CIS 700/002 : Special Topics : Industrial Control Systems

Dagaen Golomb

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

20 January 2017

Industrial Control Systems

Outdated Objectives

- Industrial control systems have traditionally been engineered with efficiency and safety as primary objectives
  - Efficient and safe manufacturing…
  - And electricity generation and distribution…
  - And …
- But what about the *safety* of these systems?

A New Hope

- Recent events have sparked interest is the security of these systems
  - Aurora Generator Experiment
  - Stuxnet
- Along with the move towards more IoT-like control systems
  - Smart Energy Meters

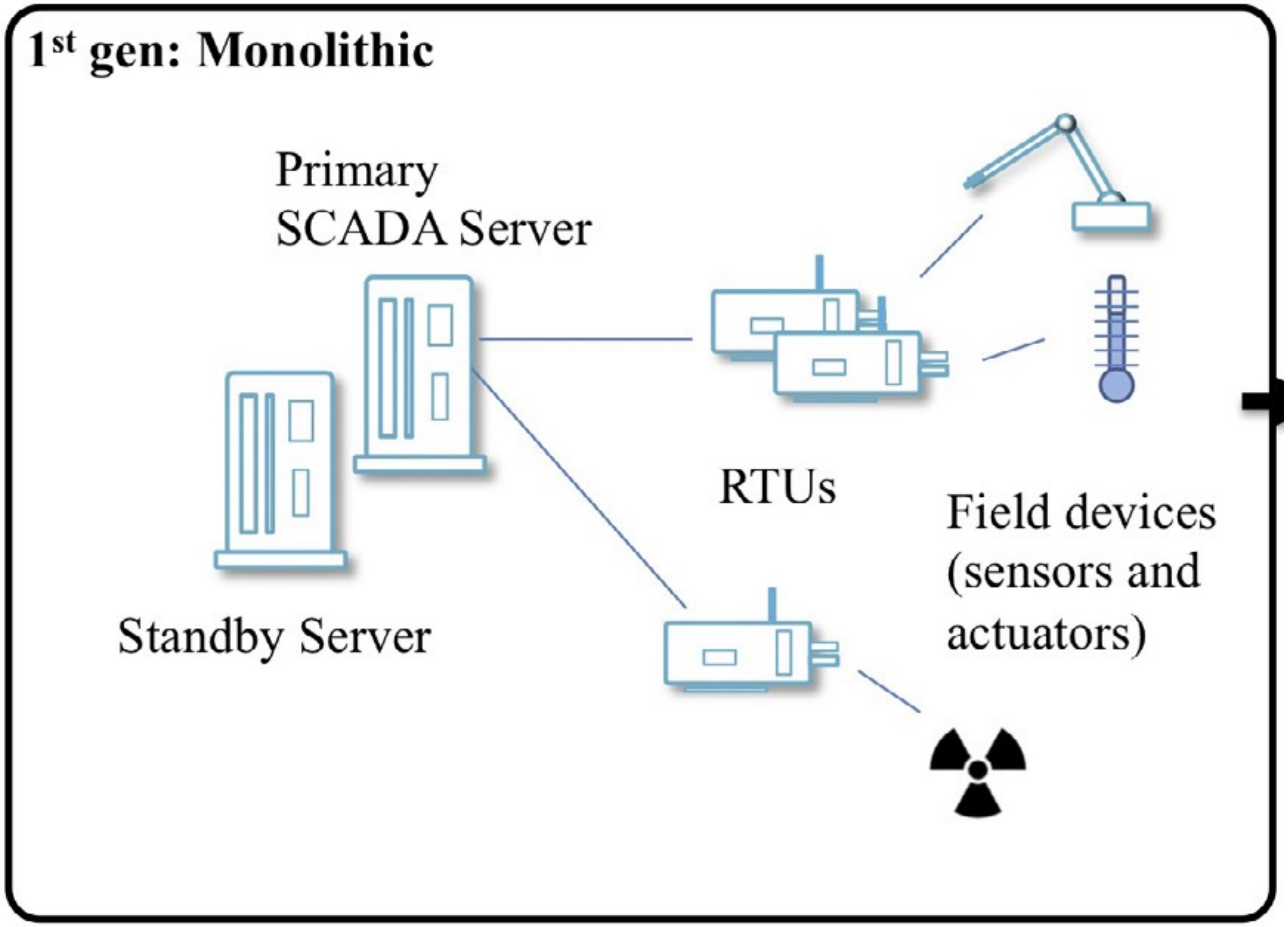
Why Is This Important?

- Industrial control systems run some of our most important systems
  - Electricity, manufacturing
- Have the ability to affect or harm many people (and geographical areas) at once
- Can have national security implications

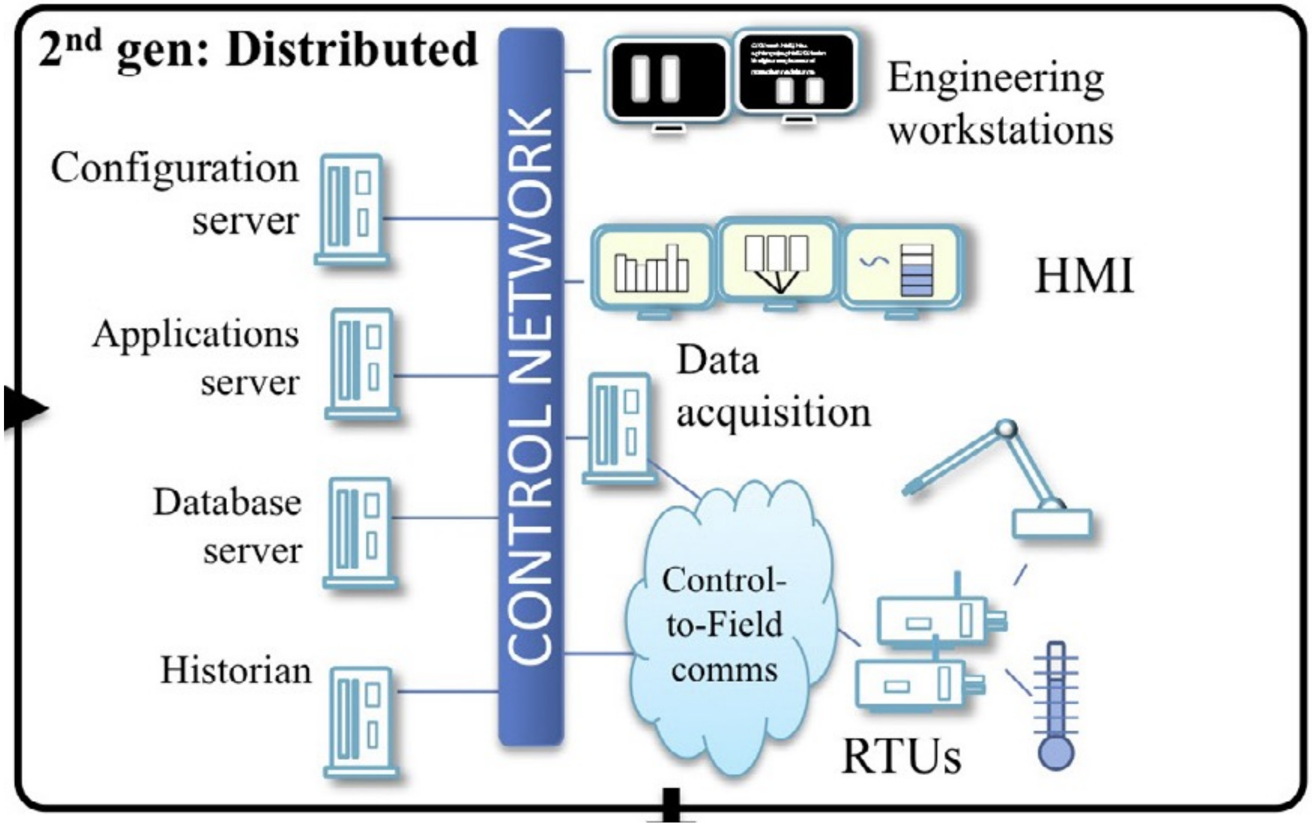
History

- Often referred to as SCADA = supervisory control and data acquisition
- Existed before the 1960's
  - But it was around this time this term evolved to mean computer-controlled systems

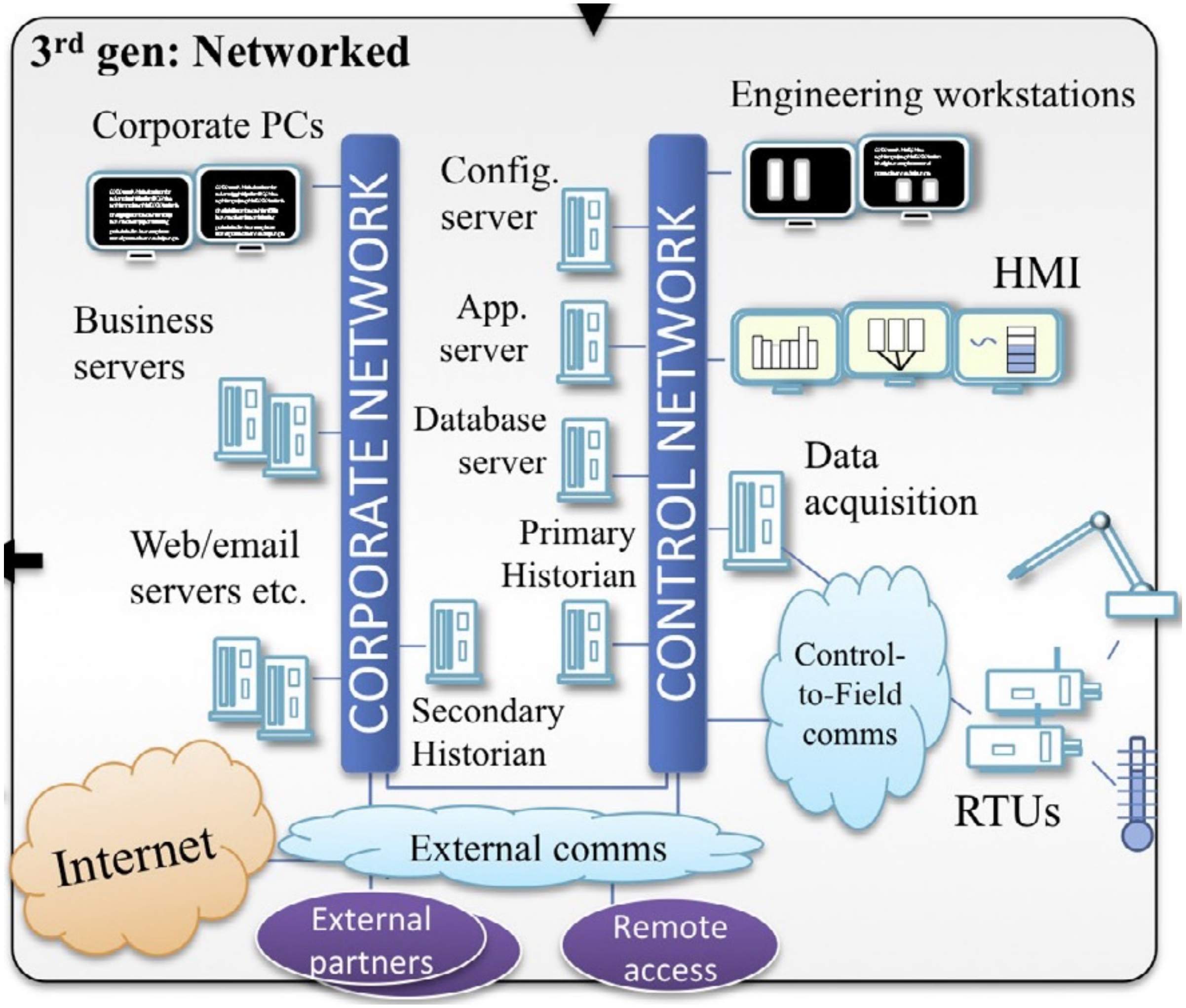
History


1st gen: Monolithic
Primary
SCADA Server
Standby Server
RTUs
Field devices
(sensors and
actuators)

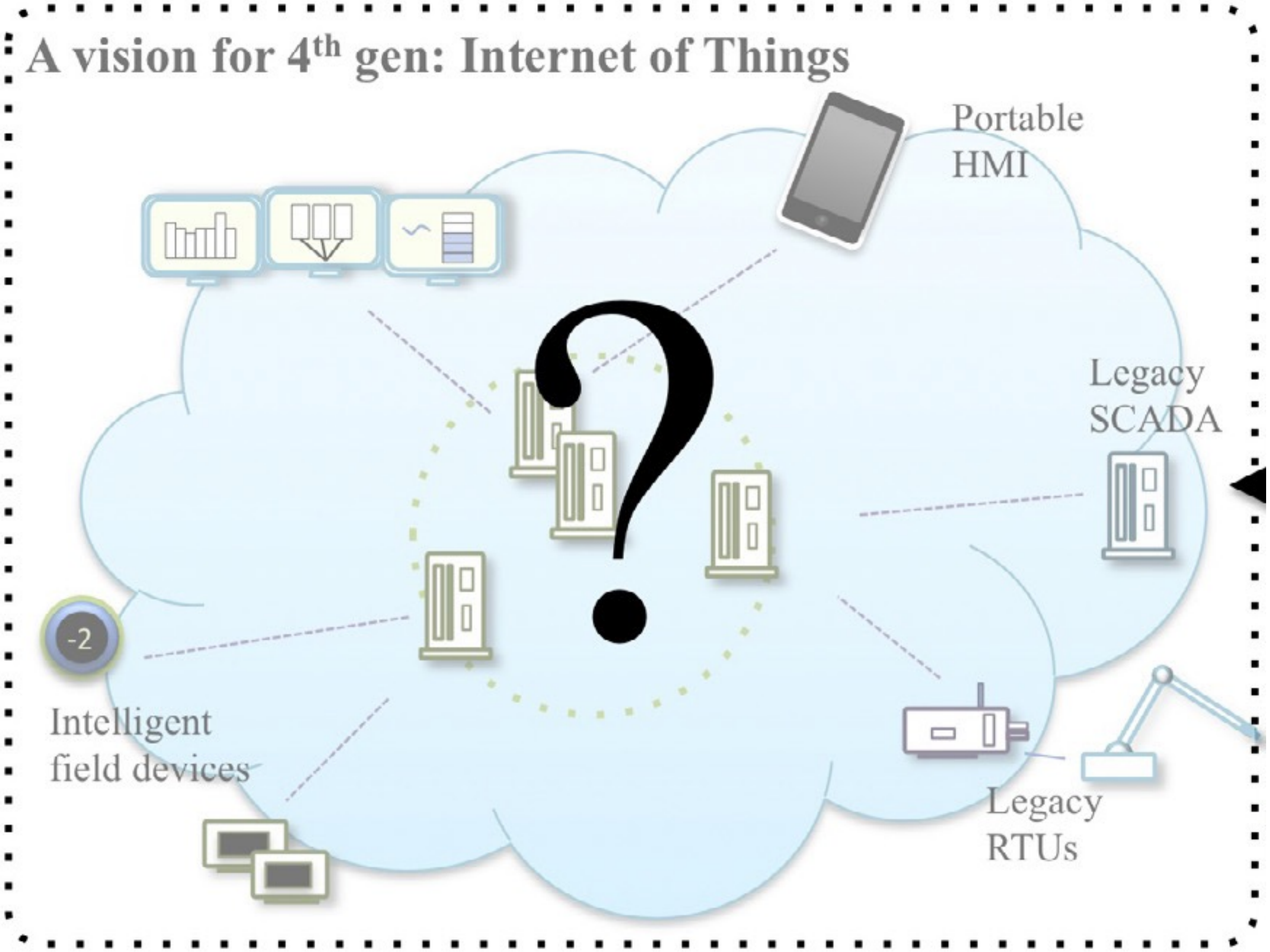
History


2nd gen: Distributed
CONTROL NETWORK
Engineering workstations
Configuration server
HMI
Applications server
Data acquisition
Database server
Control-to-Field comms
Historian
RTUs

History


3rd gen: Networked
Corporate PCs
Business servers
Web/email servers etc.
CORPORATE NETWORK
Config. server
App. server
Database server
Primary Historian
Secondary Historian
CONTROL NETWORK
Engineering workstations
HMI
Data acquisition
Control-to-Field comms
RTUs
Internet
External comms
External partners
Remote access

History


A vision for 4th gen: Internet of Things
Portable HMI
Legacy SCADA
-2
Intelligent field devices
Legacy RTUs
?

Types of Vulnerabilities*

1. Policy and procedure vulnerabilities
2. Platform specific vulnerabilities
3. Network vulnerabilities

Focus will be on #3 as this is the most significant (and new) threat to modern systems

*Breakdown provided by *Guide to Industrial Control Systems Security* by the National Institute of Standards and Technology

Old Protocols: Modbus

- Simple master/slave protocol
  - Very lightweight
  - No timestamps
- Slaves cannot send unsolicited messages
  - Can only respond to master or take an action when master requests

Old Protocols: Modbus TCP

- Allows slaves to communicate concurrently with multiple masters
- Masters can have multiple outstanding connections
- Same lack of security as original Modbus
  - Plus any TCP/IP-related attacks

Modern Protocols

- Distributed Network Protocol v3.0 (DNP3)
  - North America
- IEC 60870-5
  - Similar functionality to DNP3
  - More popular in Europe

Will focus on DNP3

DNP3

- Also Master/Slave (“outstation”)
  - Master sends requests and slaves respond, usually used to poll data anywhere from several times a second to every several minutes
  - Slaves can also initiate communication for *exceptions*, or important events
    - Allows critical event management to be event-driven

DNP3: Limitations

- Still designed for safety instead of security
  - Not uncommon for implementation to lack encryption and authentication

DNP3 Secure Authentication

- Adds authentication
  - addresses a variety of spoofing, unauthorized modification, replay, and eavesdropping attacks
  - Critical events require authentication of message
- No encryption
  - Can still collect data for privacy breeches or future attack reconnaissance

DNP3 + Hierachical SCADA Architecture

- Nodes may be master and slave
  - Master to sensors/actuators
  - But Slave to data aggregator, higher level control, etc.
- These nodes usually buffer outstation data to allow concurrent collection and to batch network traffic
  - Allows attacker to fill buffer with frivolous packets causing drops to legitimate packets

Factors Affecting SCADA Security

- Strict Real-Time Requirements
- Continuous Availability
- Misguided Security Perceptions
- Commercial-off-the-Shelf Hardware and Software
- Interconnectivity
- Internet Accessibility

The Example: Stuxnet

- A sophisticated attack on the Iranian nuclear enrichment facilities
- Commonly referred to as the first major cyber-physical attack
  - Has shocked the industry and created enormous new interest in CPS security

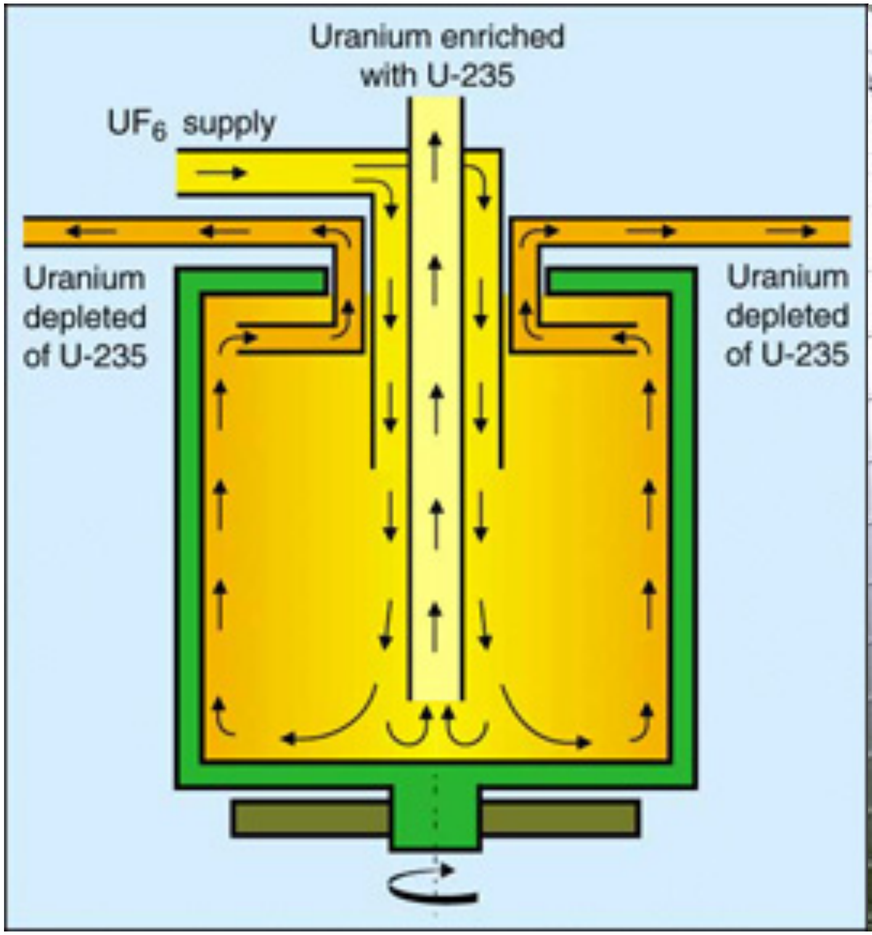
The Seeds of the Problem

- Iranian nuclear programs date back to 1950’s when US and European nuclear powers shared nuclear expertise and equipment to allies
  - Iran’s 1979 revolution came with sudden political alignments
  - Ever since Iran’s nuclear programs have been under heavy watch by the western world under suspicion of Iran’s intent to use in the Middle East for geopolitical leverage

Iran’s Solution

- Iran’s issue: it was no longer being provided enriched Uranium
- Iran now needed to enrich its U-238 to U-235 weapons grade independently
- Iran was provided designs and key components for centrifuges in the 1980’s
  - It is suspected that the same generation of centrifuges were in place during the Stuxnet infection

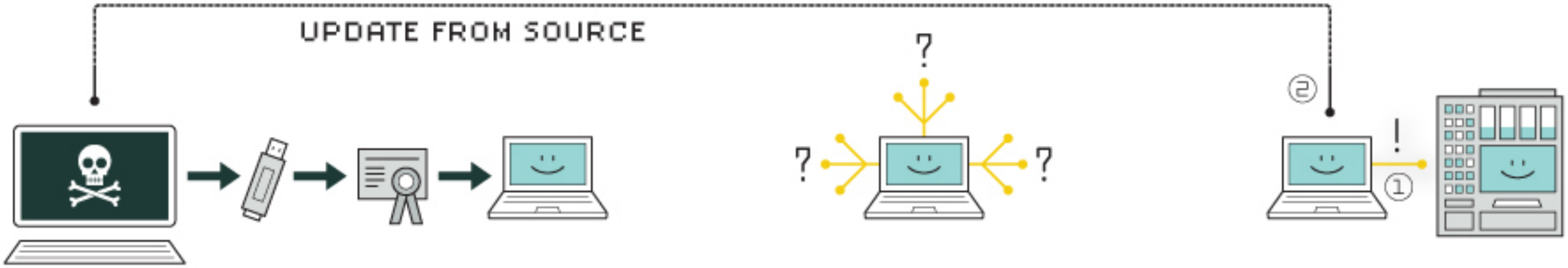
How It Works: Uranium Centrifuge


Uranium enriched with U-235
UF_6 supply
Uranium depleted of U-235
Uranium depleted of U-235

Recall: Iran's Nuclear Knowledge…

- …Was from 1980!
- Centrifuges were notorious for common breakdown
- Iran "fixed" 2 issues
  - In *To Kill a Centrifuge*, Ralph Langner more accurately refers to them as workarounds

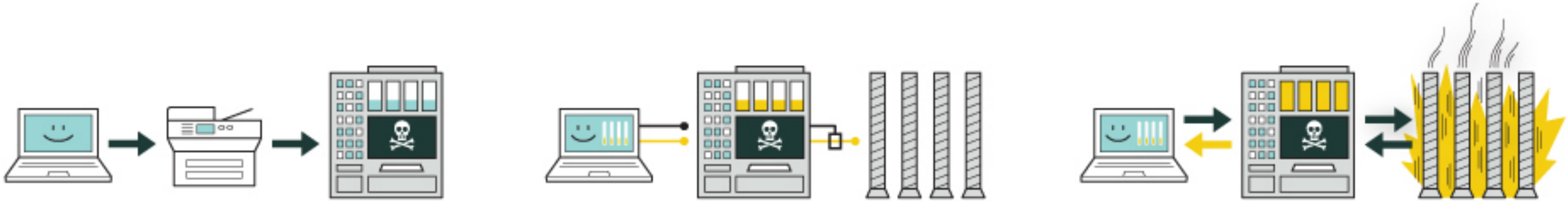
Stuxnet Mechanics



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

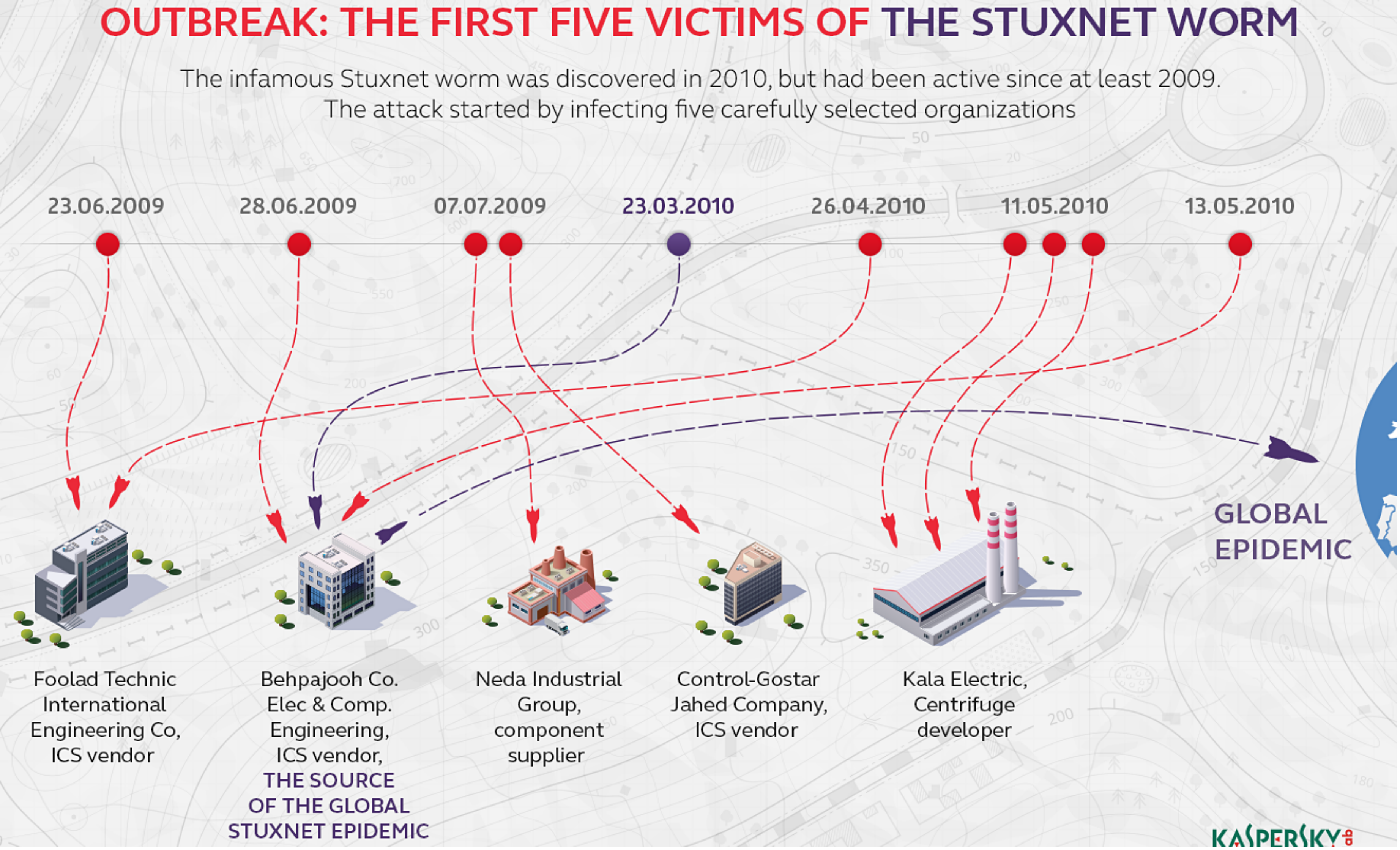
Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Attack Sophistication

- Required knowledge of the type / configuration centrifuges in use and the PLC controlling them; Iran workarounds
- Executed via 4 zero-day exploits
- Carefully selected initial targets
- Stolen digital signatures
- Very targeted: not detrimental to non-targets and included an end-of-life date

Spreading Ability



OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009. The attack started by infecting five carefully selected organizations

Foolad Technic International Engineering Co, ICS vendor

Behpajooh Co. Elec & Comp. Engineering, ICS vendor, THE SOURCE OF THE GLOBAL STUXNET EPIDEMIC

Neda Industrial Group, component supplier

Control-Gostar Jahed Company, ICS vendor

Kala Electric, Centrifuge developer

Impact and Aftermath

- 4 months after discovery, over 100,000 infected – 40% outside of Iran
  - Chevron one example of a US infection
  - Unconfirmed reports of nuclear infections outside of Iran
- Believed to have broken ~1000 centrifuges
  - Not very significant given common failure anyways
  - Iran's enrichment capacity actually slightly increased over infection timeline

Afterthoughts

- Has sparked serious interest in CPS and industrial control security
- Ethical and political considerations: what should (and will) governments do when they discover or buy zero-day exploits?

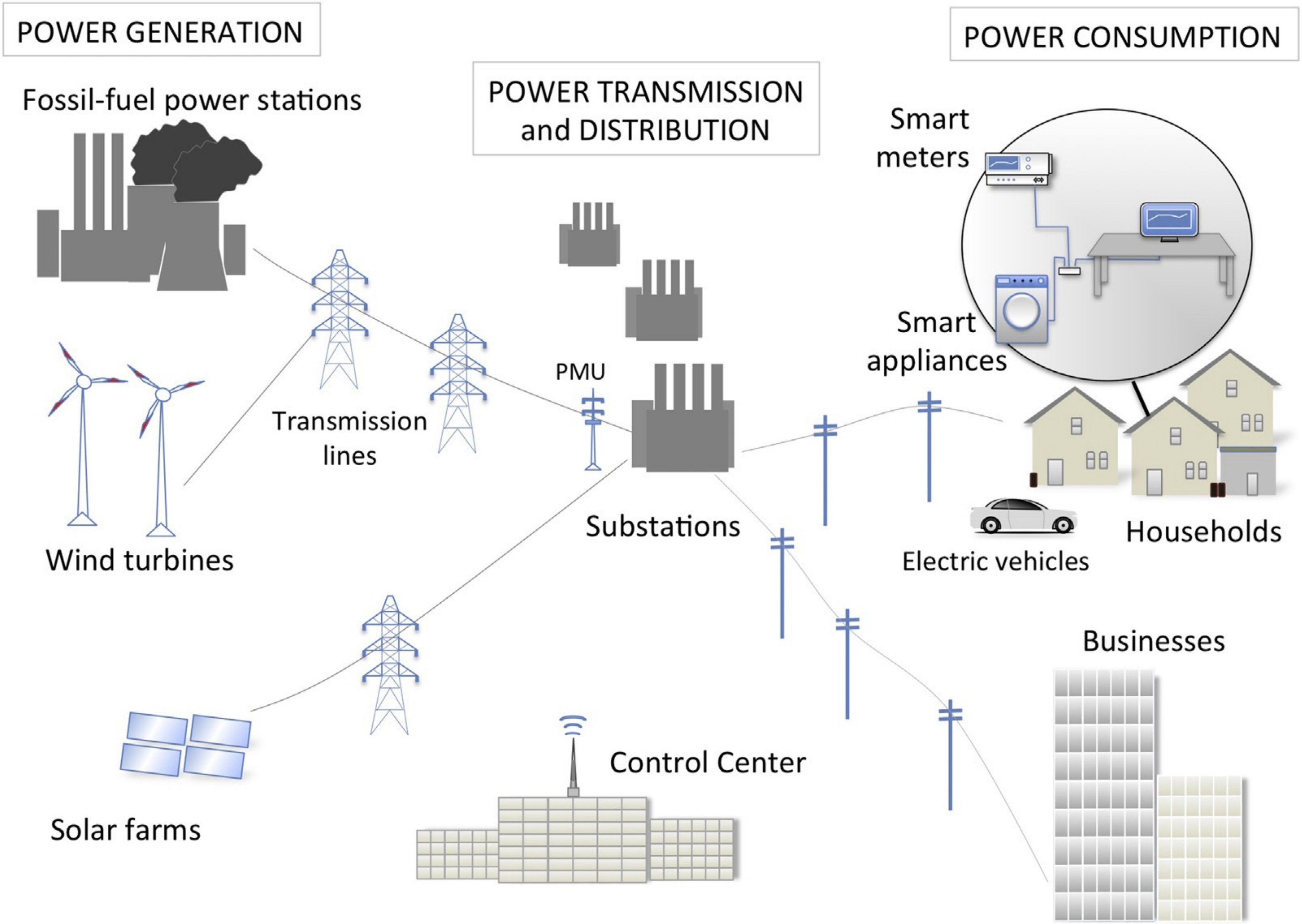
Holy Grail of ICS Attacks: Electricity Grid

- We all depend heavily on electricity
- The US electric grid is made up of just 3 large grids
  - Has been called the “world’s largest engineered system”
- Traditionally more physical, but move towards “smart grid” open up attack possibilities

Aurora Attack

- Experiment showed induced failure of generator by repeatedly cycling it on/off of grid
- Considered a hard/unlikely threat
  - Need insider access or knowledge

Smart Grid



POWER GENERATION

Fossil-fuel power stations

Wind turbines

Solar farms

POWER TRANSMISSION and DISTRIBUTION

Transmission lines

PMU

Substations

Control Center

POWER CONSUMPTION

Smart meters

Smart appliances

Electric vehicles

Households

Businesses

Major Concern: Smart Meters

- Smart meters help to accurately assess use, respond to demand/pricing, etc.
  - EU, US both have ambitious adoption timelines – all homes by 2020
- But introduce threats
  - Metering fraud
  - Privacy concerns
  - Grid Stability Concerns

Other Concerns

- Network delays during times when network needs to react
- Jamming network to cause disturbance or prevent stabilization
- GPS spoofing to hide issues in a particular geographical area

Summary

- ICS/SCALA are vital systems we take for granted
  - Recent attacks hint at the power of these attacks and has provoked great interest in securing these systems
  - And these systems are only becomes *more* networked and "smart"
- Security will have to be a primary goal going forward