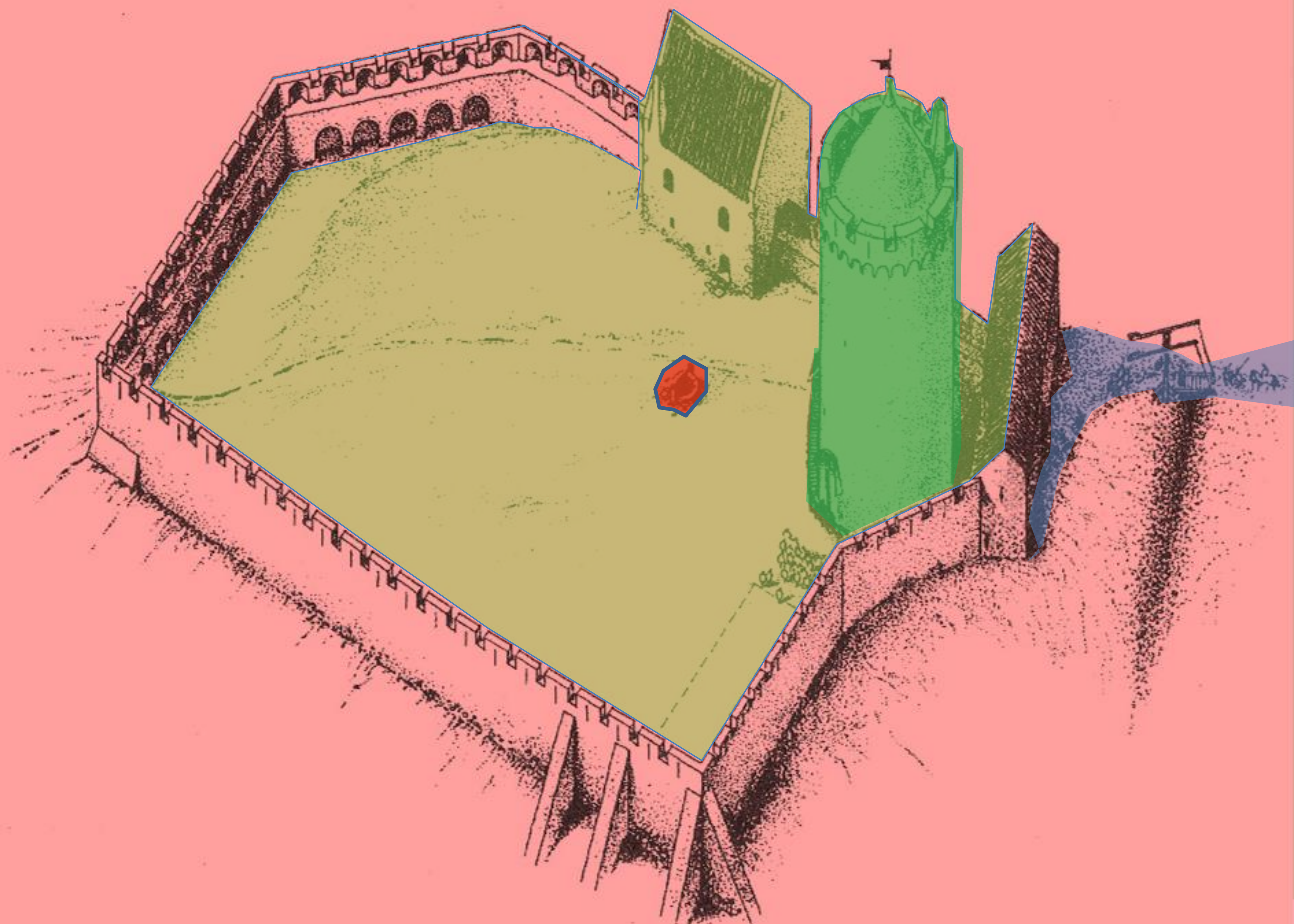




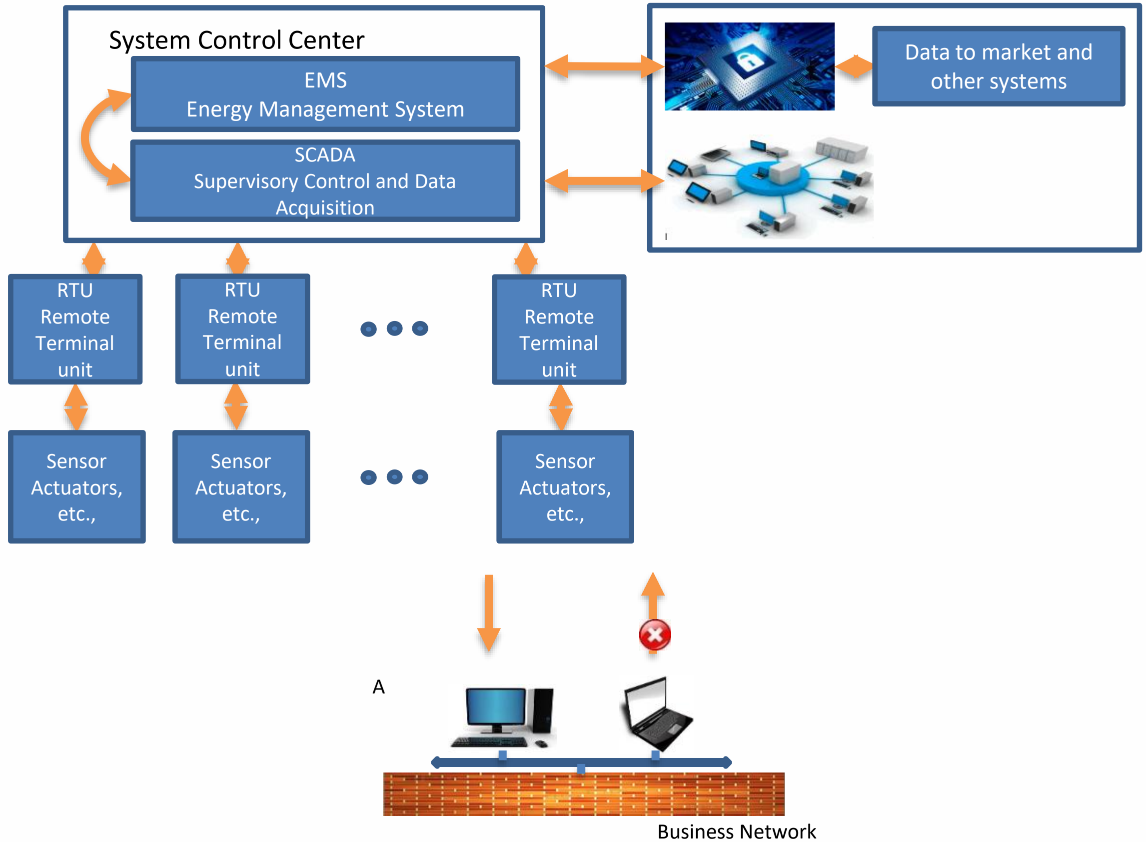








# SCADA System - from National Academies




- **Centralized Supervisory Control And Data Acquisition (SCADA)**
- **Electric Utility Control**

# Biba Model - 1975

- Integrity Levels:
- The higher the level, the more confidence
  - That a program will execute correctly
  - That data is accurate and/or reliable
- Note relationship between integrity and trustworthiness
- Important point: *integrity levels are **not** security levels*

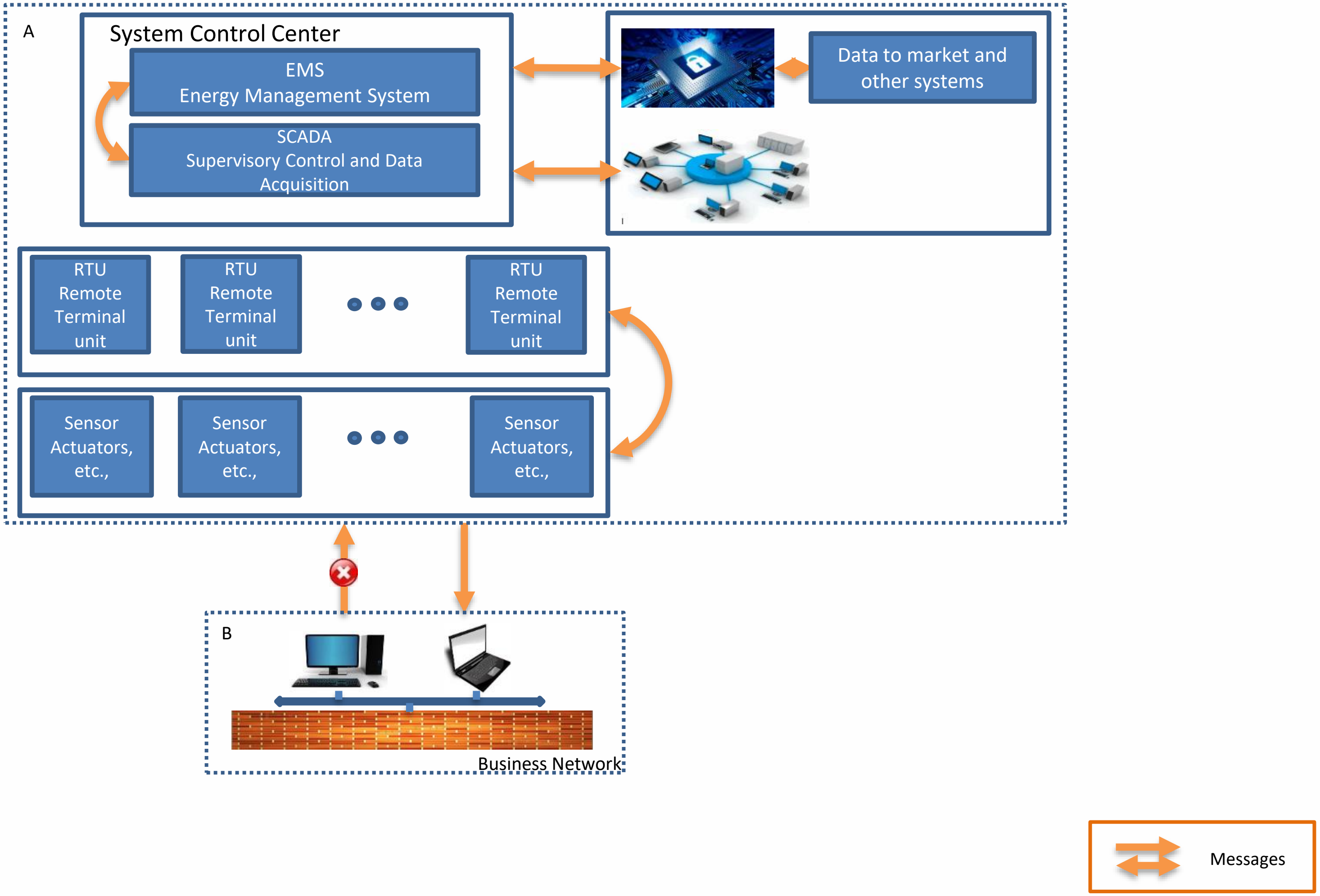
# Problems

- Subjects' integrity levels decrease as system runs
  – Soon no subject will be able to access objects at high integrity levels
- Alternative: change object levels rather than subject levels
  – Soon all objects will be at the lowest integrity level
- Crux of problem is model prevents indirect modification
  – Because subject levels lowered when subject reads from low-integrity object


KEEPING UP WITH THE
KARDASHIANS


IQ ↓

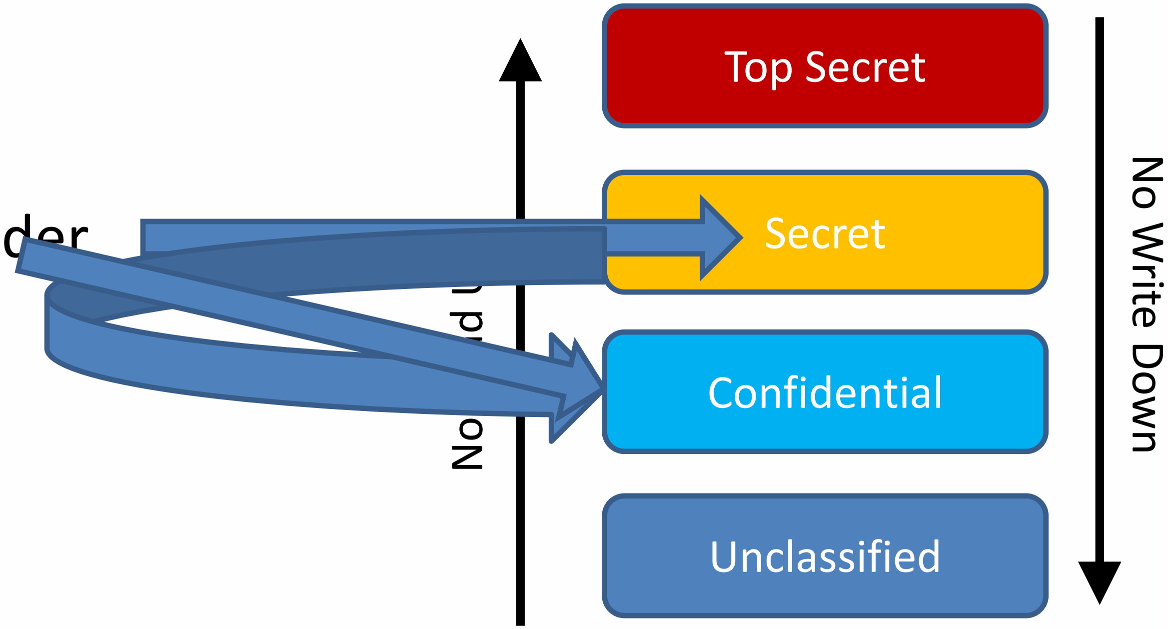
# BIBA


A
System Control Center
EMS
Energy Management System
SCADA
Supervisory Control and Data Acquisition
Data to market and other systems
RTU Remote Terminal unit
RTU Remote Terminal unit
RTU Remote Terminal unit
Sensor Actuators, etc.,
Sensor Actuators, etc.,
Sensor Actuators, etc.,
B
Business Network
Messages

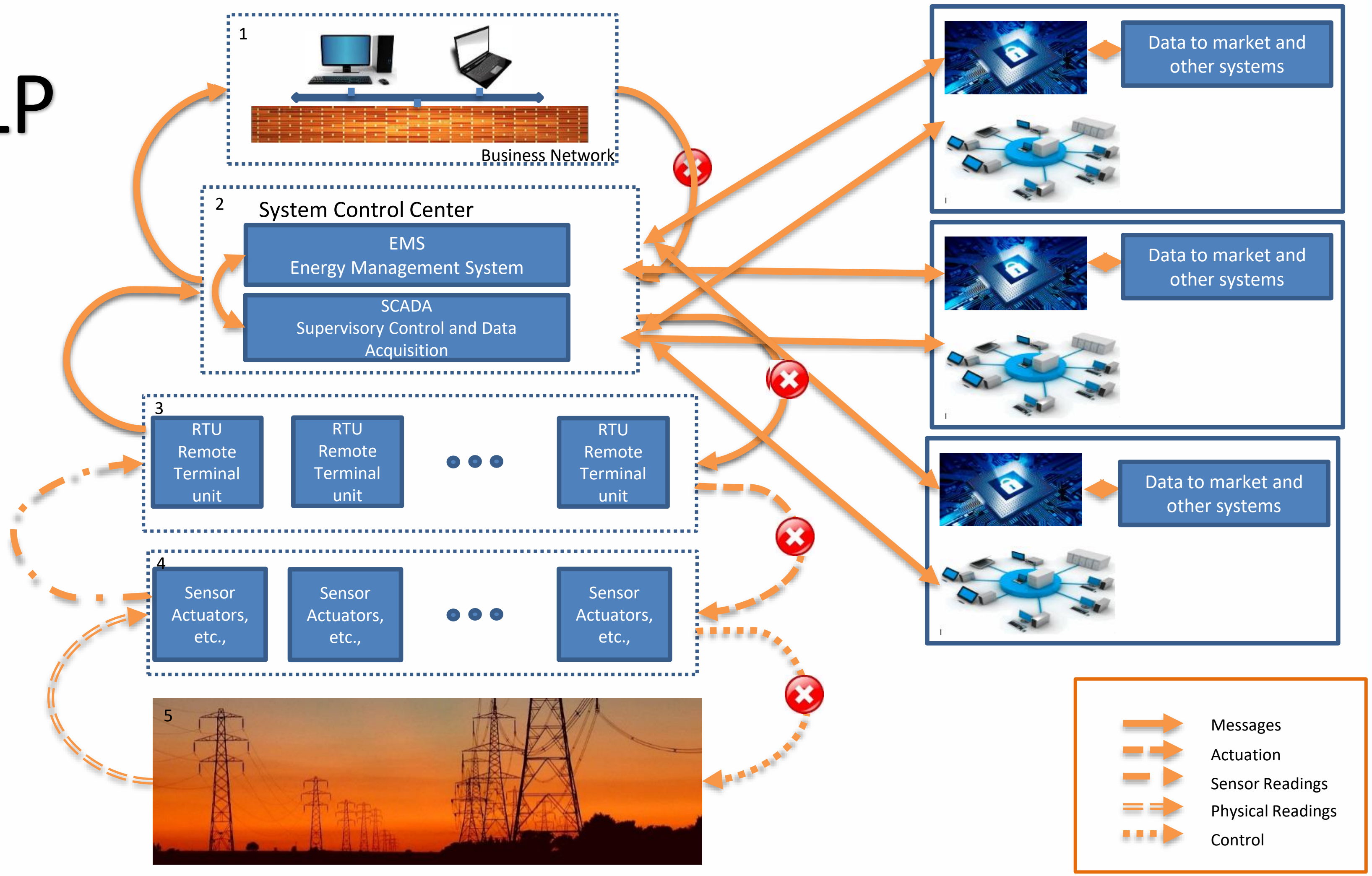
# Security? Bell-La Padula

- Military Multi-Level Security Model
  - No Read Up
  - No Write Down

- Military Commander
  - Write to troops?
  - Downgrade

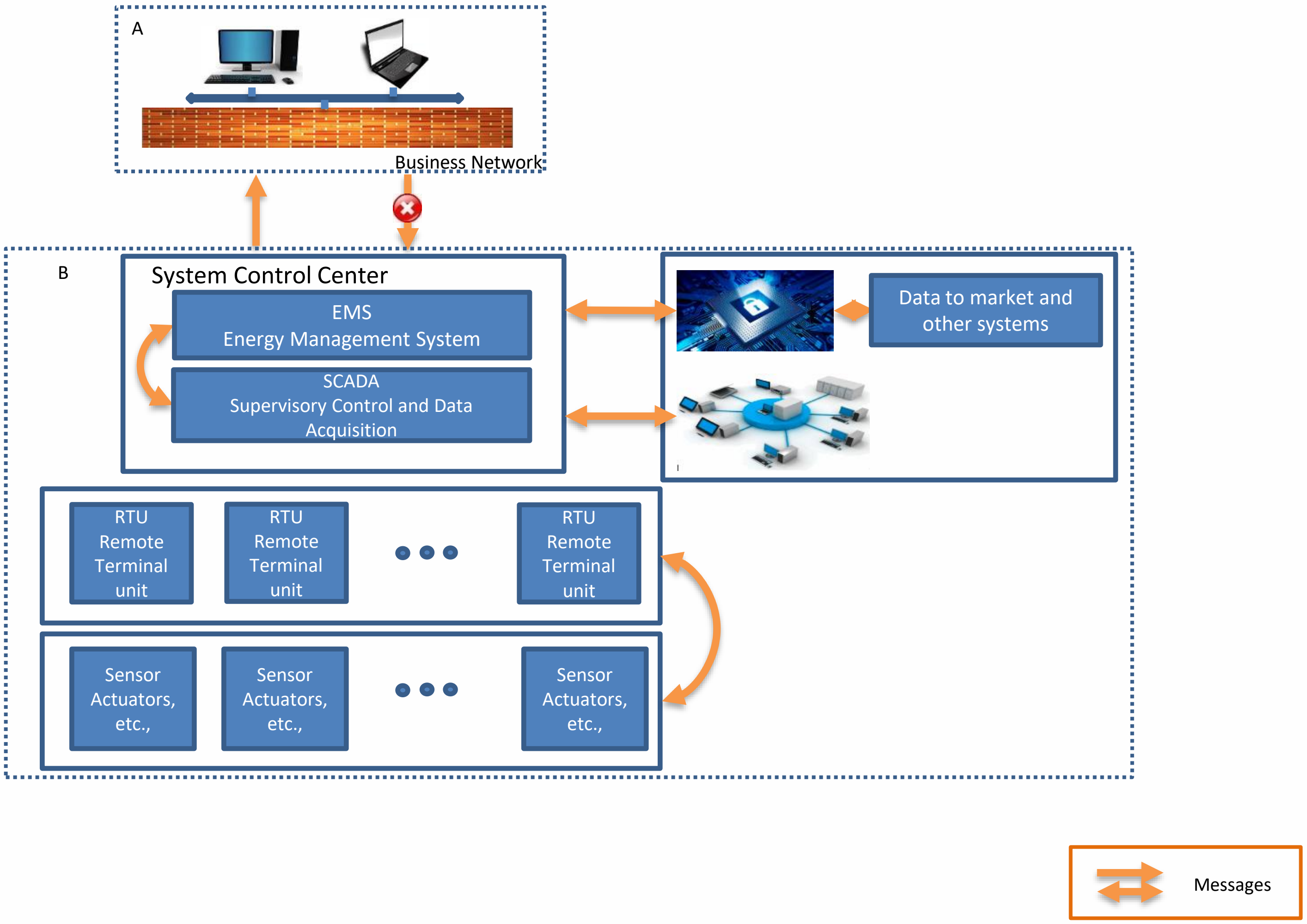


# BLP

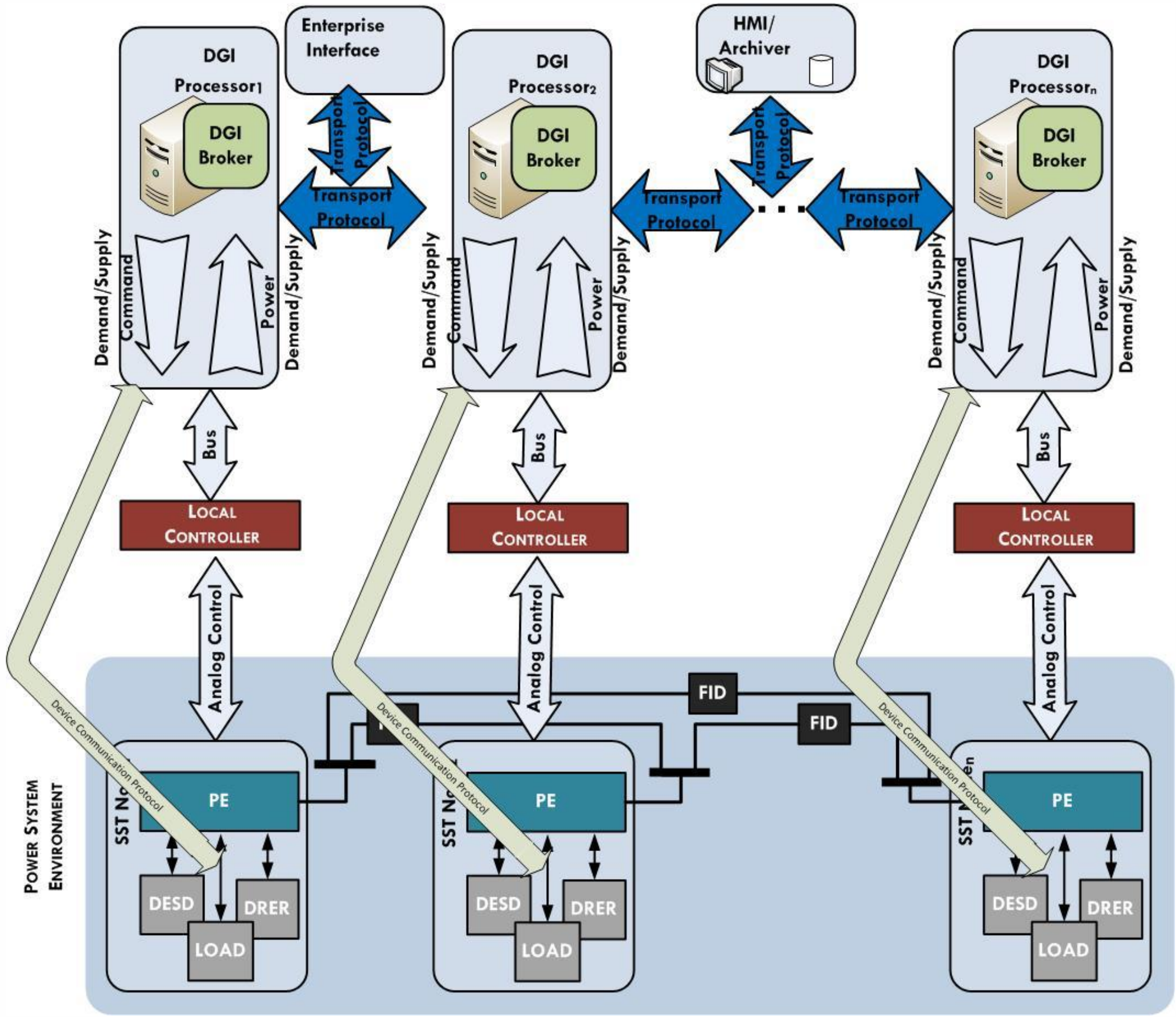


1
Business Network
2
System Control Center
EMS
Energy Management System
SCADA
Supervisory Control and Data Acquisition
3
RTU Remote Terminal unit
RTU Remote Terminal unit
RTU Remote Terminal unit
4
Sensor Actuators, etc.,
Sensor Actuators, etc.,
Sensor Actuators, etc.,
5
Data to market and other systems
Data to market and other systems
Data to market and other systems
Messages
Actuation
Sensor Readings
Physical Readings
Control

# BLP

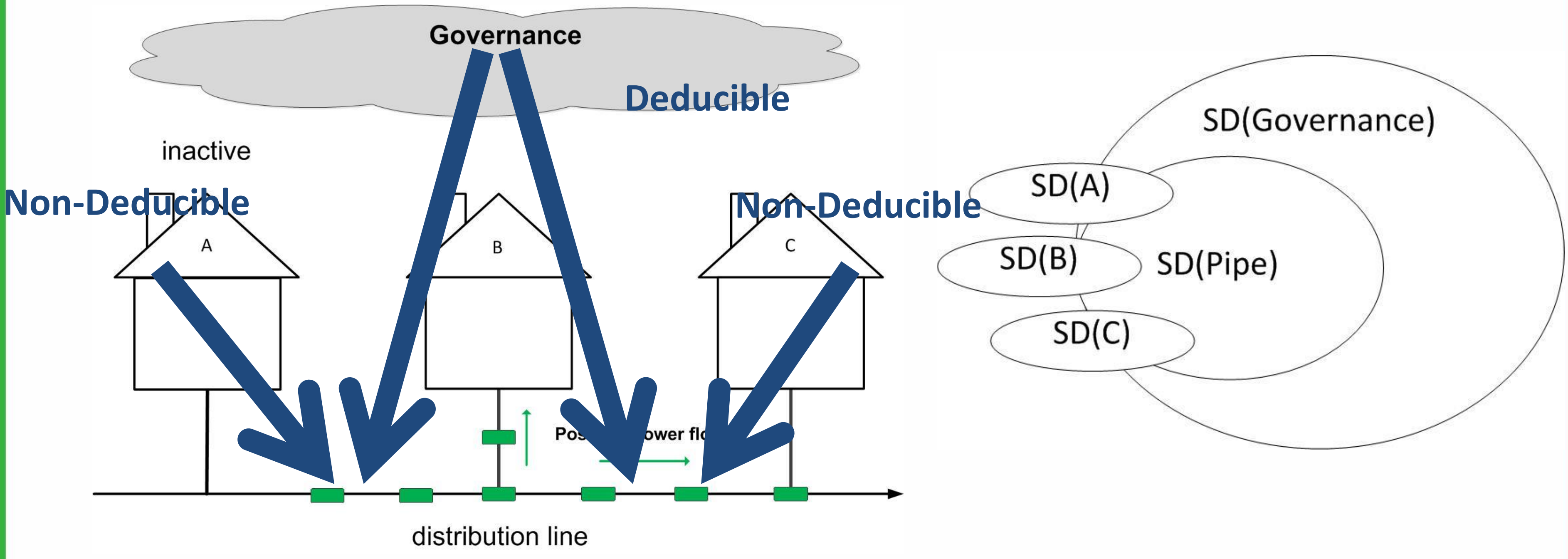

A
Business Network
B
System Control Center
EMS
Energy Management System
SCADA
Supervisory Control and Data Acquisition
Data to market and other systems
RTU Remote Terminal unit
RTU Remote Terminal unit
RTU Remote Terminal unit
Sensor Actuators, etc.,
Sensor Actuators, etc.,
Sensor Actuators, etc.,
Messages

# Fog Energy Management

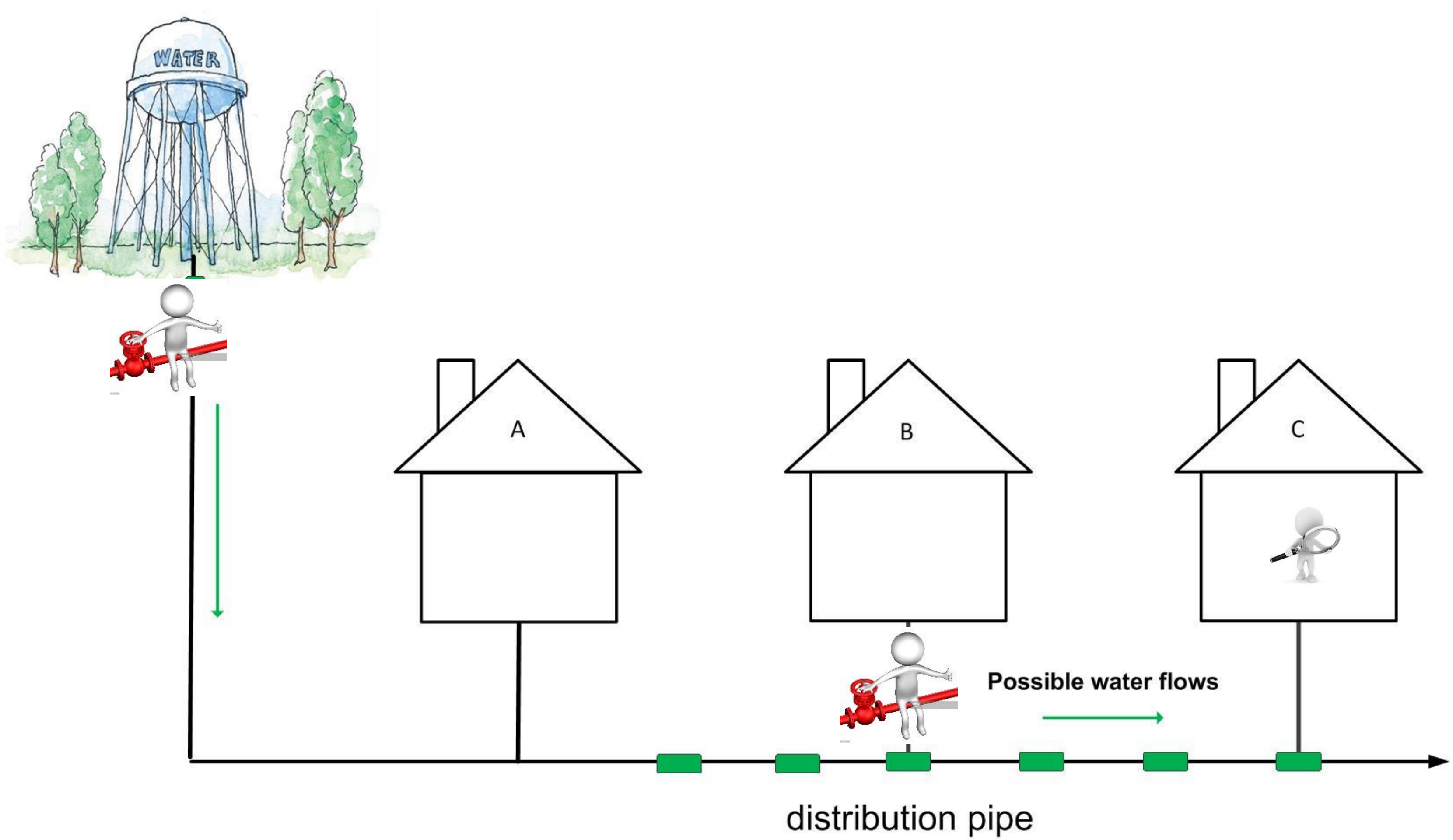



Transfer Power

# The overlapping security domains in an IoT smart grid environment.



# Information Present in the Physical Entity

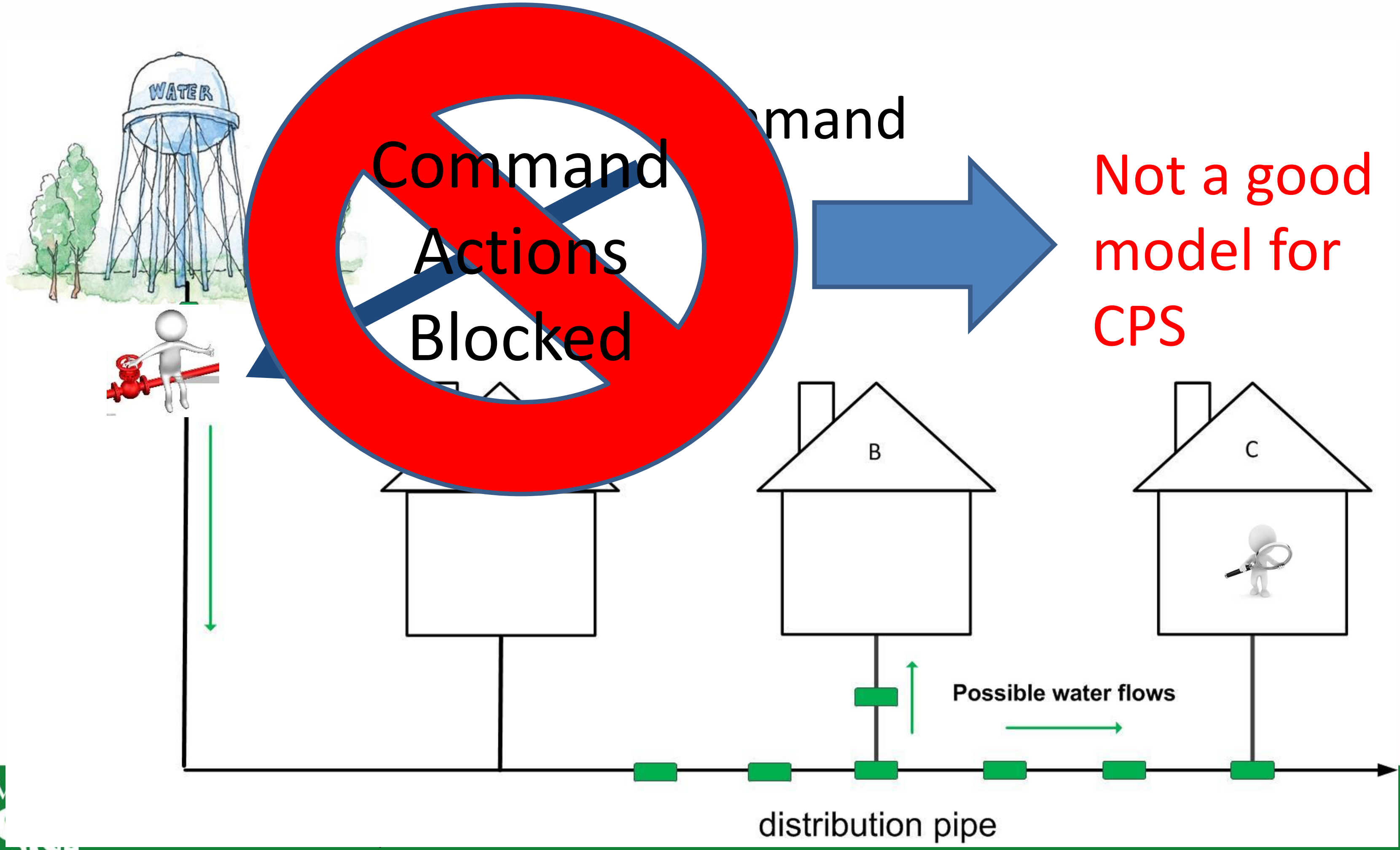


# Information Flow Models

- *A CPS performs physical actions that are observable*
- *Should keep these secret – loss of confidentiality/privacy*
- *Should not keep these secret – loss of integrity*
- *Some models*
  - *Non-interference – Goguen and Messegeur 1982*
    - High-level events do not interfere with the low level outputs
  - *Non-inference – O'Halloran 1990*
    - Removing high-level events leaves a valid system trace
  - *Non-deducibility – Sutherland 1986*
    - Low-level observation is compatible with any of the high-level inputs.

MISSOURI S&T

# Information Present in the Physical Entity (Non-interference view)



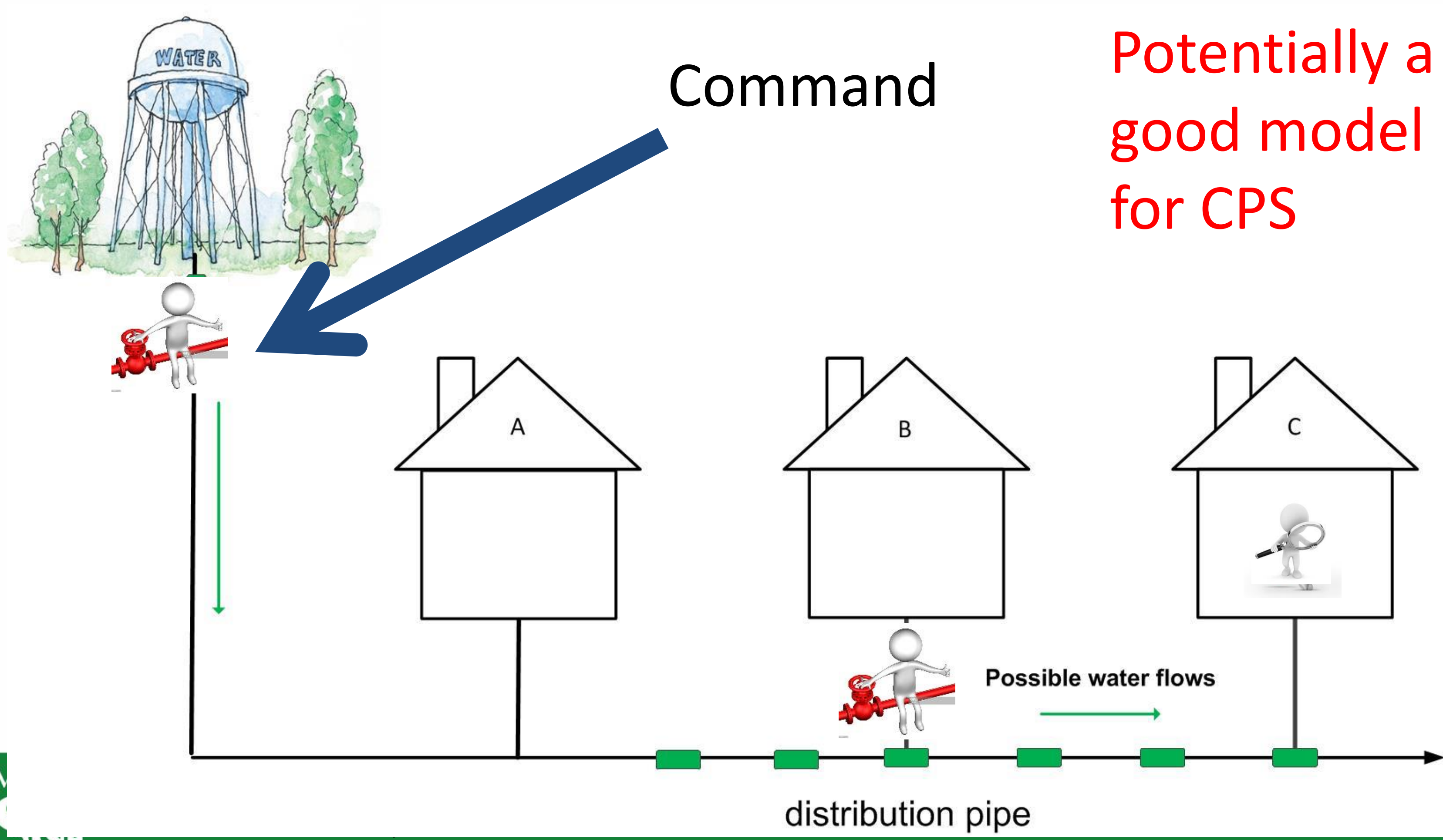

Not a good model for CPS

# Information Flow Models

- *A CPS performs physical actions that are observable*
- *Should keep these secret – loss of confidentiality/privacy*
- *Should not keep these secret – loss of integrity*
- *Some models*
  - *Non-interference – Goguen and Messegeur 1982*
    - High-level events do not interfere with the low level outputs
  - *Non-inference – O-Halloran 1990*
    - Removing high-level events leaves a valid system trace
  - *Non-deducibility – Sutherland 1986*
    - Low-level observation is compatible with any of the high-level inputs.

MISSOURI S&T

# Information Present in the Physical Entity (Non-inference view)

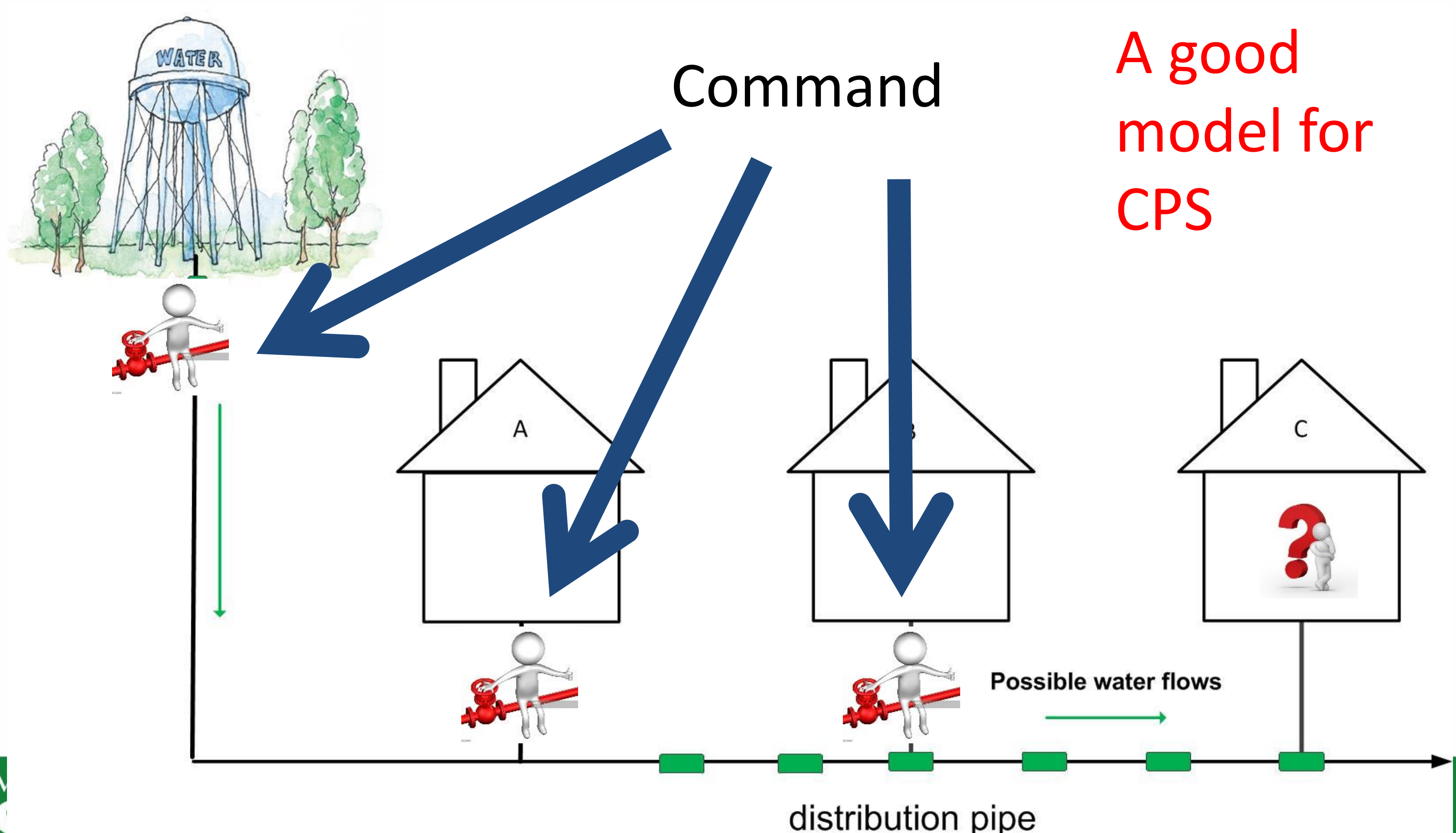



Potentially a good model for CPS

# Information Flow Models

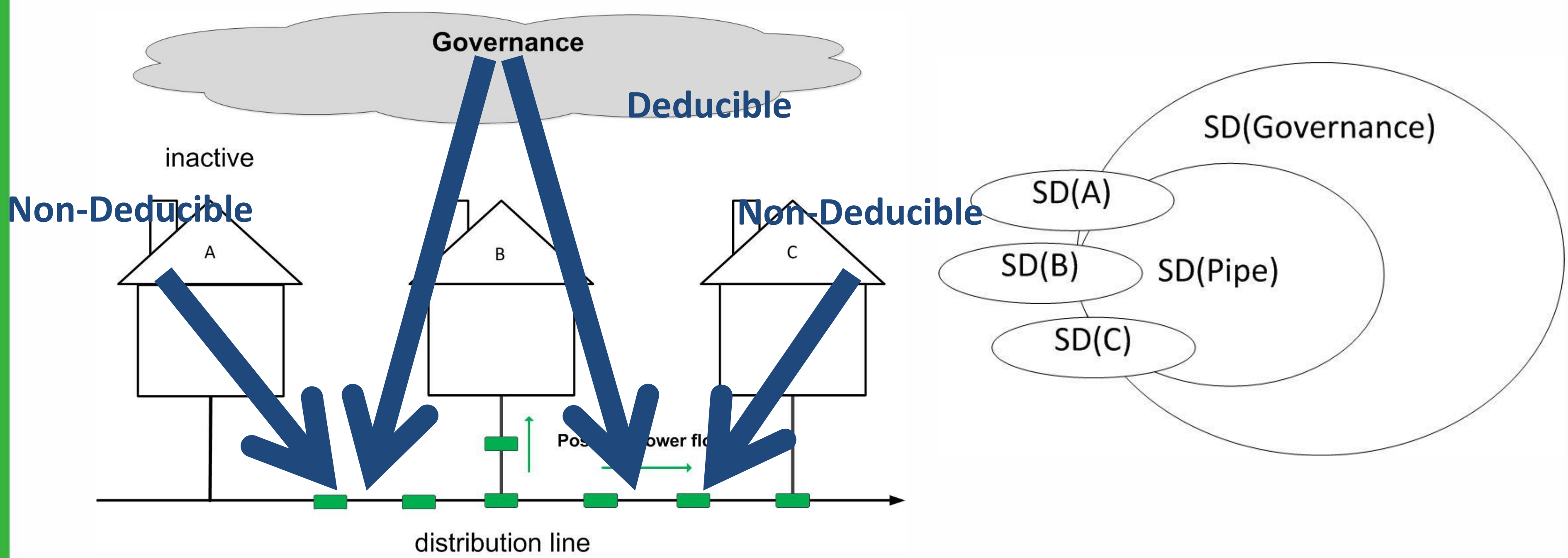
- *A CPS performs physical actions that are observable*
- *Should keep these secret – loss of confidentiality/privacy*
- *Should not keep these secret – loss of integrity*
- *Some models*
  - *Non-interference – Goguen and Messegeur 1982*
    - High-level events do not interfere with the low level outputs
  - *Non-inference – O-Halloran 1990*
    - Removing high-level events leaves a valid system trace
  - *Non-deducibility – Sutherland 1986*
    - Low-level observation is compatible with any of the high-level inputs.

# Information Present in the Physical Entity (Non-deducibility view)



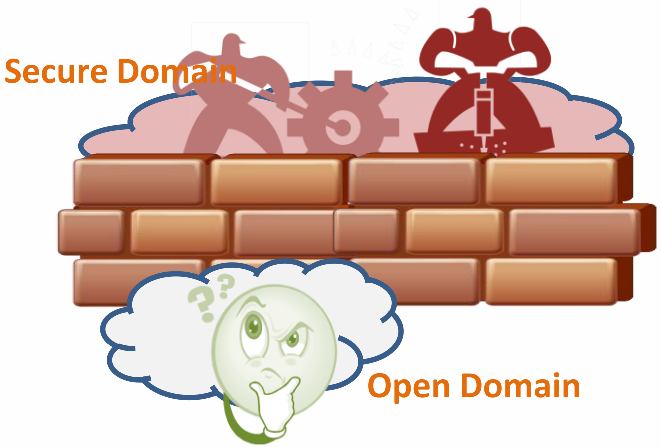

A good model for CPS

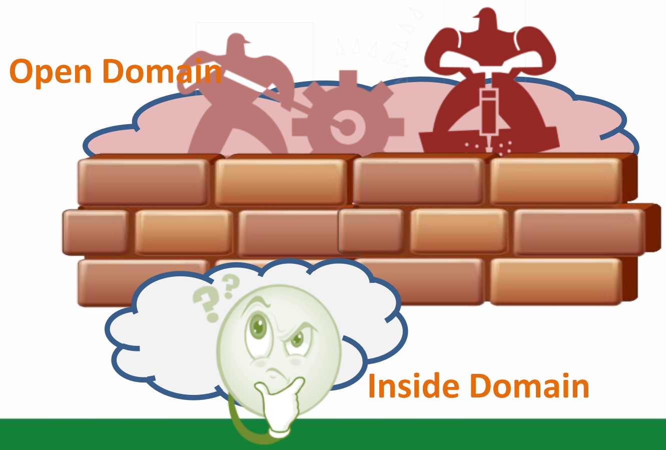
# The overlapping security domains in a CPS environment.



# Non-deducibility

- Non-deducibility
  - Good?




  - Bad?

Non-deducibility is a bidirectional model.

# The Challenge

- Prevent the bad guys from seeing confidential/private information.
- Make sure the good guys can deduce that an attack is happening from the bad guys
- In a CPS
- With the same model

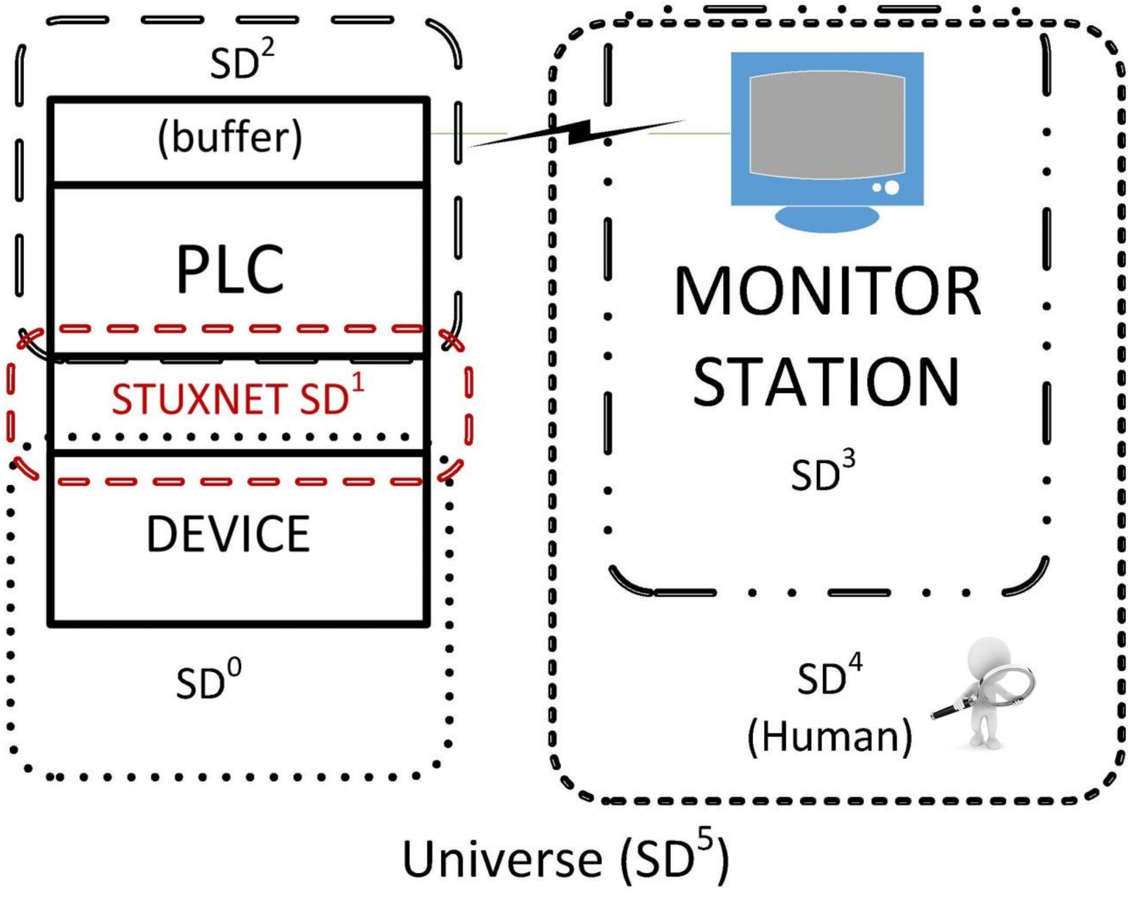
# Multiple Domain Nondeducibility

- Introduced a new model of Nondeducibility MSDND
- Defined with very few constraints
- Modal methods over Kripke frames
- Describes the CPS very well
- Provides a polynomial time reduction from ND to MSDND
- MSDND:

$$MSDND(ES) = \exists w \in W : w \vdash \Box\left[(s_x \vee s_y) \wedge \sim(s_x \wedge s_y)\right] \wedge \left[w \models (\nexists\, \mathbb{V}_x^i(w) \wedge \nexists\, \mathbb{V}_y^i(w))\right]$$

On any given world, the valuation functions, $V^i_x$ (w) , will return the value of the corresponding state variable x as seen by an entity in a partition, i.

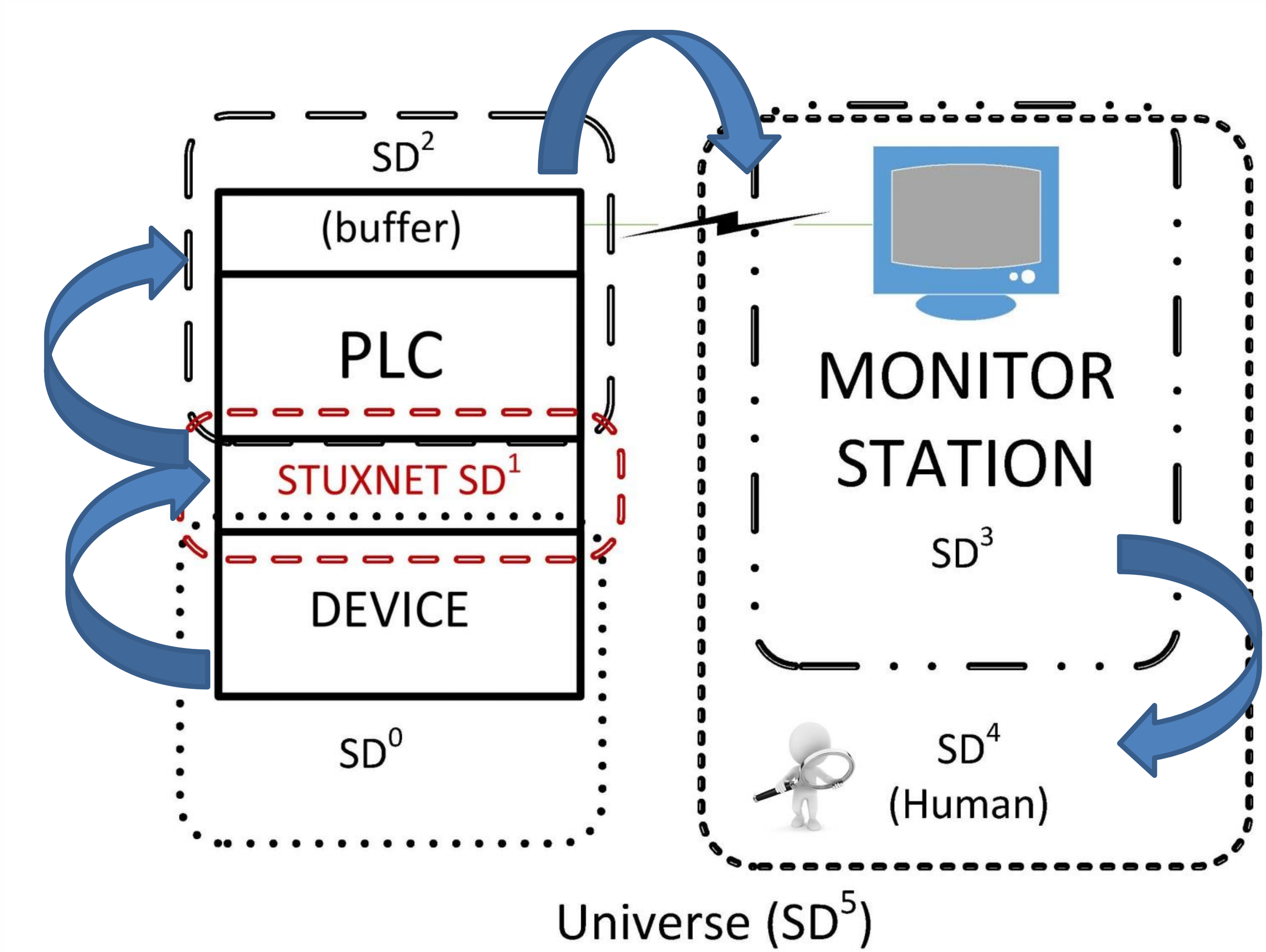
# Multiple Domains of Stuxnet



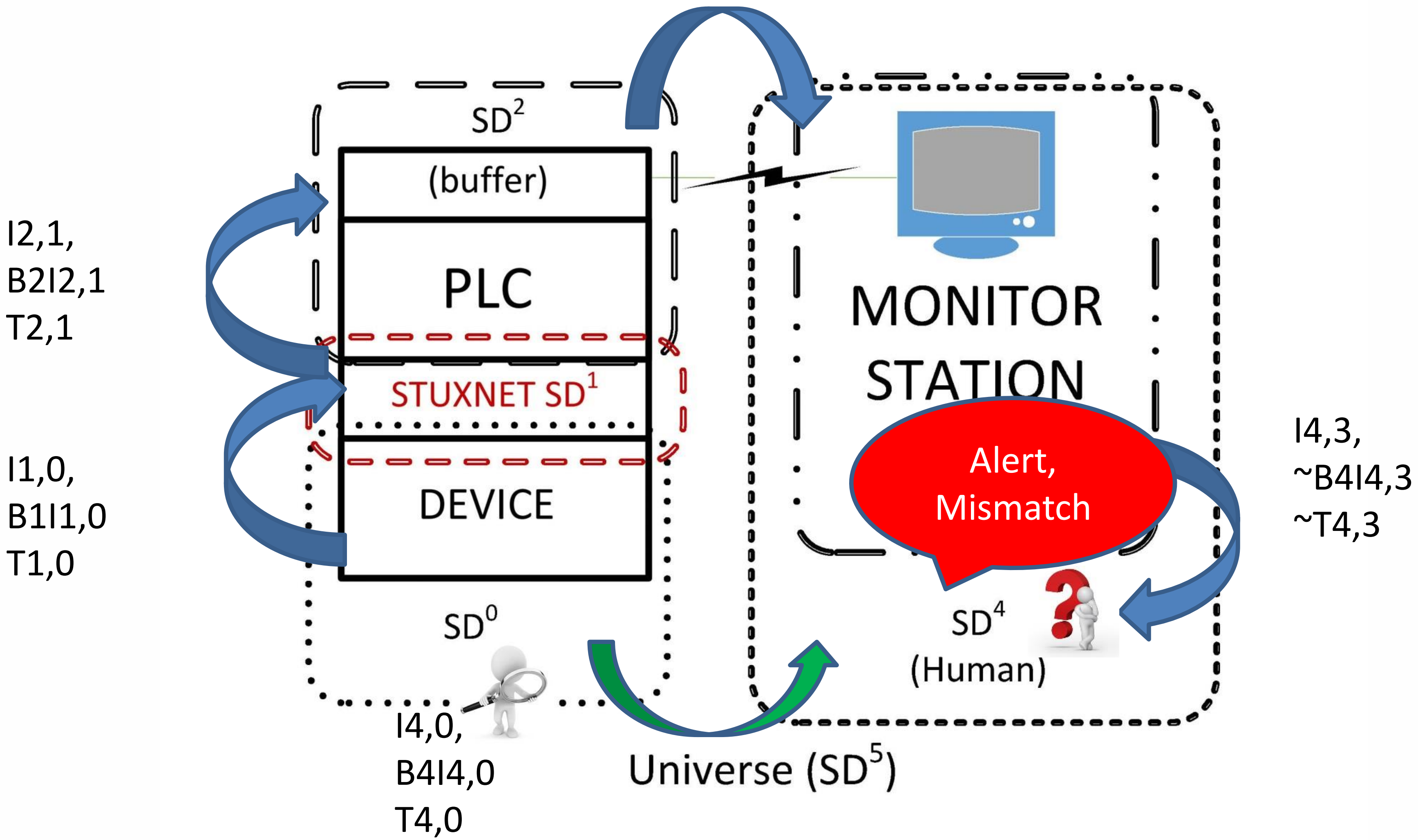
# Stuxnet Attack

I2,1,
B2I2,1
T2,1

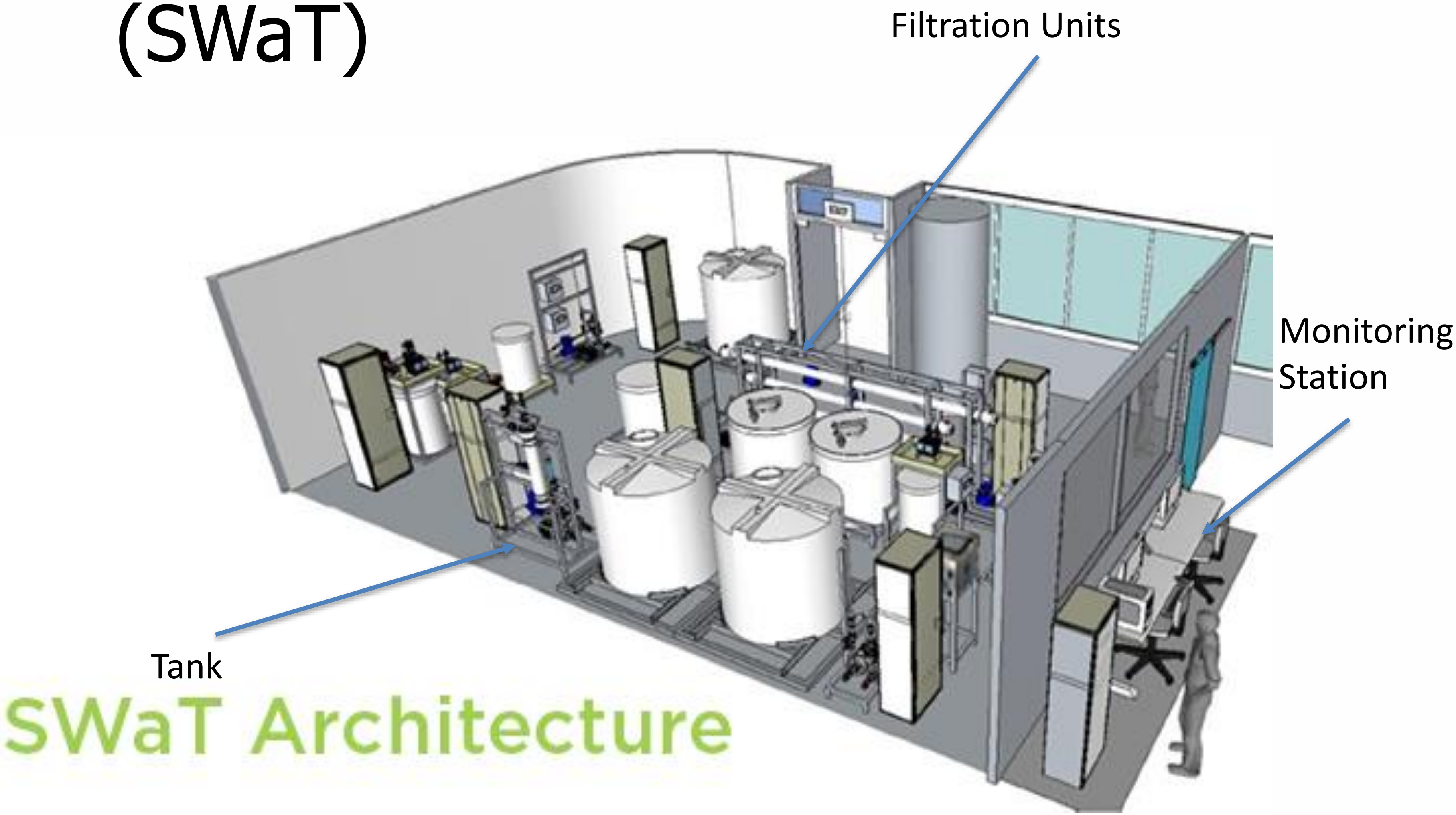
I1,0,
B1I1,0
T1,0



# Stuxnet Attack

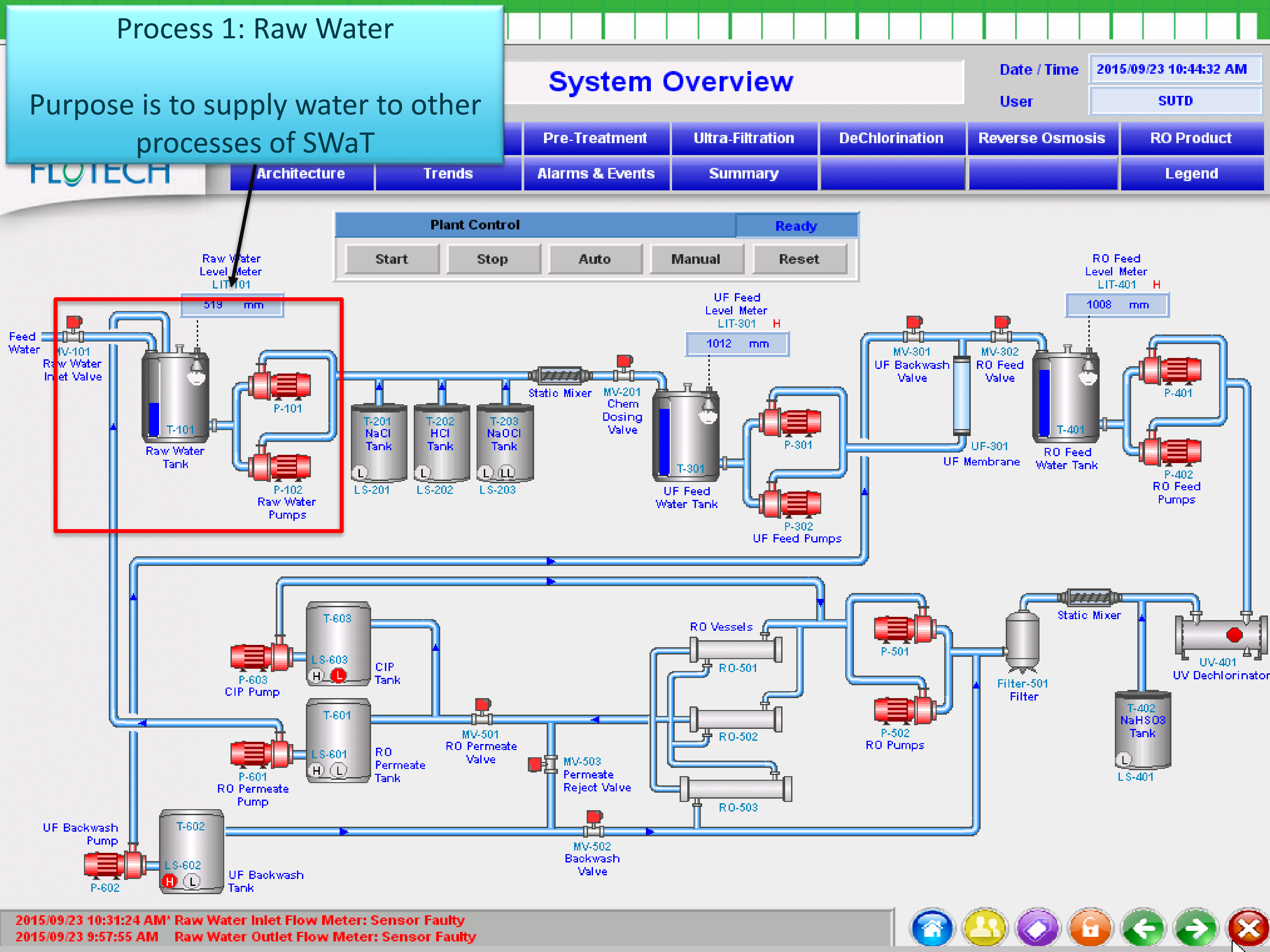


# Secure Water Treatment Testbed (SWaT)



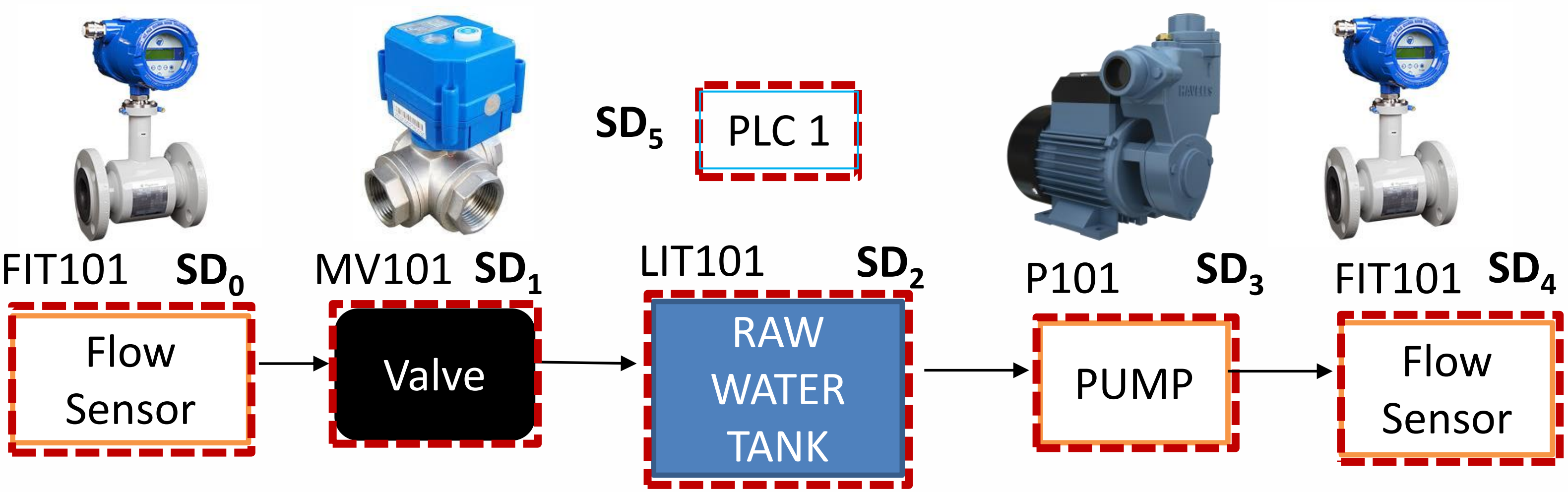
# Process 1: Raw Water

Purpose is to supply water to other processes of SWaT



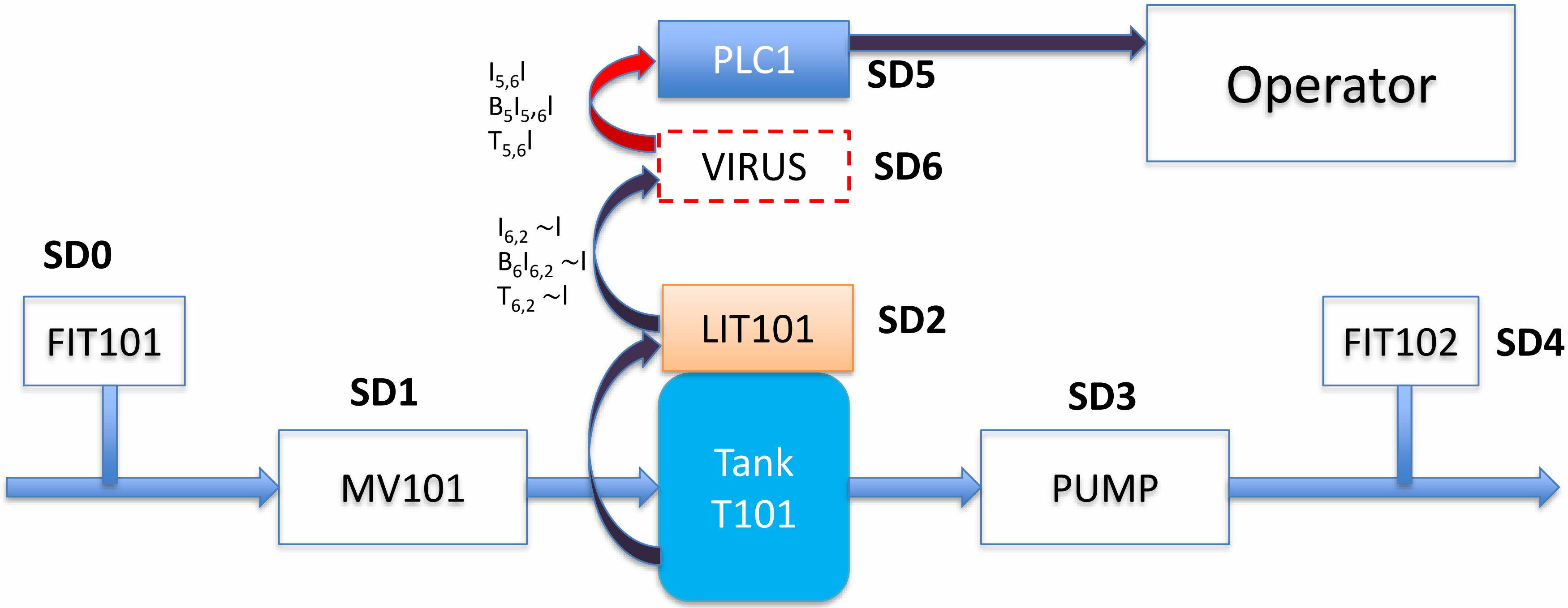
# Working of MSDND

## PROCESS 1




LIT – Level Indication Transmitter, FIT – Flow Indication Transmitter, MV101 – Motorized Valves and P - Pump

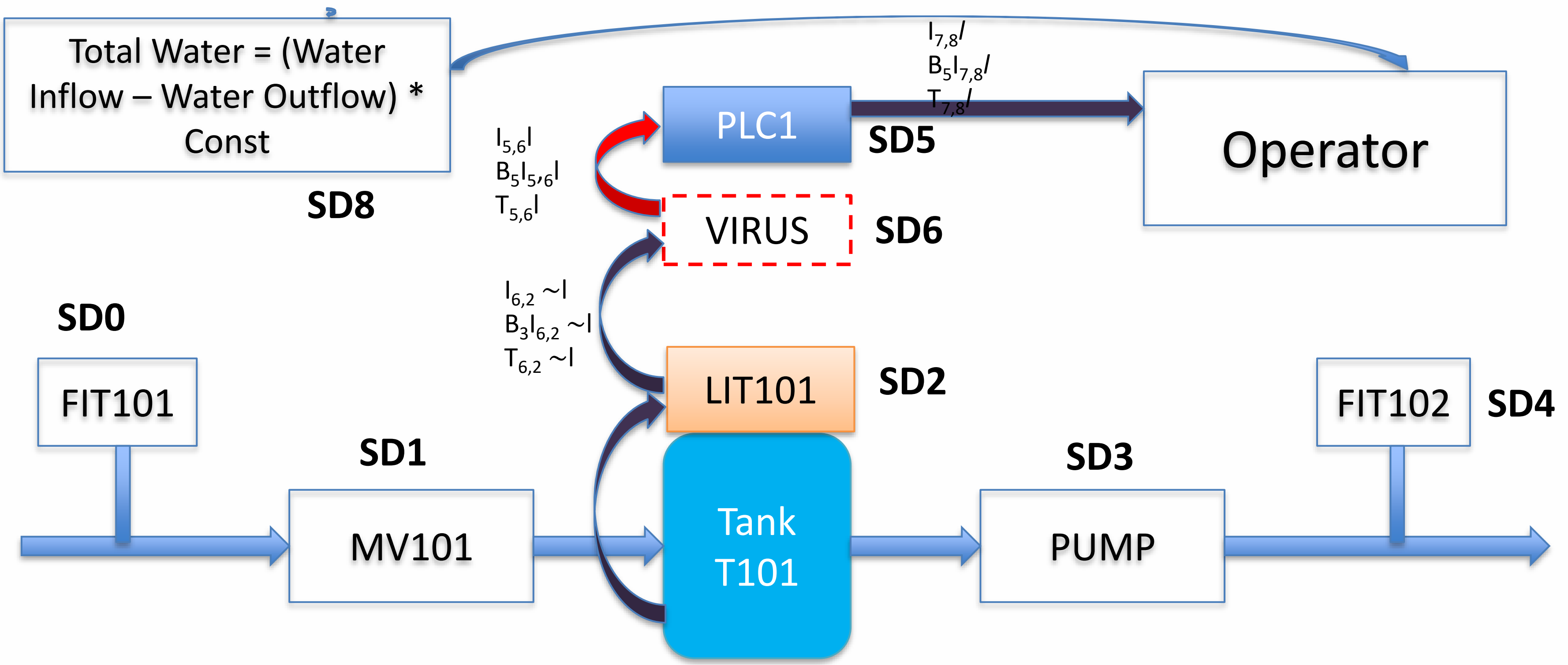
# Working of MSDND (Cont.)



# Working of MSDND (Cont.)

- Since $B_5 I_{5,6}\, l \wedge T_{5,6}\, l \rightarrow B_5\, l$, the PLC believes the lie told in all cases. Therefore, unknown to entities in SD2, $V_2 l$ (w) and $V_2 {\sim} l$ (w) cannot be evaluated. Therefore $l$ is MSDND secure from SD2.
- $MSDND(ES) = \exists\, w \in W \rightarrow [(S_l \oplus S_{\sim l})] \wedge [w \models (\nexists V^{SD5}_{\sim l}(w) \wedge \nexists V^{SD5}_{l}(w))]$
- This is BAD for the plant as the threat goes undetected

# Working of MSDND (Cont.)



# Working of MSDND (Cont.)

- Now when we take the ‘and’ operation for both the normal working and when an invariant is considered, we can conclude that the system is working normally

- $S_{invariant} \wedge S_{I} = S^{*}$; System is working normally if and if only this is true

- $MSDND(ES) = \exists\, w \in W \rightarrow [(S^{*} \oplus S_{\sim I})] \wedge [w \models (\nexists V^{SD5}_{\sim I}(w) \wedge \exists V^{SD5}_{I}(w))]$

# Working of MSDND (Cont.)


- When an invariant fails, the tile with that invariant turns red

| Process | Comp | Summary | Suggestions |
|---|---|---|---|
| Process 1 | 4 | Invariants Developed : 4<br>Invariants Matching : 4<br>Vulnerabilities remaining : 0 | Invariants for FIT and LIT should be modified to better capture multipoint attacks |
| Process 2 | 11 | Invariants Developed : 7<br>Invariants Matching : 0<br>Vulnerabilities remaining : 6 | Chemical processes should be further analyzed for getting more reliable invariants. Chemical dosing pumps and level indication should be modified. |
| Process 3 | 9 | Invariants Developed : 4<br>Invariants Matching : 3<br>Vulnerabilities remaining : 2 | Several attacks can be performed on motorized valves for damaging pumps and draining water. Install PIT near UF Unit to generate invariant for DPIT |
| Process 4 | 7 | Invariants Developed : 3<br>Invariants Matching : 3<br>Vulnerabilities remaining : 1 | Dichlorination Unit and NaHSO3 dosings effects chemical properties of water, using this, better invariants should be made as it effects RO Unit |

| Process | Comp | Summary | Suggestions |
|---|---|---|---|
| Process 5 | 16 | Invariants Developed : 7<br>Invariants Matching : 0<br>Vulnerabilities remaining : 9 | Many MSDND Secure paths are identified, invariants should be developed to break the MSDND security |
| Process 6 | 7 | Invariants Developed : 2<br>Invariants Matching : 0<br>Vulnerabilities remaining : 5 | Level switches should be replaced with level indicators, and more FIT’s should be installed for getting invariant |

# Another Typical Result

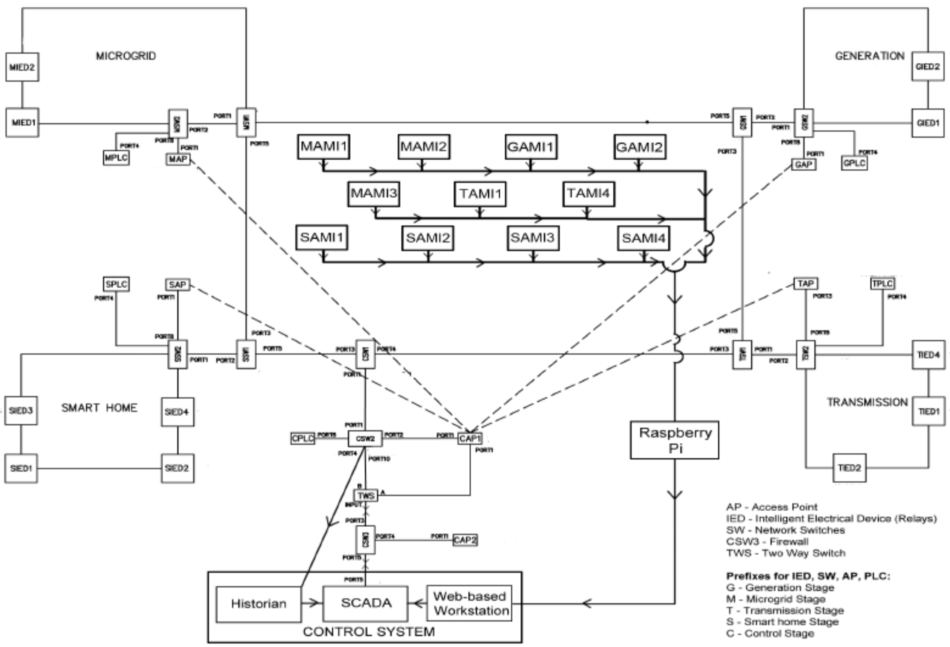



Figure 4: Power Testbed– Network Diagram

Power System Testbed in Singapore

- Solar
- Batteries
- Generators
- Loads

| Summary | Count |
|---|---|
| Information paths analyzed | 100+ |
| MSDND secure paths found | 89 |
| MSDND secure paths broken using invariants (Total invariants generated) | 73 |
| Invariants implemented in the system | 24 |

MISSOURI S&T

# WHAT TO DO WITH THIS INFORMATION?

# What to do with this information?

- Measure System Security Resilience
  - Using the uniform information flow model
- Improve Design
  - Mitigate MSDND paths
- Mitigate Attacks through Engineered Knowledge to Break MSDND
  - Active defense against
    - Cyber Enabled Physical
    - Physically Enabled Cyber



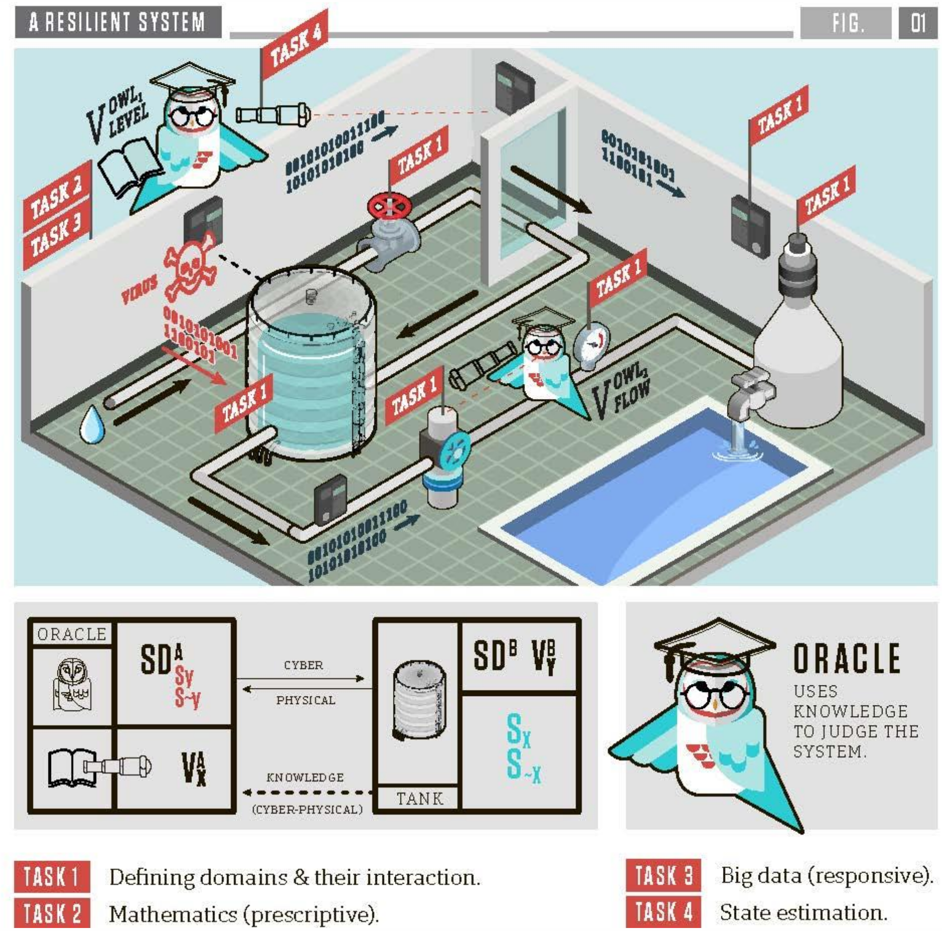


This is Hard to Do

How to provide a functioning CPS without relying on assumptions of trust, but instead developing trust among components?

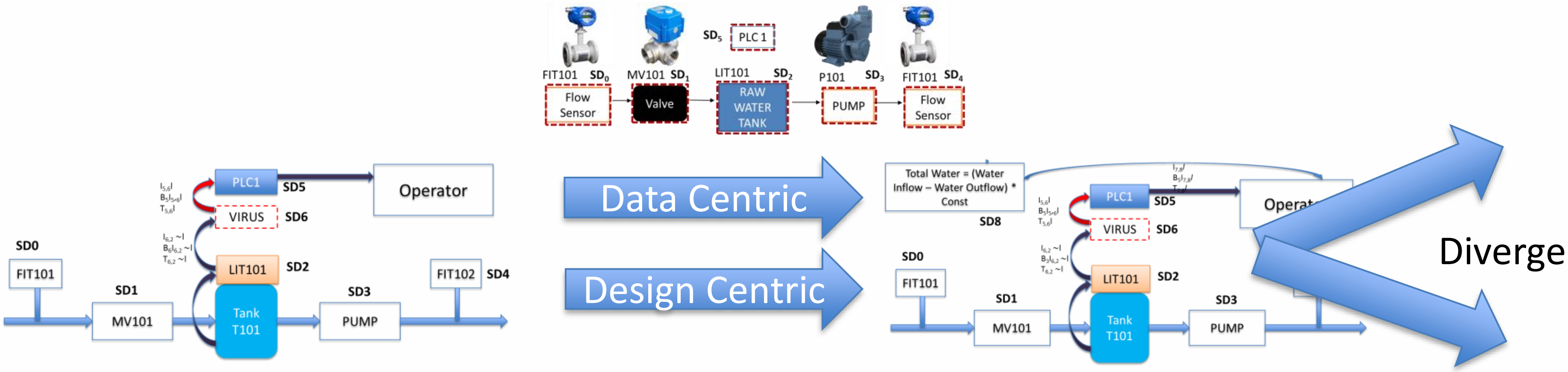
## Goals

- Automated Security Domain Construction
  - Semantic Bridges and Oracle Owls
- Design-Centric
  - Port Hamiltonian Systems
- State Estimation
  - Algebraic, Spatio-temporal & Real-Time Dynamic State Estimation
- Data Science
  - Learn behavior with ground truth

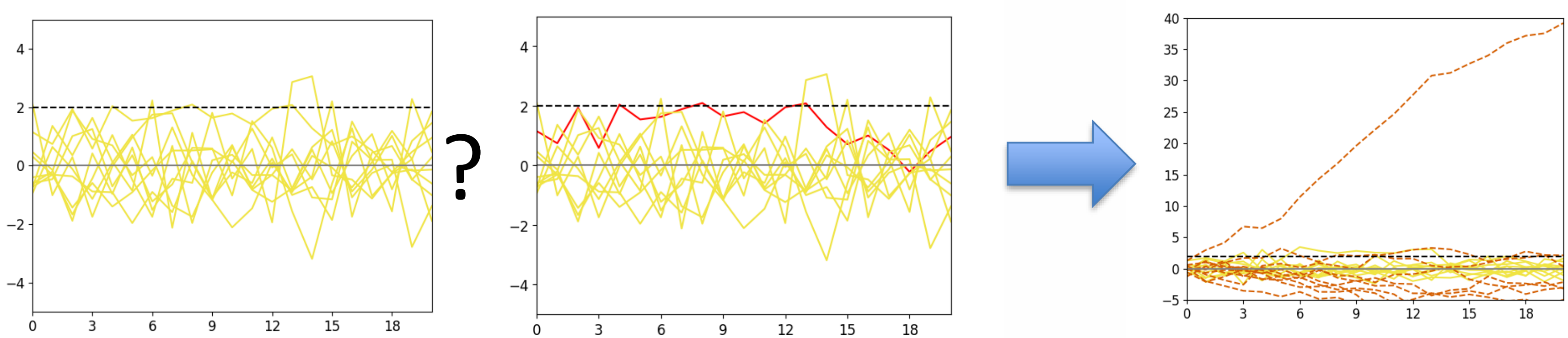



- Experimentation on real infrastructures
  - Power, Water, Manufacturing, Transportation

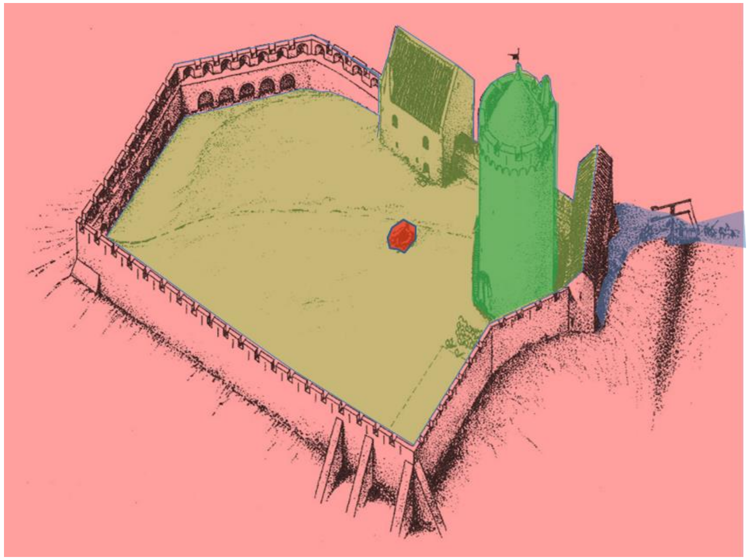
# Findings




Association Rule Mining, Generalized Linear Modeling

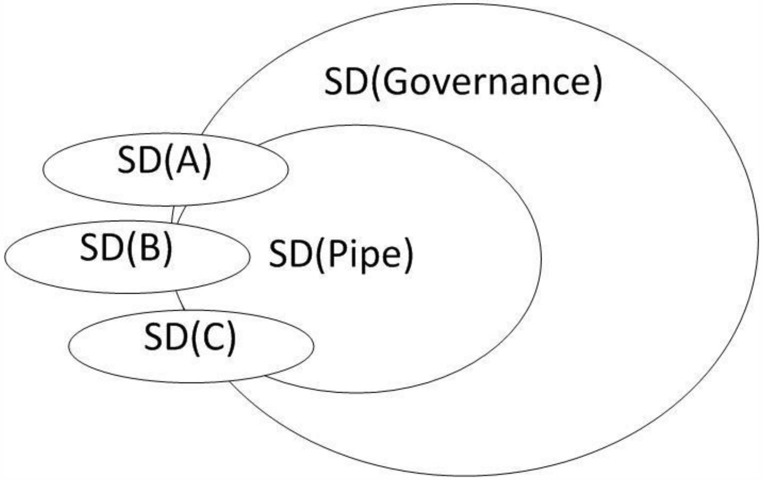



Subtle Theft, Slow Drift

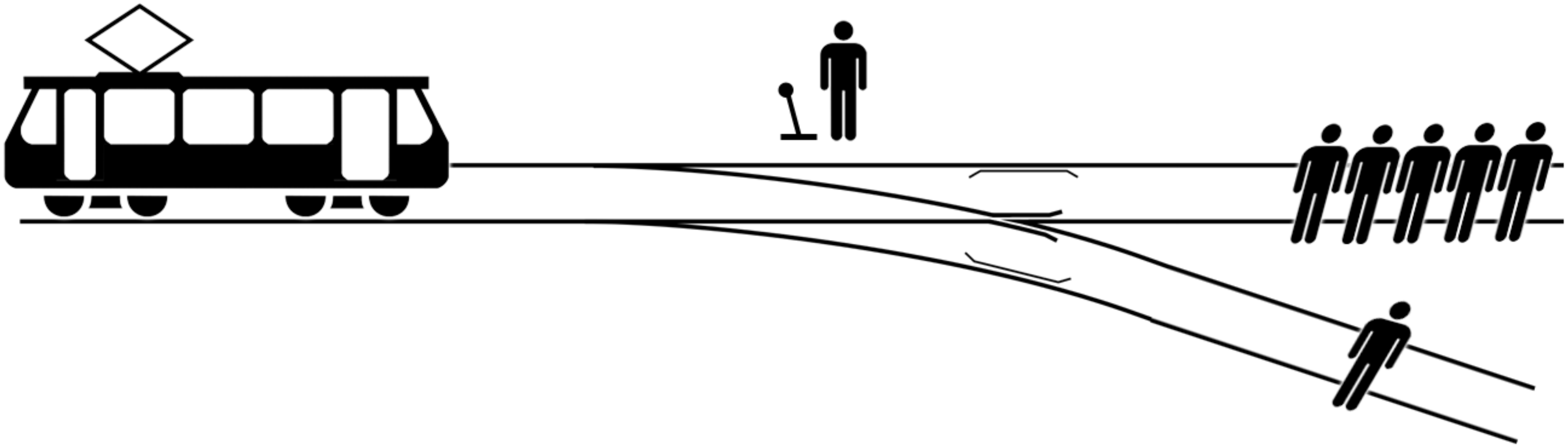


- Traditional View – Castle/Maginot Line/BLP
  - High level vs low level
  - Firewalls, Defense in Depth
  - Does not address cyber-physical nor insider attacks

- Modern Environment
  - Multiple security domains
  - High/low, Insider vs Outsider has changed
    - We are INSIDE the system
  - How do we secure the cyber-physical?



# Ethics in these systems



Trolley Problem

# Will people use this?

- Privacy
  - Norway vs. USA
- Resilience
  - Cyber threats
- Fog?
  - Ethical Issues


# Your Thoughts?

# A Professional Society

- Local Seminars
- Get-together
- Quality
  - Accreditation
  - Peer Review
  - Standards

# Cyber-Physical Security Through Information Flow

**Bruce McMillin**

**Professor and Interim Chair, Department of Computer Science**
**2018-2020 Distinguished Visitor**
Missouri University of Science and Technology
325 Computer Science, 500 W. 15th St., Rolla, MO 65409
o/ (573) 341-6435 e/ ff@mst.edu