Cybersecurity Workshop

http://www.pollev.com/nwright999

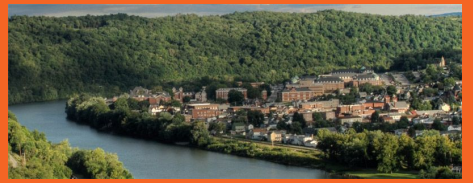
Nigel Wright

March 7, 2020
Penn Highlands

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

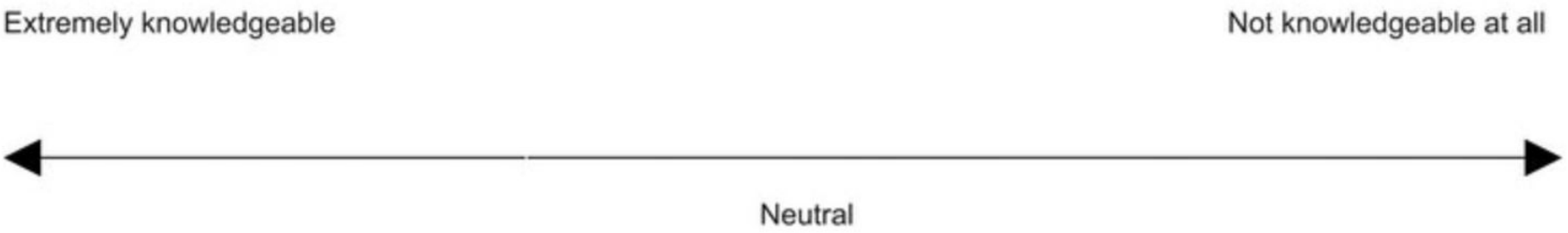
How are you feeling today?

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?

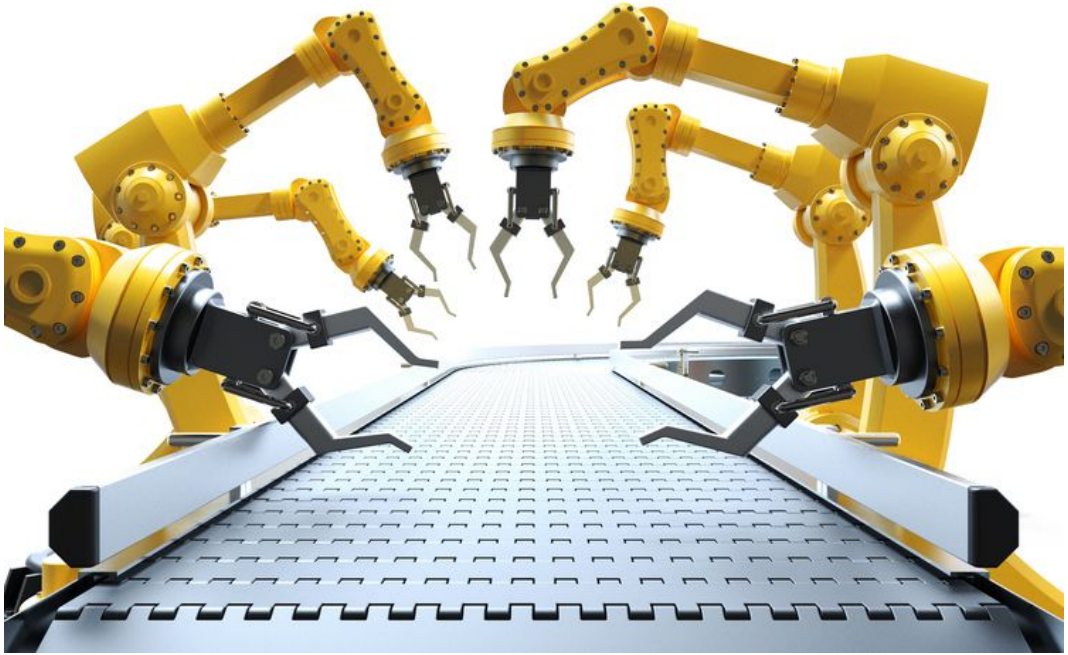
Knowledge of Industrial Systems?



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 it's own design life, update cycle, and iterations.

Used by highly skilled and non skilled technicians.

Low -> No Tolerance for Failures


< 3.5 minutes frequency

What type of cyber security risks would be present in this system?

Networking

Misuse

Unintended design

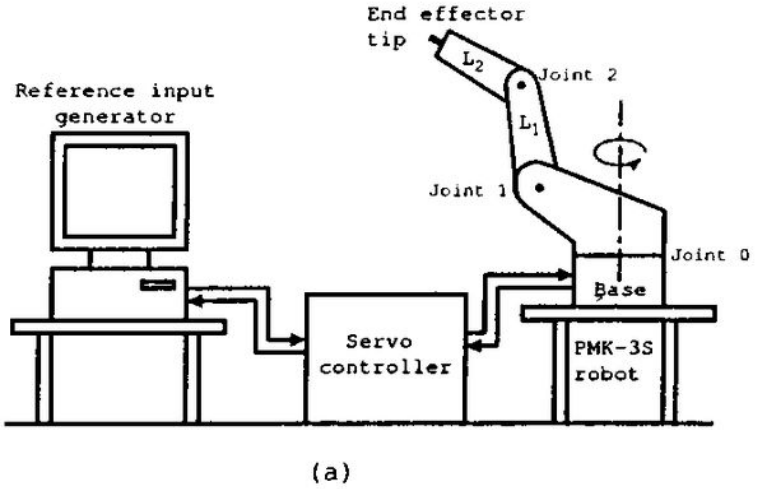
Malware

Zero-day exploit

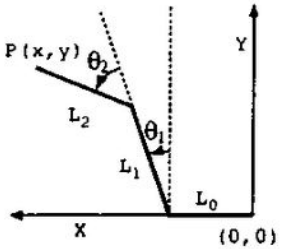
Man in the middle

It depends

Systems Engineering



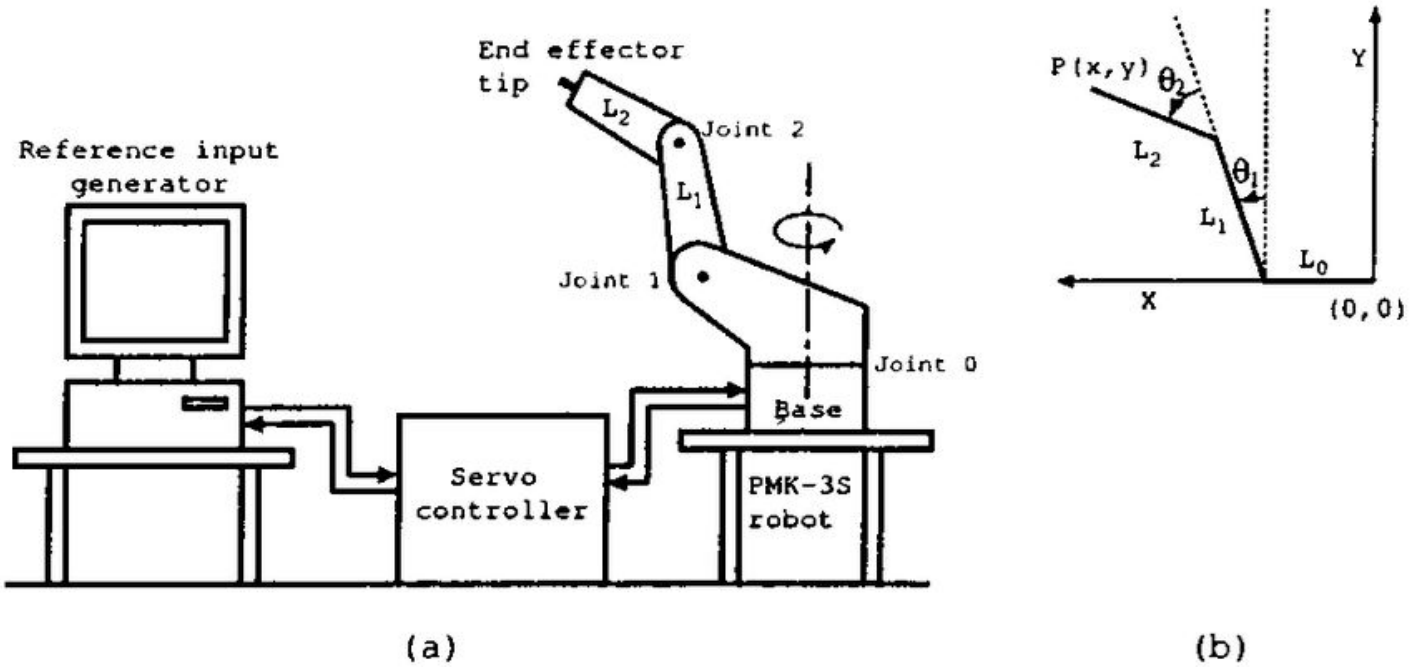
(a)



(b)

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.

Systems Engineering & Cybersecurity



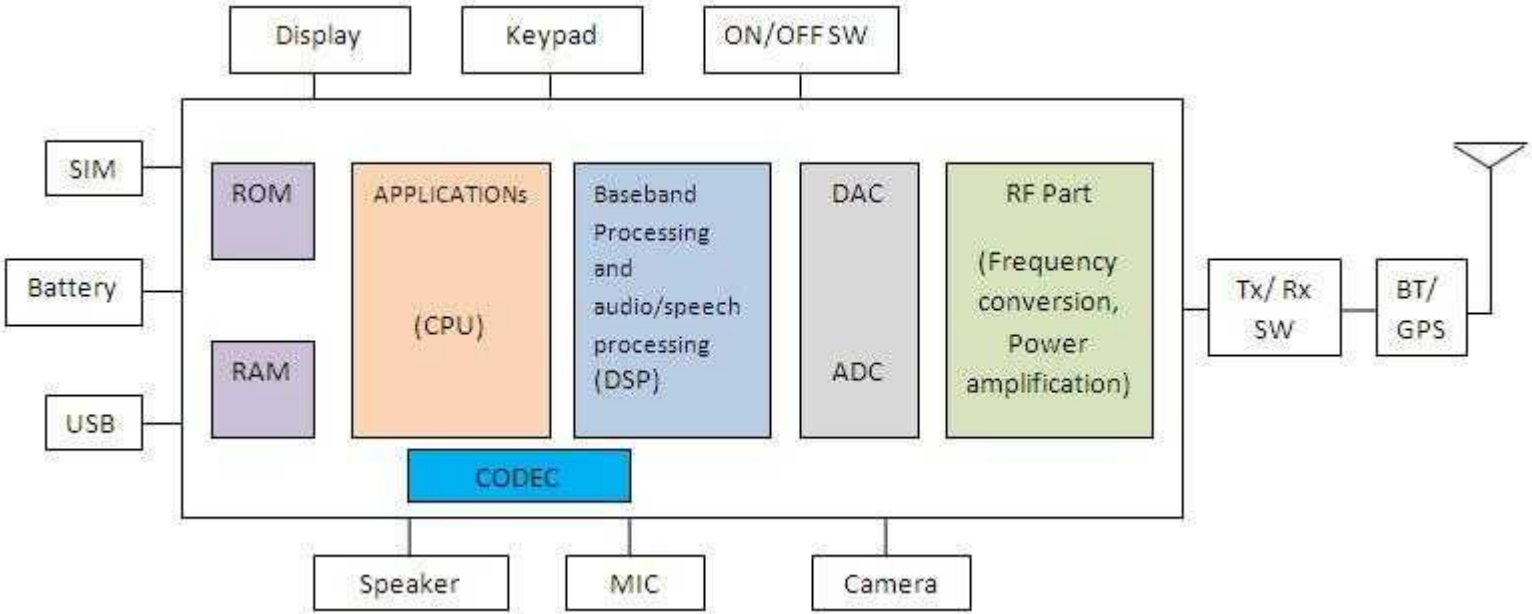
What is vulnerable in this diagram?

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

Decomposing System



What is this System?

Agenda;

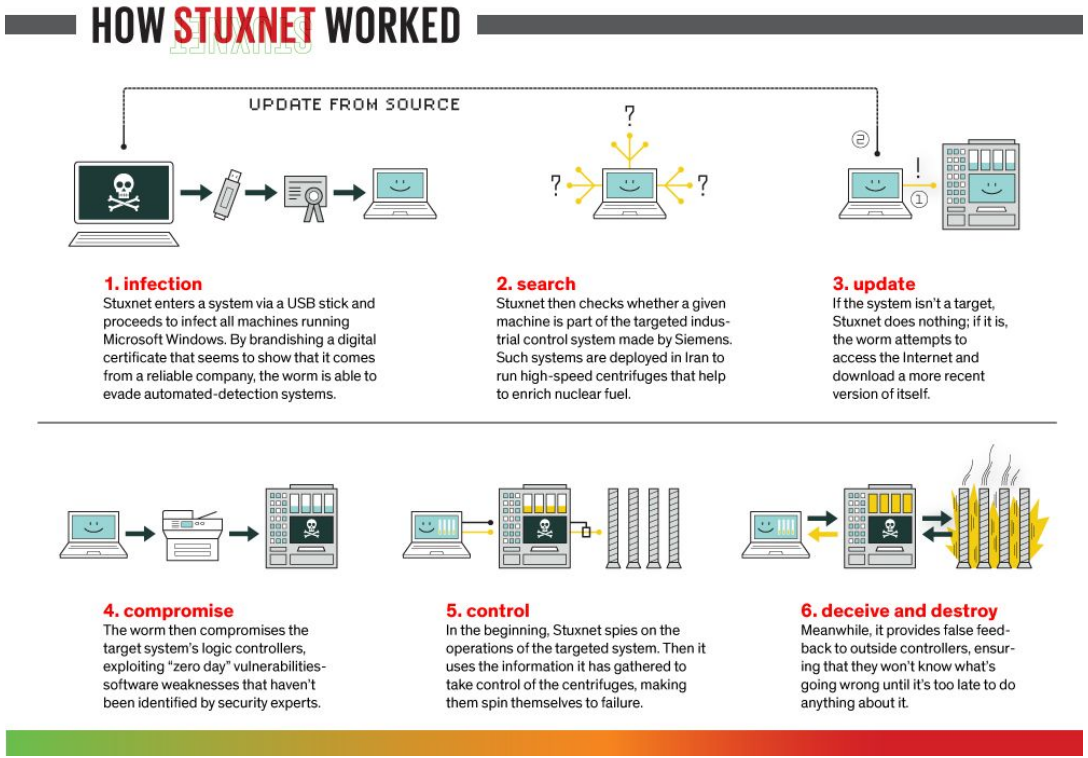
Cyber Security in Industrial Systems
System Analysis 101
Examples of System Exploits
Identifying & dealing with Risks & Vulnerabilities
Speed Reading with Program Management Techniques

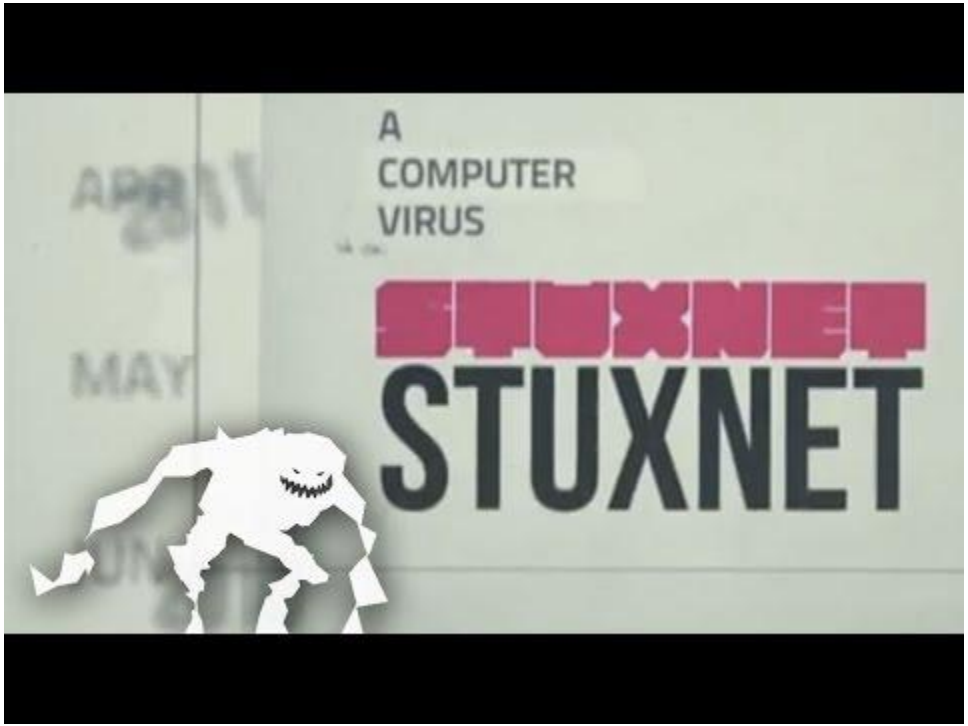
Malicious actors vs. Bad Design

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?



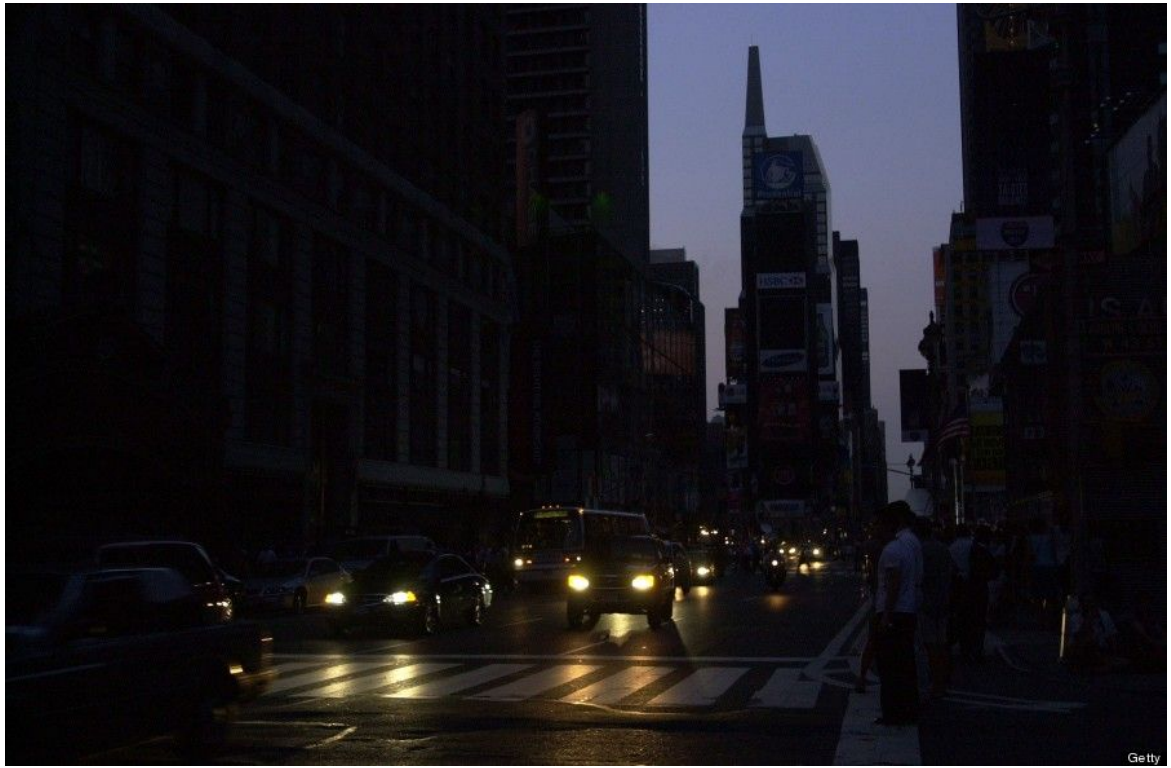

A
COMPUTER
VIRUS
STUXNET
STUXNET

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 vibrate, alerting the driver of an unintended lane change.

How do we design against adversarial use?

Agenda;

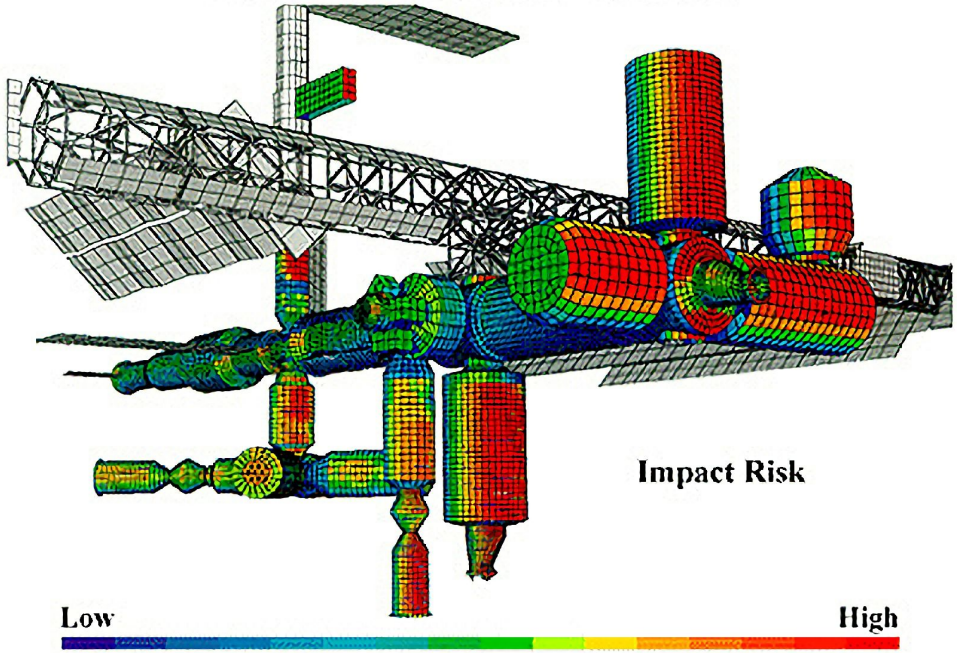
Cyber Security in Industrial Systems
System Analysis 101
Examples of System Exploits
Identifying & dealing with Risks & Vulnerabilities
Speed Reading with Program Management Techniques

As an engineer you need to embrace risk based thinking!

Focus your efforts on those that are most needed!

International Space Station

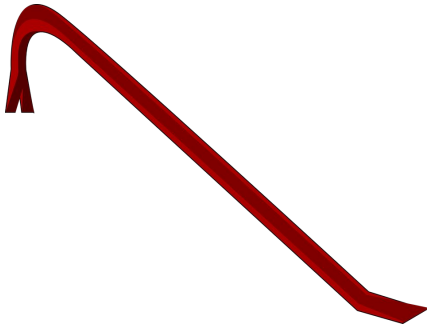
Probability of No Impacts From a > 1 cm Ø Debris



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?

Program Management 101

What is a project?

What is a project?

Large body of work with specific deliverables

Constraints driven

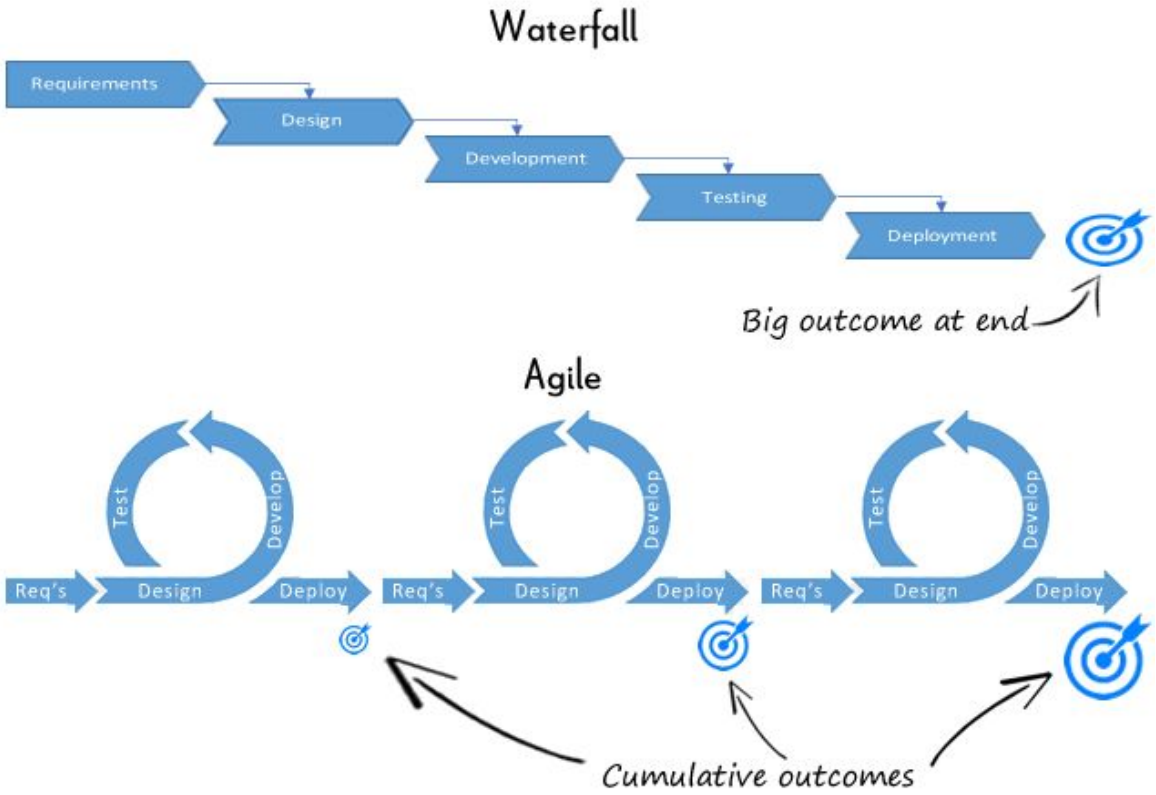
Basic; Time, Quality, Cost

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



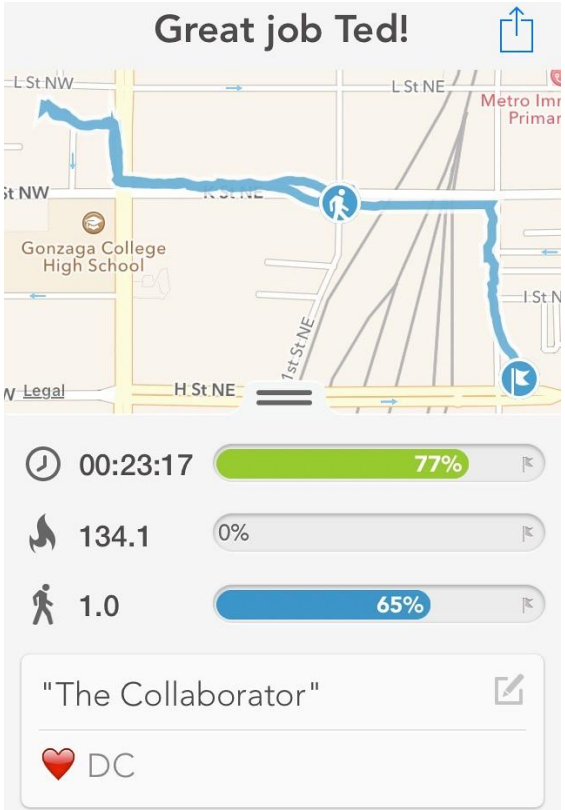
Not all projects are equal!

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

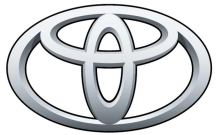
Agile

Waterfall

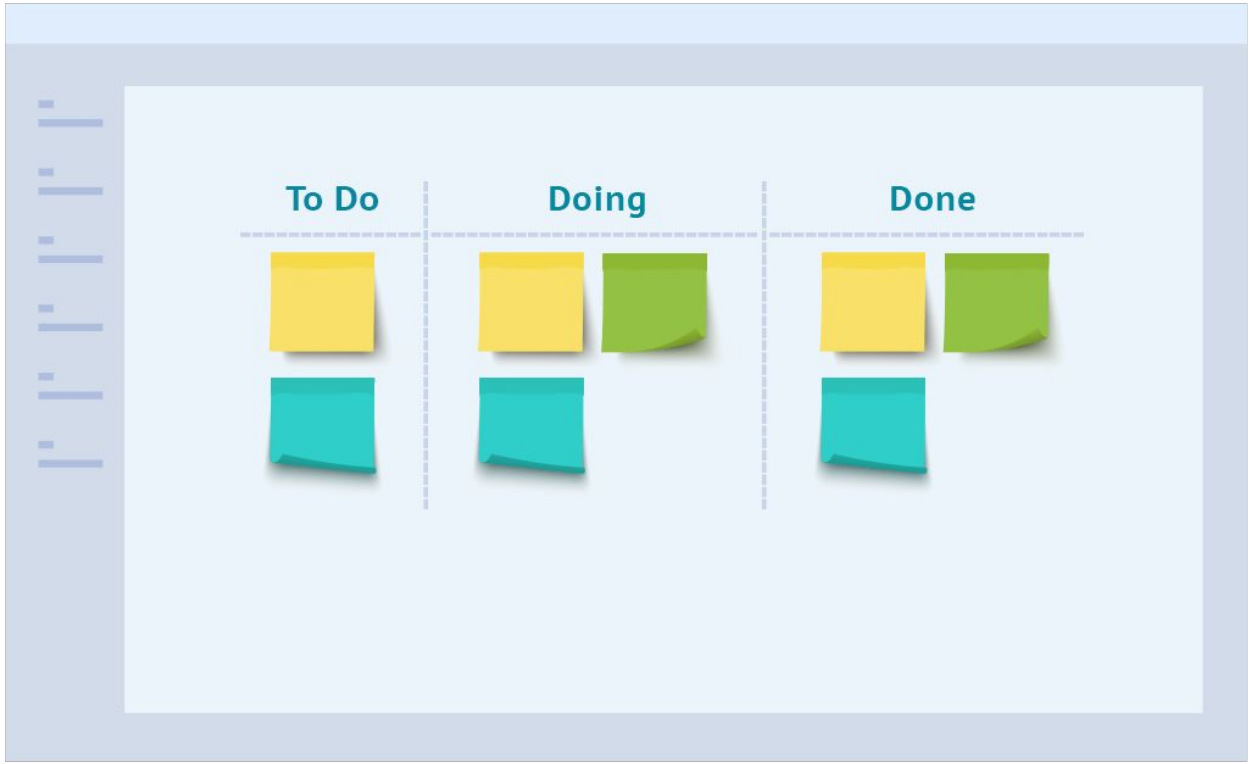
Kanban

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

Agenda

~~Hour 1~~

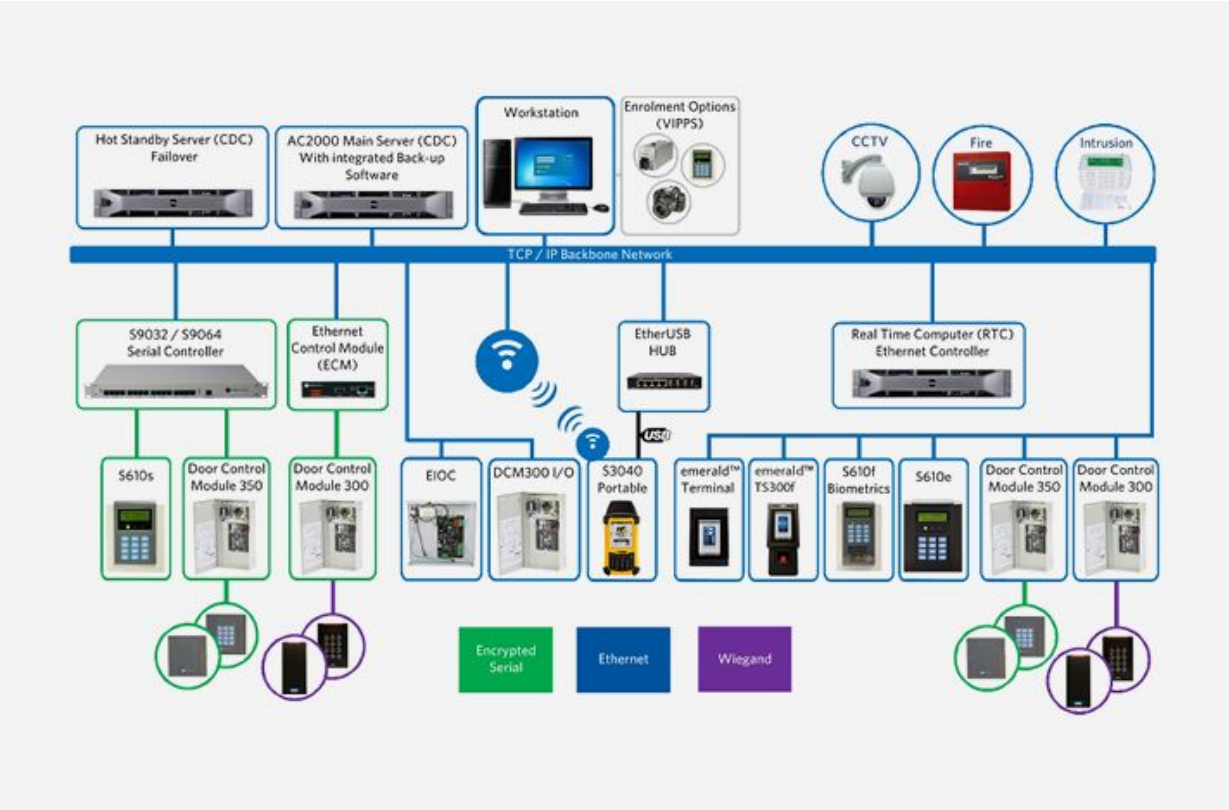
- ~~Cyber Security in Industrial Systems~~
- ~~System Analysis 101~~
- ~~Examples of System Exploits~~
- ~~Identifying & dealing with Risks & Vulnerabilities~~
- ~~Speed Reading with Program Management Techniques~~

~~<10 Minute BREAK>~~

Hour 2

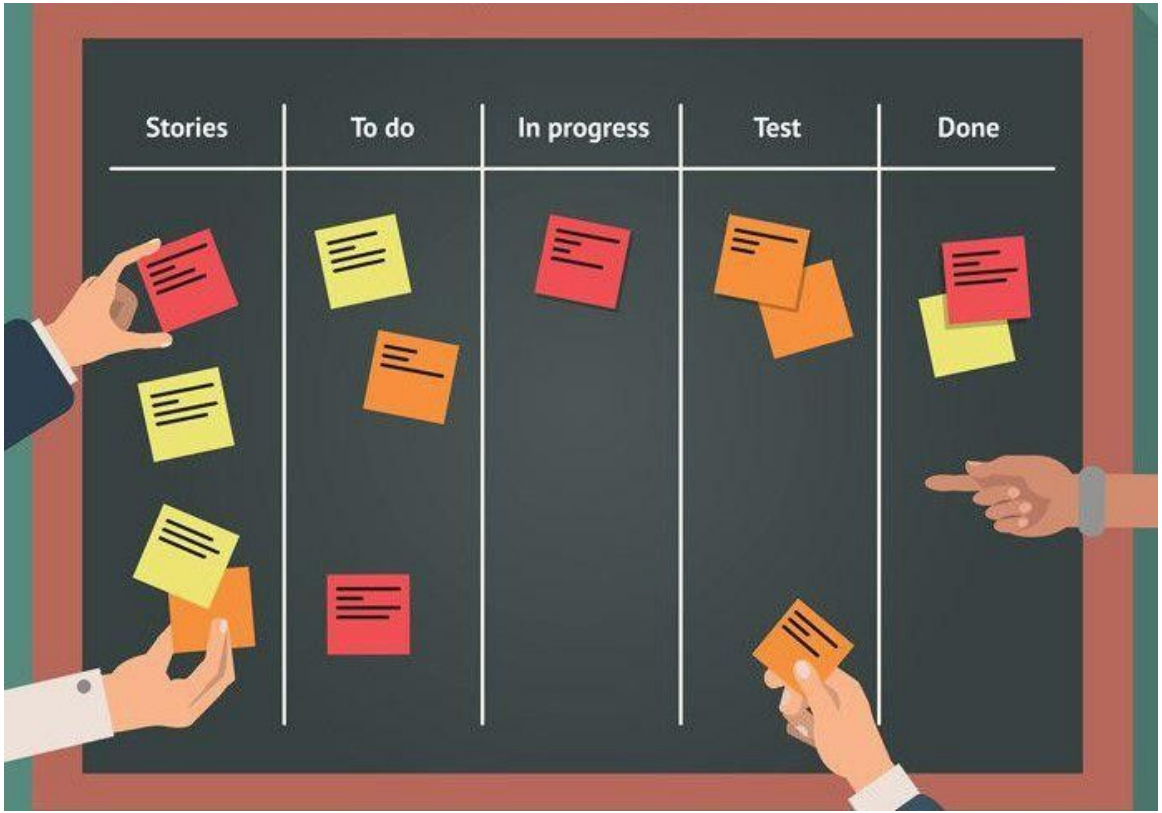
- Exercise & Group Work
  - Overview of an example of Theoretical Airport Security System Design by generating set of Risks
  - Group Exercise
  - Group Review of Exercise

Airport Control System - System Decomp



Airport Control System - Risk Generation

Airport Control System - Kanban Risk Priority



Airport Control System - Kanban Risk Mitigations