Cybersecurity Workshop

Nigel Wright

March 7, 2020
Penn Highlands

http://www.pollev.com/nwright999
Hello!

About Nigel!

➔ **Pittsburgher**
   Grew up south of Pittsburgh in California, PA. Parents are fans of British Rock!

➔ **Breaking Computers Since 1989**
   The best way to fix something is to break it first!

➔ **Working on Robot Cars!**
   Previous roles involved creating product lines for Automated Rail Signaling
Agenda

Hour 1

○ Cyber Security in Industrial Systems
○ System Analysis 101
○ Examples of System Exploits
○ Identifying & dealing with Risks & Vulnerabilities
○ Speed Reading with Program Management Techniques

<10 Minute BREAK>

Hour 2

○ Exercise & Group Work
  ■ Overview of an example of Theoretical Airport Security System Design by generating set of Risks
  ■ Group Exercise
  ■ Group Review of Exercise
How are you feeling today?
Agenda;

Cyber Security in Industrial Systems
System Analysis 101
Examples of System Exploits
Identifying & dealing with Risks & Vulnerabilities
Speed Reading with Program Management Techniques
What is an industrial system?
Industrial Control System (def)

Industrial control system (ICS) is a collective term used to describe different types of control systems and associated instrumentation, which include the **devices**, **systems**, **networks**, and controls used to operate and/or automate industrial processes.
Industrial Control System (def)

Made up of *many* items, each with its own design life, update cycle, and iterations.

Used by highly skilled and non-skilled technicians.

Low -> No Tolerance for Failures
What type of cyber security risks would be present in this system?

- Networking
- Misuse
- Unintended design
- Malware
- Zero-day exploit
- Man in the middle
It depends
Systems engineering is an interdisciplinary field of engineering and engineering management that focuses on how to design and manage complex systems over their life cycles.
What is vulnerable in this diagram?
Agenda;

Cyber Security in Industrial Systems

System Analysis 101

Examples of System Exploits

Identifying & dealing with Risks & Vulnerabilities

Speed Reading with Program Management Techniques
Decomposing a System

Coal-fired power plant

Inputs
- Coal
- Air
- Limestone
- Cooling water

Outputs
- Electricity
- Flue gas (with CO2)
- Gypsum
- Fly ash, bottom ash
- Cooling water
Decomposing System

- Display
- Keypad
- ON/OFF SW
- SIM
- ROM
- Battery
- RAM
- USB
- APPLICATIONs (CPU)
- Baseband Processing and audio/speech processing (DSP)
- DAC
- ADC
- RF Part (Frequency conversion, Power amplification)
- Tx/Rx SW
- BT/GPS
- Speaker
- MIC
- Camera
What is this System?
Agenda:

- Cyber Security in Industrial Systems
- System Analysis 101
- Examples of System Exploits
- Identifying & dealing with Risks & Vulnerabilities
- Speed Reading with Program Management Techniques
Malicious actors vs. Bad Design
Stuxnet

➔ Stuxnet is a malicious computer worm, first uncovered in 2010

➔ Targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program.

➔ Although neither country has openly admitted responsibility, the worm is widely understood to be a jointly built American/Israeli cyberweapon
How did STUXNET get in?

**1. infection**
STUXNET enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By branding itself 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 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.
A COMPUTER VIRUS
STUXNET
STUXNET
2003 Cascading Blackout

- The Northeast blackout of 2003 power outage through United States, and the Canadian

- August 14–28, 2003, beginning just after 4:10 p.m. EDT. Some power was restored by 11 p.m.

- Most did not get their power back until two days later. In other areas, it took nearly a week or two for power to be restored.

- At the time, it was the world's second most widespread blackout in history,
2003 Blackout
What would be your first response?
Tesla Lane Monitoring

➔ Tesla Model S comes with Advanced Lane Assistance Systems with their 2014 release.

➔ Uses the front facing cameras and computer vision system to recognize the lanes.

➔ The system beeps and the steering wheel vibrates, alerting the driver of an unintended lane change.
How do we design against adversarial use?
Agenda:

- Cyber Security in Industrial Systems
- System Analysis 101
- Examples of System Exploits
- Identifying & dealing with Risks & Vulnerabilities
- Speed Reading with Program Management Techniques
As an engineer you need to embrace risk based thinking!

Focus your efforts on those that are most needed!
International Space Station
Probability of No Impacts From a > 1 cm Ø Debris

Impact Risk

Low

High
Everyday elements can be misused, have exploits and present vulnerabilities!
What is this?
Risk: Design Misuse!
What types of screwdriver misuse can you think of?
Marketplace Misuse!
Agenda:

Cyber Security in Industrial Systems
System Analysis 101
Examples of System Exploits
Identifying & dealing with Risks & Vulnerabilities
Speed Reading with Program Management Techniques
Examples of Project's you've worked on?
What is a project?
What is a project?

Large body of work with specific deliverables

Constraints driven
- Basic: Time, Quality, Cost
- 6 (+ Risk, Opportunity, Scope)

Collection of stakeholders
Like it or not, you have all worked on a project in your life?
Waterfall vs. Agile Project Methods

Waterfall:
1. Requirements
2. Design
3. Development
4. Testing
5. Deployment

Big outcome at end

Agile:
1. Test
2. Design
3. Develop
4. Deploy
5. Repeat

Cumulative outcomes
Not all projects are equal!

Some are sprints, some are marathons. The constraints will inform your management approach.
What methodology would you use?

Project:
Create a calorie tracking app for seniors

Constraints:
Duration: 9 Weeks
Budget: $1,000
Quality: 1 Demo with Investors
Which Methodology

Waterfall

Agile
What methodology would you use?

**Project:**
Upgrade existing steel chemistry reporting system

**Constraints:**
*Duration:* 15 Weeks  
*Budget:* $100,000  
*Quality:* 0 Missed Reports for initial production run (100 coils of steel)
Which Methodology PT 2

Agile

Waterfall
Kanban (看板) (signboard or billboard in Japanese) is a scheduling system for lean manufacturing and just-in-time manufacturing (JIT). Taiichi Ohno, an industrial engineer at Toyota, developed kanban to improve manufacturing efficiency. Kanban is one method to achieve JIT. The system takes its name from the cards that track production within a factory.

Kanban became an effective tool to support running a production system as a whole, and an excellent way to promote improvement. Problem areas are highlighted by measuring lead time and cycle time of the full process and process steps. One of the main benefits of kanban is to establish an upper limit to work in process inventory to avoid overcapacity.
Simplified Kanban Board
Kanban & you

WHAT IS KANBAN?
Agenda

Hour 1

- Cyber Security in Industrial Systems
- System Analysis 101
- Examples of System Exploits
- Identifying & dealing with Risks & Vulnerabilities
- Speed Reading with Program Management Techniques

<10 Minute BREAK>

Hour 2

- Exercise & Group Work
  - Overview of an example of Theoretical Airport Security System Design by generating set of Risks
  - Group Exercise
  - Group Review of Exercise
Airport Control System - System Decomp
Airport Control System - Risk Generation

1. Identify the risk factors
2. Who can be harmed and how
3. Evaluate the risks
4. Record your findings
5. Monitor & review

Management Standards
## Airport Control System - Kanban Risk Priority

<table>
<thead>
<tr>
<th>Stories</th>
<th>To do</th>
<th>In progress</th>
<th>Test</th>
<th>Done</th>
</tr>
</thead>
</table>

![Kanban Board Diagram](image)
Airport Control System - Kanban Risk Mitigations