Industrial Control Systems Security

Victoria Yan Pillitteri
Computer Security Division
victoria.yan@nist.gov

Federal Computer Security
Program Managers' Forum
June 5, 2013

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing

Overview

- Industrial Controls System (ICS) Vulnerabilities in the Headlines
- ICS Overview
- ICS Security Considerations
- Current Initiative: NIST Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems Security*
- Additional Related NIST Work and Resources for ICS Security
- Questions

Industrial Control System Vulnerabilities the Headlines

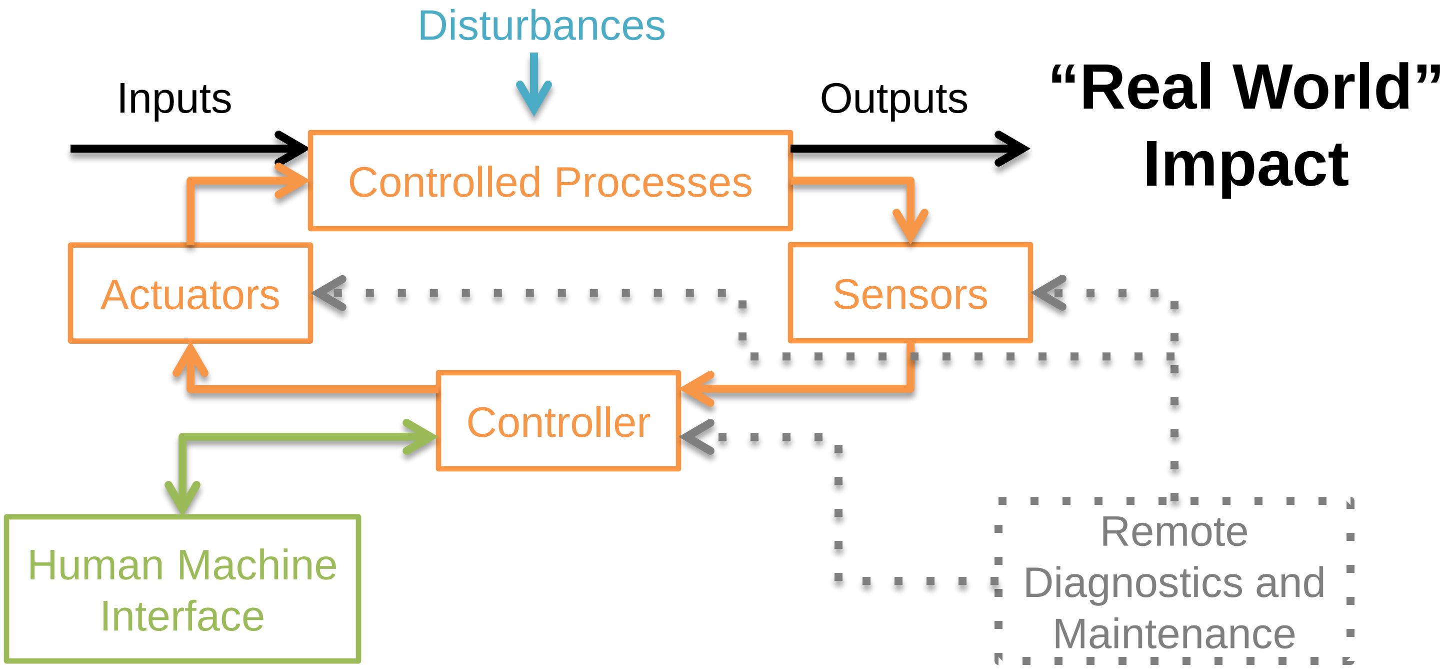
“Google Hack Attack Was Ultra Sophisticated, New Details Show …used unprecedented tactics that combined encryption, stealth programming and an unknown hole in Internet Explorer…**”**
http://www.wired.com/threatlevel/2010/01/operation-aurora/

“Oil, gas and petrochemical companies targeted were hit with technical attack on their public-facing websites …used persuasive social-engineering techniques to get key executives…**”**
http://www.pcworld.com/article/219251/article.html

“Microsoft Corp said hackers exploited a previously unknown bug in its Windows operating systems…”
http://www.reuters.com/article/2011/11/01/us-microsoft-cyberattack-idUSTRE7A06ZX20111101

Graphics Source: http://www.mcafee.com/us/mcafee-labs/technology/high-profile-threats.aspx

Industrial Control Systems Overview



Disturbances

Inputs

Outputs

Controlled Processes

“Real World” Impact

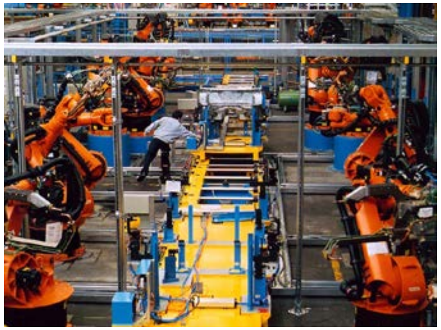
Actuators

Sensors

Controller

Human Machine Interface

Remote Diagnostics and Maintenance



Industrial Control Systems Overview

“An information system used to control industrial processes such as manufacturing, product handling, production, and distribution.”

- Industrial control system (ICS) is a general term that encompasses several types of control systems, including:
  - Supervisory control and data acquisition (SCADA) systems
  - Distributed control systems (DCS)
  - Programmable logic controllers (PLC)

- Industrial control system failure could result in:
  - Safety risks
  - Environmental Impact
  - Lost production and revenue
  - Equipment damage
  - Information theft

ICS Overview: SCADA Systems Example

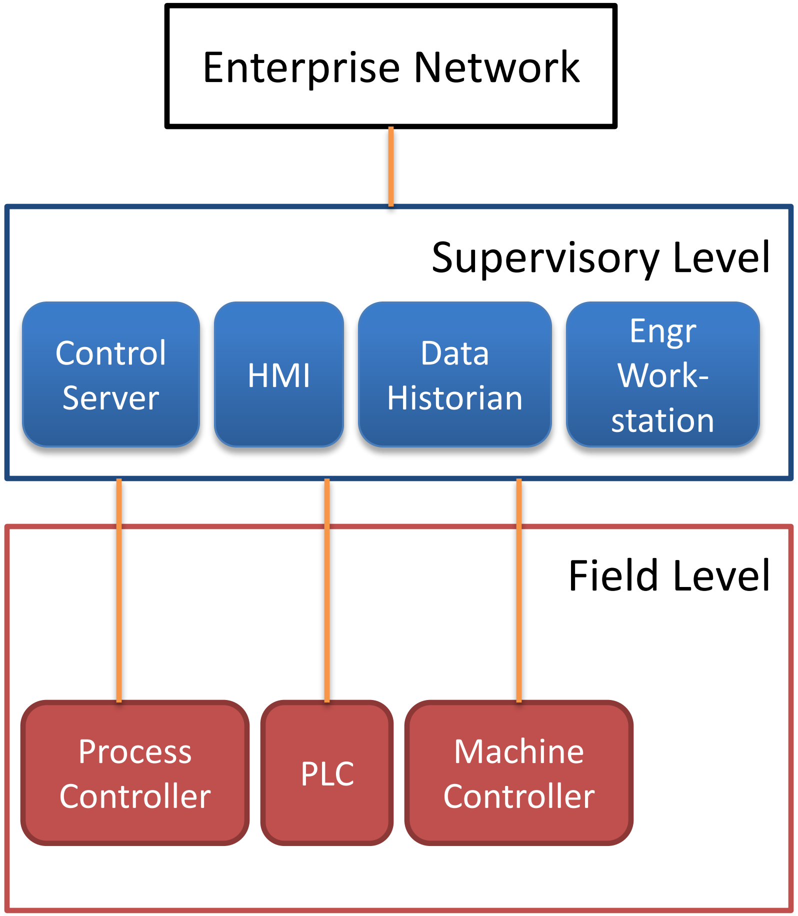
High-level functions:

1. Data Acquisition
2. Networked data communication
3. Data presentation
4. Control

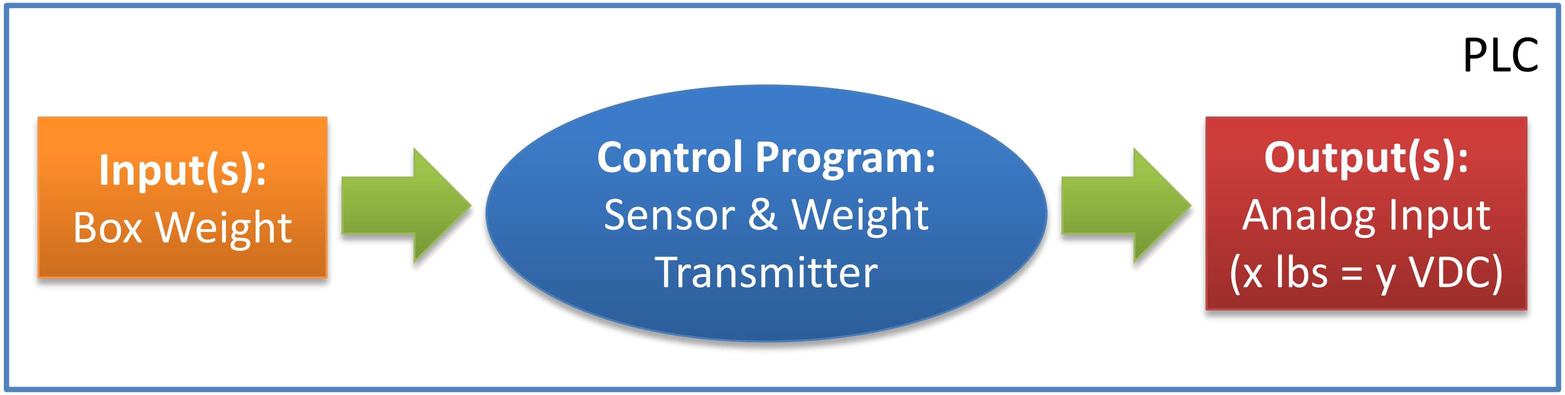
SCADA components:

- Sensors
- Remote telemetry units (RTUs)
- Control center
- Communications network

ICS Overview: Distributed Control Systems Example



ICS Overview: Programmable Logic Controllers Example

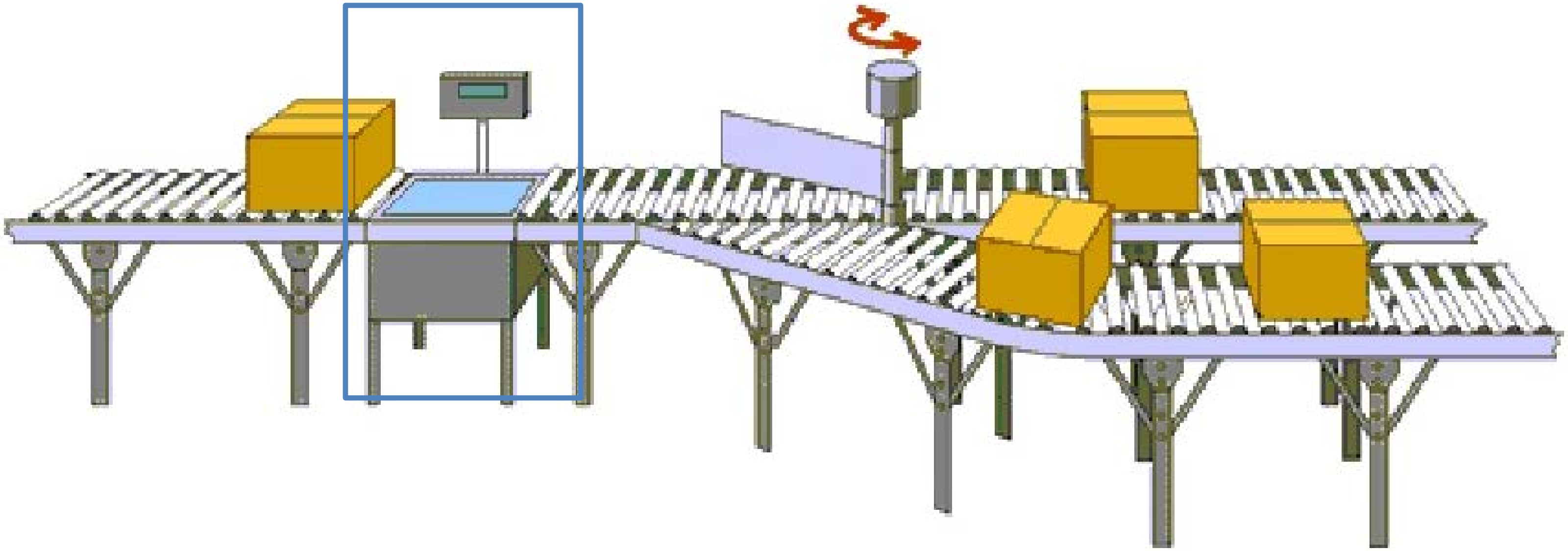


PLC

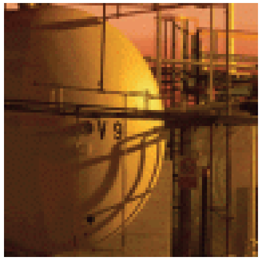
Input(s):
Box Weight

Control Program:
Sensor & Weight Transmitter

Output(s):
Analog Input
(x lbs = y VDC)



Critical Infrastructure Sectors are Interdependent



Chemical

Communications

Dams

IT

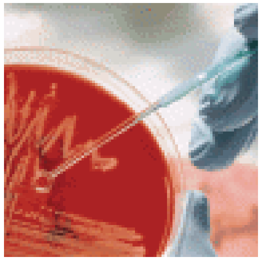
Emergency Services

Critical Manufacturing

Financial Services

Energy

Food & Agriculture



Healthcare

Nuclear

Transportation

ICS Security Considerations

- Performance requirements
- Availability requirements
- Risk Management
- Architecture security focus
- Physical interaction
- Time-critical responses
- System operation

- Resource constraints
- Communications
- Change management
- Managed support
- Component Lifetime
- Access to components

Common Weaknesses Identified in ICS

Rank	CSSP Site Assessment	ICS-CERT Incident Response	CSET Gap Areas
1	Credentials Management	Network Design Weakness	Lack of formal documentation
2	Weak Firewall Rules	Weak Firewall Rules	Audit and Accountability (Event Monitoring)
3	Network Design Weaknesses	Audit and Accountability (Event Monitoring)	Permissions, Privileges, and Access Controls

Data from: Common Cybersecurity Vulnerabilities in Industrial Control Systems, May 2011

Current Initiative: NIST Special Publication 800-82, Revision 2, Guide to Industrial Control Systems Security

- NIST SP 800-82 Rev. 1 published May 15, 2013
  - Updated to include integration of Appendix I ICS material transferred from NIST SP 800-53, Rev. 3 into SP 800-82 Appendix G

- NIST SP 800-82 Rev. 2 major update underway
  - Two drafts for public comment – late summer 2013 and winter 2013
  - Final – spring 2014

NIST SP 800-82, Rev 2

- Updates to ICS threats and vulnerabilities, ICS risk management, recommended practices and architectures, security capabilities and technologies for ICS, additional alignment with other ICS security standards and guidelines

- New tailoring guidance for NIST SP 800-53, Rev. 4 security controls, including the introduction of overlays

- ICS Overlay using NIST SP 800-53 Rev. 4 Controls
    - Provide tailored security control baselines for Low, Moderate, and High impact ICS
    - Will be an Appendix, but could also be used as stand-alone document

NIST SP 800-82 Rev. 2 ICS Overlay

The ICS overlay, which will be an Appendix to SP 800-82 Rev. 2, will consist of 8 sections:

1. Identification
2. Overlay Characteristics
3. Applicability
4. Overlay Summary
5. Detailed Overlay Control Specifications
6. Tailoring Considerations
7. Definitions
8. Additional Information/Instructions

Additional Related NIST Work

- Executive Order 13636, Improving Critical Infrastructure Cybersecurity
  - Cybersecurity Framework
- Smart Grid Program
  - Smart Grid Interoperability Panel Smart Grid Cybersecurity Committee
- Smart Grid Test Bed [In development]
- Cyber-Physical Systems
- Cyber-Physical Systems Test Bed [In development]

Additional Resources for ICS Security

- National Cyber Security Division's Control Systems Security Program (CSSP) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- ISA99, Industrial Automation and Control Systems Security

- National Security Agency, A Framework for Assessing and Improving the Security Posture of Industrial Control Systems

- National Vulnerability Database (NVD)

- Department of Energy Control Systems Security Publications Library

- Idaho National Laboratory Critical Infrastructure Protection Program

- Sandia National Laboratories Center for Control System Security

Questions