# Autonomous Fault Management of Cyber-Physical Systems

David Scheidt
david.scheidt@jhuapl.edu

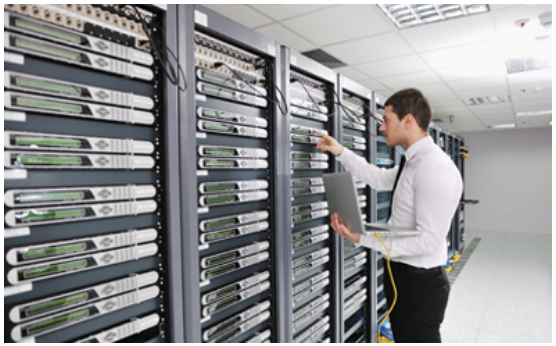
# The Need for Unified Cyber-Physical Fault Management

# The Need for Unified Cyber-Physical Fault Management

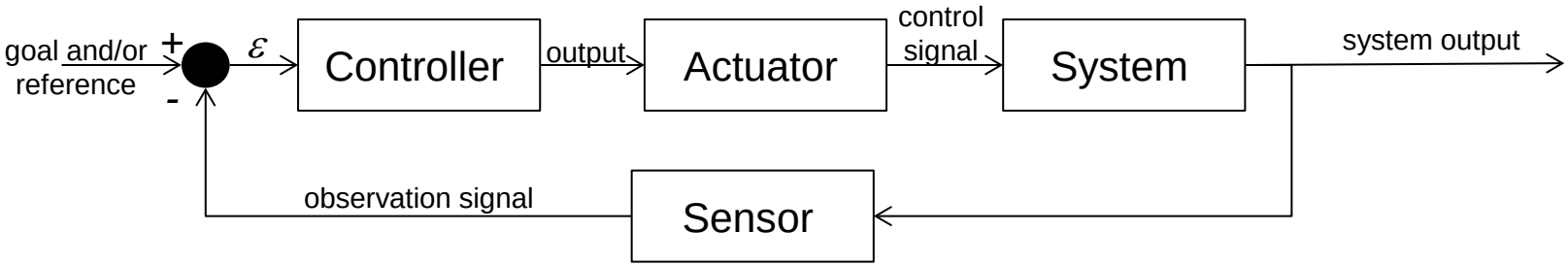
# Cyber and physical systems should be designed and operated holistically

Control actions within the cyber-system must consider effects within the physical system, likewise control actions within the physical system must consider effects within the cyber system.

Cyber-physical system design requires intimate knowledge of the physical plant within the cyber system, and vice versa; or, better still, a unified cyber-physical controller.



# Defining the Cyber-physical System




We assume that the cyber-physical system includes a physical system designed to produce some effect in the natural world (which may include producing information) and that the system utilizes feedback control to achieve its goals. The control infrastructure that is used to execute the control policy is the cyber system. Combined as a single holistic system the cyber and physical systems constitute a cyber-physical system.

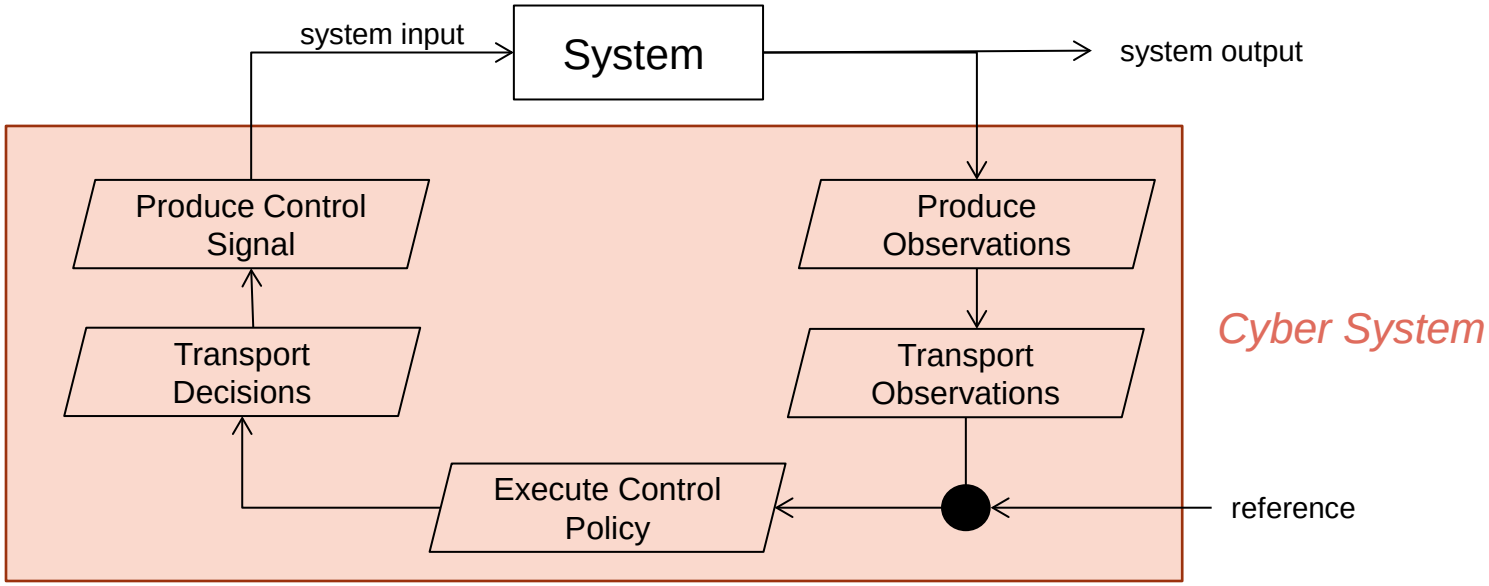
Control of the cyber-physical system, which includes propriaception, must sometimes be performed autonomously (as will be discussed later).

Three cyber-physical systems are considered:

1. Ship Auxiliary Systems
2. Air Traffic Control systems
3. Spacecraft

These systems are all complex, multi-physics and time-sensitive.

# Characterizing the Cyber System as it relates to the Physical System




The control infrastructure is responsible for translating physical phenomena into information, moving information to decision-making processes, executing the control policy to produce a decision, transporting the decision to actuation nodes and translating the decision to an actuation command.

Sensors and actuators can be viewed as components within both the physical system *and* the cyber system.

# Ship Auxiliary Systems

**Mission –** Provide continued capability through continuous vital load operational capability. Vital load operations require service from ship auxiliary systems.

**Sources of disruption**

- Damage events (fire & flooding)
- Isolated failures

**Physical subsystems**

- Power distribution
- Fluid distribution
- HVAC

**Cyber subsystems**

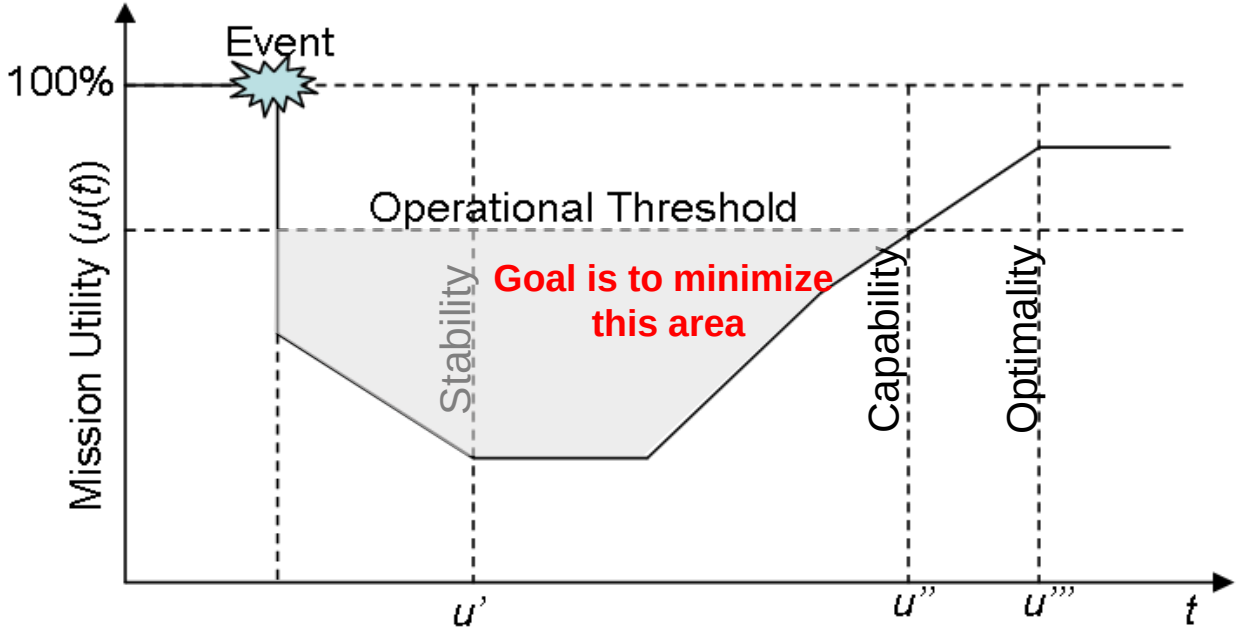
- Real-time network
- Programmable Logic Controllers
- Control software

**System Characteristics**

- Acyclic
- Highly redundant
- Connected (one-dimensional relationships with branches)
- Real-time requirements

# Fitness Criteria

Objective – Provide for resilient ship systems that can maintain mission utility in the presence of both cyber and physical disruptions

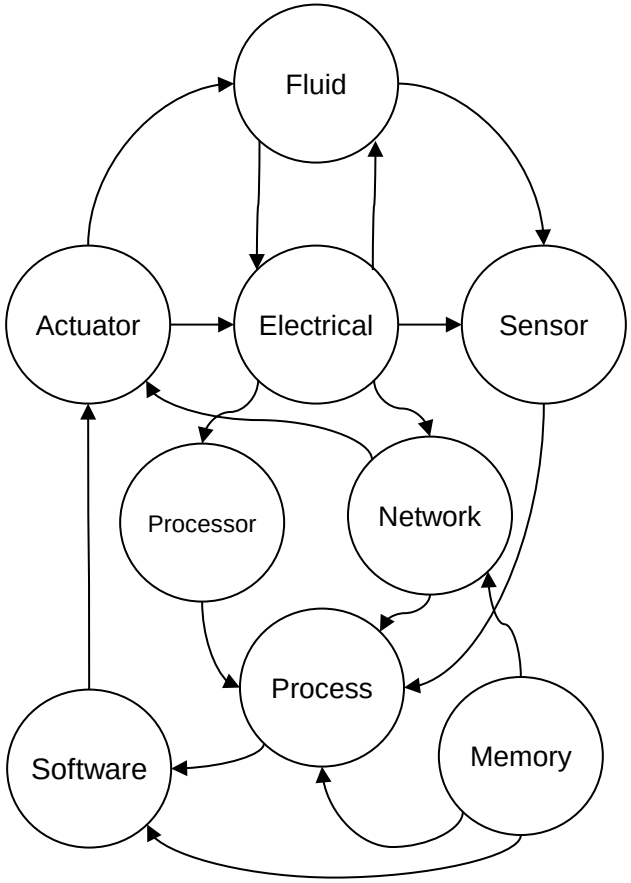



Approach – Develop an autonomous control system that is capable of diagnosing and reconfiguring

Derived from Ed Zivi, ASNE Reconfiguration and Survivability Symposium, Panel Session, Atlantic Beach FL, 16 Feb. 2005

# Ship Auxiliary System Dependencies

- **Cyclic dependencies**
- **Co-dependent physical subsystems**
- **Co-dependency between the cyber and the physical**



# Air Traffic Control System

**Mission** – Coordinate the movement of air traffic to-from the airport without risk of collision.

**Sources of Disruption**

- Terrorist-based RF interference
- Isolated hardware faults
- Malware

**Physical subsystems**

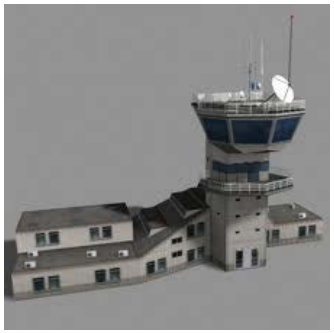
- Aircraft movement, 6-DoF

**Cyber subsystems**

- Radar
- RF Communications
- On-board network
- On-board computers
- On-board software
- Tower network
- Tower computers
- Tower software

**System Characteristics**

- Both cyber and physical operate in Euclidean space
- Distributed control
- Multi-cast network

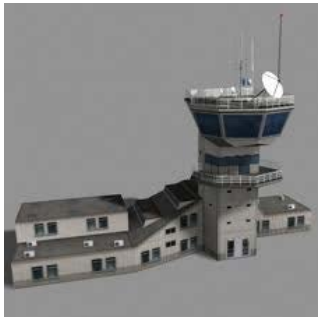


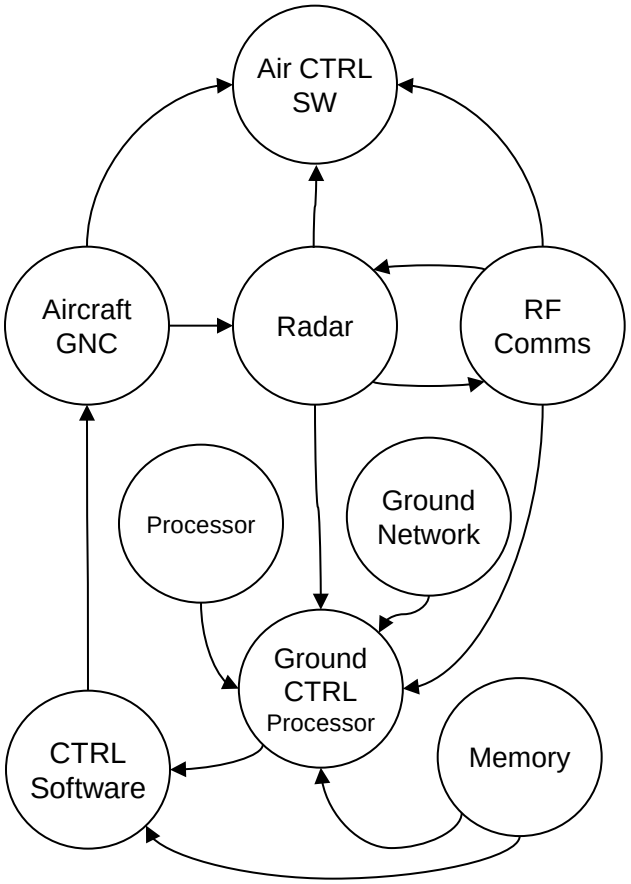
# Air Traffic Control System Dependencies

- RF dependencies defined by:
  - Frequency
  - Geo-spatial
  - Time

RF co-dependencies impact two key cyber functions:

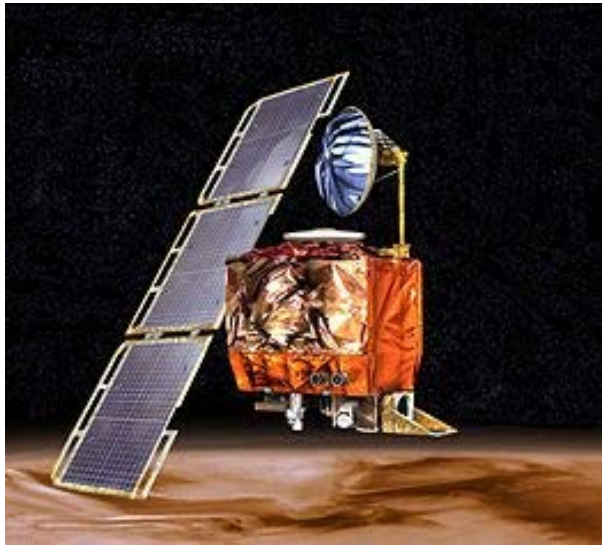
- Sensing
- Communications

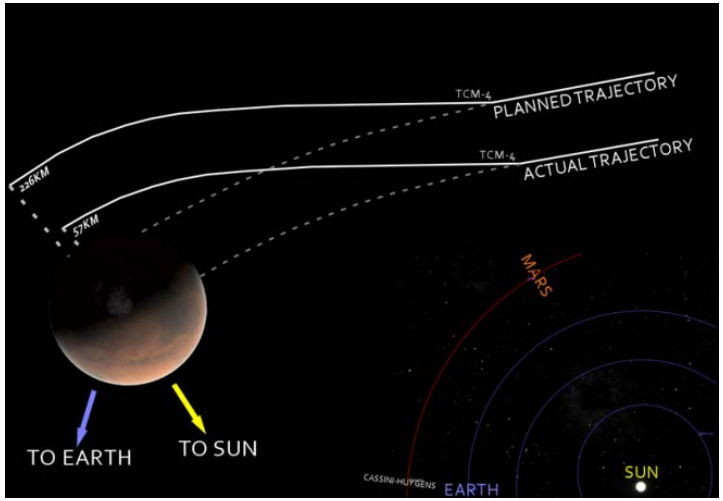




# NASA Mars Climate Orbiter Failure

- Root Cause: Failure to use metric units in the coding of ground based computer software which produced output in non-SI units of pound-seconds (lbf×s) instead of the metric units of newton-seconds (N×s)






Stephenson, Arthur G.; LaPiana, Lia S.; Mulville, Daniel R.; Rutledge, Peter J.; Bauer, Frank H.; Folta, David; Dukeman, Greg A.; Sackheim, Robert et al. (November 10, 1999). "Mars Climate Orbiter Mishap Investigation Board Phase I Report"

# NASA NEAR Mission

Fault Management designed by failure means and effects (FMEA) analysis.

Fault management software produced unintended consequences that would have caused mission failure.

Alert mission operations team recognized impending doom, shut down fault management system and (fortunately) everything worked.

What if, the mission operations team couldn’t communicate with the spacecraft in time.

# NASA New Horizons

# NASA Stereo Spacecraft

**Mission** – Gather 3D data from the Sun and transmit to Earth.

**Sources of Disruption**

- RF interference (from the Sun)
- On-board HW failure (Physical & Cyber)
- Malware

**Physical subsystems**

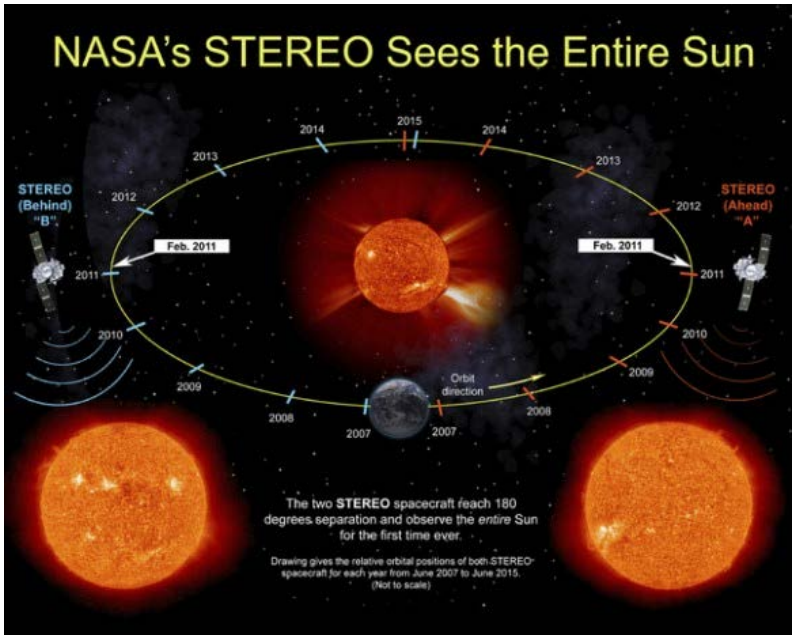
- Propulsion
- Electrical
- Payload sensors

**Cyber Subsystems**

- Guidance and control
- On-board network
- Downlink
- Uplink
- On-board computing
- Off-board computing
- Off-board LAN

**System Characteristics**

- Includes RF and wired networks
- Minimum temporal delay between nodes
- Distributed control
- On-board Autonomy



# NASA Stereo Spacecraft Cyber-physical Dependencies

Partial list of cyber-physical dependencies for STEREO

| |
|---|
| Between RTS dish and Signal processing (N104 to/from N101) |
| RTS ethernet between Network Hardware and Command and Control servers |
| RTS Ethernet between Signal Processing and Command and control servers |
| Command and Control to RTS antennae (N102 to/from n104) |
| Fiber Between RTS network Hardware and Signal Processing Systems |
| GPS RF to RTS Command And Control (to N012) |
| Network Between RTS and SOC |
| Phsyical Systems interface to RTS |
| External Supply links to RTS (power, water etc) |
| Terrestrial Comms Encrypters to Telemetry interface software |
| Terrestrial Comms Encrypt to Payload Decrypters |
| Payload Decrypters to interface software |
| Telemetry interface Software to Telemetry processor |
| Telemetry interface Software to Command Processor |
| Telemetry core data processor to mission data processor |
| Mission Data processor to user terminal |
| router to remote user terminal |
| Mission Data processor to Repository |
| Power, Water links internal to SOC |
| External Supply links to SOC (power, water etc) |
| Telemetry and command core Daat Bus to repository |
| T&C Archive Logs to Repository |
| Flight and Mission Support tools local area network |
| T&C Core to Flight Support Planner and Scheduler |
| T&C core LAN |

# Characteristics of Cyber-Physical Systems Suitable for *Autonomy*

- System must be complex
- System must be mission critical
- System must be time sensitive
- System performance must be dependent upon cyber subsystem

# Modeling Cyber-physical Systems

Autonomous control of cyber-physical systems requires an ability to:

- Determine the state of the cyber-physical system which presents a “reasoning under uncertainty’ problem as the system we use to observe the cyber-system is itself the cyber system.
- Determine an appropriate course of action

To do this we would like to have a cyber-physical model that allows us to:

- Identify faults by comparing observations with expectations
- Predict results of courses of action

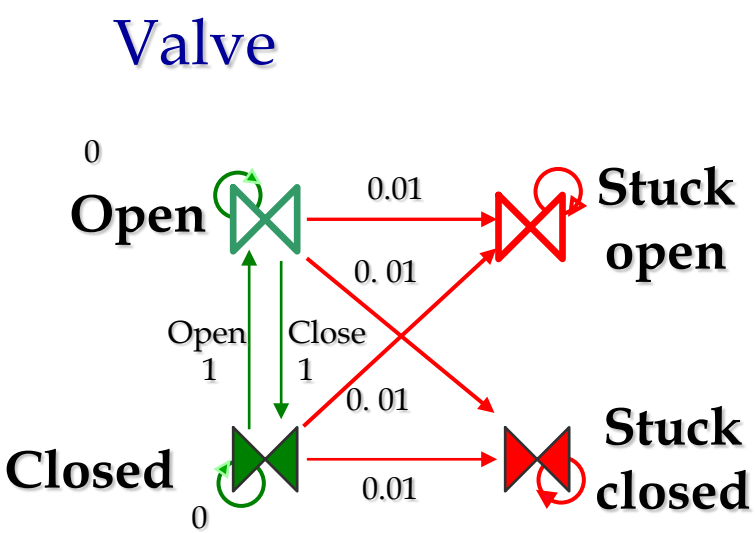
If we assume that we have quality models of the physical subsystem, we can produce a holistic cyber-physical model if we:

- Model-the cyber subsystem(s)
- Model the dependencies between the cyber and physical subsystems.

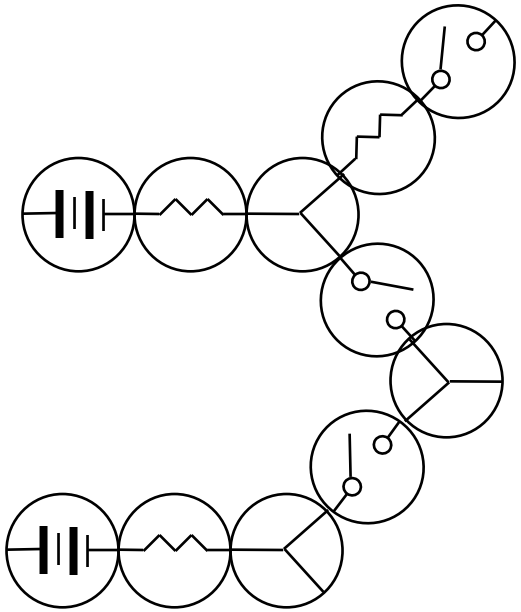


*Sensors are Additional Components That Are Subject To Failure*

# Physical Plant Modeling (an example)




Logical models lack expressiveness, but are amenable to reasoning.

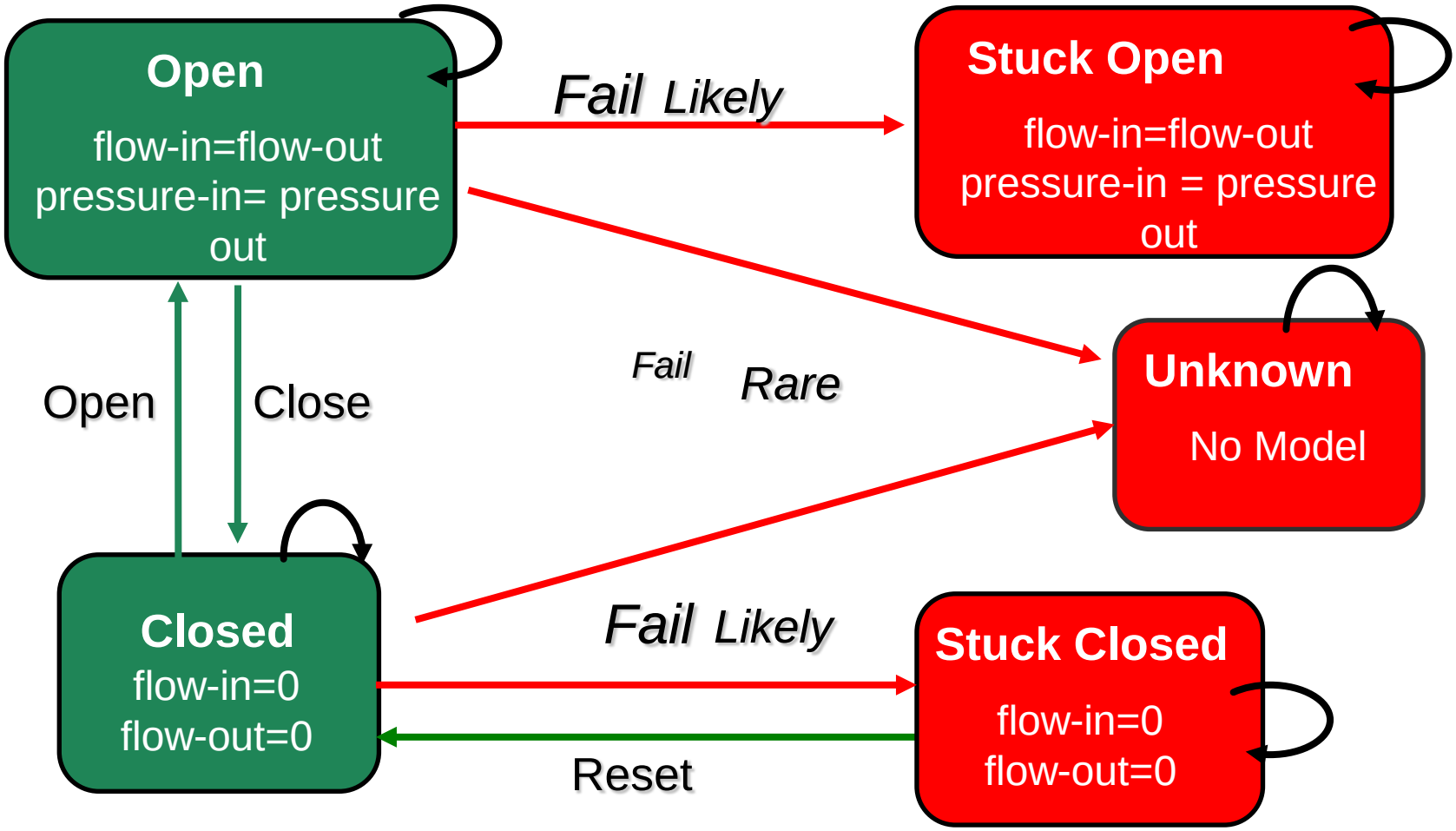


System Models are constructed by mirroring the physical system by constraining component models together



Williams, B., and Nayak, P. 1996. A model-based approach to reactive self-configuring systems. In *Proceedings of AAAI-1996*.

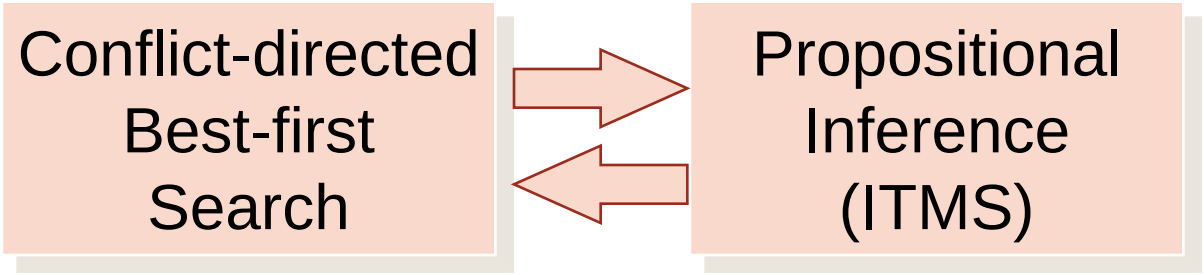
# Logical Physical Plant Modeling Valve (an example)




Williams, B., and Nayak, P. 1996. A model-based approach to reactive self-configuring systems. In *Proceedings of AAAI-1996*.

# Model-based Reasoning

- Mode identification and Mode reconfiguration formulated as combinatorial optimization problems
  - …solved using conflict-directed best-first search coupled with propositional inference




Fast propositional inference provided using an ITMS



Williams, B., and Nayak, P. 1996. A model-based approach to reactive self-configuring systems. In *Proceedings of AAAI-1996*.

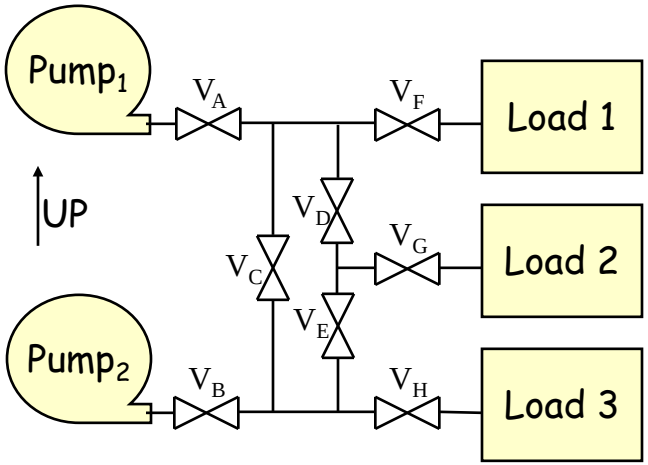
# Issues with Logical Models

1) Oversubscribed

$Pump_2$ = Off; $V_B$, $V_C$ = Closed
Observation: $Load_1$ Overheating
Incorrect Diagnosis: $V_F$ = Stuck Closed

2) Resource Loss

$Pump_2$ = Off; $V_C$, $V_E$ = Closed
Reality: $V_A$ is Leaking 7 cfs
Observation: $Load_1$ Overheating
Incorrect Diagnosis: $V_F$ = Stuck Closed

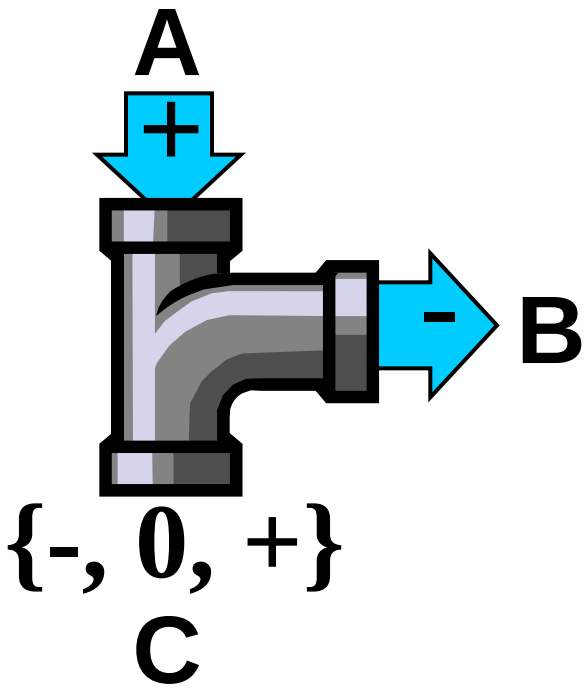


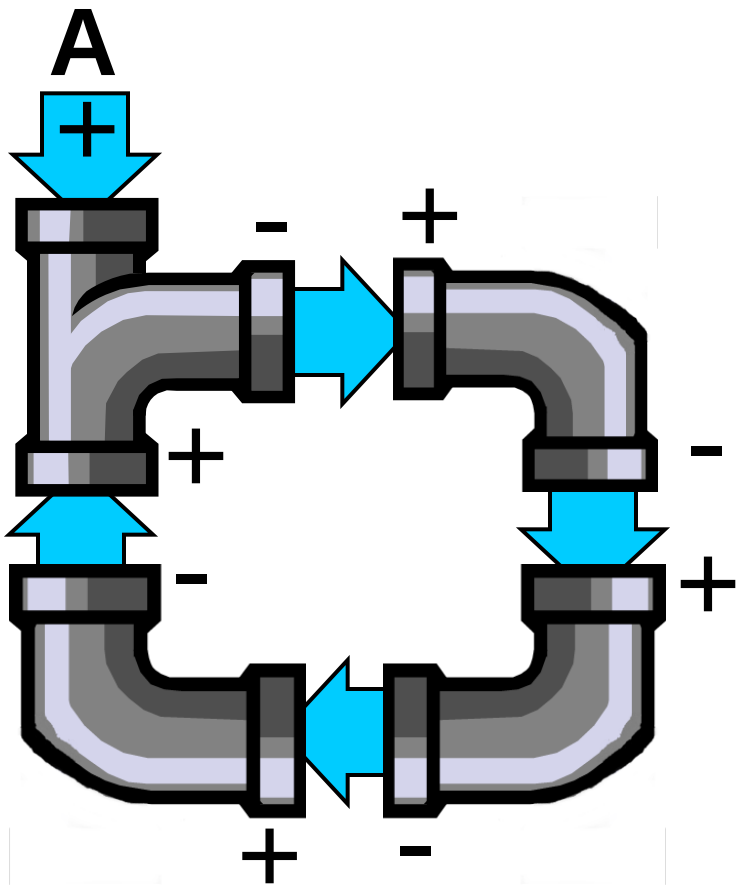

Pump nominal output = 20 cfs
Load requirement = 10 cfs
Return and Recirc not shown
Load Thermistors only sensors

# Issues with logical models

- **Qualitative version of KCL with Flow: {-, 0, +}.**

| A | B | C |
|---|---|---|
| 0 | 0 | 0 |
| 0 | + | - |
| 0 | - | + |
| + | 0 | - |
| + | - | 0 |
| + | + | - |
| + | - | + |
| + | - | - |
| - | 0 | + |
| - | + | 0 |
| - | - | + |
| - | + | - |
| - | + | + |

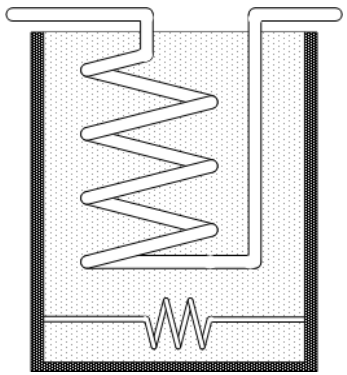


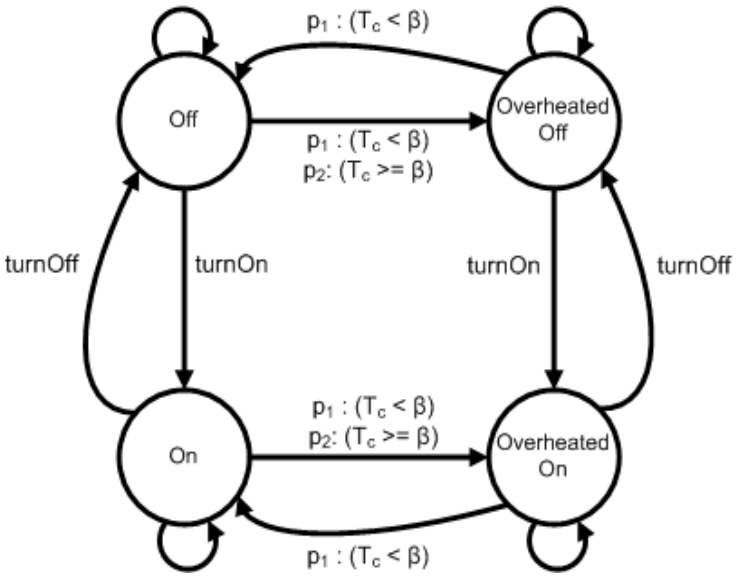
# Hybrid Models Modeling

## Continuous Dynamics

$$\dot{T}_c = \frac{I^2 R_e' L - \dot{m} c_p (T_o - T_i)}{\rho V c_v}$$

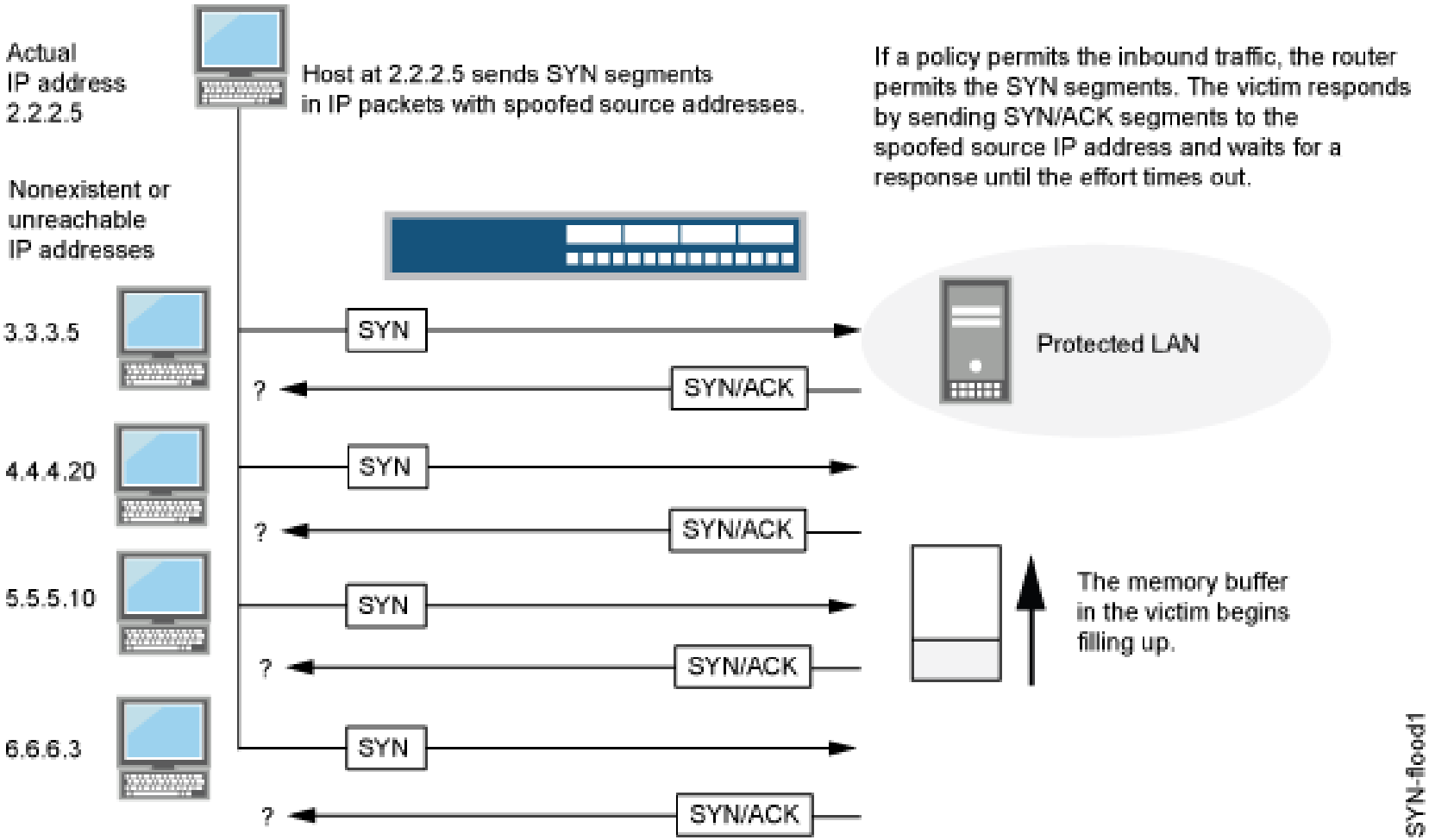


## Discrete States

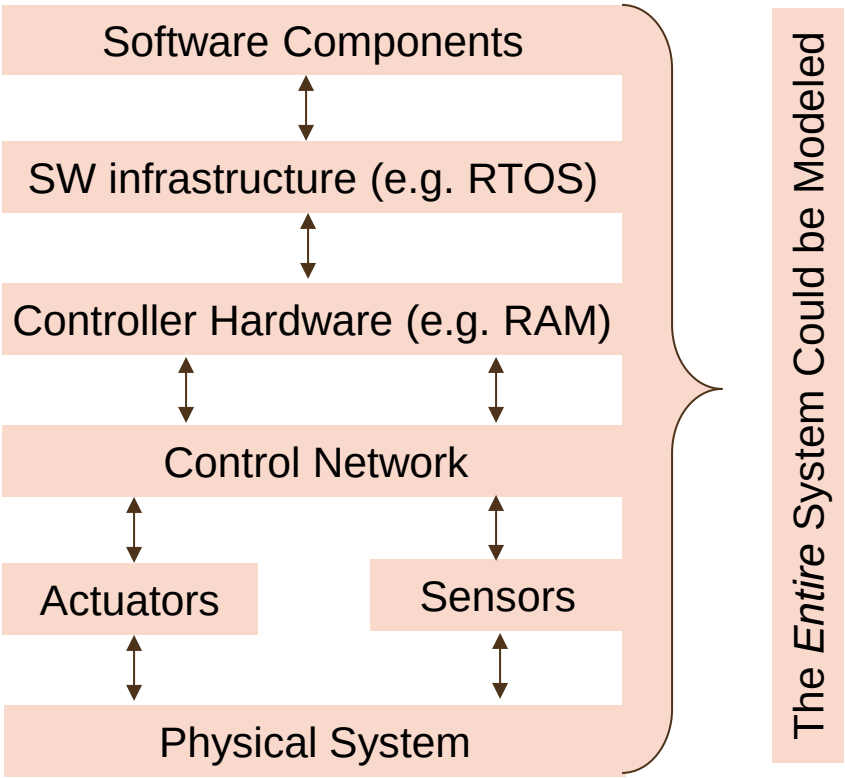



Components can be modeled by a hybrid models that include discrete states and continuous dynamics. Dynamics can be represented as logical constraints on nodes and/or edges.

# Modeling Cyber Faults – Syn Flood Attack



# Modeling Cyber-physical Systems



# Modeling the Cyber System

Model the cyber system as another constrained resource distribution system, where the resource is *information*

- Information
  - Used to identify the current state of some part of the system
  - Used to issue a command
  - Timeliness
  - Correctness

- Information variables

  d: data, measured in bits

  i : Information, measured in bits

  t: time, measured in seconds

$$i(d,t) = -\log(P(d,t))$$

Cyber-faults (man-made or natural)

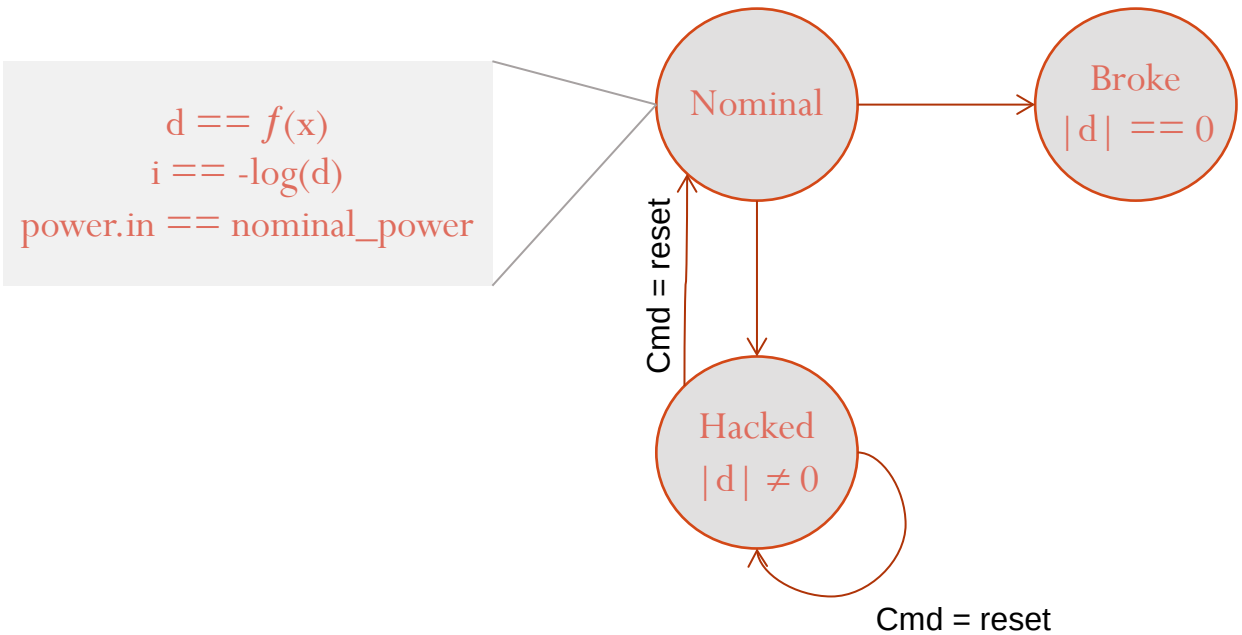
- Integrity
- Confidentiality
- Accessibility
  - Delayed delivery
  - Delivery blocked

data and time are used to model accessibility

data, time and information are required

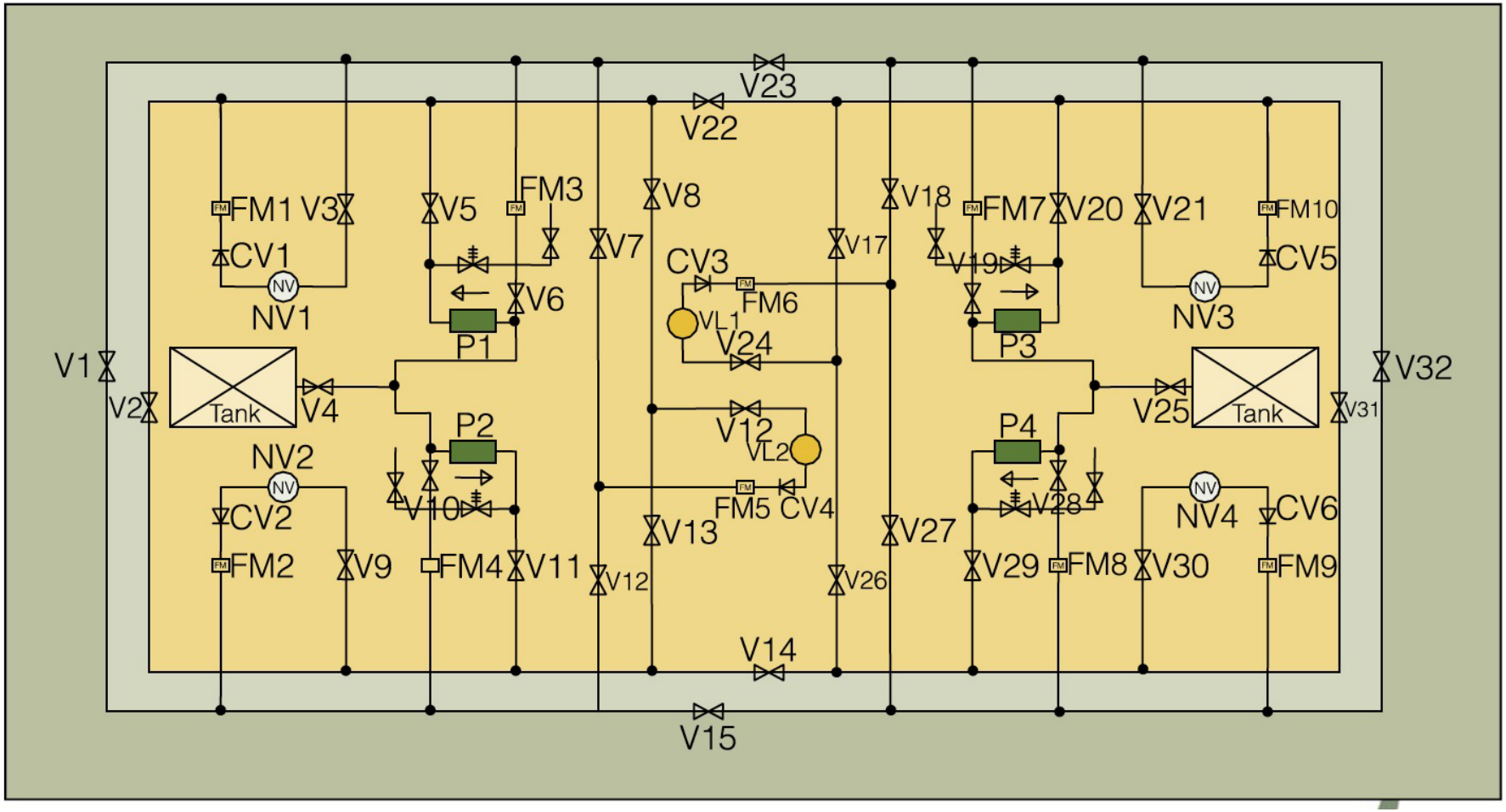
# Simple Cyber Component Model

Sensor Model

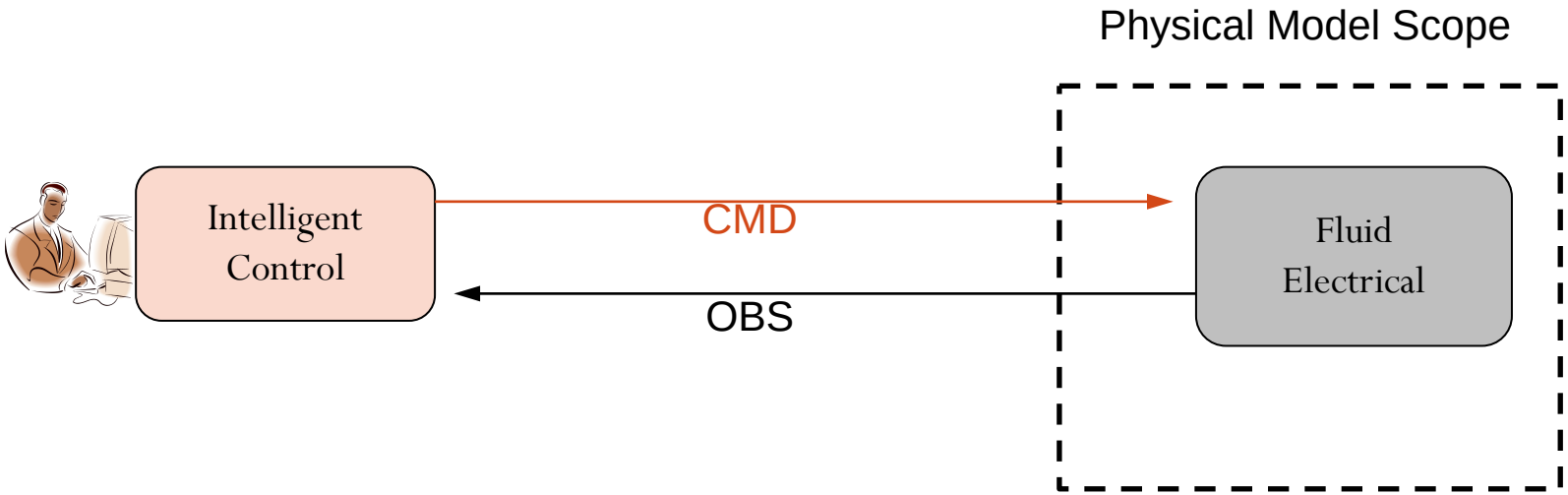



$f$(x) -> d is the transfer function
that turns a signal into data

# Cyber-Physical Test Case
# Ship Electrical-Fluid-Control System



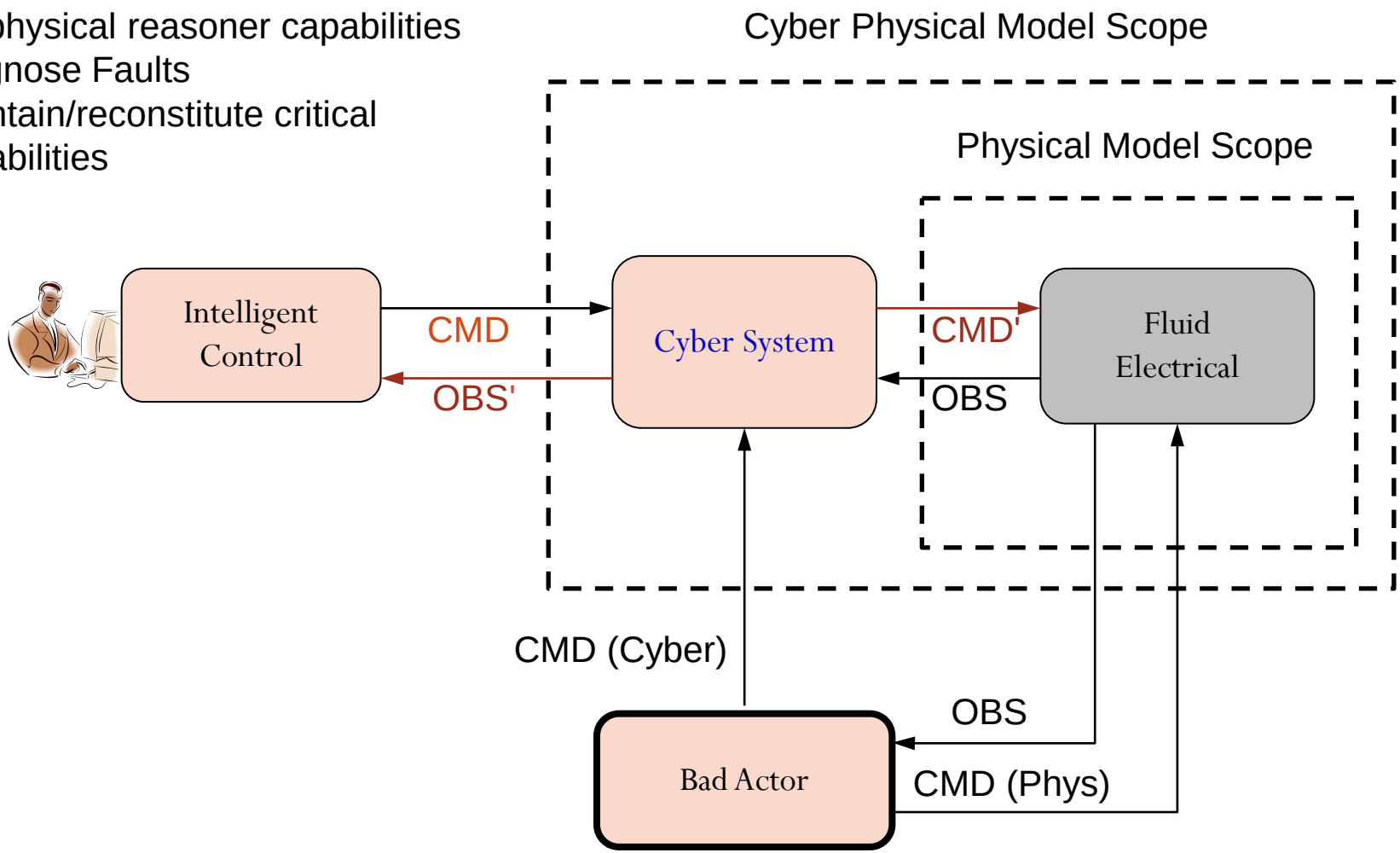
# Prior Work – Intelligent Control of Tabletop System



# Autonomous Cyber-Physical System Controller

Cyber-physical reasoner capabilities

- Diagnose Faults
- Maintain/reconstitute critical capabilities

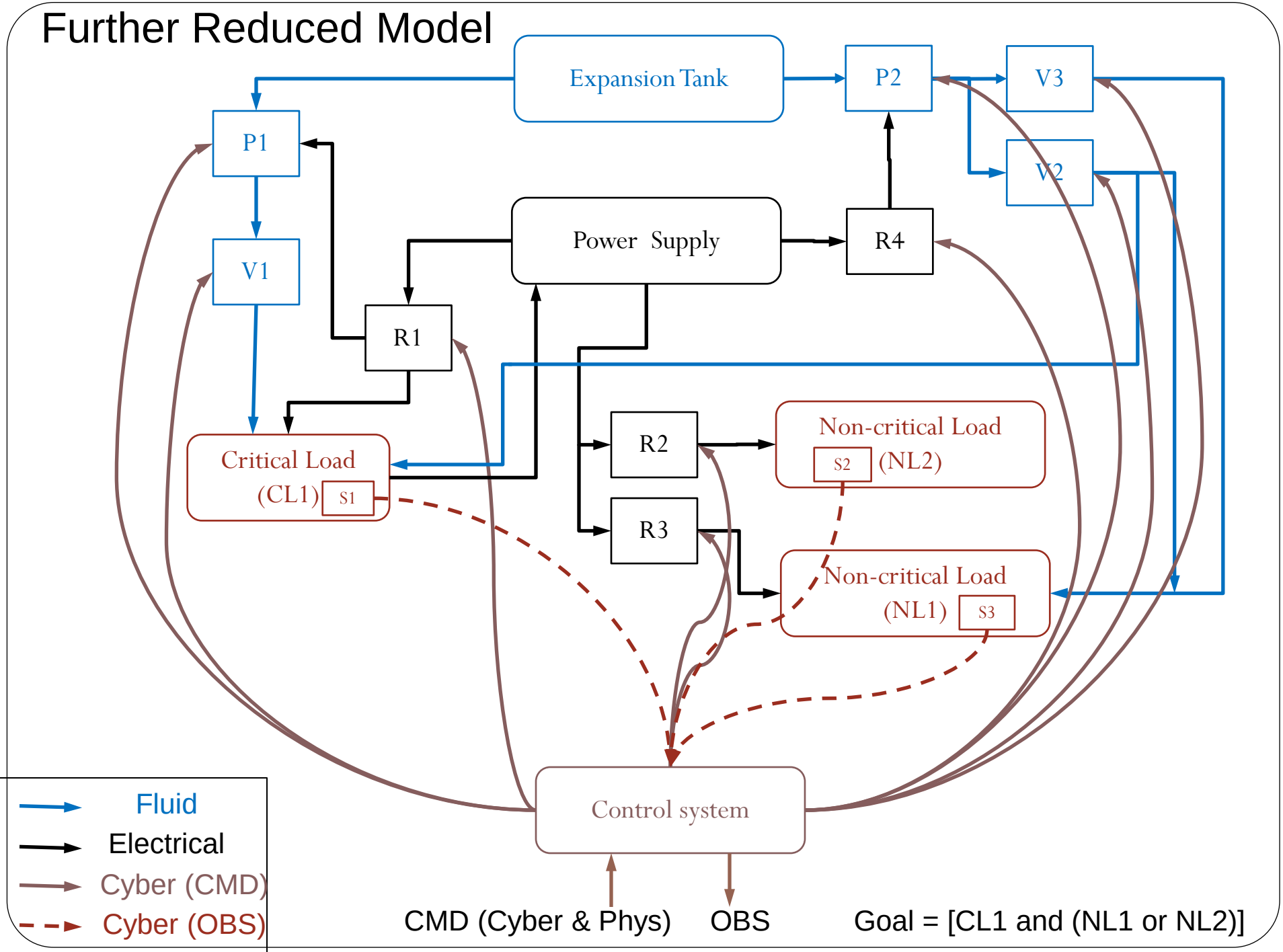


# Cyber Physical Model Overview

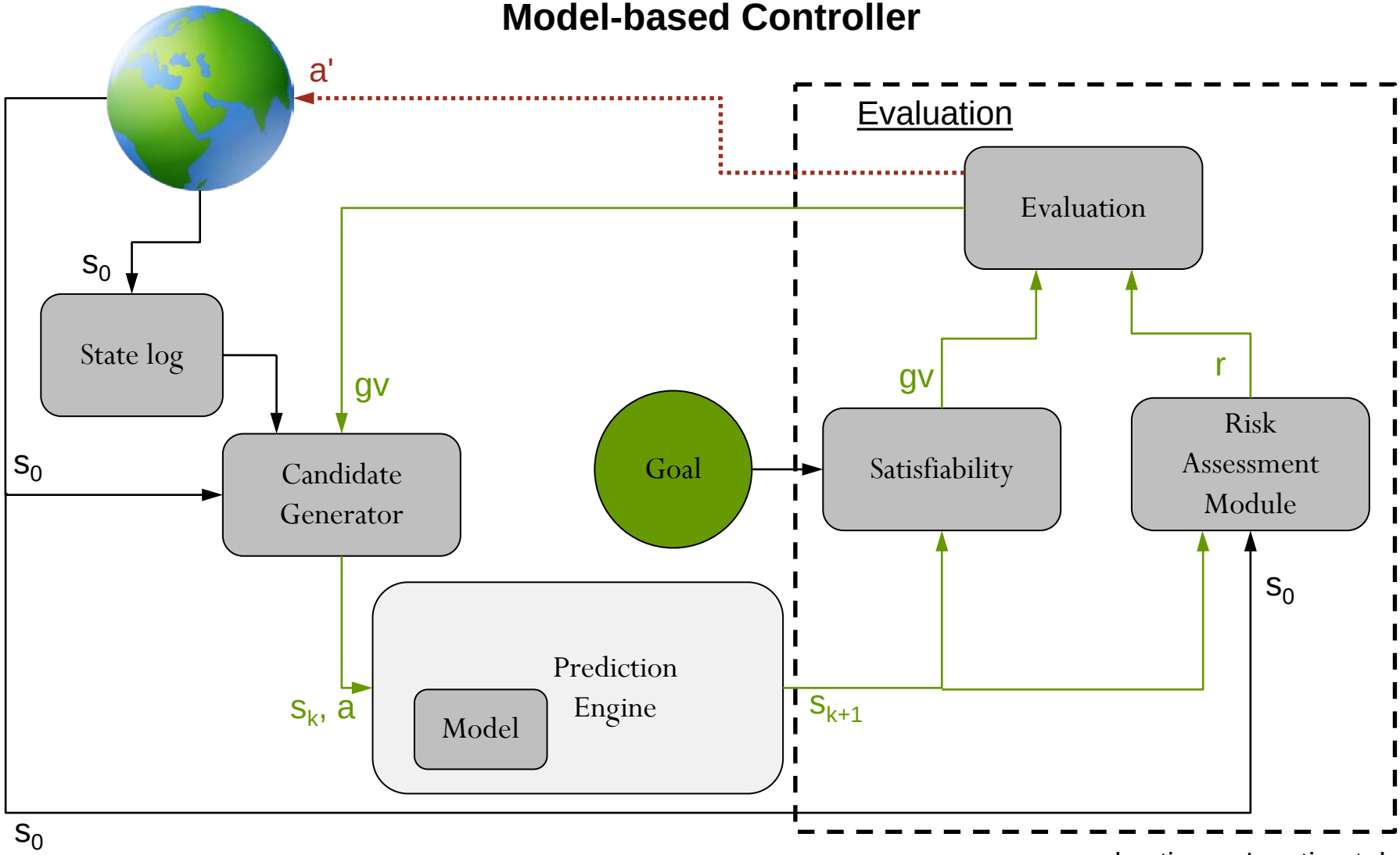
| Resources | Loads w/sensors | Physical Control Components | Cyber Control Components |
|---|---|---|---|
| fluid | load_ef | fluid_pump | sensor_interface |
| electricity | load_e | fluid_valve | command_interface |
| data | | electrical_relay | |

- Control components and loads are modeled as interconnected finite state machines (FSM)
  - FSMs and loads are interconnected per physical topology
  - States of FSMs affect propagation of resources through topology
  - A state transition may depend on resource availability
- Cyber control components inserted into the topology to represent flow of commands and observations
  - command_interface is placed between each physical control component and the Intelligent Control/operator
  - sensor_interface is placed between each load and the Intelligent Control/operator
- Goals are represented by desired load states

# Further Reduced Model



# Model-based Controller




a=proposed action, a'=action taken, $s_k$=system state, gv=goal violations, r=risk

- **<u>Scalable</u>: Can compute solutions for larger state space than can be enumerated a priori**
- **<u>Adaptable</u>: Changes in configuration of cyber-physical system do not require change in software**

# Modeling Cyber-physical Systems

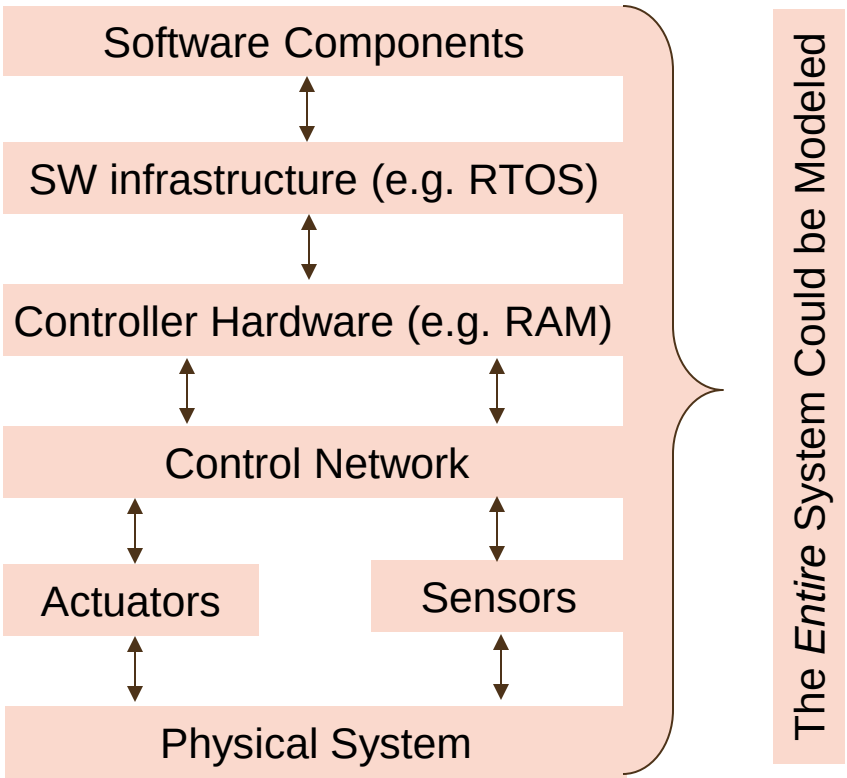
**OK. That was really unsatisfying.**

**Cyber modeled as a single block. Really?**

We have the same problems with Cyber that we had with physical models:

- Logical models cannot fully express cyber phenomena*
- Performance degrades exponentially with the size of the system.

Unlike physical systems, the ability to sense and observe the system is dependent with the cyber system.




*actually, they could, but not in a way that is tractable.

# Cyber Modeling – *What* to model?

## Software

- Instruction
- Process/Thread
- Executable
- Component/Module/Class
- Data/Variable

## Hardware

- Chip
- Memory
- Bus
- Port
- Power Supply
- etc.

## Network

- Packet
- Waveform
- Connection
- Route
- OSI levels 1..7

## Physical Devices

- Computer
- PLC
- Switch
- etc.

How deep down the rabbit hole do we go?
Model each transistor?

No? Then what if that transistor fails?

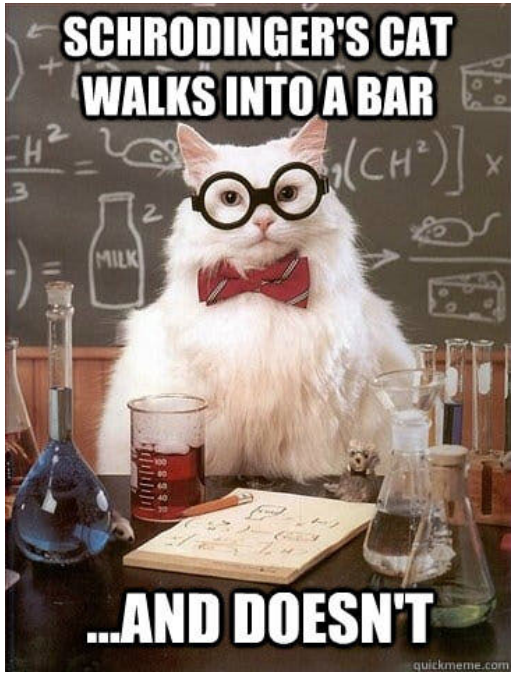
Gödel's Incompleteness theorem informs us that we cannot model a cyber system completely, unless we use a larger cyber system than the one being modeled; and the system being modeled is so very large and complex…

# Cyber modeling paradox

The cyber-system is too complex to comprehensively model in real time (Gödel), yet very small unanticipated perturbations can cause  very large unanticipated effects.

So, how can we intelligently model the cyber-portion of the cyber-physical system.

An answer comes from an understanding of the impact of *time* on the cyber-physical system.



# Temporal Variability in Ship Auxiliary Systems

**Response time:**

- **Electrical << 1 sec**
- **Fluid is seconds**
- **Thermal is minutes**

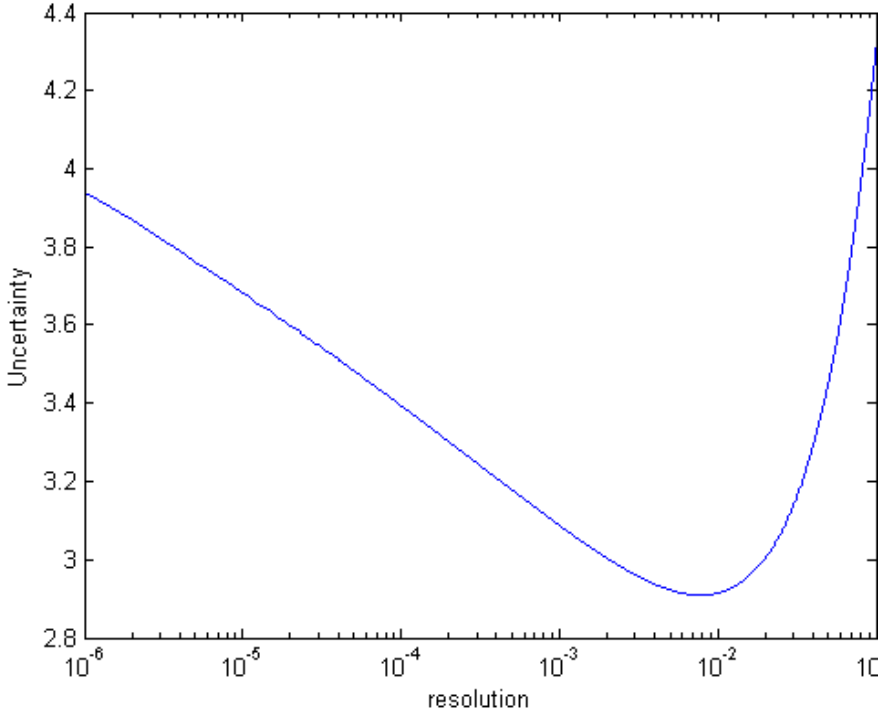
**When attempting to diagnose system state after a command is issued, when should we perform diagnosis?**

# Optimal control period is defined by the Information Equilibrium

- How many bits is required to represent an system state?
- What is the minimum time required to:
  - Develop Situational Awareness?
  - Devise a Course of Action?
- At What Rate Does Situation Change?

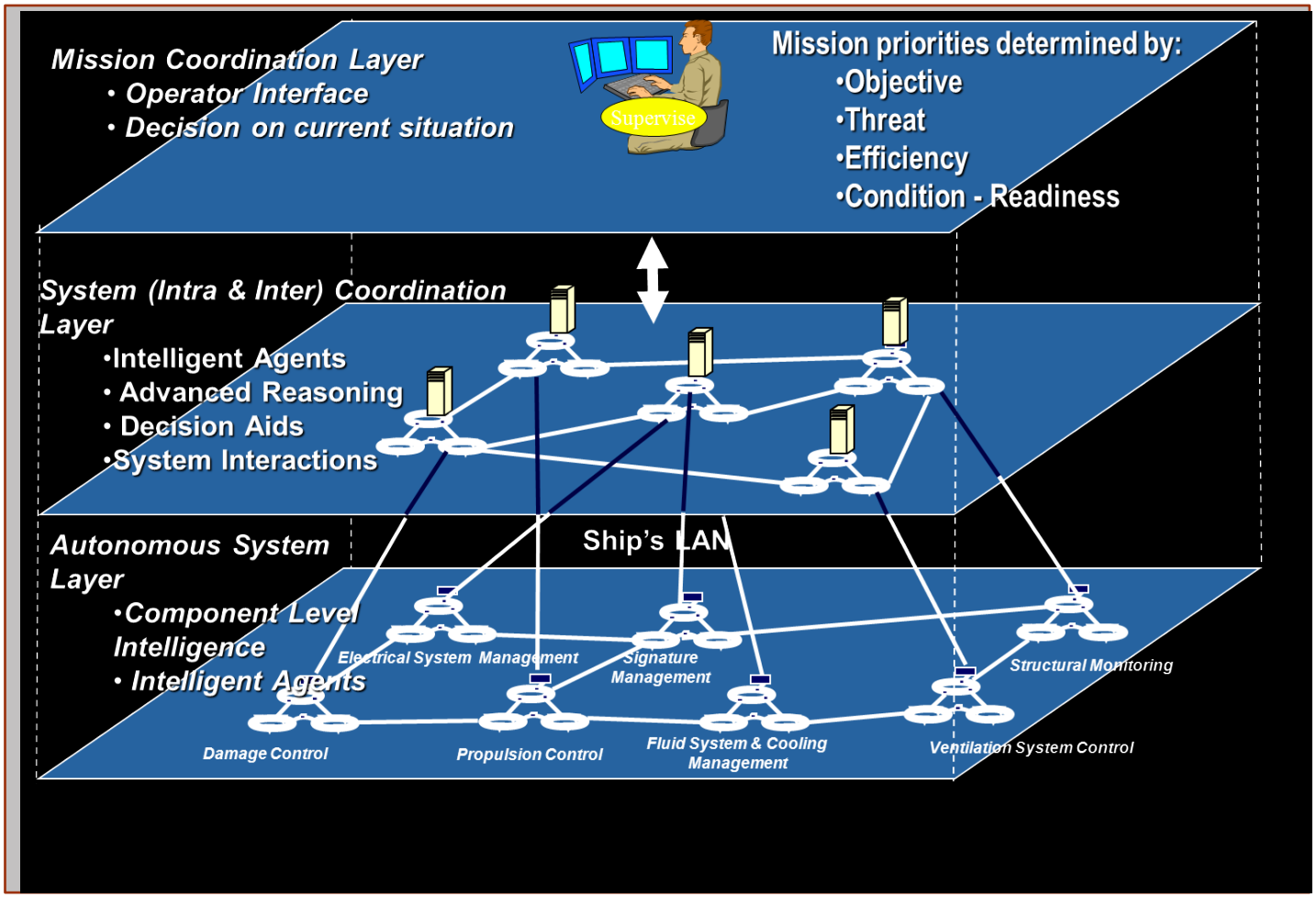
In dynamic systems an optimal level of fidelity exists for both diagnosis and control. As fidelity is increased an equilibrium point is reached beyond which any attempts to measure or control a system more precisely results in a decrease in knowledge or control efficacy.

Optimal Resolution of an Dynamic System




D. Scheidt, M. Pekala, The Impact of Entropic Drag on Command and Control, *Proc. of 12th International Command and Control Research and Technology Symposium (ICCRTS)*, Newport, RI, June 19-21, 2007.

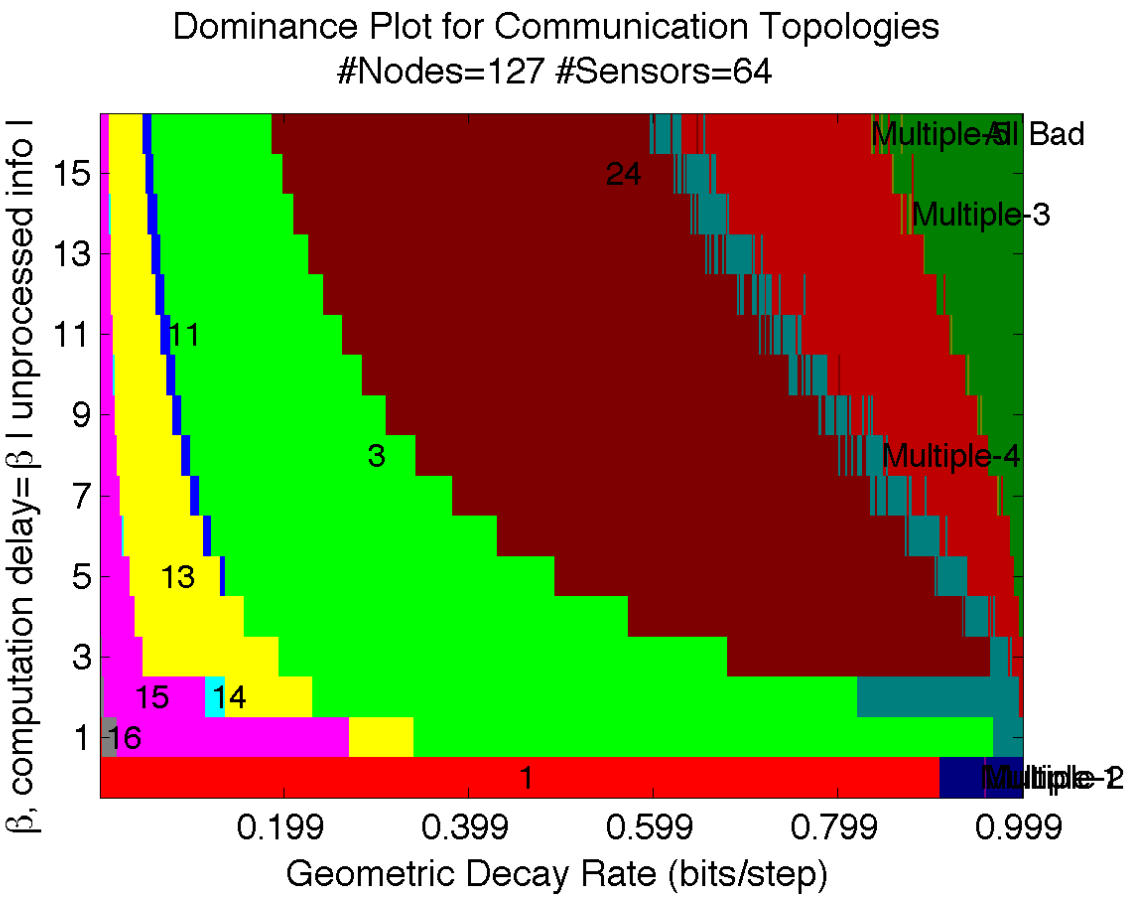
# Complexity management through hierarchical decomposition.



# Complexity Management through Hierarchical Decomposition

Layers reduce complexity at the cost of additional latency

Optimal control topologies can be identified by situational complexity and entropic drag.



# Cyber Modeling – *How* to model?

## Software

- Instruction
- Process/Thread
- Executable
- Component/Module/Class
- Data/Variable

## Hardware

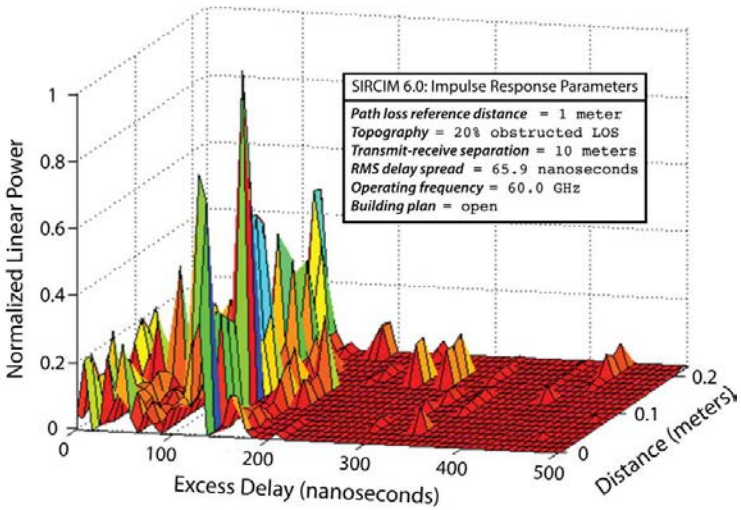
- Chip
- Memory
- Bus
- Port
- Power Supply etc.

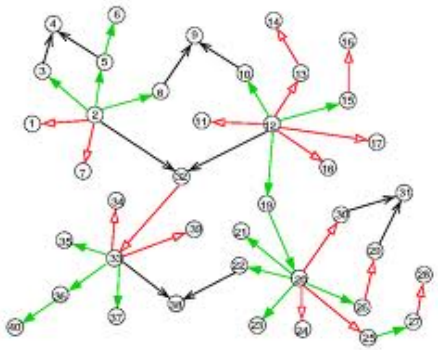
**Network**

- Packet
- Waveform
- Connection
- Route
- OSI levels 1..7

**Physical Devices**

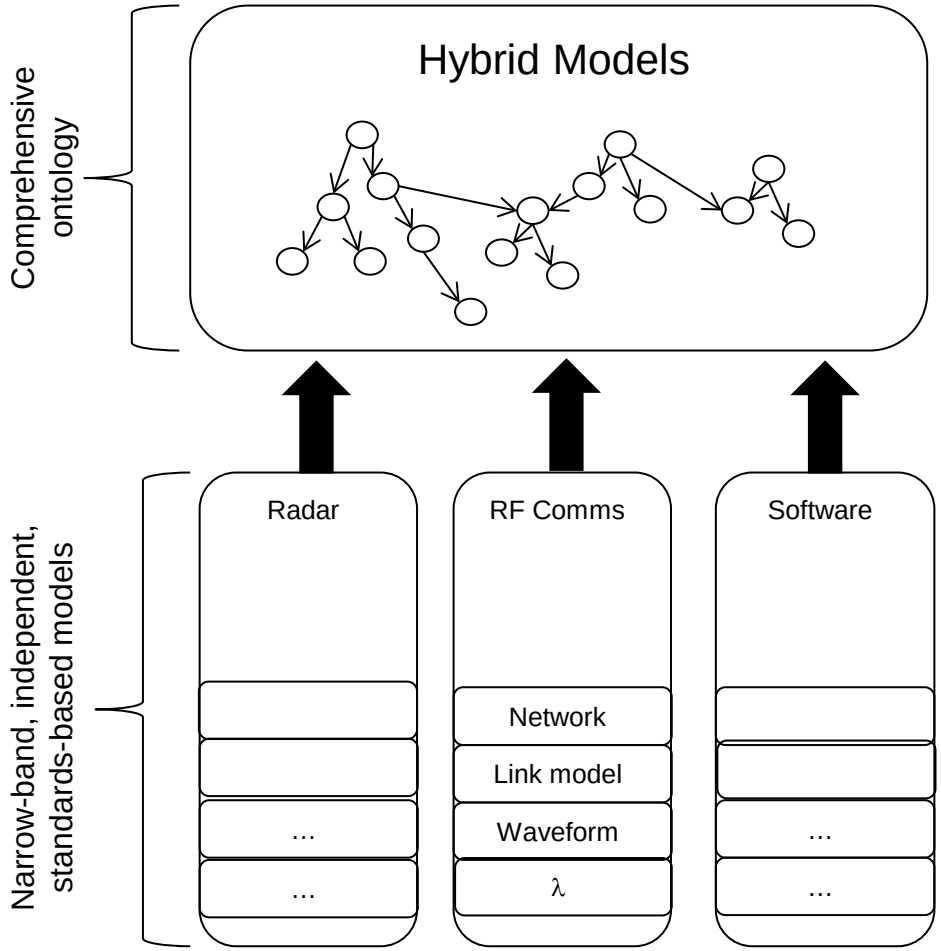
- Computer
- PLC
- Switch
- etc.



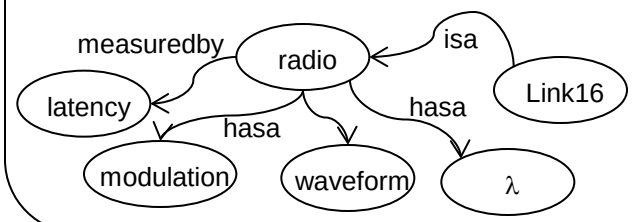
**Each of these model elements can be modeled in great detail; yet no single modeling technique can be used to represent all elements of the cyber system.**

# Hybrid Cyber-Physical Models

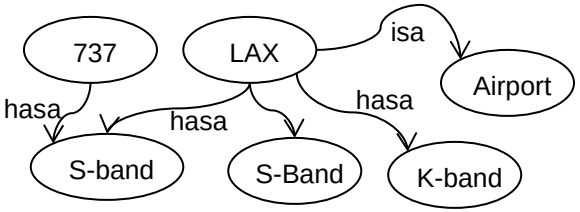


# Managing EM Interdependencies with Hybrid Ontological Networks

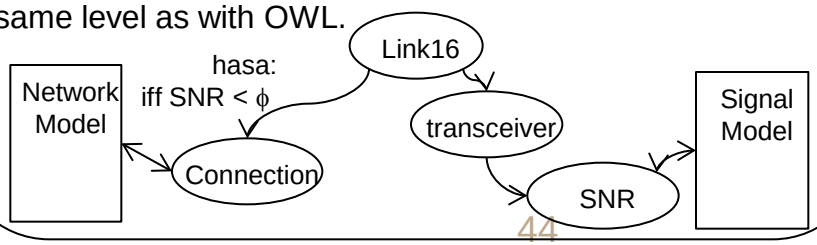
**Issue:** Expressing EM emitter and receiver behavior requires descriptions of disparate, inter-dependent domains.
**Solution:** Use an ontology to express multi-domain associations on a first principals basis.




**Issue:** Objects such as planes, radars and threat emitters incorporate sense and act across multiple domains
**Solution:** Use ontology to express characteristics of tactical elements.




**Issue:** Cross-domain dependencies require expressiveness not found in dominant languages such as the Web Ontology Language (OWL).
**Solution:** Hybrid models that constrain relationships with highly expressive mathematical equations and pointers to domain specific models will be used to greatly expand framework expressiveness while retaining tractability at the same level as with OWL.




**Issue:** The framework must be capable of managing numerous types of uncertainty including:

- Structural uncertainty within the model
- Compositional uncertainty within an engagement
- Partially observable engagements
- Measurement uncertainty

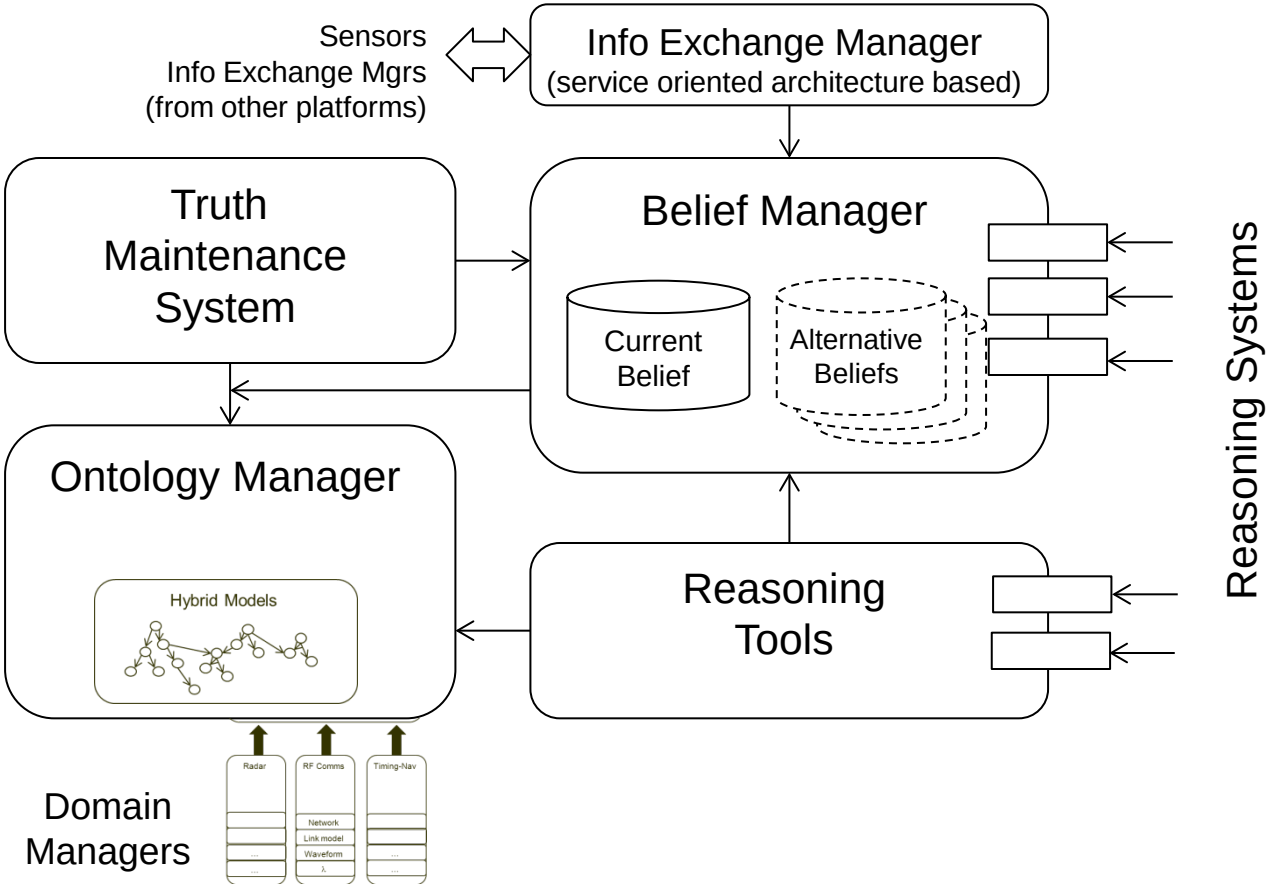
**Solutions:**

1) Incorporate semantics that explicitly models uncertainty
1) Provide tools that support reasoning with alterative beliefs

(useful for multi-hypothesis reasoning and non-monotonic reasoning).

UC Berkeley's BLOG, used by APL on DARPA's Compressed Sensing program, provides statistical basis for managing ontological uncertainty

# Distributed cyber-physical control with RF communications




The Cognitive framework is a software/networking infrastructure that provides for the storage and sharing of C2 permanent and ephemeral knowledge as well as providing basic algorithms necessary for reasoning with C2 systems.

# and in conclusion…

- Resilient control of Cyber-Physical systems requires an ability to identify and mitigate the physical effects of cyber faults “left of catastrophe”
- Cyber-physical systems are complex, which requires an ability to
- Time

# and in conclusion…

Cyber-physical systems are complex, both in terms of scale (NP-hard), but chaotic as well. Small changes can have profound effects on the system, or no effect at all.

Cyber-physical systems are resistant to abstract models, as we learn from a repeated history of catastrophic faults produced by small changes.

Cyber-physical failures may be time-based temporal (e.g. syn-flood), which will require a sophisticated temporal models.