Cyber Defense of Complex Ground Systems

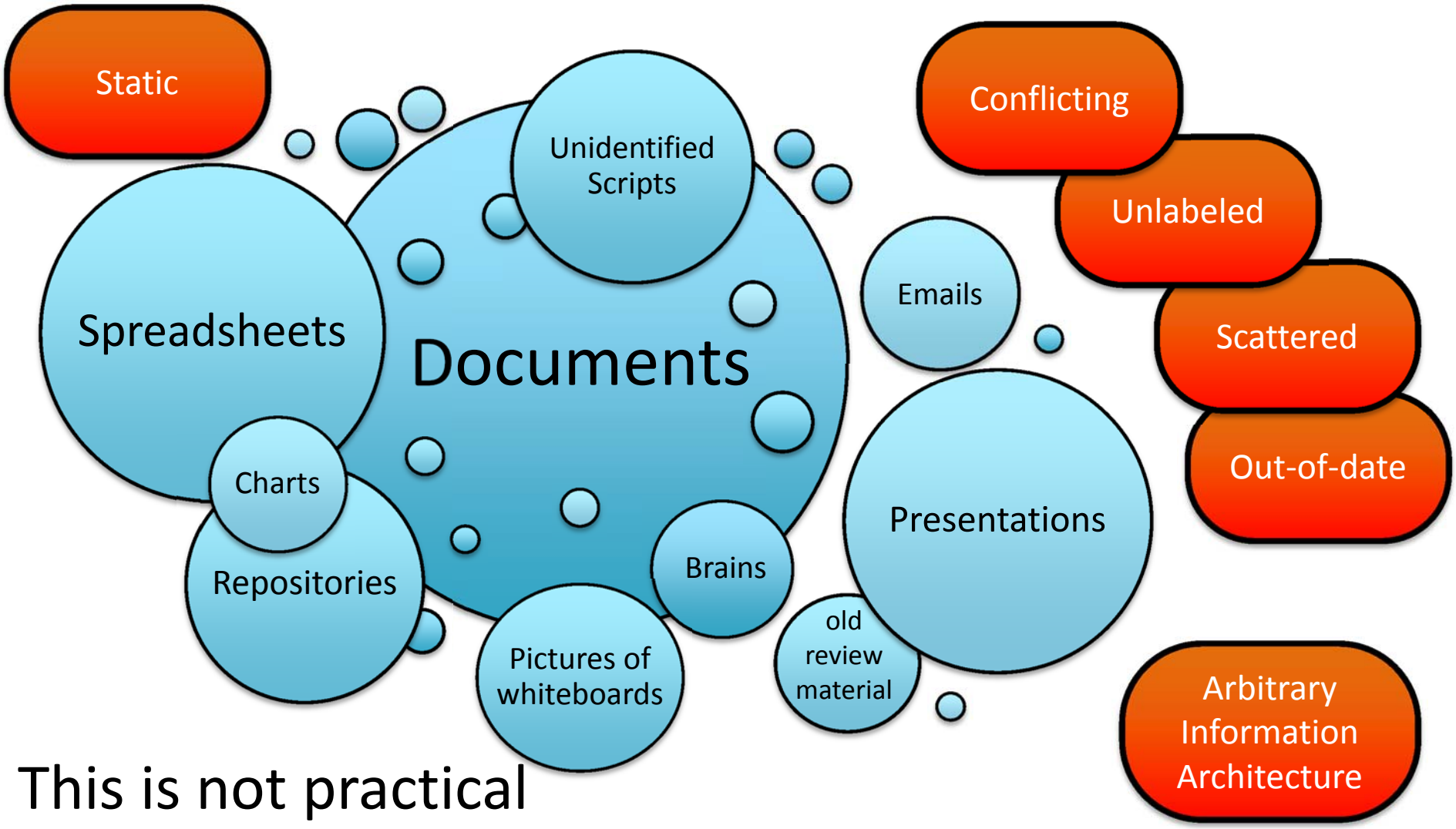
Can you defend what you don't understand?

Maddalena Jackson

Eric Rice

Elyse Fosse

State of the Art: System Knowledge

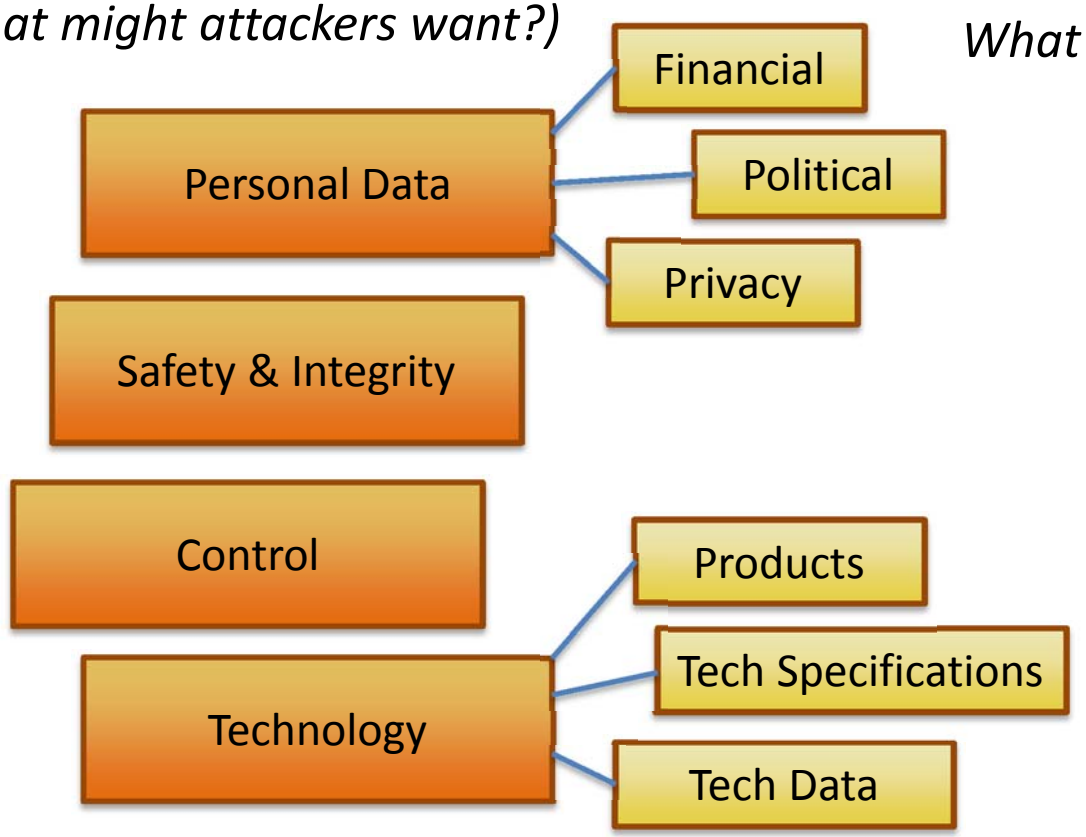


This is not practical

A few first principles…

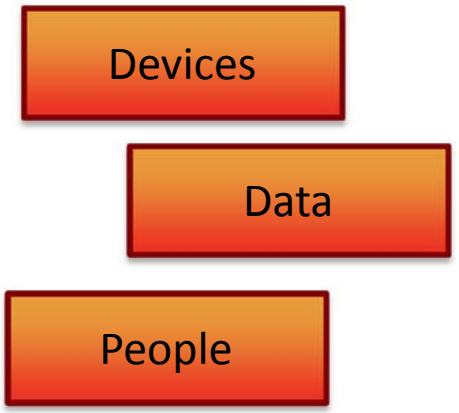
What are we protecting?

(What might attackers want?)



How do we protect those?

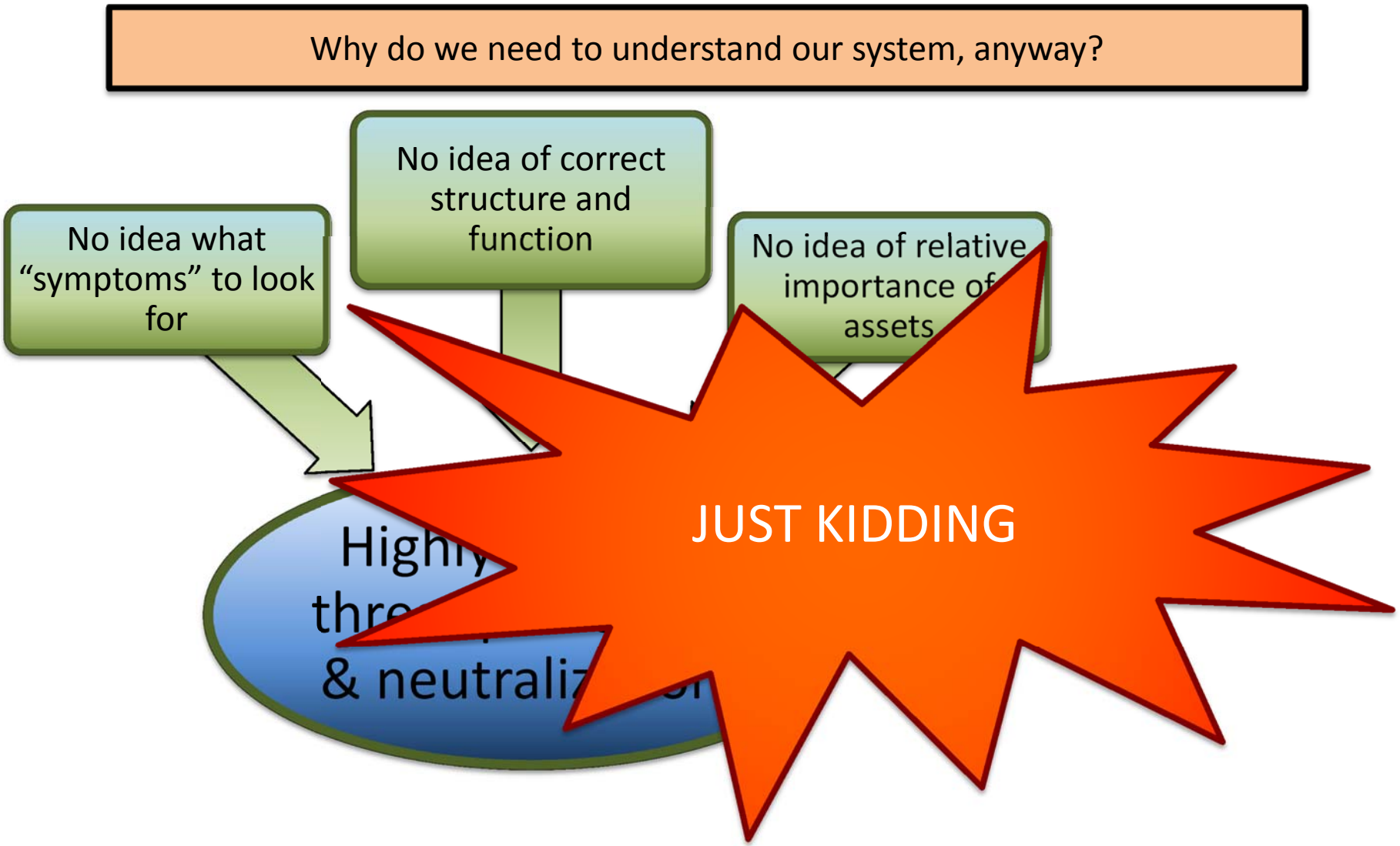
What can attackers affect?



Cyber attacks no longer directed only at sensitive data…

Of course, we are also protecting these from accidents and non-malicious faults and failures

Let's be absurd for a minute…



Back to reality…

- **Can we effectively defend if we…**
  - Don't know what symptoms to look for?
  - Don't know correct structure and function?
  - Don't know importance of each part?

- **Why do we need new approaches here?**
  - Are you completely confident that your system is
    - Totally impenetrable, or
    - Entirely resilient to attack
  - Is every single person a SME in every aspect of your system?
  - Do you have an all-knowing benevolent AI that you are keeping to yourself?

How do we think about the problem?

Assumptions:
- Systems will be attacked
- Attacks will evolve

Focus of our effort:

Give defenders tactical advantages - respond **quickly** & **accurately** to threats

Aware of current attack

Potential impacts of current attack

Strategies to neutralize attack

System Knowledge
Goals, assets, relationships, criticality, existing vulnerabilities, etc.

Observables in the System
Current and historical state of assets, access to assets, exchanges of data, etc.

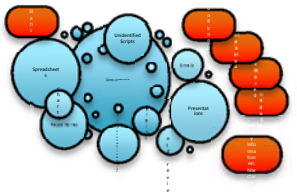
System Assessment
What is system supposed to be doing? What is it actually doing? What might happen in the future? What happened in the past?

Intent

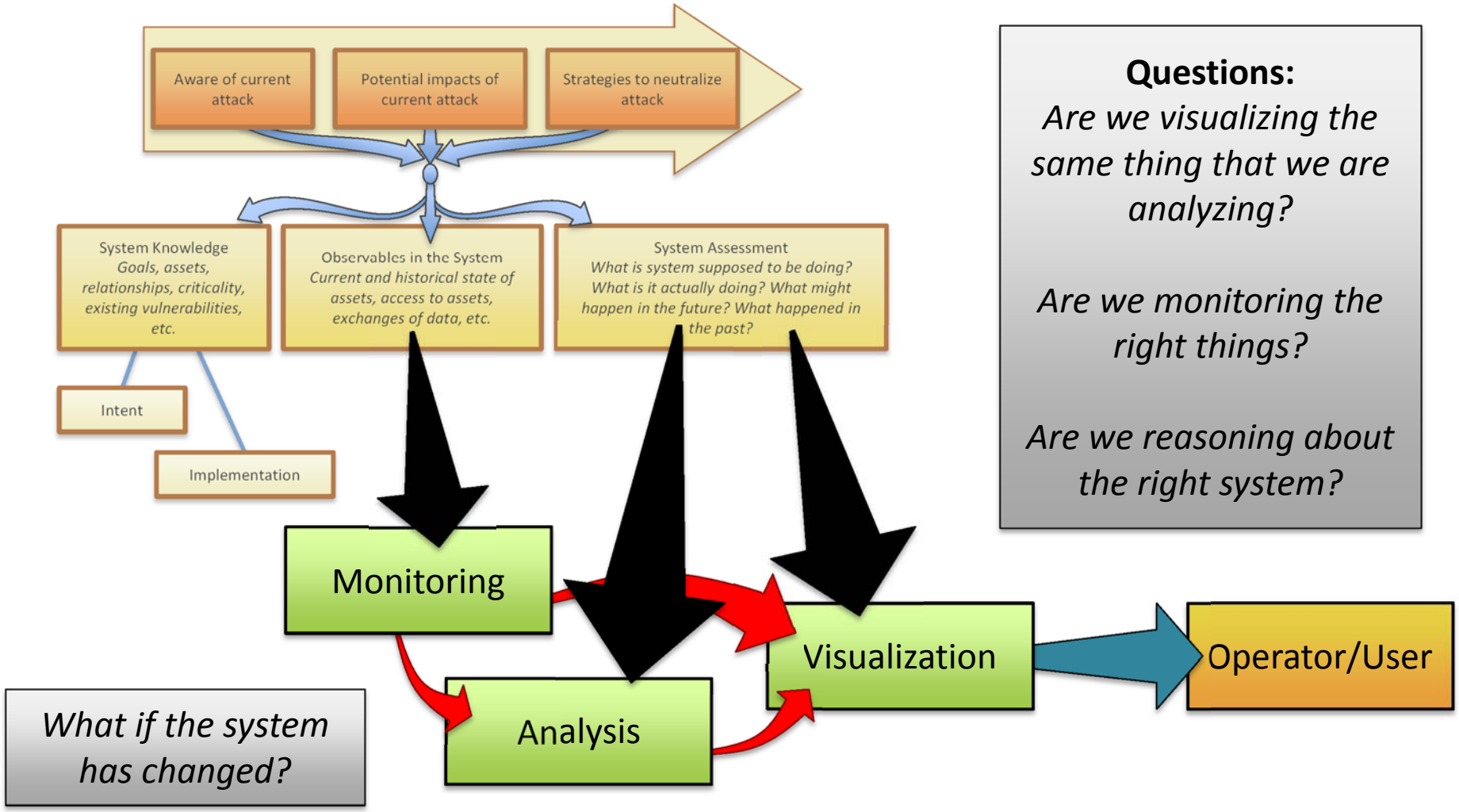
Implementation

Can't we do this now?

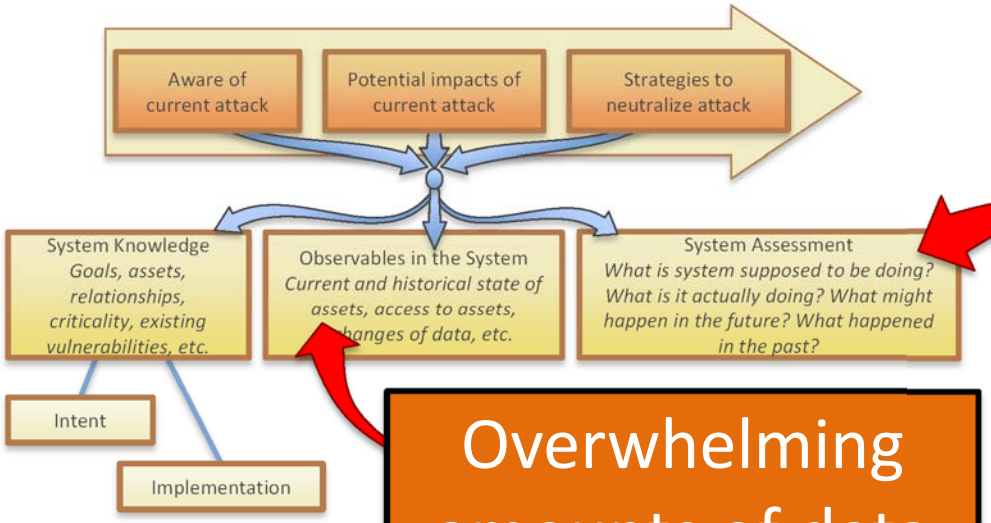
Yes, but we could be more effective.



What do we want to provide?



Areas of complexity



Limited impact assessment

Access to information to build mental model: slow, difficult, tedious

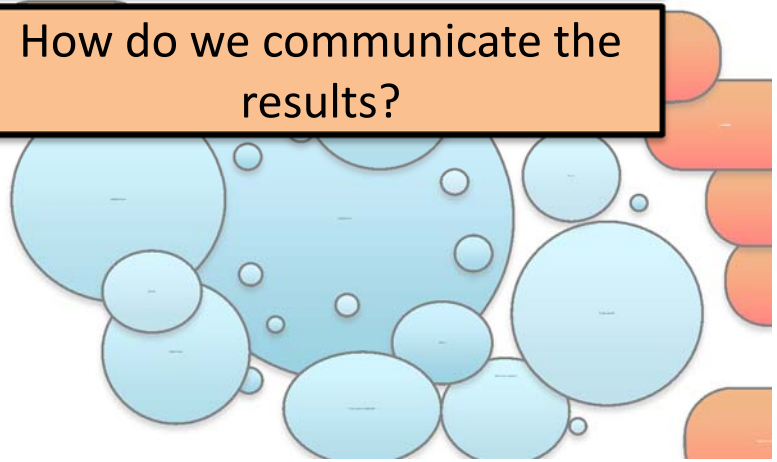
Overwhelming amounts of data

What are we assessing?

How do we communicate the results?

What should we monitor?
Should we just monitor EVERYTHING?

Distinguish important data from noise

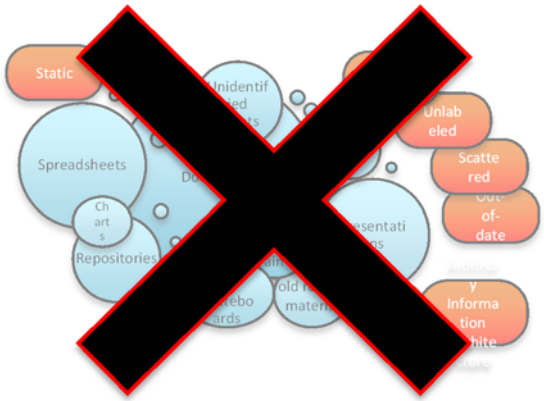


A system model…

Analysis and visualization require system context; knowledge must be **CONSISTENT**

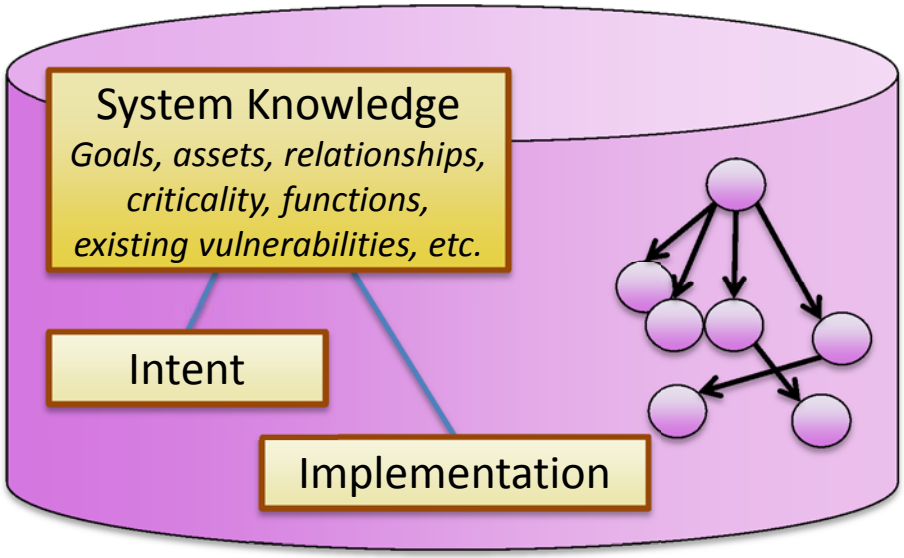
We need…

Integrated Source of Truth
A model of the system

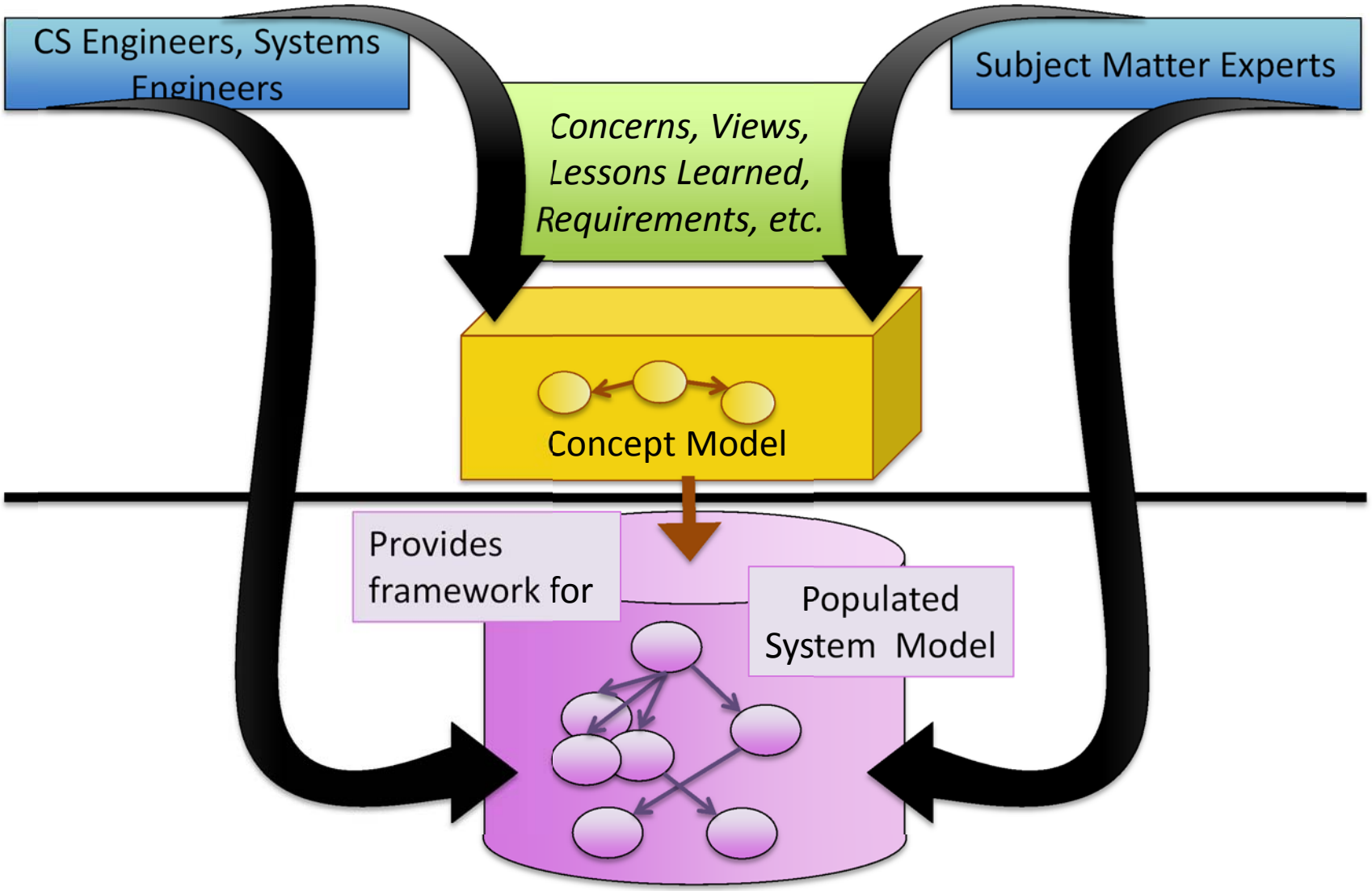


- Machine-readable
- Structured
- Dynamic
- Consistent
- Adaptable
- Queryable

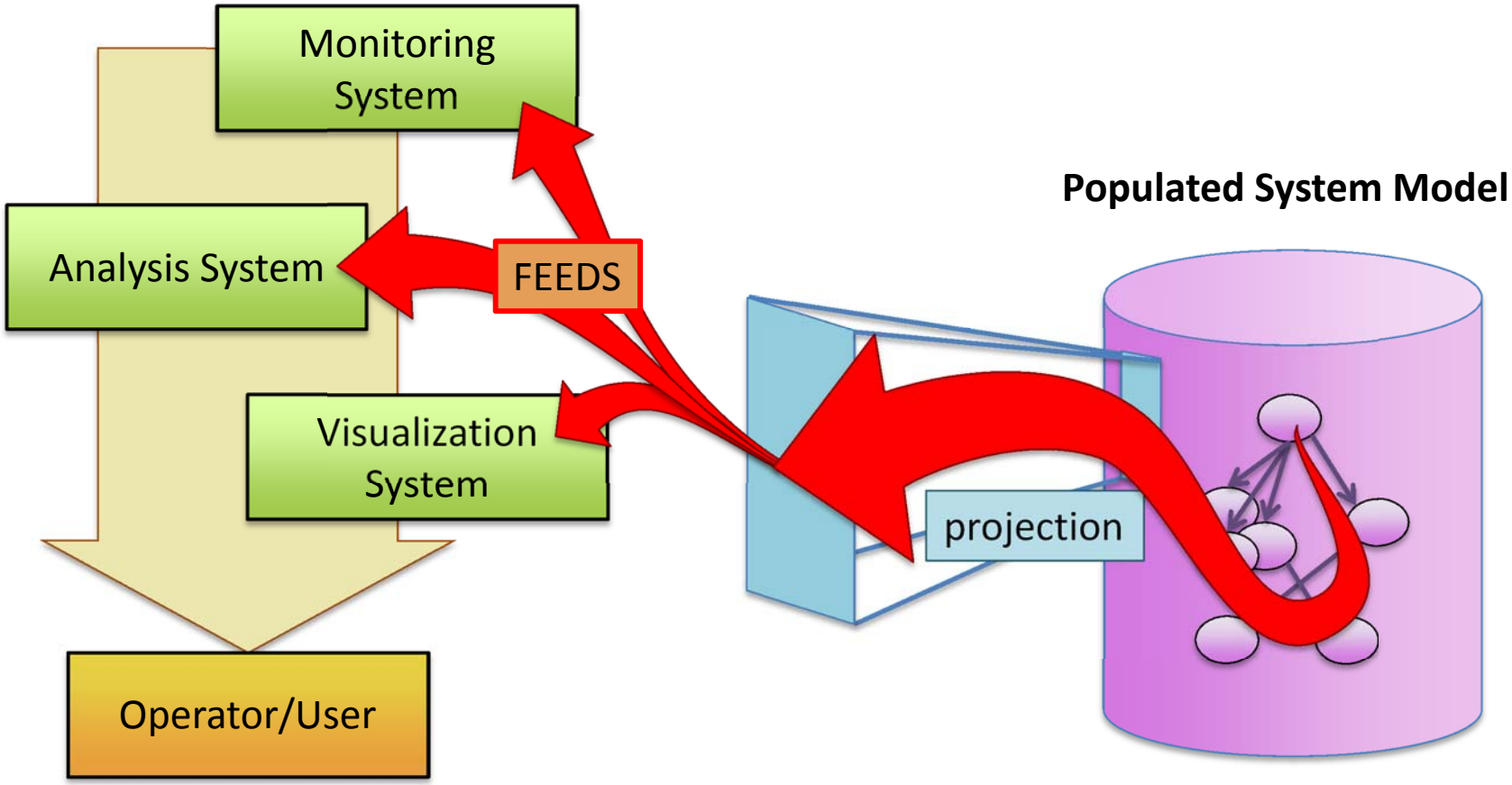
Populated System Model



Building the system model

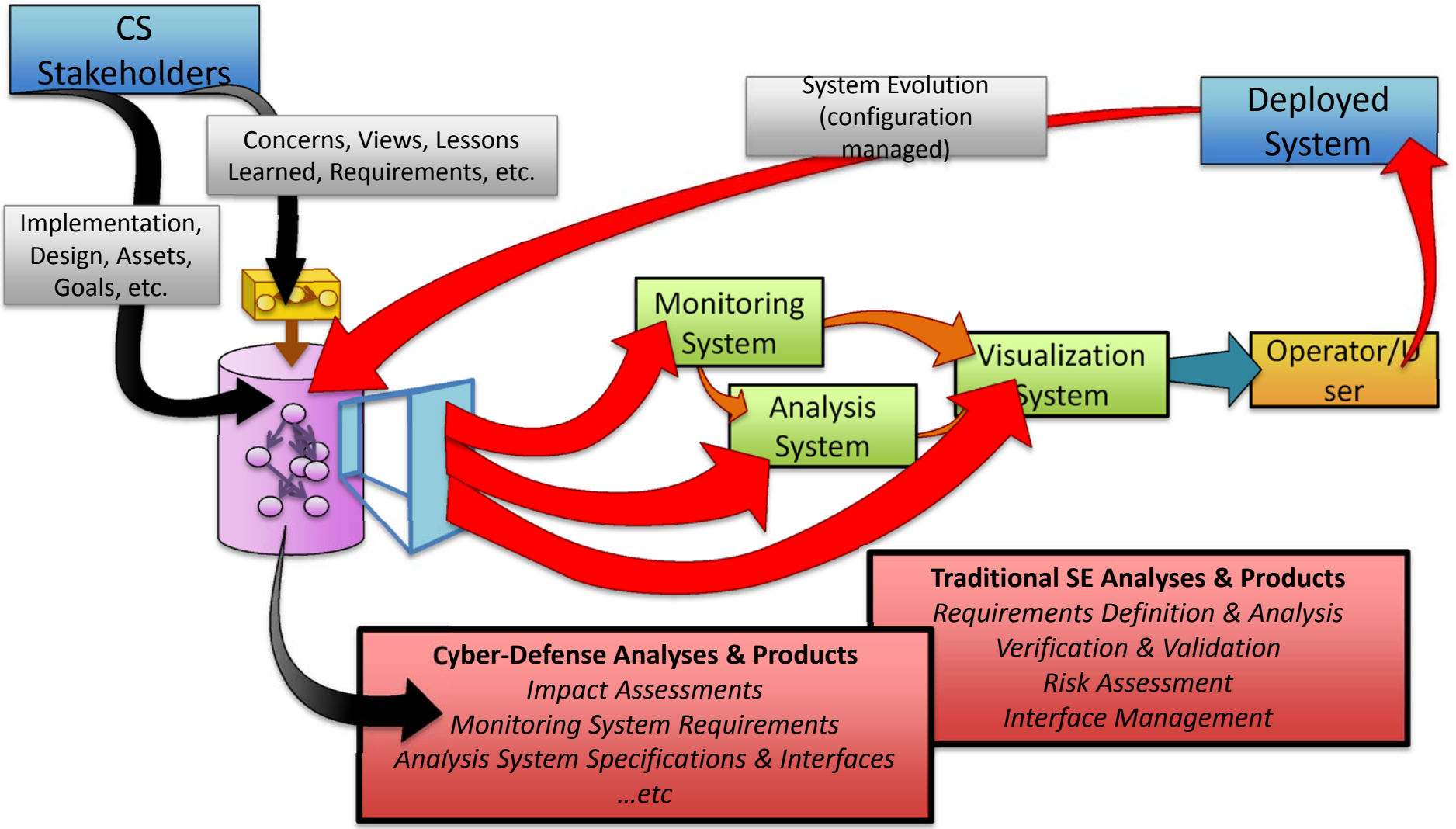


How does this actually work?



This process is the "common way to discuss, reason about, detect, diagnose and remediate"

Future concept



Research areas

- Information architectures
  - Detection, Diagnosis, Remediation system concerns
  - Operator & Stakeholder views
  - Systems Engineering Domains applied to CS
    - Verification & Validation, Fault Analysis, Mission Goals & Definition, GDSE, Interface Management, etc.
- Capture & assessment of system design vs. operational behavior
- Visualization
  - Concise presentation of complex analysis
    - Future state projections
    - Differences in expected and observed behavior
    - Impact assessments
    - Root cause analysis
    - Instinctive understanding of system state
- Interoperability with existing models
- Keeping models current
  - Knowledge infusion back to model
  - Configuration management & gatekeeping

Questions?

Acknowledgements & references

- References

  - J. Holsopple, et al., “Enhancing situation awareness via automated situation assessment,” *IEEE Comm. Mag,* vol. 48, no. 3, 2010, pp. 146-152.
  - J. Bayuk and B. Horowitz, “An Architectural Systems Engineering Methodology for Addressing Cyber Security,” 2011 Wiley Periodicals, Inc. Syst Eng 14: 294–304, 2011
  - X. Li, et al., “Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges,” *IEEE Comm. Mag,* vol. 50, no. 8, 2012, pp. 38-45.
  - E. Rice, A. AlMajali, “Mitigating The Risk Of Cyber Attack On Smart Grid Systems,” *Conference on Systems Engineering Research (CSER),* 2014
  - A. Almajali, E. Rice, A. Viswanathan, K. Tan, C. Neuman, “A Systems Approach to Analysing Cyber-Physical Threats in the Smart Grid,” *IEEE International Conference On Smart Grid Communcations,* 2013
  - A. Viswanathan, “Effective Situation Assessment in Critical Systems,” *Doctoral Dissertation, University of Southern California [In Preparation].*

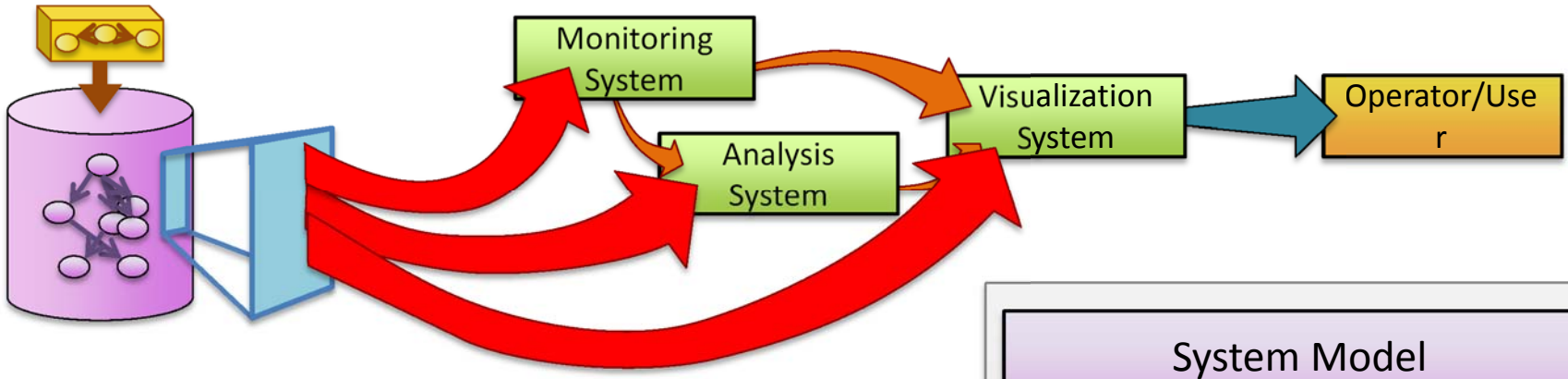
- Acknowledgements

  - Thom Mcvittie, JPL
  - Arun Viswanathan, USC/ISI
  - Kymie Tan, JPL
  - Frank Kuykendall, JPL
  - Marc Sarrel, JPL

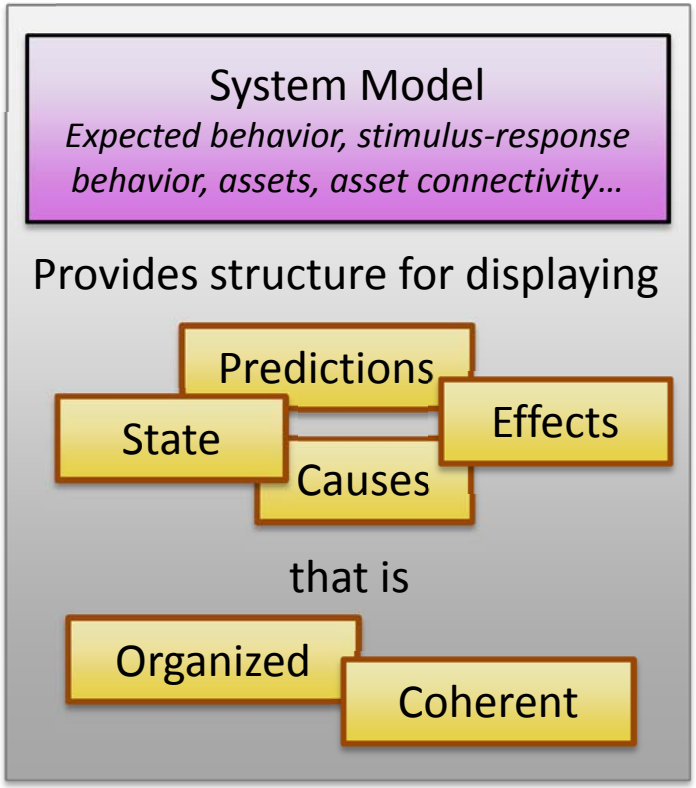
Questions?

Backup

What would you visualize?

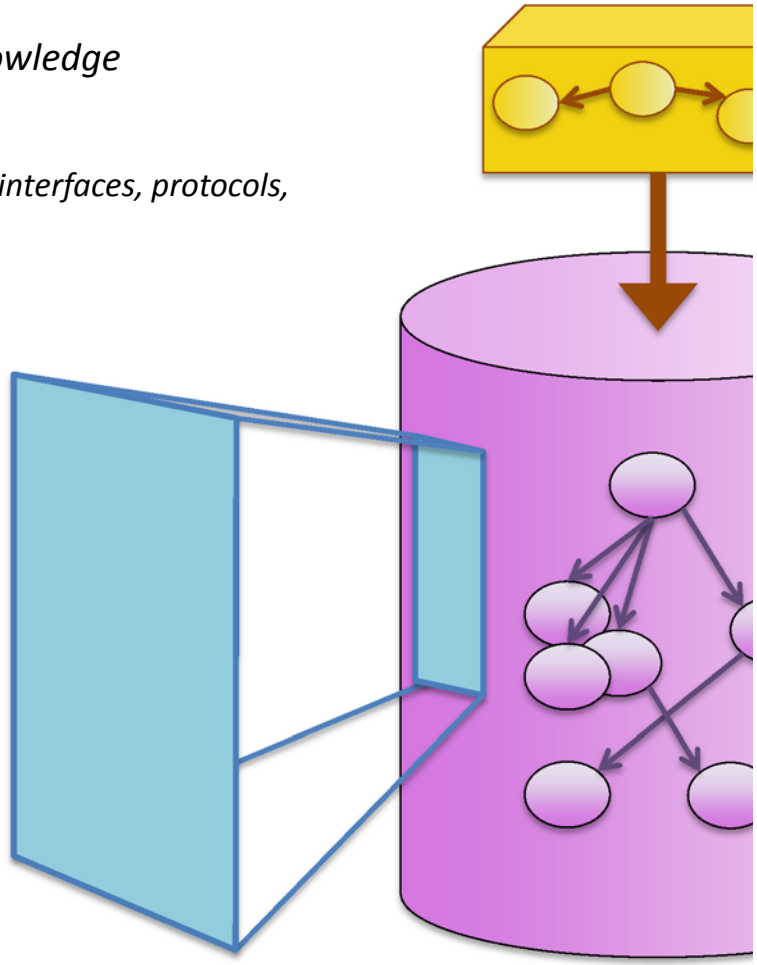


- Goal: Defenders…
  - Act *quickly*
  - Understand *what is happening*
  - Act on *latest information*
  - Understand *consequences*
  - *trust* information



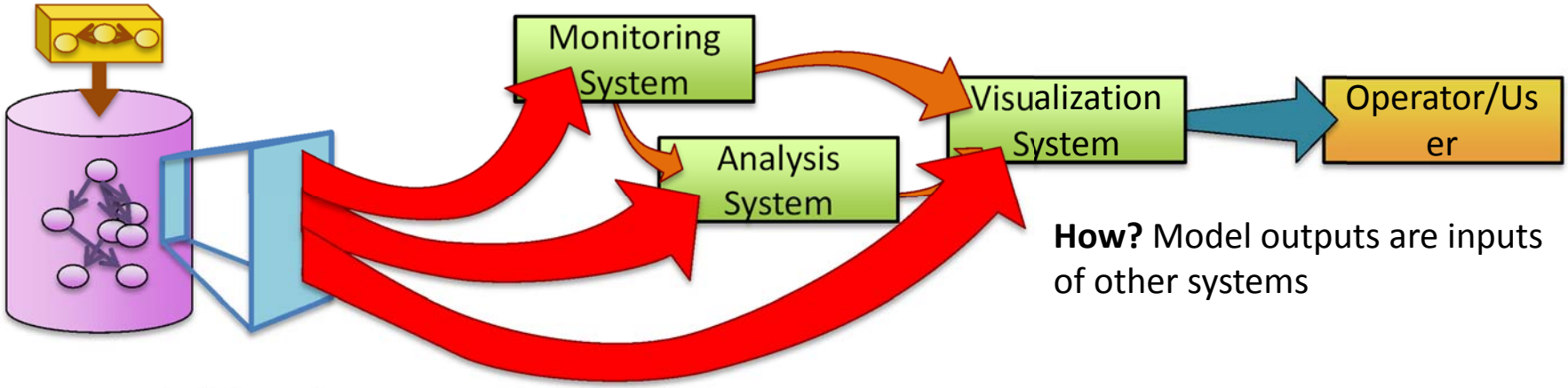
What does the model do?

- **Capture:**
  - **Combined system models** *representing multi-faceted knowledge*
    - *What the system is **intended** to do*
    - *What the system **actually** does*
    - *System deployment and configuration (hardware, software, interfaces, protocols, geographic locations, versions, data paths, etc.)*
- **Automate:**
  - **Analyses & calculations** *normally done by hand*
- **Extract (Query):**
  - *DOCUMENTS, diagrams, matrices, tables, etc.*
  - Analysis & calculation results
  - Operations concept documents, operational constraints
  - Asset criticality information (docs, tables)
  - Asset accessibility reports
  - Interfaces – specifications, requirements, diagrams
  - Risk assessment – reports, tables
  - Impact assessments (via modeled or inferred dependencies)
  - Simulations
  - Known vulnerability and threat reports
  - Deployment configurations – networks, software, hardware, testbeds, processes, etc.



Application: model-driven DDR

- **Model-driven analysis & visualization system**
  - Enhances interoperability with monitoring system & analysis system



- **Model feeds…**
  - Expected behaviors, actual designs, relations of functions to systems, hardware & software, relation of intended information exchanges to actual system interfaces, goals, criticality, schemas/specifications of data, events **to analysis system**
  - Same information to **Visualization System**
  - **Result:** visualization system displays information consistent with analysis & monitoring

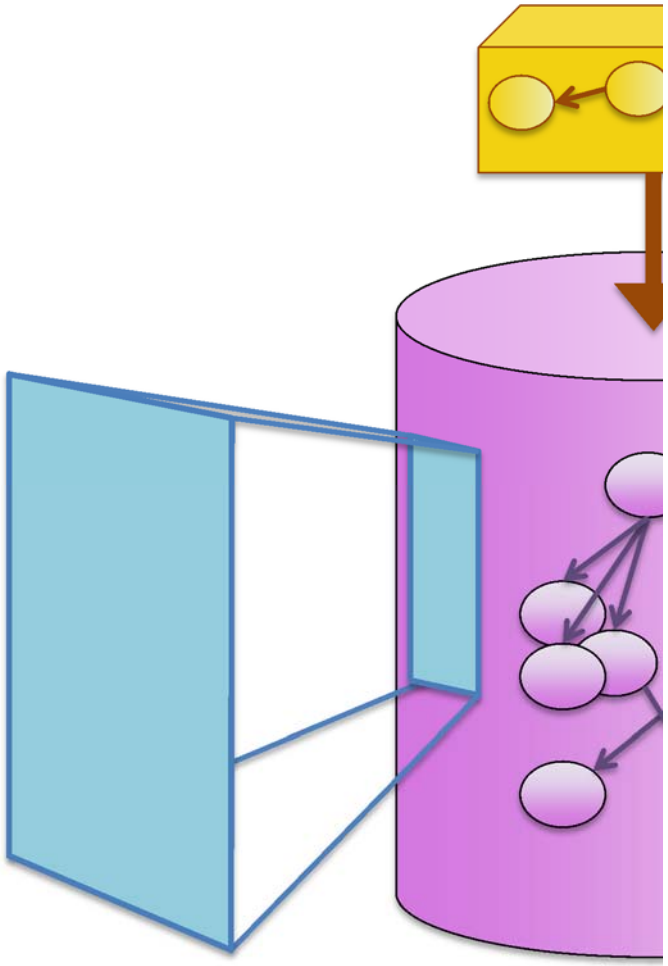
Engineering Process

- **How can you implement this?**
  - **Develop** information architecture
  - **Choose** modeling tool / infrastructure
  - **Populate** the model

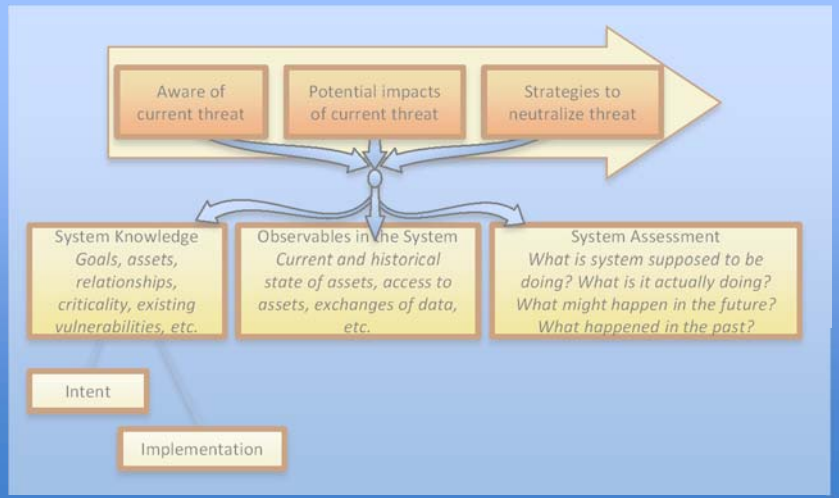
During Design

- Requirements definition of
  - monitoring systems
  - analysis engines
  - visualization
- Model information gathering & CM processes, feedback loops

- **How can you implement this?**
  - **Develop** information architecture
  - **Choose** modeling tool / infrastructure
  - **Populate** the model
  - Requirements definition & implementation of monitoring systems
  - Requirements engineering, design, implementation of DDRtype stuff
  - Requirements design of visualization systems
  - Model information gathering & CM processes, feedback loops



Assess the Problem



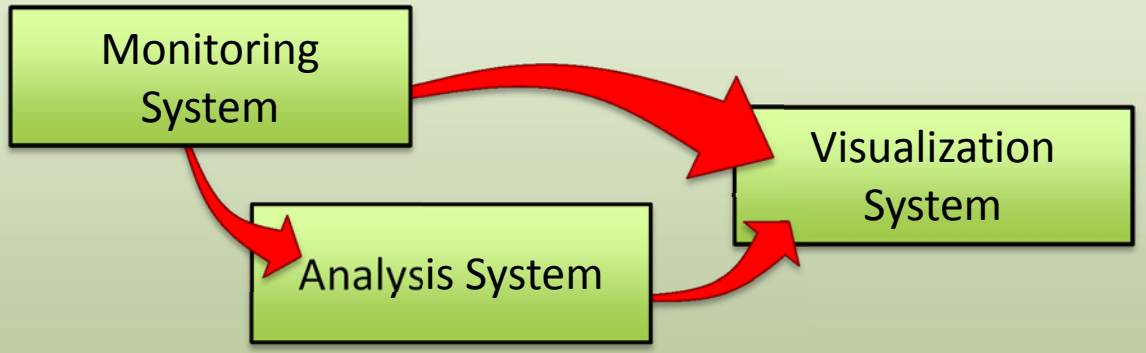
Problem breakdown

- Knowledge
- Observations
- Assessment

How does a person do it?

Observe → Analyze → Explain

How does a machine do it?



Not just useful in a deployed system!