FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

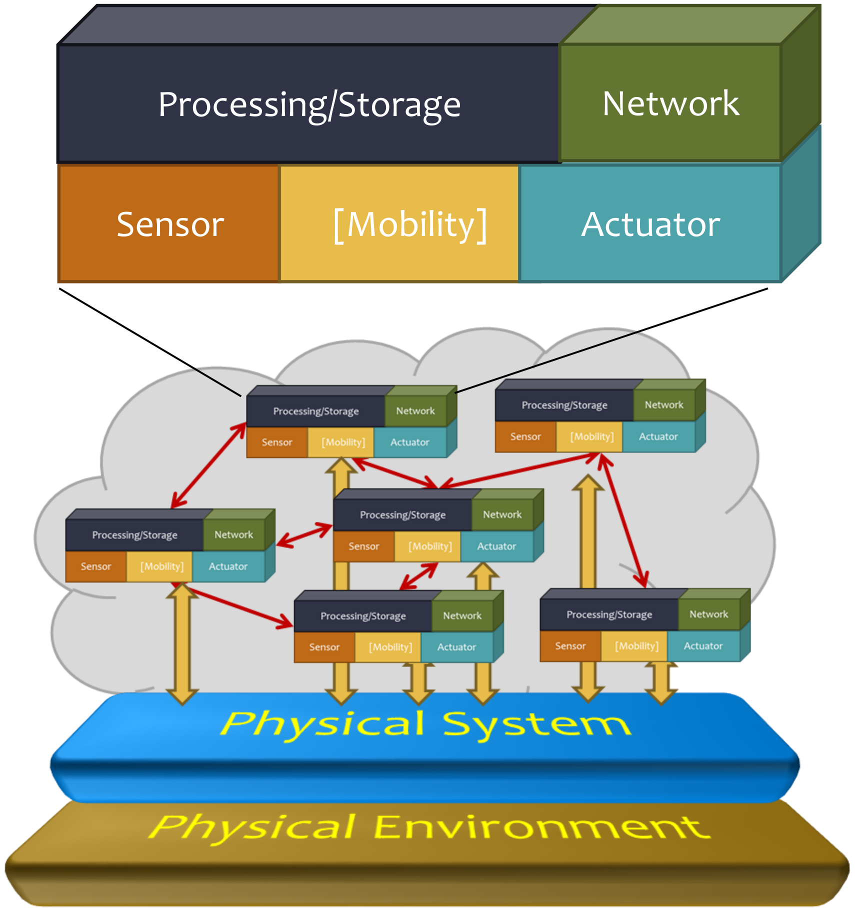
Experimental Evaluation Platform for Resilience in CPS

Will Emfinger, *Gabor Karsai*,
Himanshu Neema, Pranav Kumar
Vanderbilt University

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

Goal: Evaluating CPS Resilience

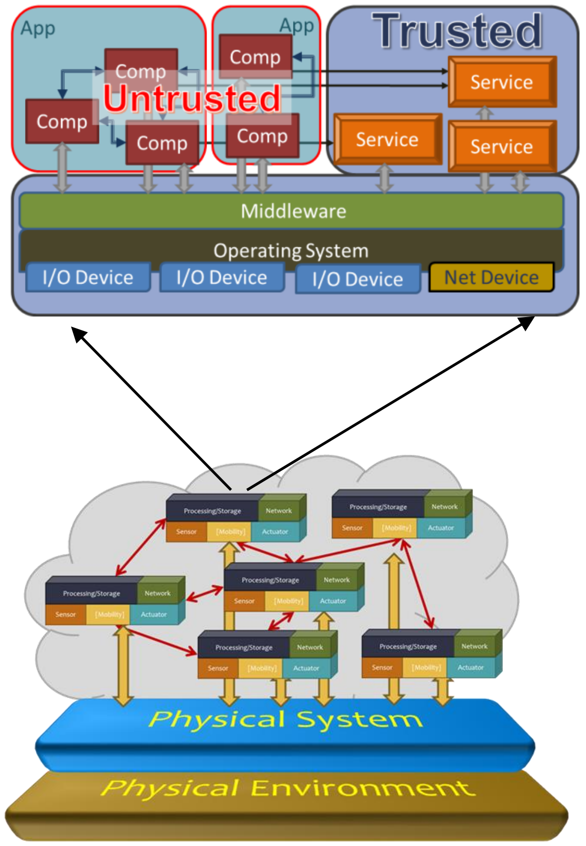
- Resilience is a system-level property, permeating the entire CPS architecture
  - → Must be evaluated in the *system* context
- CPS Software is *not* constant, it is continuously updated and extended
  - → Must rely on a *software platform* that provides core abstractions and services for the applications
- *Interactions* across and within the physical and cyber domains is a key feature of CPS
  - → Must be recognized and managed throughout the system's lifecycle



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Goal: Evaluating CPS Resilience

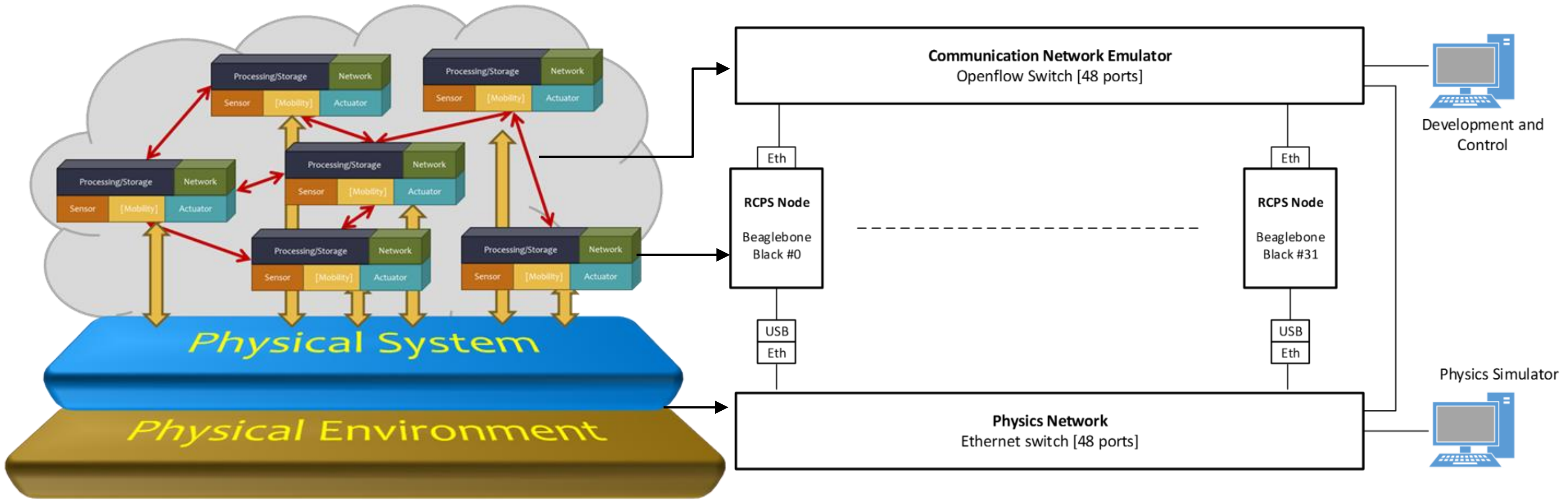
- CPS Software Model:
  - Trusted (dependable, protected) *platform* + Untrusted *apps (components)*
- Challenges:
  - How to model the resilient architecture? What makes it resilient?
  - How to build a resilient software application platform for CPS?
  - How to analyze in a scalable manner to obtain assurances for resilience?



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

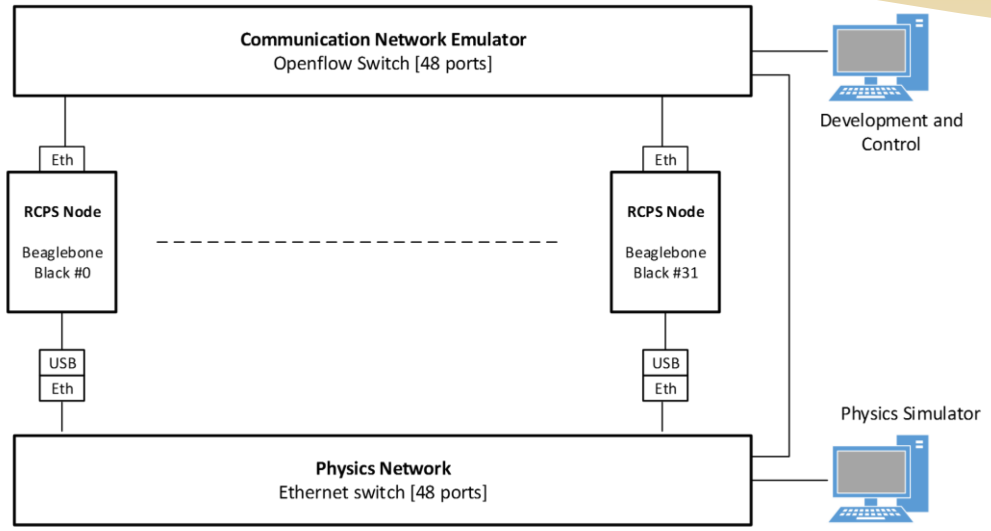
Design: Testbed

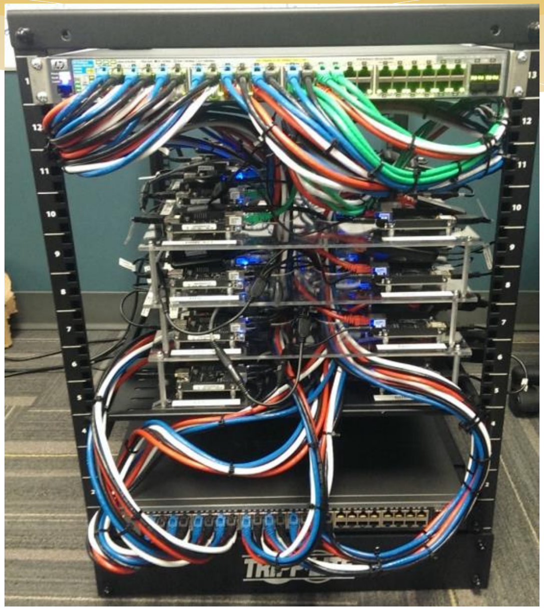
- RCPS Node: embedded computer, running the core platform software, executes applications, communicates with other RCPS nodes, interacts with the (simulated) physical environment
- Communication Network Emulator: facilitates network flows between the nodes, flows can be controlled and restricted (bandwidth limitations, communication dropouts, etc.)
- Physics network: provides connectivity between the RCPS nodes and the physics simulator



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Design: Testbed



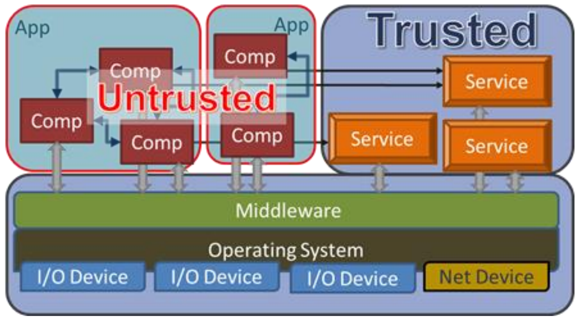


* Physics Simulator: simulates the physical platform, the attached sensors and actuators, and the external environment. RCPS nodes receive data from the simulated sensors and send commands to the simulated actuators. May also send relevant data to network emulator to change network performance on the fly.
* Development and Control: a desktop machine for all development and experiment control activities: building applications, uploading applications to the RCPS network nodes, running and controlling experiments.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Design: Software Infrastructure

- A Resilient CPS (Software) Platform
  - Component-based application model: *component model* with interaction semantics
  - Application *deployment model*: trusted and managed deployment
  - Resource *monitoring* and constrained *information flows* on the platform level
  - Hardened *platform interfaces* and *services* (for resilience)



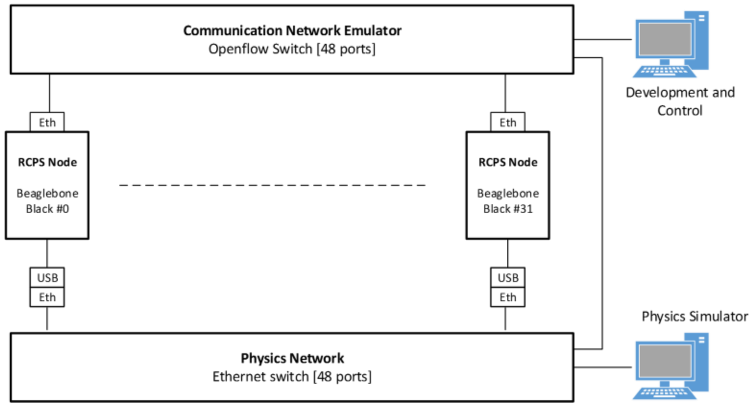
ROSMOD: An Extension to the Robot Operating System (ROS) – work in progress
https://github.com/rosmod

P. Kumar,W. Emfinger, A. Kulkarni, G. Karsai, D.Watkins, B. Gasser, C. Ridgewell, and A. Anilkumar. ROSMOD: A Toolsuite for Modeling, Generating, Deploying, and Managing Distributed Real-time Component-based Software using ROS. In Proceedings of the IEEE Rapid System Prototyping, RSP 2015, Amsterdam, Netherlands, 2015. IEEE

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Experimentation

Resilience to…	Realize it in ….
Physical plant faults	Physics simulator
Sensor/actuator faults	Physics simulator
Unforeseen environment	Physics simulator
Cyber effects on controller	RCPS node
Cyber effects on network	Network emulator
Cyber effects on sensors/actuators	Physics simulator



Assumptions:

- Physics simulator is timing accurate w.r.t dynamics, can realistically simulate faults, has sufficient I/O bandwidth
- Network emulator can realistically emulate network conditions (limited bandwidth, latency, jitter, packet drops) and cyber effects on the network (DDOS, protocol attacks, etc.)
- RCPS node running embedded control software is realistic; including I/O behavior

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Experiments

Domain: Fractionated Spacecraft

- 32 RCPS nodes running component-based flight software application for fractionated ('cluster') satellites
  - **Cluster Flight Control:** handles cluster trajectory and management
  - **Satellite Flight Control:** Retrieves satellite state from sensors, actuates satellite thrusters and communicates internal state to all other satellites
  - **Wide-area Monitoring:** Imaging applications with distributed camera sensors to produce processed images
- RCPS nodes maintain coordinated cluster flight to perform wide-area sensing

Emergency response:

- Cluster scatters on reception of an emergency scatter command
- Applications run on testbed using **ROSMOD** integrated with **Orbiter**
  - Send scatter command at random intervals to cluster leader
  - Reliably disseminate command to rest of cluster and obtain consensus
  - Satellites scatter – seen in Orbiter

Threat model:

- Malicious applications
- Rogue satellites
- DDOS attack on the network
- Physical faults (damaged satellite)

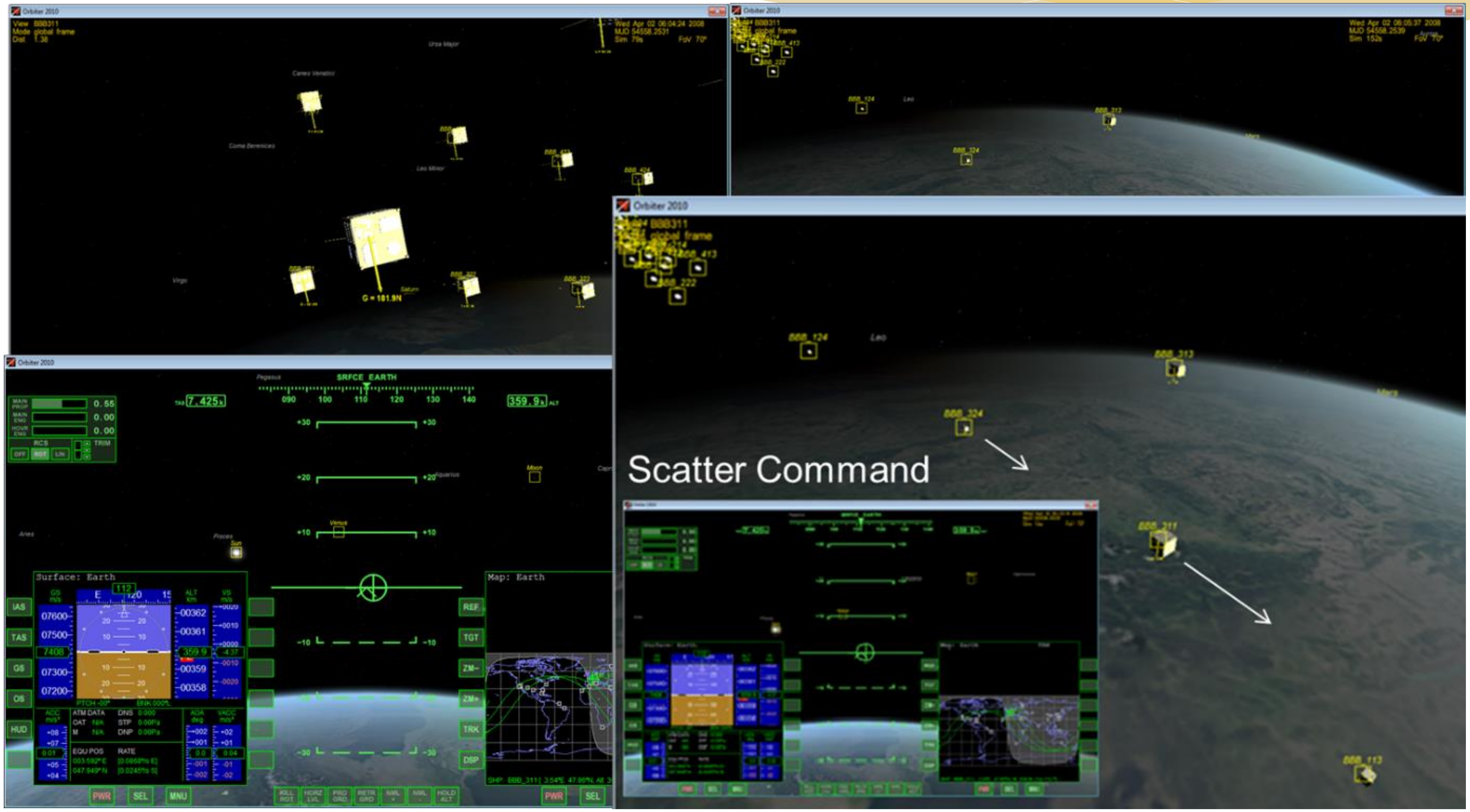
Research challenges:

- Resilient coordination among CPS nodes for control actions
- Detection and mitigation of targeted DDOS attacks
- Protection against malicious applications

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Supported, in part, by DARPA/AFRL

Orbiter Space Flight Simulator

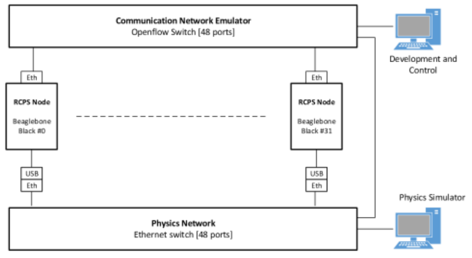


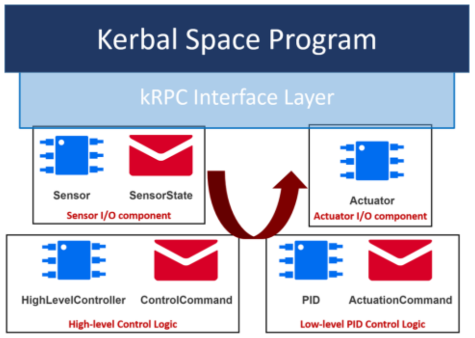
Page 10

Domain: Vehicle Control Systems

Kerbal Space Program (KSP)

- Popular space flight and vehicle dynamics simulator
- Aerodynamic, gravitational & rigid body Simulations
- Every man-made object follows Newtonian Dynamics
- Rocket thrust and aerodynamic forces are accurately applied to the vehicles based on directions and precise positions in which the force-affected elements are mounted
- Autonomy & Control Testing:
  - Flight Control – Takeoff, cruise control, and land
    - https://www.youtube.com/watch?v=G15u-AtQVWY
  - Self-driving car – Follow waypoint-based state machine
    - https://www.youtube.com/watch?v=Ygp8VF7R49c





Threat model:

- Cyber effects on the vehicle control bus
- DDOS on connected vehicle networks
- Malicious embedded applications

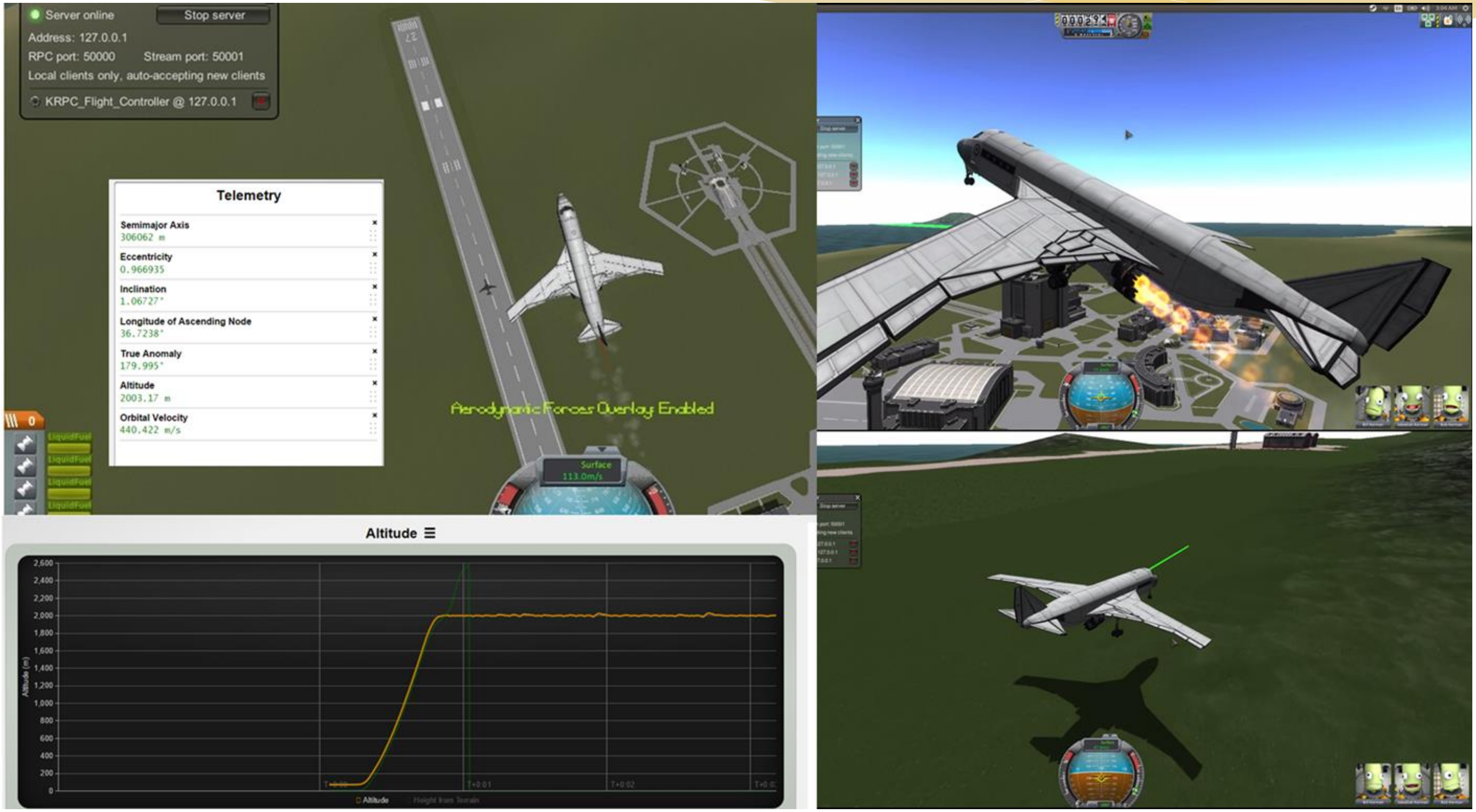
Research challenges

- Preventing integrity attacks on the control bus
- Mitigating DDOS effects
- Detection and isolation of malicious applications

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Supported, in part, by AFRL

Stearwing A300 Flight Control in KSP



Server online

Stop server

Address: 127.0.0.1

RPC port: 50000 Stream port: 50001

Local clients only, auto-accepting new clients

KRPC_Flight_Controller @ 127.0.0.1

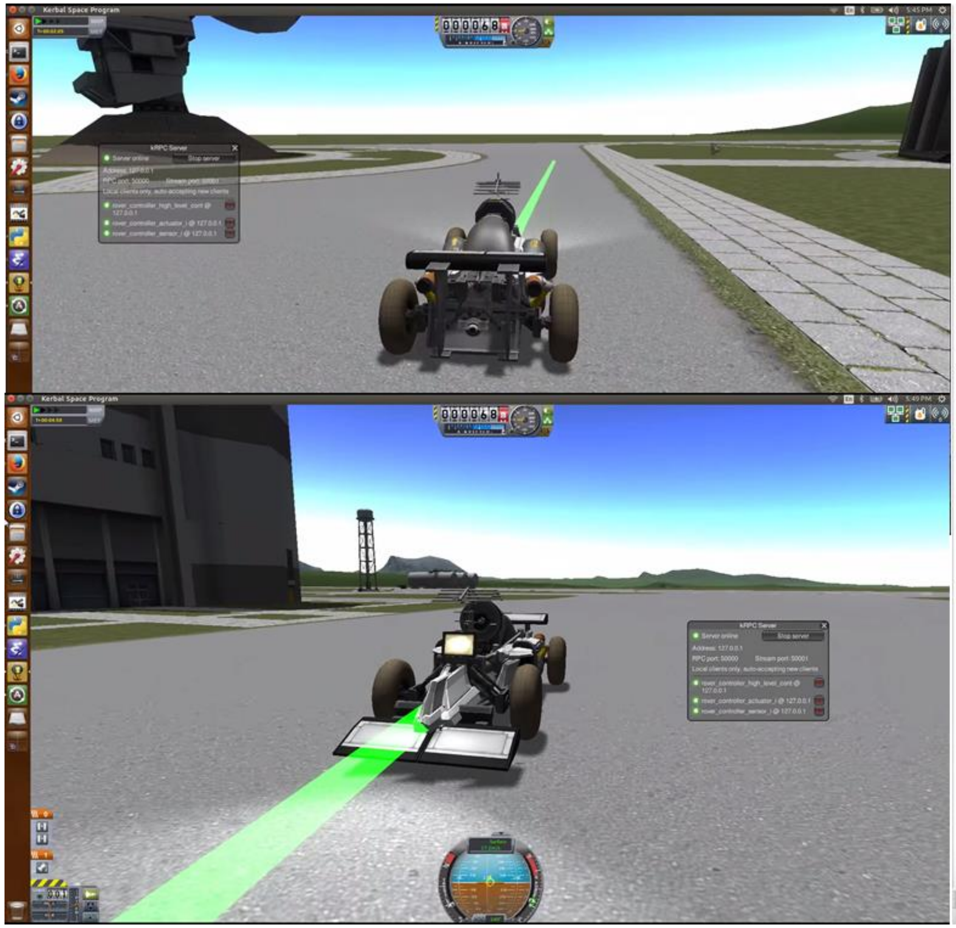
Telemetry

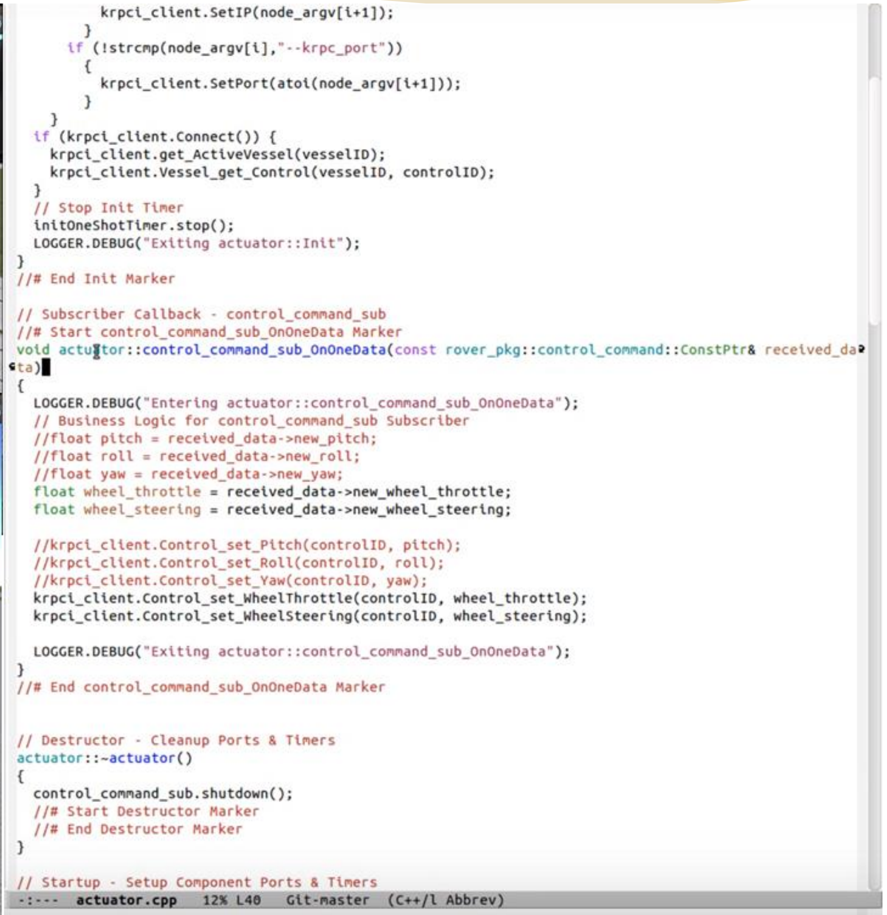
Semimajor Axis	306062 m
Eccentricity	0.966935
Inclination	1.06727°
Longitude of Ascending Node	36.7238°
True Anomaly	179.995°
Altitude	2003.17 m
Orbital Velocity	440.422 m/s

FORCES

FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Self-Driving Car Control in KSP
Pre-planned Waypoints





```
                krpci_client.SetIP(node_argv[i+1]);
              }
            if (!strcmp(node_argv[i],"--krpc_port"))
              {
                krpci_client.SetPort(atoi(node_argv[i+1]));
              }
          }
  if (krpci_client.Connect()) {
    krpci_client.get_ActiveVessel(vesselID);
    krpci_client.Vessel_get_Control(vesselID, controlID);
  }
  // Stop Init Timer
  initOneShotTimer.stop();
  LOGGER.DEBUG("Exiting actuator::Init");
}
//# End Init Marker

// Subscriber Callback - control_command_sub
//# Start control_command_sub_OnOneData Marker
void actuator::control_command_sub_OnOneData(const rover_pkg::control_command::ConstPtr& received_da
ta)
{
  LOGGER.DEBUG("Entering actuator::control_command_sub_OnOneData");
  // Business Logic for control_command_sub Subscriber
  //float pitch = received_data->new_pitch;
  //float roll = received_data->new_roll;
  //float yaw = received_data->new_yaw;
  float wheel_throttle = received_data->new_wheel_throttle;
  float wheel_steering = received_data->new_wheel_steering;

  //krpci_client.Control_set_Pitch(controlID, pitch);
  //krpci_client.Control_set_Roll(controlID, roll);
  //krpci_client.Control_set_Yaw(controlID, yaw);
  krpci_client.Control_set_WheelThrottle(controlID, wheel_throttle);
  krpci_client.Control_set_WheelSteering(controlID, wheel_steering);

  LOGGER.DEBUG("Exiting actuator::control_command_sub_OnOneData");
}
//# End control_command_sub_OnOneData Marker


// Destructor - Cleanup Ports & Timers
actuator::~actuator()
{
  control_command_sub.shutdown();
  //# Start Destructor Marker
  //# End Destructor Marker
}

// Startup - Setup Component Ports & Timers
-:---  actuator.cpp    12% L40    Git-master  (C++/l Abbrev)
```

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Domain: Road Transportation Systems

- The behavior and performance of transportation systems is influenced by a number of factors, including the topology of the road network, the actual traffic conditions, the available sensors and their types, the specific traffic signals, the communication network, the control algorithms, etc.
- The cyber components of the system are characterized by the topology of the network, the physical link, the protocols and the control algorithms used

Threat model:

- DDOS on the sensor/actuator network
- Malicious or spoofed sensors

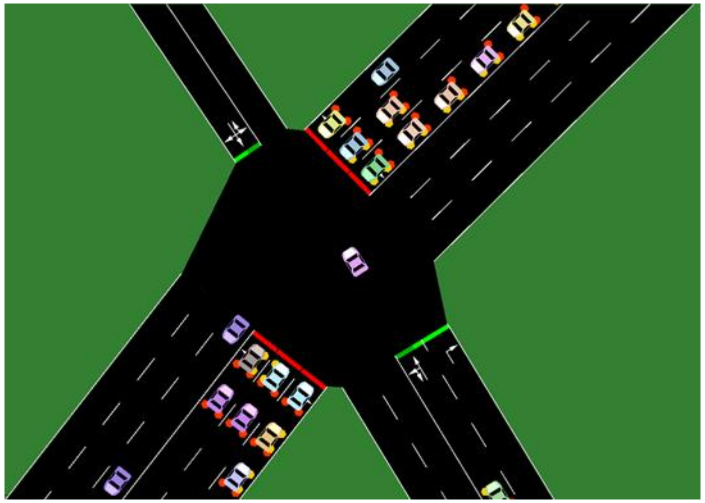
Research challenges:

- Resilient, robust, and cost-effective monitoring and control algorithms
- Timely detection of potential threats

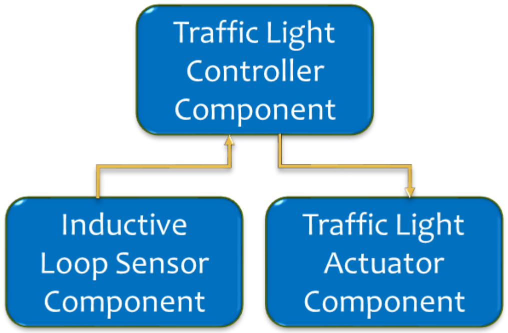
FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

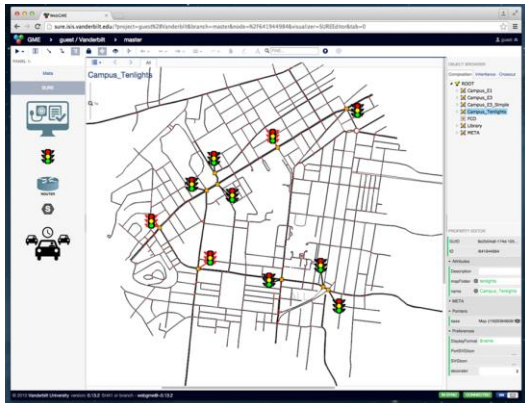
Supported, in part, by DoD/AFRL

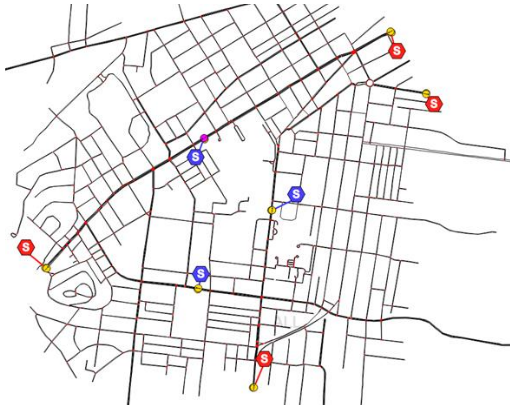
Resilient Sensing to Cyber-Attacks Evaluation using SUMO – a traffic simulator



- Deploy sensors, actuators, and controllers on the network
- Attack specific components or the system overall with e.g. DDoS
- Analyze how the application and system responded to the attacks
  - Develop optimal sensor/actuator placement and network configuration for resilience against faults and attacks

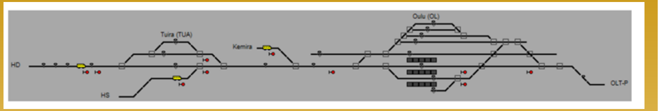

Traffic Light Controller Component
Inductive Loop Sensor Component
Traffic Light Actuator Component



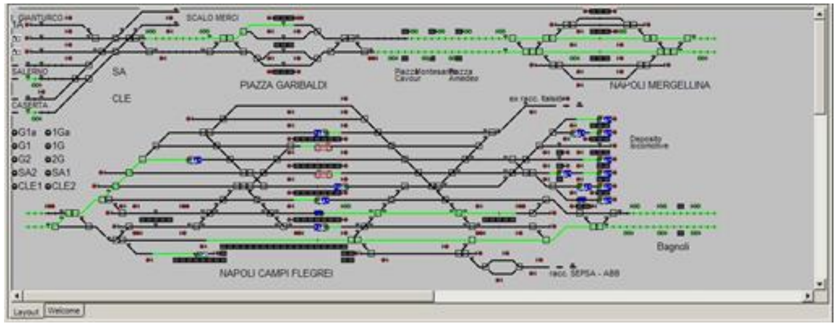


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Domain:
Railway control systems

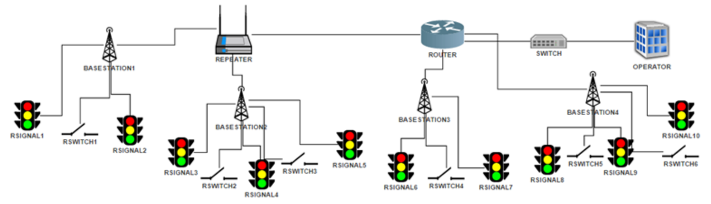


Railway controls systems rely on a local controllers, distributed supervisory control systems, and a communication network.



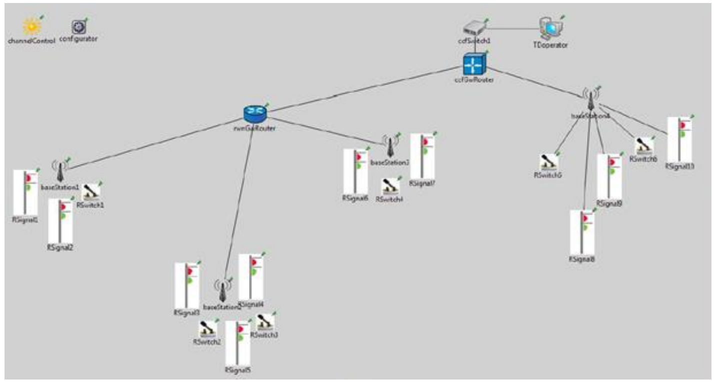
Threat model:

- DDOS attack on the network
- Integrity attacks on communications



Research challenges:

- Vulnerability analysis of existing systems
- Robust monitoring and control
- Attack mitigation techniques



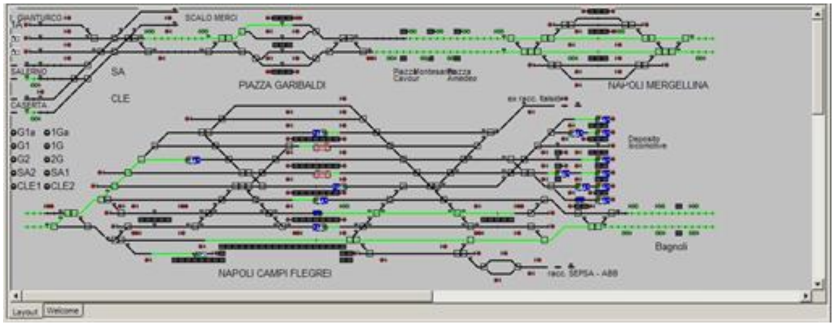
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

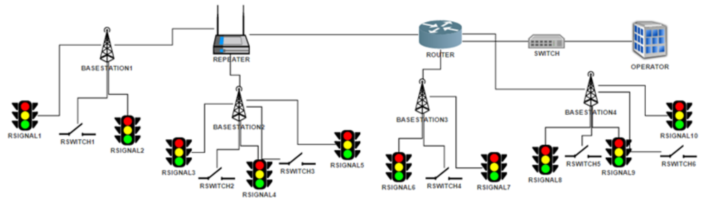
Supported, in part, by NIST

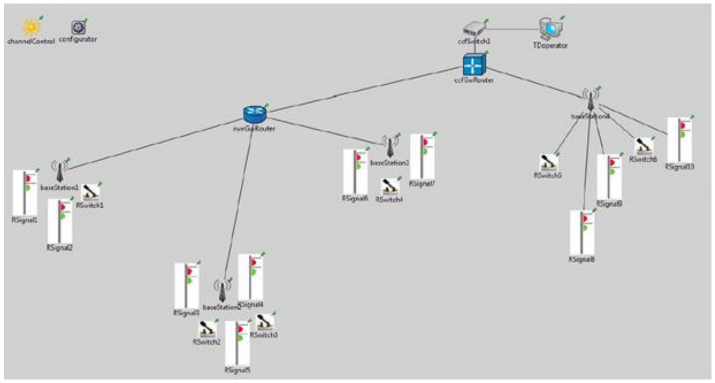
Train Director – A railway system simulator

Analysis of Attack Mitigation Techniques in Railway Systems

- Use the testbed to show that the baseline railway control system is vulnerable to two types of attacks:
  - DDoS
  - Integrity
- Implement defense against integrity attacks (using authentication) and measure how the risk associated with DDoS attacks changes
  - Hypothesis: For the same degree of DDoS capability, the negative impact on the railway CPS decreases







Domain:
Power Transmission and Distribution Systems

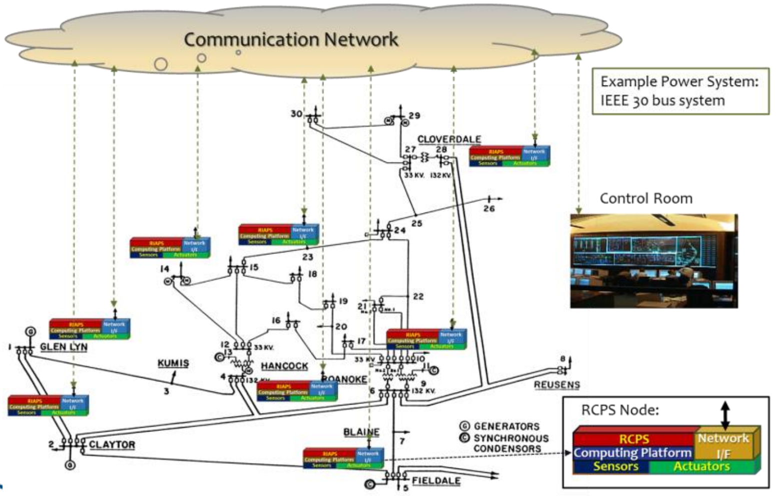
Power systems are potentially vulnerable on all components: generators, transmission and distribution system, end-user loads, protection system, power management systems

Threat model:

- DDOS attack on the network
- Integrity attacks on communications
- Malicious applications on the network

Research challenges:

- Vulnerability analysis of existing systems
- Detection and isolation of DDOS attacks
- Resilient control algorithms
- Shadow network for emergencies
- Recovery management



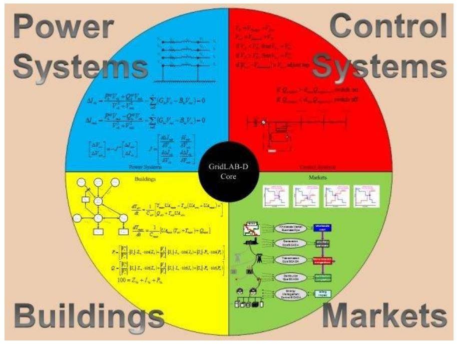
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Supported, in part, by NIST

Gridlab-D – a power system simulator

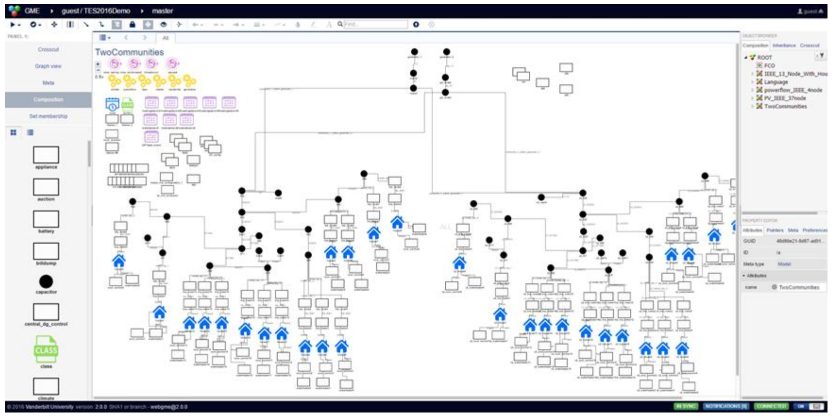
Analysis of Reactive Behavior and Attack Propagation

- Distributed, coordinated simulation of
  - Communications networks
  - Power generation, transmission, distribution, and consumption
  - Power system controllers



Related application: Transactive Energy

- Reactive community controllers
  - Select generators based on current price and loads
- Reactive generator controllers
  - Set price based on current loads compared with pre-determined generation profile
- Communications network transfers the data for price and load sensing
  - Has its own timing characteristics, faults, and vulnerabilities



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Summary / Future work

- RCPS Testbed provides a cost-effective platform for experimentation with resilience in a realistic setting
  - Realistic computing hardware for embedded controllers
  - Network is emulated through a programmable OpenFlow switch
  - Physics is simulated on a dedicated real-time simulator
  - Cost = ~$5K ; Design and software infrastructure is open source
- Experimentation with physical faults and cyber effects
  - Data logging ; results are post processed
- Next steps:
  - Make it available via the web https://rcps.isis.vanderbilt.edu
  - Improve experimental control and data collection framework
  - Investigate how simulation performance can be improved
    - Parallelized simulation / C2WT/HLA-based distributed simulation

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS