

SCADA and YOU

Dr. Ken Dick

Dr. Robin Gandhi

Dr. Bill Mahoney

Overview

- Terminology
 - What is that new alphabet soup?
- SCADA Examples – why is this a problem?
- SCADA requirements and standards
 - NIST, NERC, DOE regulations....
- Our ongoing research
- Findings and Future work
- Questions



The Empire State Building and midtown New York City are shown during the 2003 blackout. (AP Photo)

Electricity Grid in U.S. Penetrated By Spies

Article

Video

Comments (105)

KEY SUBSCRIBER CONTENT PREVIEW

FOR FULL SITE ACCESS: [SUBSCRIBE NOW](#)

By SIOBHAN GORMAN



Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

WASHINGTON -- Cyberspies have programs that could be used to disrupt security officials.

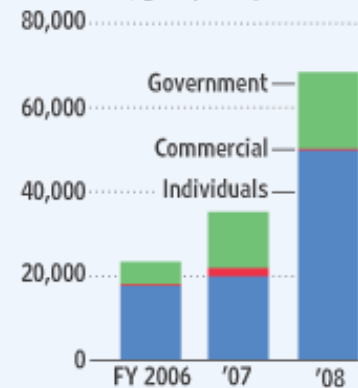
The spies came from China, Russia to be on a mission to navigate the U.S. sought to damage the power grid or during a crisis or war.

"The Chinese have attempted to map senior intelligence official. "So have the

The espionage appeared pervasive across region, said a former Department of Homeland Security official, "The espionage are growing," the former official said,

Stealth Attacks

Number of reported cybersecurity breaches in the U.S., grouped by sector



Note: Fiscal year ends Sept. 30
Source: Department of Homeland Security

software national-
ere believed
ders haven't
y could try
said a
company or
, and they
ot last year."

Terminology



Terminology

- Industrial control systems (ICS) includes:
 - Supervisory control and data acquisition (SCADA)
 - Distributed control systems (DCS)
 - Others: Programmable Logic Controllers (PLC)
- SCADA systems provide supervisory control for distributed assets using centralized data acquisition
 - Essentially, it is a computer system that controls and monitors a process, **all remotely !**

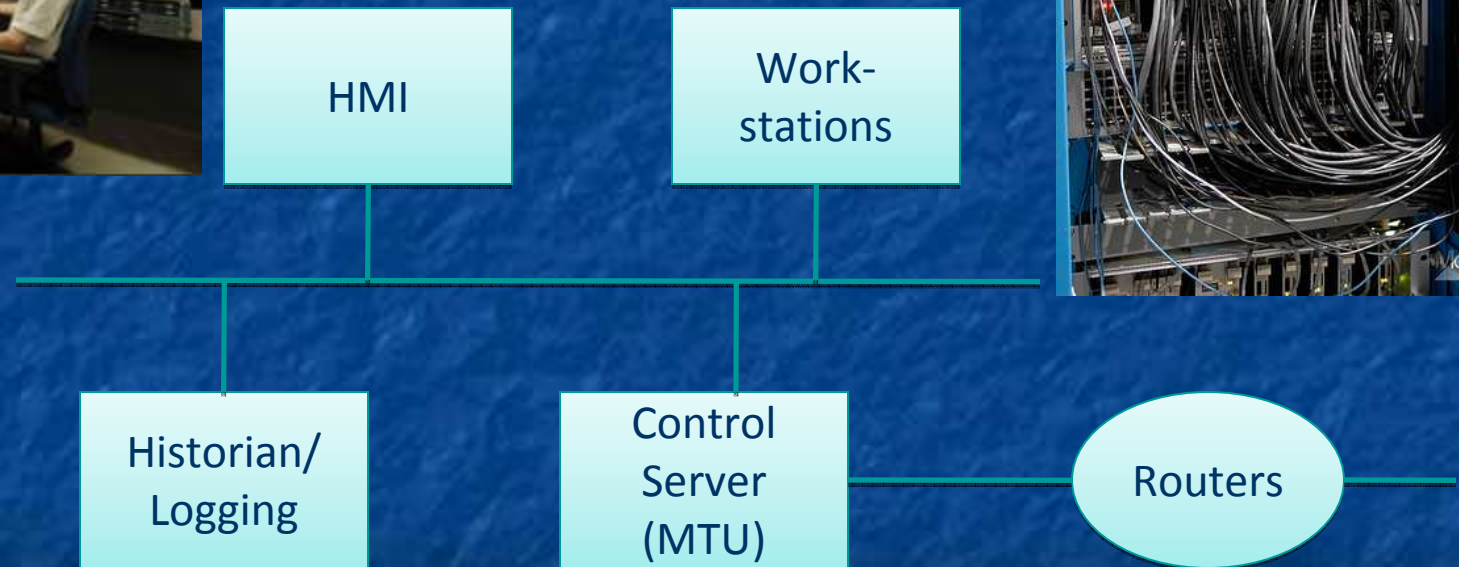
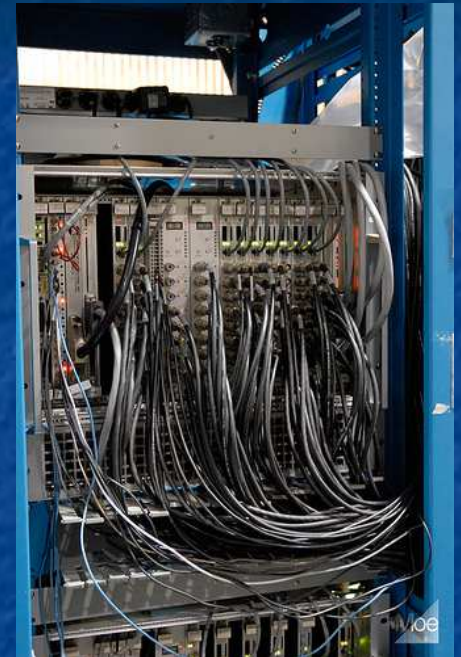
What's so special about SCADA?

- Highly **distributed systems**
 - Control **geographically dispersed assets**, often scattered over thousands of square kilometers
- Control and monitoring data transmitted over **Long-distance communications** networks
- **The controlled assets are critical to our way of life**
 - Examples: Distribution systems such as **water distribution** and **wastewater collection** systems, **oil and natural gas pipelines**, **electrical power grids**, and **railway transportation systems**.
 - **These are critical to Nebraska's Economy.**

SCADA Components

- **A Human-Machine Interface or HMI**
 - Graphical presentation /simulation of the process
 - Configure, monitor and control the process
- **A supervisory system (Central Server)**
 - Acquire data on the process
 - Send control commands to the process
- **Remote Terminal Units (RTUs, PLCs, IEDs etc)**
 - Connecting to sensors of the actual process devices
 - Converting sensor signals to digital data
 - Sending digital data to the supervisory system
- **Communication infrastructure**
 - Connects the supervisory system to the Remote Terminal Units

Supervision/Monitoring and Control End



Remote End



Modulators/
Protocol translators

PLC/IED
(Dumb
Controller)

Actuators

Sensors

Modulators/
Protocol translators

RTU

Actuators

Sensors

Environment / Process



Communications (Middle)



Telephone,
Power Lines



Radio,
Microwave,
Cellular



Satellite



WAN/LAN



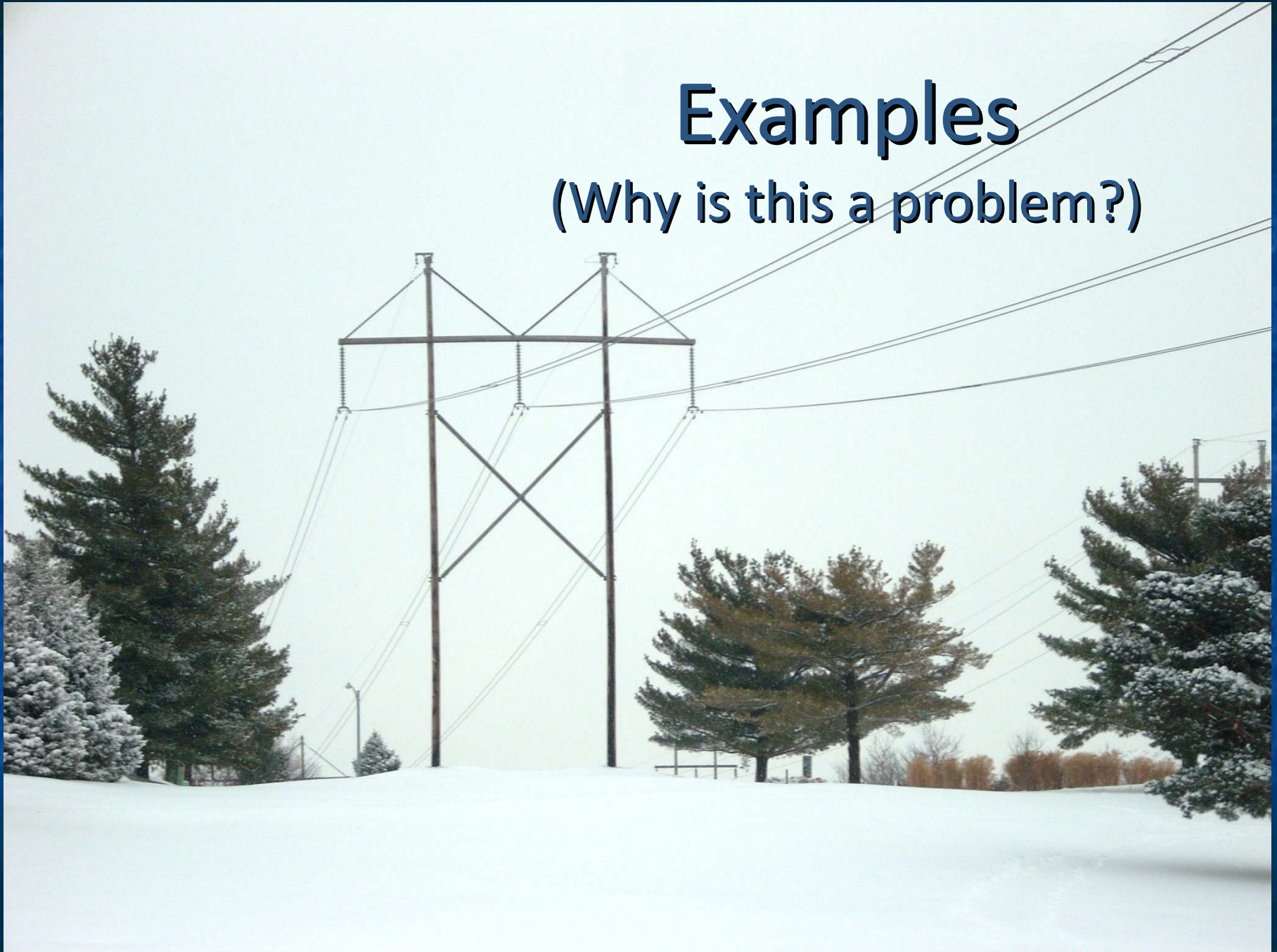
Terminology

(Acronyms Abound!)

- * AGA - American Gas Association
- * ANL - Argonne National Laboratory
- * API - American Petroleum Institute
- * BCIT - British Columbia Institute of Technology
- * CIDX - Chemical Industry Data Exchange
- * CSRC - Computer Security Resource Center
- * CSSP - Control Systems Security Program
- * DCS - Distributed Control System
- * EMS - Energy Management System
- * I3P - Institute for Information Infrastructure Protection
- * IEC - International Electrotechnical Commission
- * IEEE - Institute of Electrical and Electronics Engineers
- * INL - Idaho National Laboratory
- * ISA - International Society of Automation
- * ISID - Industrial Security Incident Database
- * NERC - North American Electric Reliability Corporation
- * NISCC - National Infrastructure Security Co-ordination Centre
- * NIST - National Institute of Standards and Technology
- * NSTB - National SCADA Test Bed
- * PCSF - Process Control Systems Forum
- * PCSRF - Process Control Security Requirements Forum
- * PNNL - Pacific Northwest National Laboratory
- * SCADA - Supervisory Control and Data Acquisition
- * TSWG - Technical Support Working Group
- * US-CERT - United States Computer Emergency Readiness Team

Examples

(Why is this a problem?)



Why is Security an issue for SCADA?

- The SCADA environment is different:
 - SCADA computations and logic have a direct affect on the physical world
 - Safety and efficiency sometimes conflict with security in the design and operation of control systems
 - Ordered list of security expectations from SCADA
 1. availability
 2. integrity
 3. confidentiality

The Key Point

- Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents
 - Bottom-line:
 - **They are starting to represent IT systems**

Key SCADA security problems

- Blocked or delayed flow of information
- Unauthorized changes to instructions, commands, or alarm thresholds
- Inaccurate information sent to system operators
 - (Authentication) Military problem
 - Sensor Networks, Key Mgmt.
- SCADA software or configuration settings modified, or software infected with malware
- Interference with the operation of safety systems, which could endanger human life.

Examples

- In late 2006, a foreign hacker penetrated security at a water filtering plant near **Harrisburg, Pennsylvania**, planting malicious software capable of affecting the plant's **water treatment** operations.
- April 2000, Vitek Boden, a former contractor, took control of the SCADA system controlling the **sewage and water treatment** system at Queensland's Maroochy Shire. Using a wireless connection and a stolen computer, Boden released **millions of gallons of raw sewage and sludge into creeks, parks and a nearby hotel**.

Examples

- In January 2008, a **teenage boy** who hacked into a Polish tram system used it like **“a giant train set,” causing chaos and derailing four vehicles**. The 14-year-old, described by his teachers as a model pupil and an electronics “genius,” adapted a television remote control so it could change track points in the city of Lodz.
- The **“Aurora Generator Test”** was conducted in March 2007 by the US Department of Homeland Security (DHS) and involved the remote accessing of a generator control station by a foreign hacker. It resulted in the **partial destruction of a \$1 million large diesel-electric generator**.

But these are not typical, right?

Wrong.

People are discovering new vulnerabilities in SCADA systems as recently as the last month or two. For example...

Examples

RealWin SCADA server FC_INFOTAG/SET_CONTROL buffer overflow

Description:

RealWin SCADA server is vulnerable to a stack-based buffer overflow. By sending an overly large FC_INFOTAG/SET_CONTROL packet to TCP port 910, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash.

Platforms Affected:

DATAC Control International, RealWin SCADA Server 2.0

Remedy:

No remedy available as of February 16, 2009.

Consequences:

Gain Access

Examples

Gas refineries at Defcon 1 as SCADA exploit goes wild

At least they should be

By Dan Goodin in San Francisco

Posted in Security, 8th September 2008 18:32 GMT

Gasoline refineries, manufacturing plants and other critical facilities that rely on **computerized control systems just became more vulnerable to tampering or sabotage with the release of attack code that exploits a security flaw in a widely used piece of software.**

The exploit code, published over the weekend as a module to the Metasploit penetration testing tool kit, attacks a vulnerability that resides in CitectSCADA, software used to manage industrial control mechanisms known as SCADA, or Supervisory Control And Data Acquisition, systems. In June, the manufacturer of the program, Australia-based Citect, and Computer Emergency Response Teams (CERTs) in the US, Argentina and Australia warned the flawed software could put companies in the aerospace, manufacturing and petroleum industries at risk from outsiders or disgruntled employees.

And worst of all...



SCADA controls all sorts of things, such as winery systems, and ...

... such as the Budweiser Plant in St. Louis, Missouri!



Standards



The Standards Labyrinth

- The good thing is that
 - There's plenty to choose from!
- NIST
 - Enhancement to 800-53
 - 800-82
- NERC
 - In Hindi it means "Hell", what coincidence!
 - Cyber protection CIP augmentations, Being enforced from July 2009
- ISO / IEC standards



Some of the NERC Top 10 Vulnerabilities in 2007

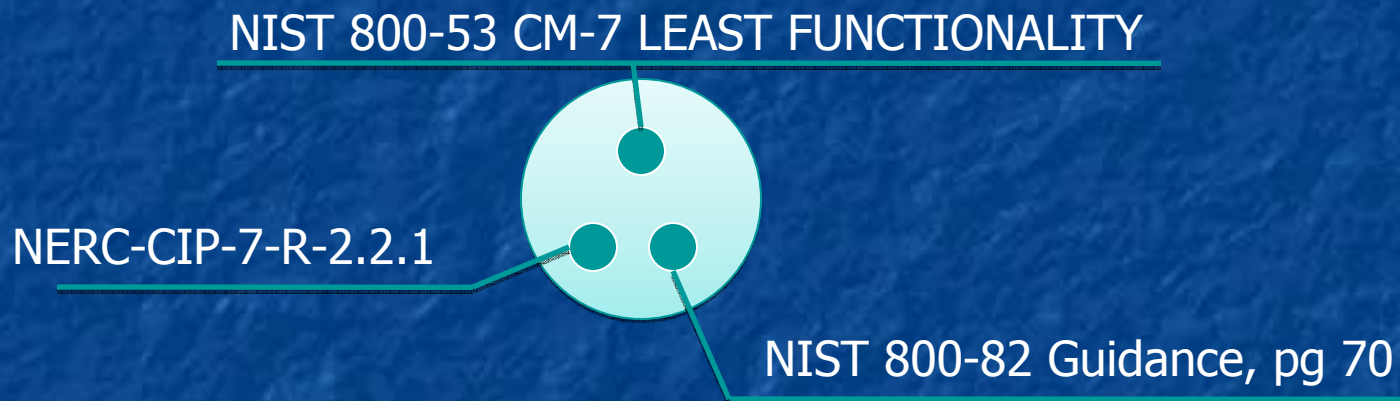
- Remote access to the control system without appropriate access control
- Use of inadequately secured wireless communication for control
- Insufficient application of tools to detect and report on anomalous or inappropriate activity
- Unauthorized or inappropriate applications or devices on control system networks
- Control systems command and control data not authenticated

Overlaps are typical among standards

- NERC-CIP-7-R-2.2.1:
 - The Responsible Entity shall enable only those ports and services required for normal and emergency operations
- NIST 800-53 CM-7 LEAST FUNCTIONALITY
 -provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services
- NIST 800-82 Guidance, pg 70
 - Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis.

Significant Overlaps among the Standards

- Why not have them all relate to each other?



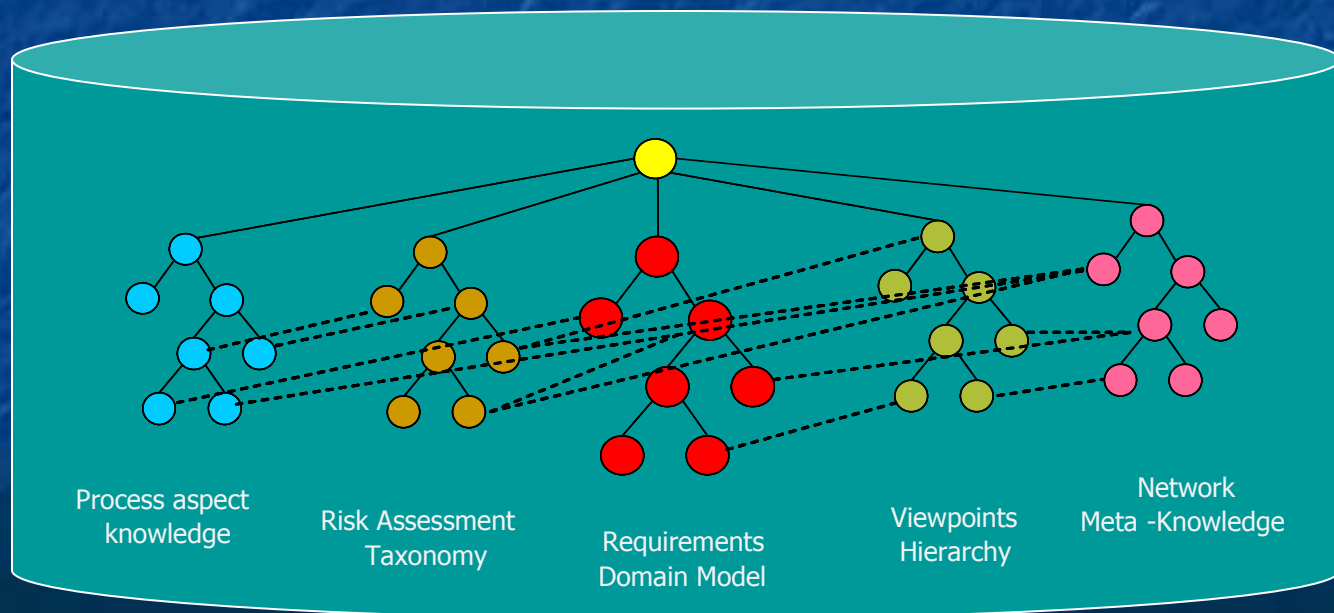
The Definition of a Common Language

- NL Regulatory Requirements (Directives, Security Requisites and manual)
- SCADA related domain knowledge



Categorization (i.e. Systems, Software etc.)
Classification (i.e. DITSCAP process etc.)

- Hierarchical representations of the requirements
- Structured representations through the decomposition of the requirements; Top (General) – Bottom (Specific), Properties
- Advanced KR technique enables to capture the conceptual domain model



SCADA Problem Domain Ontology

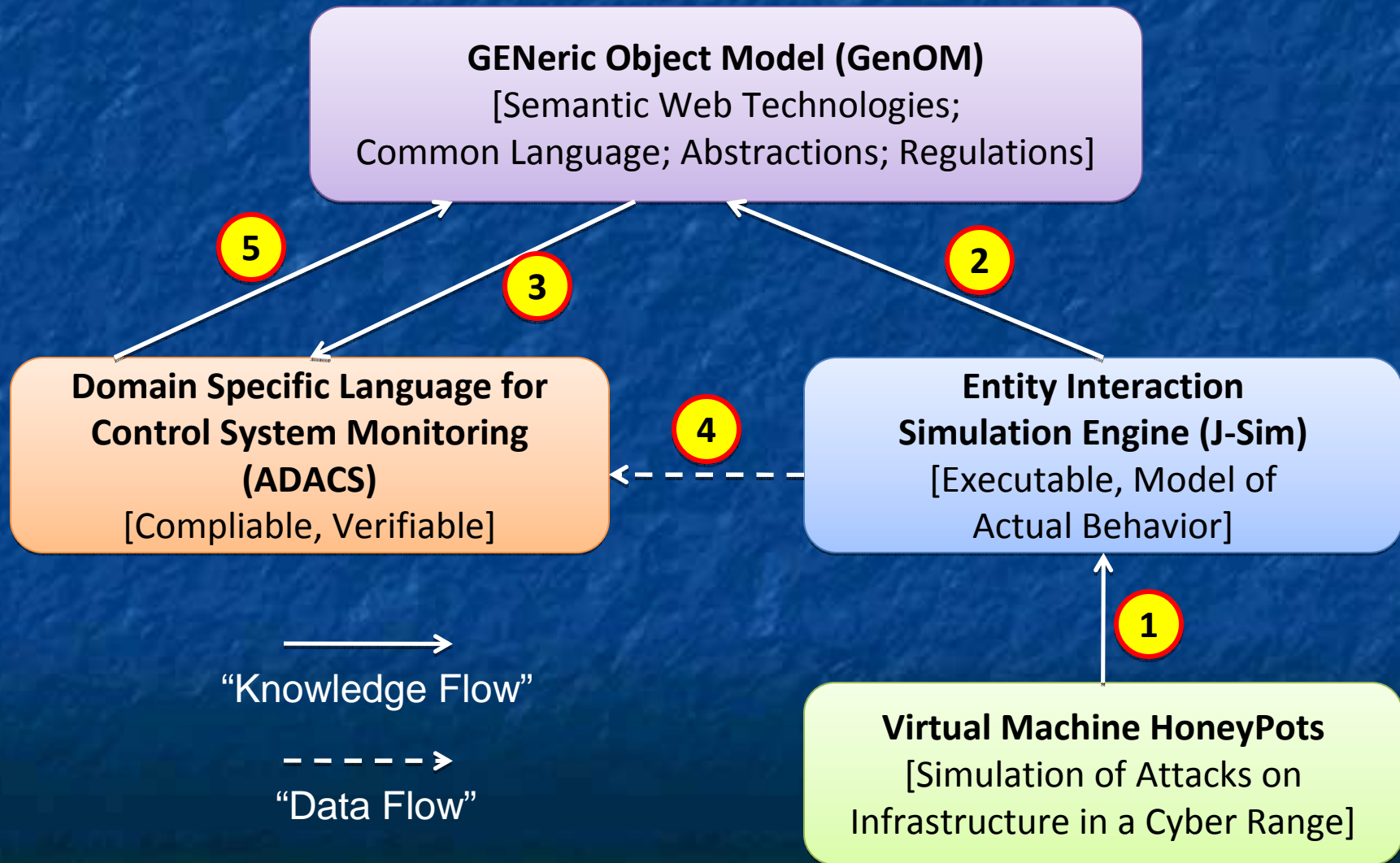
Research



Framework Characteristics

- Operate in an event driven fashion
 - Asynchronous operation
 - Adaptive and reactive to suspected violations of policy
- Pluggable architecture
 - Distributed and autonomous
 - Scalable
- Domain-specific language for policy specification
 - Executable language for enforcement of policy
- Domain ontology defines concepts, their properties, and relationships among the concepts used in the policy specification
 - Policy interdependencies, consistency, and portability
- Generic data format

An Integrated Framework



Connecting Simulation and Physical Systems

- Simulation allows to verify the behavior of the system policies prior to deployment
- Tight coupling between simulation and physical systems will link the theoretical and operational models providing end to end traceability and monitoring capabilities

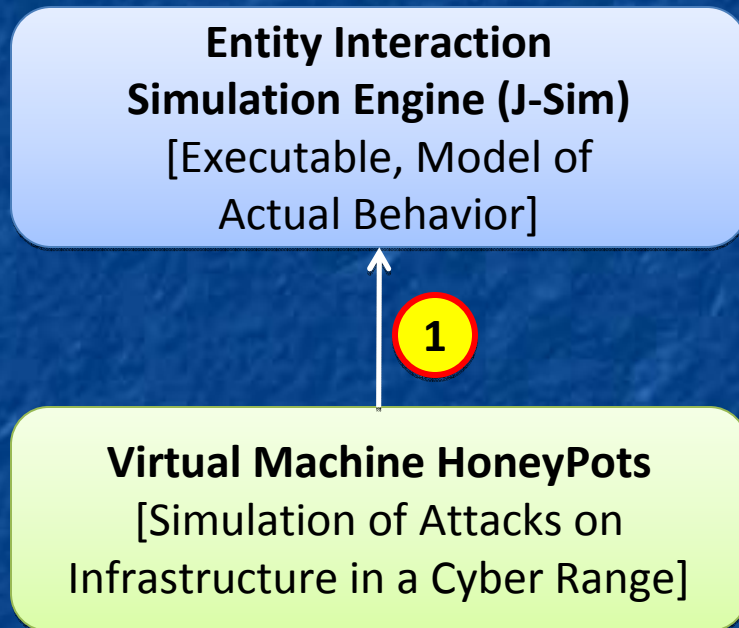
Research

- ADACS (pronounced A – Daks)
 - **A**utonomous component based policy
Description language for
Anomaly monitoring in
Control
Systems.
- It is also SCADA spelled backwards !
 - What a coincidence !

Things to be modeled for each autonomous component

- Allowed communications
 - Functions that are allowed and necessary for normal operation
- Communication patterns (normal)
 - Ports scanning and denial or service can be detected if the normal patterns are known
- Maintained Protocol state
 - Communication requested without authentication
- Trusted partners
 - What other components does the current component normally communicate with?

Research



- Creation of Virtual Environments that emulate real systems
 - Allows to launch attacks
- Analyze effects of the attacks on a simulation of the SCADA environment

Research

GENeric Object Model (GenOM)
[Semantic Web Technologies;
Common Language; Abstractions; Regulations]

- Use simulation objects to build network meta-models
 - Reason about a cascading effect at higher levels of abstraction

2

**Entity Interaction
Simulation Engine (J-Sim)**
[Executable, Model of
Actual Behavior]

Research

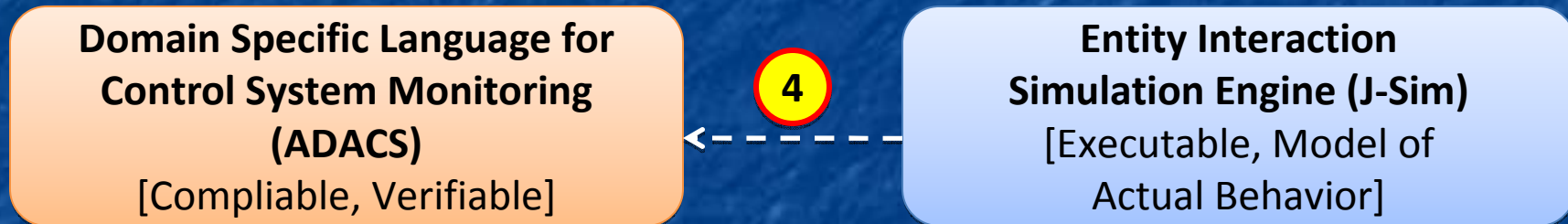
GENeric Object Model (GenOM)
[Semantic Web Technologies;
Common Language; Abstractions; Regulations]

3

**Domain Specific Language for
Control System Monitoring
(ADACS)**
[Compliant, Verifiable]

- Use abstractions to compose executable policy descriptions
- Policies are enforced at each component level
- An end-to-end approach

Research



- The simulation reports any violations of the defined policies
 - Policies are compiled directly into each autonomous simulation component

Research

GENeric Object Model (GenOM)
[Semantic Web Technologies;
Common Language; Abstractions; Regulations]

5

**Domain Specific Language for
Control System Monitoring
(ADACS)**
[Compliant, Verifiable]

- Translate policy violations into user understandable content
 - Determine compliance violations in real-time
 - Reason about likelihood of an adverse event and business impact

Conclusions / Questions



References

[NIST 800-53](#)

http://www.theregister.co.uk/2008/09/08/scada_exploit_released/

http://en.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition