CPS Research & Development at DHS S&T

CPS Week 2010

Stockholm, Sweden

April 13, 2010

Dr. Nabil Adam (nabil.adam@dhs.gov), Fellow/Senior Program Manager

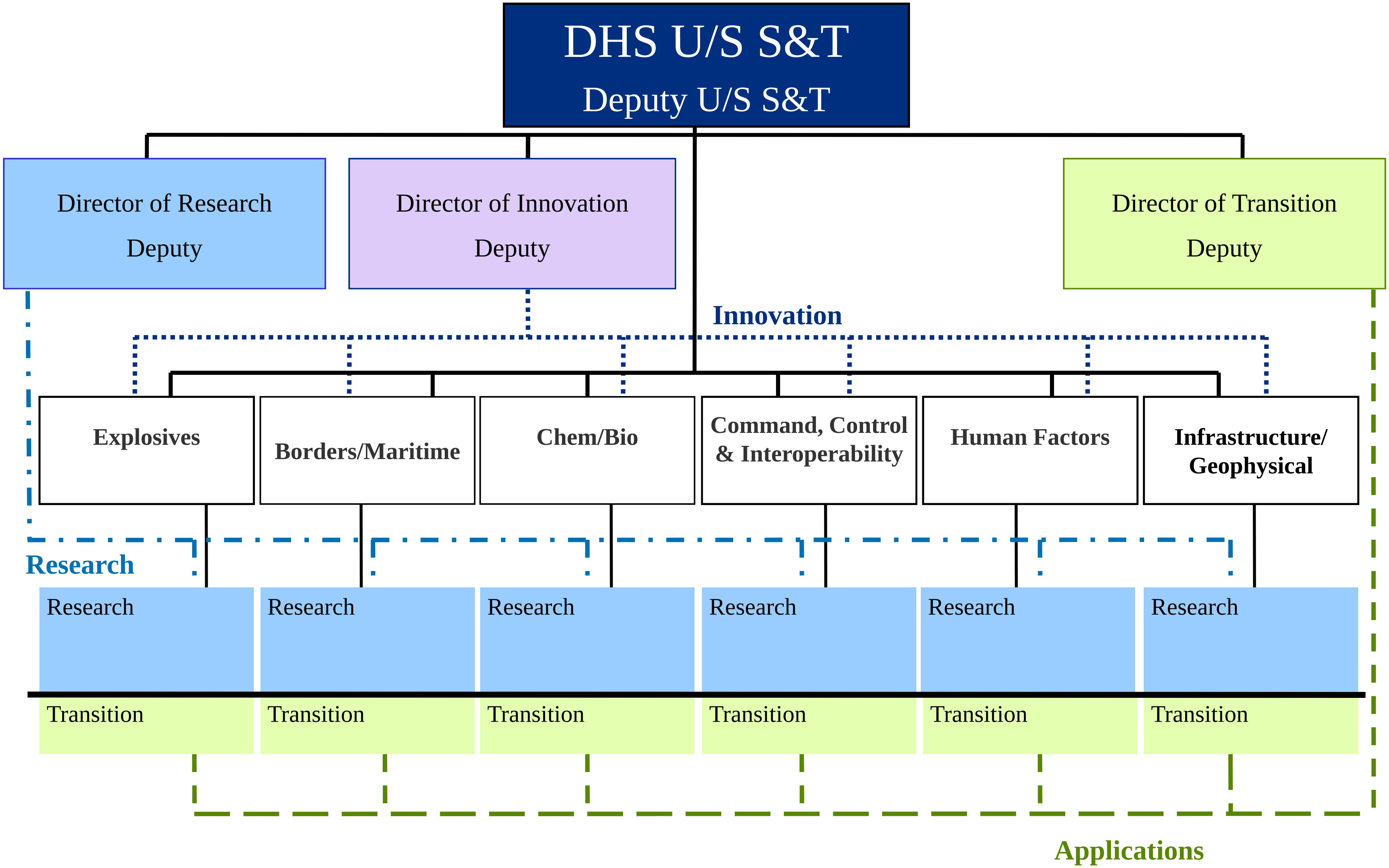
Infrastructure & Geophysical Division

Science and Technology Directorate, U.S. Department of Homeland Security

Homeland Security

Science & Technology Directorate
U.S. Department of
Homeland Security

S&T Organization



DHS S&T FY09 Investment Portfolio

Balance of Risk, Cost, Impact, and Time to Delivery

Product Transition (0-3 yrs)	Innovative Capabilities (2-5 yrs)
• Focused on delivering near-term products/enhancements to acquisition • Customer IPT controlled • Cost, schedule, capability metrics	• High-risk/High payoff • "Game changer/Leap ahead" • Prototype, Test and Deploy • HSARPA
Basic Research (>8 yrs)	**Other (0-8+ years)**
• Enables future paradigm changes • University fundamental research • Gov't lab discovery and invention • Homeland Security Institute	• Test & Evaluation and Standards • Laboratory Operations & Construction

Customer Focused, Output Oriented

Homeland Security S&T Enterprise

Centers of Excellence Alignment

S&T DIVISIONS

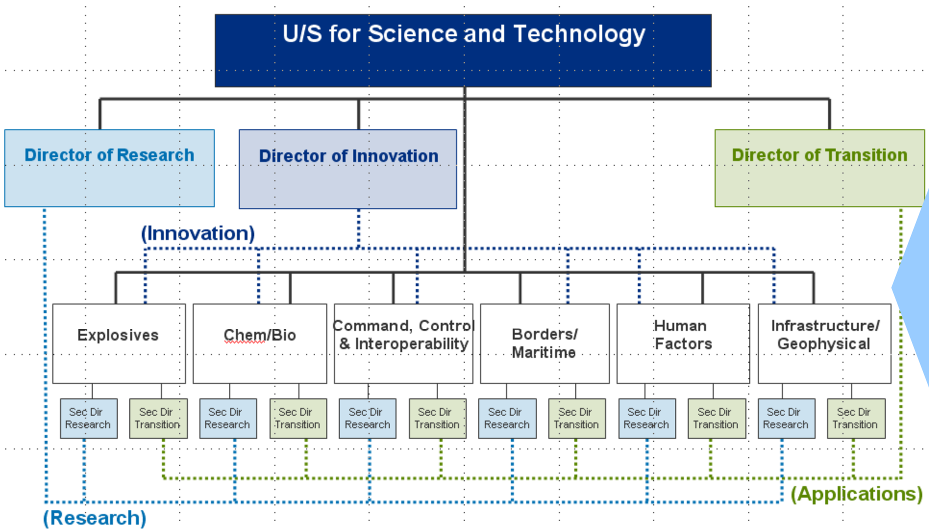
Explosives	Chemical/Biological	Command, Control & Interoperability	Borders/Maritime	Human Factors	Infrastructure / Geophysical
COE for Explosives Detection, Mitigation & Response *COE for Transportation Security*	National Center for Food Protection and Defense FAZD CENTER CAMRA PACER A Homeland Security Center of Excellence	IDS-UACs RVACs *Consolidated CCI Center* *COE for Transportation Security*	*COE for Border Security & Immigration* *COE for Maritime, Island & Remote/Extreme Environment Security*	START	PACER A Homeland Security Center of Excellence *COE for Natural Disasters, Coastal Infrastructure & Emergency Management* *COE for Transportation Security*

Risk, Economics and Operations Analysis

Risk Sciences Branch & HSI Risk Determination

CREATE Homeland Security Center

Infrastructure and Geophysical Division (IGD)

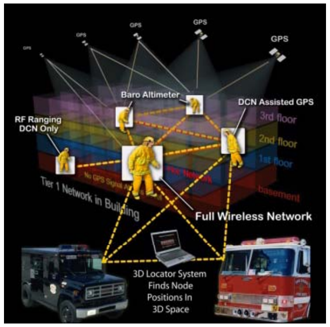


Objectives

- Develop capabilities to identify and mitigate the vulnerabilities of the 18 critical infrastructure
- Improve the ability of the Nation to prepare for, respond to, and recover from all-hazards emergencies to keep our society and economy functioning

Program Elements

- Critical Infrastructure Protection
- Geophysical
- Preparedness & Response
- Cyber-physical Systems Security



IGD R&D Programs: My Focus

1. Unified Incident Command & Decision Support (UICDS)
2. Complex Modeling, Simulation, and Analysis (CMSA)
3. Cyber-physical Systems Security (CPS) – New initiative

UICDS

- Information Sharing (intelligent)
  - Policies, Security, and Privacy
  - Sensors (numerous types)
  - Information Management & Planning documents and data
- Incident Management
  - Provide reasoning capabilities to assist IC for identifying:
    - Appropriate response plan
    - Required resources and their location
    - Response activity specific agencies
  - Provide functionalities, data, and tools for Incident response planning, execution, monitoring/tracking
- Interoperability and Expandability

  Provide the building blocks (data, basic functionalities & tools) for composing new applications
- Data Analysis

  Provide plug and play support to external data analysis applications

Complex Event Modeling Simulation & Analysis (CEMSA)

- **Objective**
  - Provide Models, tools, techniques, methodologies, to enable CIKR owners/operators and decision makers to:
    - Assess, in a tangible way, impact of their decisions on the infrastructure
      - when dealing with multiple events (man-made attacks or natural) occurring possibly within close proximity - spatially or temporally
  - Valuable insight
    - Interdependencies
    - Cascading effects

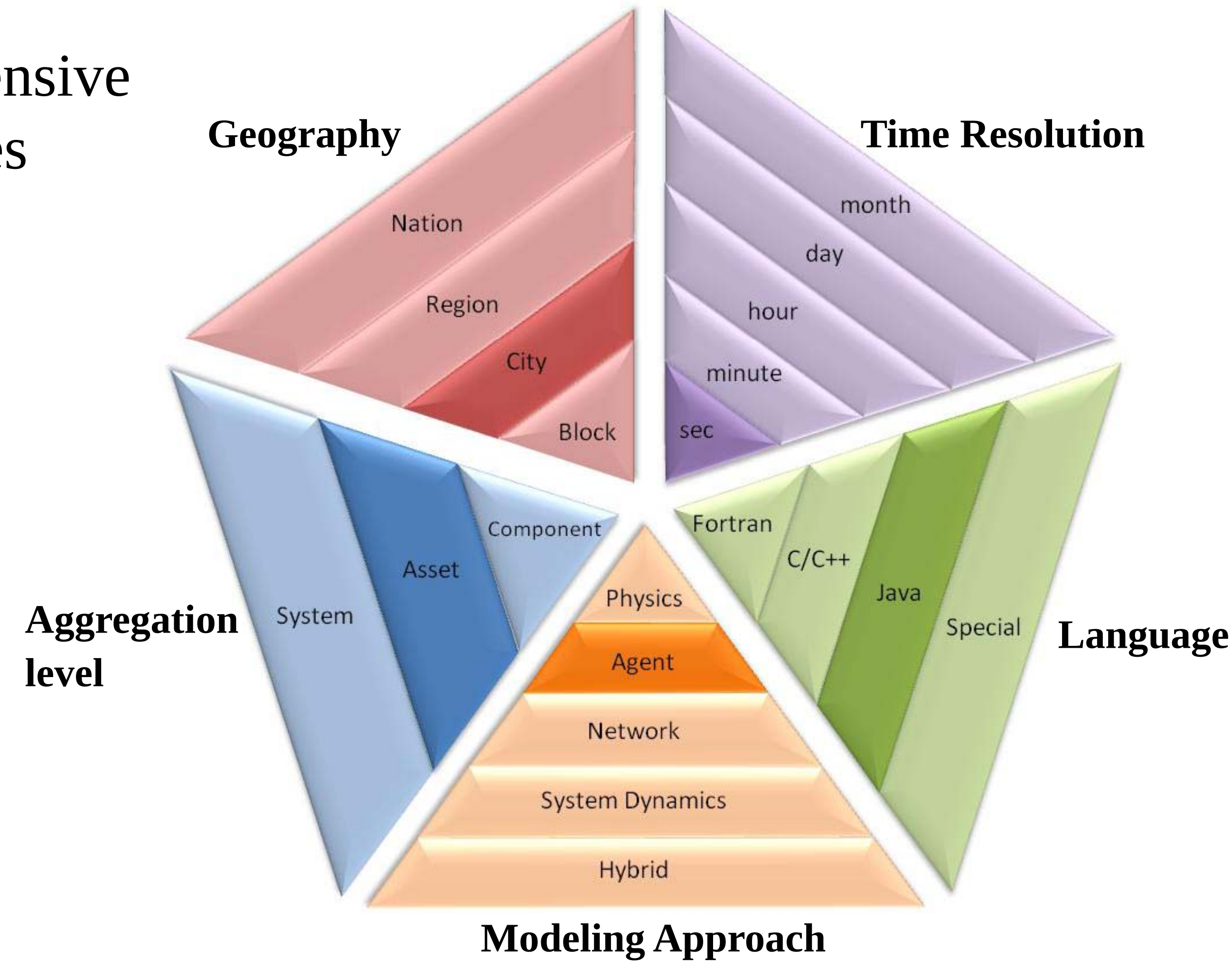
Complex Event Modeling Simulation & Analysis (CEMSA)

Program Structure

- CEMSA is a 5-year program - Major milestones:
  - Initial Operational Capability (IOC)
    - Deliverable: Minimum system components
    - Functionality: Consequence analysis of multiple, concurrent disruptions.
    - Delivery date: 2nd Quarter 2013
  - Full Operational Capability (FOC)
    - Deliverable: Final platform
    - Functionality: Complete the CEMSA system and satisfies all requirements.
    - Delivery date: 2nd Quarter 2015

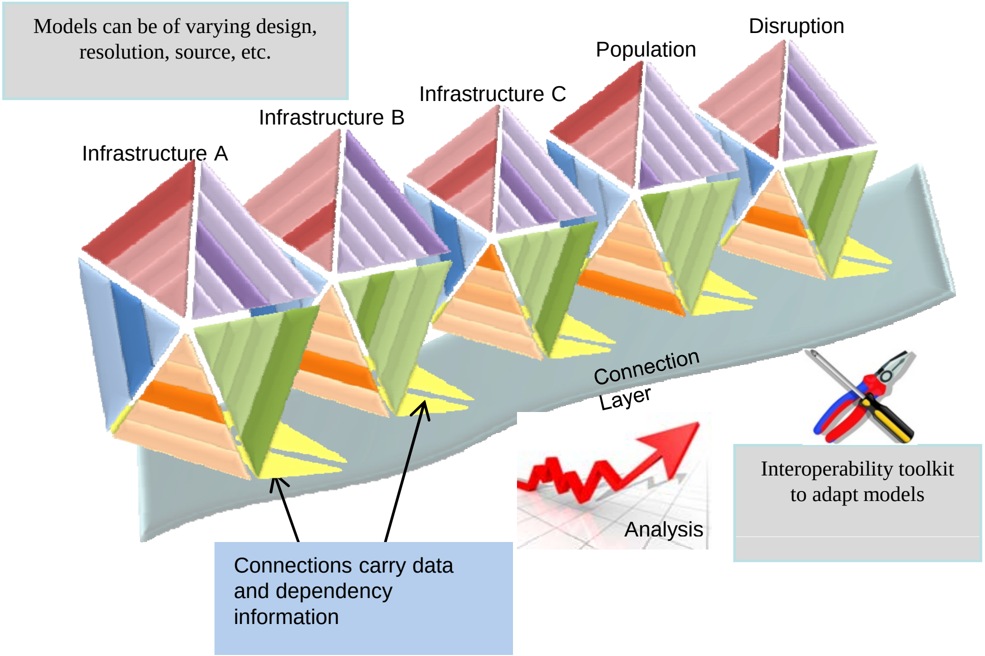
Current System

- Manual/human-intensive
- Sequential processes
- Inconsistent
  - Methods
  - Results



Desired Capabilities

1. "On the fly" integration
   - Time constraints
   - Fidelity consequences analysis
2. Well defined "semantics"
3. Architecture and process enabling
   - Timely analysis using best available
     - infrastructure
     - Performance
     - Systems behavior
     - Disruption models
4. Domain behavior model analysis
5. System-wide behavior analysis of (worst-case scenarios)



Current Status and Future Events

"Future Directions in Critical Infrastructure Modeling & Simulation" workshop (October 2008)

- 150 SMEs
- Infrastructure Protection
- Future Directions in Critical Infrastructure Modeling & Simulation Workshop Report (December 2008)

CEMSA Broad Agency Announcement

- Published (August 2009)
- Selection Evaluation Board (SSEB) review completed (December 2009)
- SSEB award recommendation (January 7, 2010)

"Grand Challenges in MSA for Homeland Security" workshop (March 2010)

- Over 200 SMEs

Next generation CEMSA Broad Agency Announcement

- Published (2nd Qtr 2010)

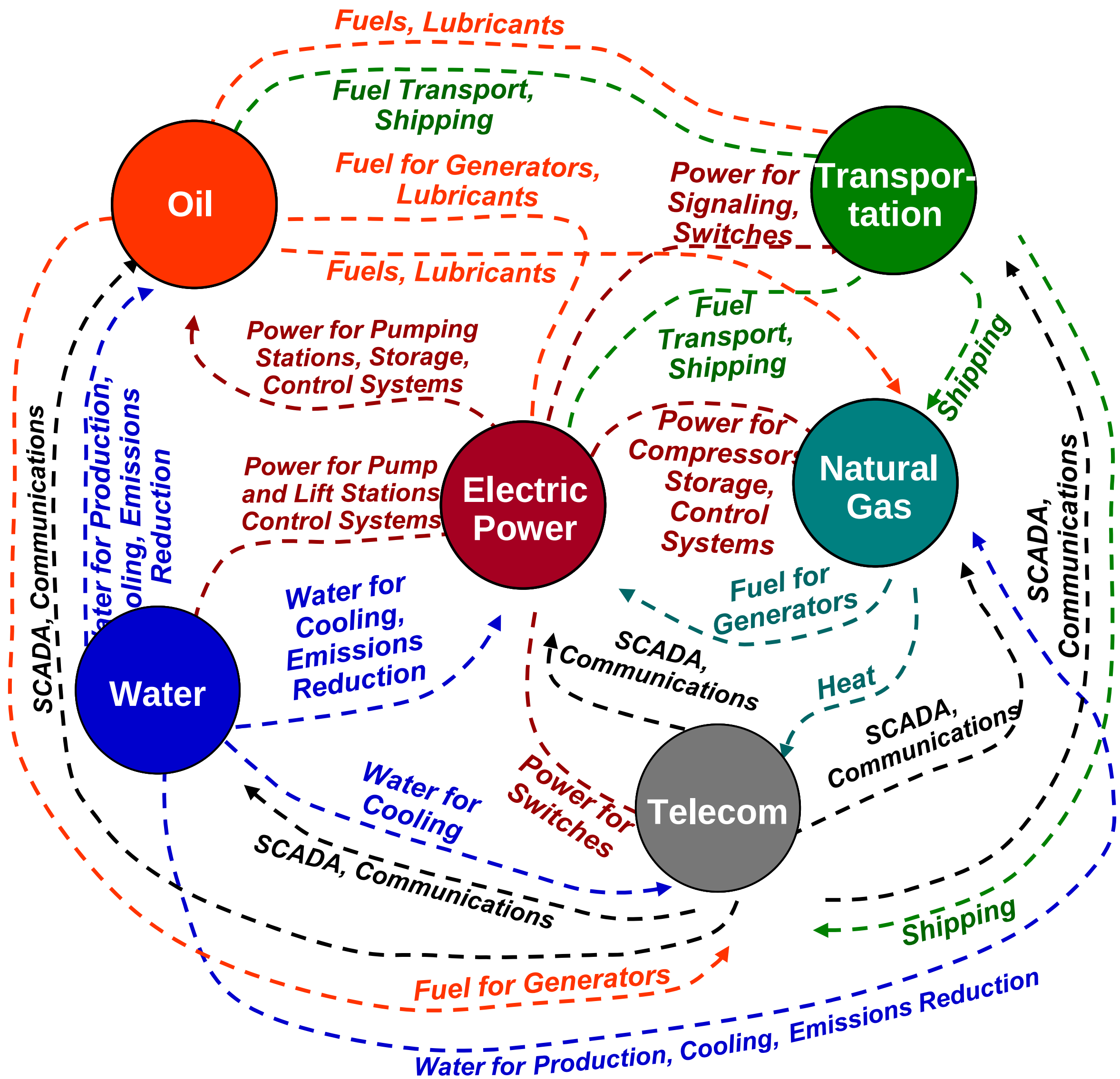
Cyber-physical Systems Security (CPS)

Cyber-Physical system (CPS)

- Tightly coupled and coordinated System of Systems (SoS)
  - Computational and information management components
  - Sensing components
  - Communication components
  - Physical components and processes
- Prevalent in most infrastructures
- Current trend
  - “Smart” Technologies
  - Future expansion of CPS in multiple domains

Electric Grid: A Complex Network

- U.S. Electric Power Grid
  - Largest
  - Most complex
- Interconnected
  - Local
  - Regional
  - National levels
    - Power generation
    - Transmission
    - Distribution
- Highly interdependent network of nodes
  - Failure of single node could potentially have cascading effects



CPS Security Threats

- Susceptible
  - Accidental events
    - Natural disasters
    - Mechanical failure
    - Inadvertent actions of authorized users
  - Deliberate unauthorized access
    - Insider threat
    - Hackers
    - Adversaries

CPS Security Threat: Consequences

- System susceptibilities may cause critical infrastructure failures or disruptions
  - Human health impacts
  - Loss of life
  - Public endangerment
  - Environmental damage
  - Loss of public confidence
  - Severe economic damage

Cybersecurity

- Traditional view
  - Network security
    - Data security
    - Preventing “denial of service”
  - Authentication and authorization
  - Software security, trustworthiness, and reliability
    - Protection from malicious software
    - Security in COTS-based systems

CPS Security is an emerging area of development

CPS Security

- Methodology must view CPS as an integrated and unified SoSs.
  - **Cyber components**
    - Network security
    - Authentication & authorization
    - Software trustworthiness
  - **Physical components** (behavior modeled by continuous dynamics)
    - Safety requirements
    - Security policy
  - **Physical processes**
    - Progressive state changes
  - **Interactions**
    - Account for interdependencies

Supervisory Control & Data Acquisition (SCADA)

PAST

- Proprietary protocols, techniques and underlying control system
- No public information
- No telecommunications or only point-to-point connections via leased/owned lines
- No connections to administrative business network or Internet
- Implementation without adequate security mechanisms due to perceived "hacker-free" environment
- Totally controlled and secure
- Protocol implementation took no account of "stress conditions"

PRESENT

- Technology and operational environment have not kept pace with rapid technical and operational developments
- Protocols are open standard; description on Internet
- Runs as application on Windows or Linux and uses Internet protocols that can be exploited
- Remote access by maintenance personnel is commonplace
- New option on PLC boards that cannot always be disabled provides remote access
- Recent efforts provide guidelines for specific security policy, but are general

Example – Distillation Column in a Chemical Plant - Safety & Security Analysis

- Start-up process of a distillation column
  - The dynamics is described by differential equations using the process variables
    - Process variables include, bottom temperature, top temperature, feed flow, tops flow, and reflux flow
  - The column operates in different control modes; switching between these control modes is caused by:
    - The value of the continuous variables exceed a given threshold; or
    - Manual control actions by users,
      - e.g., opening/closing of a steam valve
  - System dynamics is modeled as a hybrid automaton

Hybrid Automaton based Framework

- Allows representation of system dynamics, safety requirements, and security policies in a unified manner
- Uncover system vulnerabilities by providing answers to such questions as:

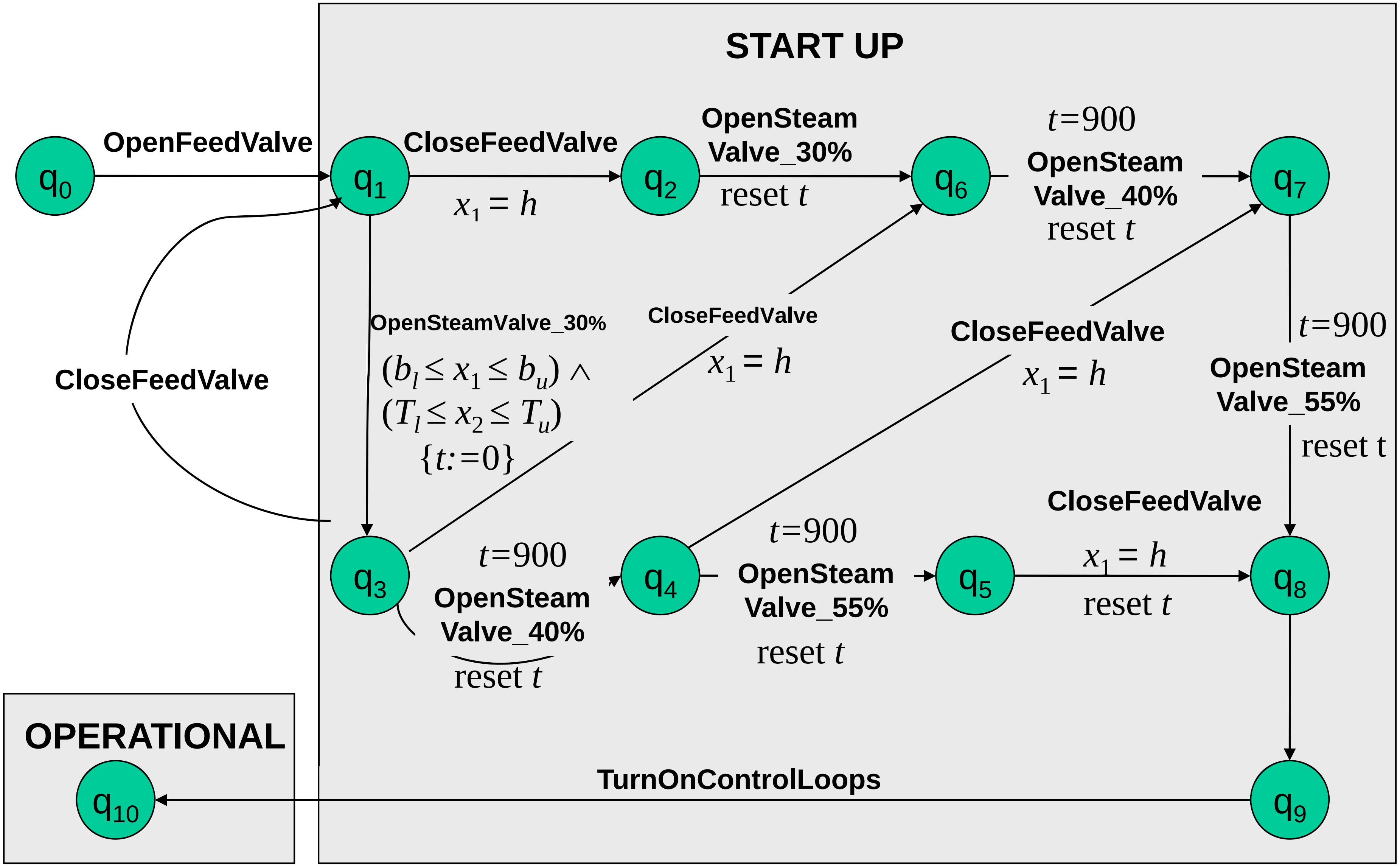
  Q1. Will the system be in undesirable state?

  Q2. Does the security specification ensure the least privilege requirement?

  (i.e., the system cannot go into an undesirable/unsafe state due to accidental or malicious actions of over-privileged users.)

  Q3. Is security specification sufficient to guarantee all safety requirements?
- Possible Approach
  - Reachability analysis of hybrid automaton
    - Use HyTech tool for reachability analysis
  - Deadlock and liveness analysis

Hybrid Automaton of the Startup Process

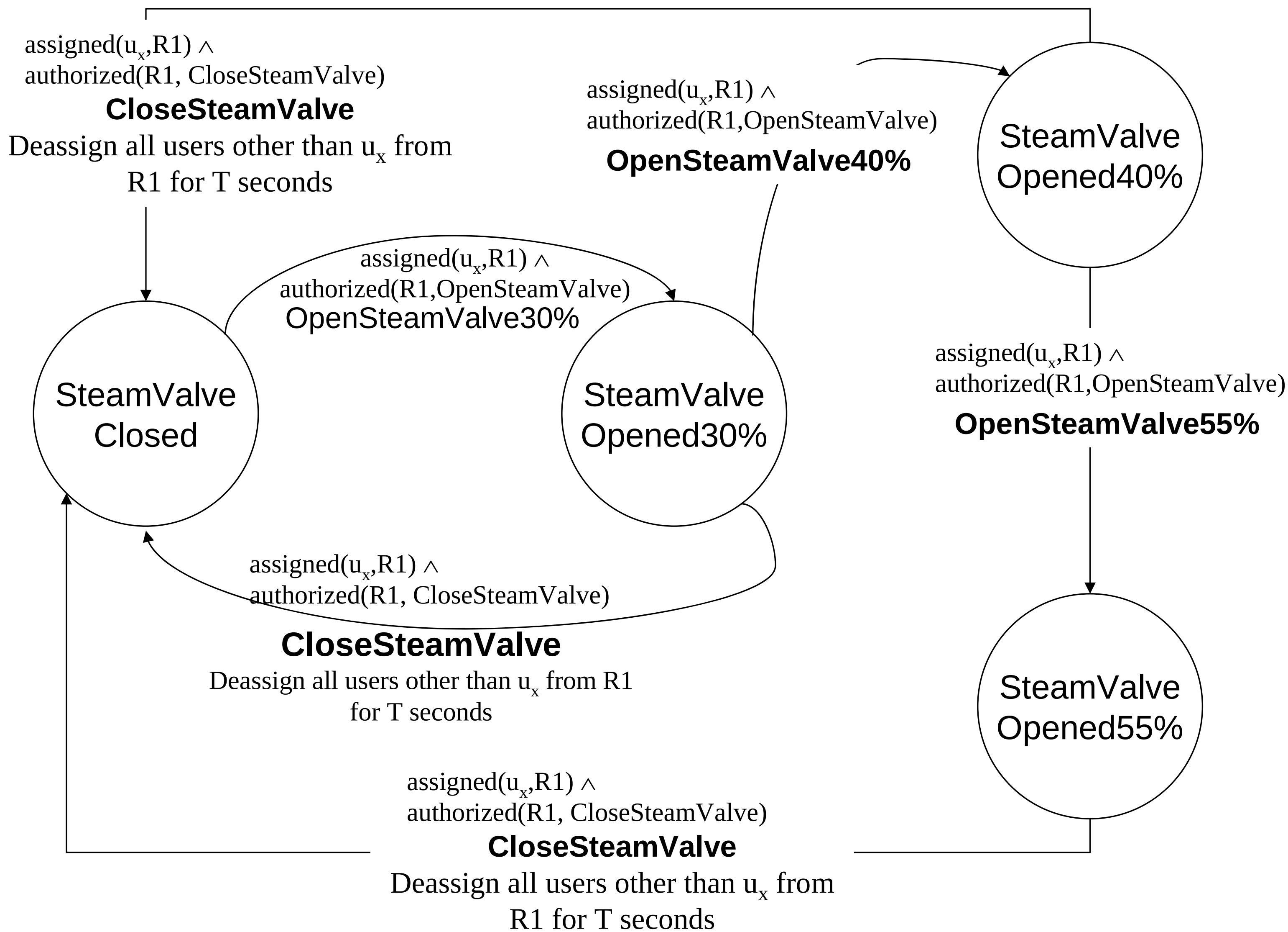


Safety Requirements – Security Policy

- **Safety, e.g.,**
  - If the chemical in distillation column is heated by steam for more than 5 minutes (300 seconds); then steam supply must not be discontinued before chemical feed valve is closed, otherwise, the chemical would be wasted.
    - This implies that if the cumulative time elapsed in mode q3 is 5 minutes (300 seconds) or more than the column must not be switched to mode q1.
  - A steam valve opened at 30% flow rate must not be switched to 40% flow rate in less than 900 seconds,; otherwise there is a risk that heat shock will fracture part of the physical distillation column.

- **Security Policy, e.g.**,
  - Opening/Closing of Steam Valve
    - Only users assigned to role R1 can change the setting, i.e., open or close steam valve
    - A steam valve cannot be closed repeatedly by different users; i.e., if a steam valve is closed by some user, then it cannot be closed again by other user.
  - Opening of Reflux Valve
    - Only users assigned to role R2 can open the reflux valve.
    - A user who closes the steam valve cannot open the reflux valve (separation of duty)
  - Policy configuration
    - Users u1, u2 assigned to R1; u3 assigned to R2
    - R2 inherits the permissions of role R1

Policy Automaton for Steam Valve Opening & Closing



Example – Distillation Column in a Chemical Plant: Safety & Security Analysis

- Start-up process of a distillation column
  - The dynamics is described by differential equations using the process variables
    - Process variables include, bottom temperature, top temperature, feed flow, tops flow, and reflux flow
  - The column operates in different control modes; switching between these control modes is caused by:
    - The value of the continuous variables exceed a given threshold; or
    - Manual control actions by users, e.g., opening/closing of a steam valve
  - System dynamics is modeled as a hybrid automaton

CPS Security – Research Needs (1)

1. Models and theories that bridge the cyber world and the physical world:
    - Comprehending both the discrete and continuous perspectives
    - Integrating multiple models and views
    - Model abstractions that span different levels of granularity
2. New security strategies (methods & techniques) for integrated CPS dealing with:
    - Verification & Validation (V&V) techniques
        - Continuous dynamics of the physical world
        - Discrete logical transitions of the cyber-world
    - Authentication & authorization of millions of devices
    - Trusted systems from untrusted components

CPS Security – Research Needs (2)

3. Performance and risk assessment testbeds that can span multiple CPS sectors:
   - Provide a controlled environment where we have access to the ground truth (e.g., stress level, risk, interdependency, component interactions)
   - Enable vulnerability assessment of Cyber-physical SoSs by
     - Replicating a multitude of control system specifications
     - Running simultaneous cyber/physical attacks on multiple systems
4. Coherent security performance metrics of CPS in different sectors
5. More dialogue among the stakeholders of CPS and the nation's critical infrastructure

Initial Focus

- Coordinate, collaborate, and leverage related work
  - Internal DHS directorates
  - External agencies
    - NRC
    - DOE
    - NSA
- Define initial focus sectors
  - Nuclear
  - Energy
  - Transportation
  - Medical devices
  - Chemical
- Develop basic and applied research initiatives

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security