

# Applying ICS Cyber Security Principles to Health Care

Mike Ahmadi

*Director Of Business Development*



***Protecting Mission Critical Devices***

# Agenda

- State of The Industry
- Comparing ICS to Health Care
- Core Security Principles
- Solutions and Opportunities

## State of The Industry

- Blackhat Hacks
- GAO Report
- FDA Stepping Up
- Media Blitz

# Control Systems

- **Definition of Control System:** A device, or set of devices to manage, command, direct or regulate the behavior of other device(s) or system(s).
  
- **Types Of Control Systems:**
  - **Logic Controller** – Sequenced events
  - **On-Off Controller** – Responds to event
  - **Linear Controller** – Maintains acceptable range

Source: Wikipedia ([http://en.wikipedia.org/wiki/Control\\_system](http://en.wikipedia.org/wiki/Control_system))

## NIST SP 800-82 Table 3.1

Category	IT System	Health Care System
<b>Risk Management Requirements</b>	Fault tolerance is less important – momentary downtime is not a major risk	Fault tolerance is essential, even momentary downtime may not be acceptable
<b>System Operation</b>	Systems are designed for use with typical operating systems	Differing and possibly proprietary operating systems, often without security capabilities built in
<b>Resource Constraints</b>	Systems are specified with enough resources to support the addition of third- party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
<b>Communications</b>	Standard communications protocols	Many proprietary and standard communication protocols
<b>Component Lifetime</b>	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years

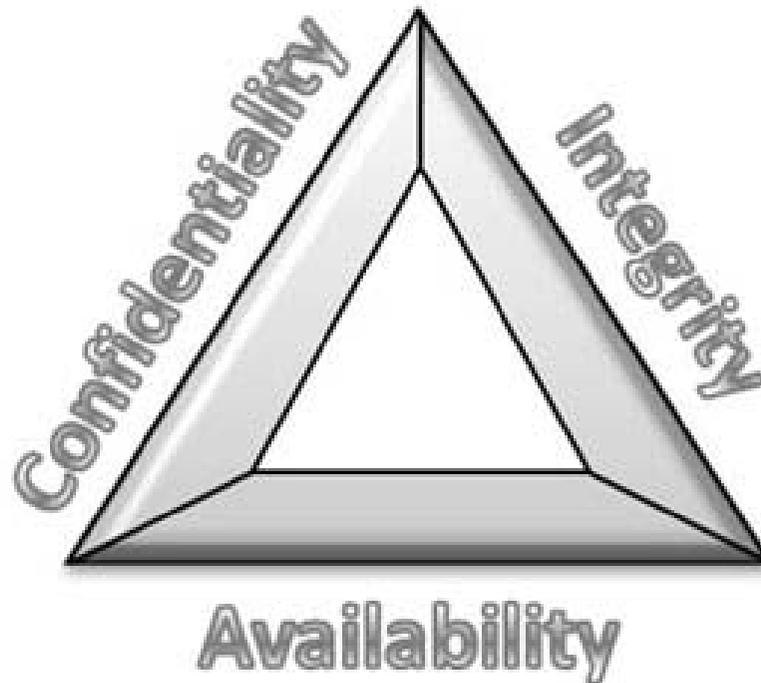
## Examples

- **Logic Controller** - Dialysis
- **On-Off Controller** – Defibrillator, Insulin Pump, Neuro Stimulator
- **Linear Controller** – Pacemaker, Insulin Pump, Infusion Pump, Ventilator

**The system being controlled is human life.**

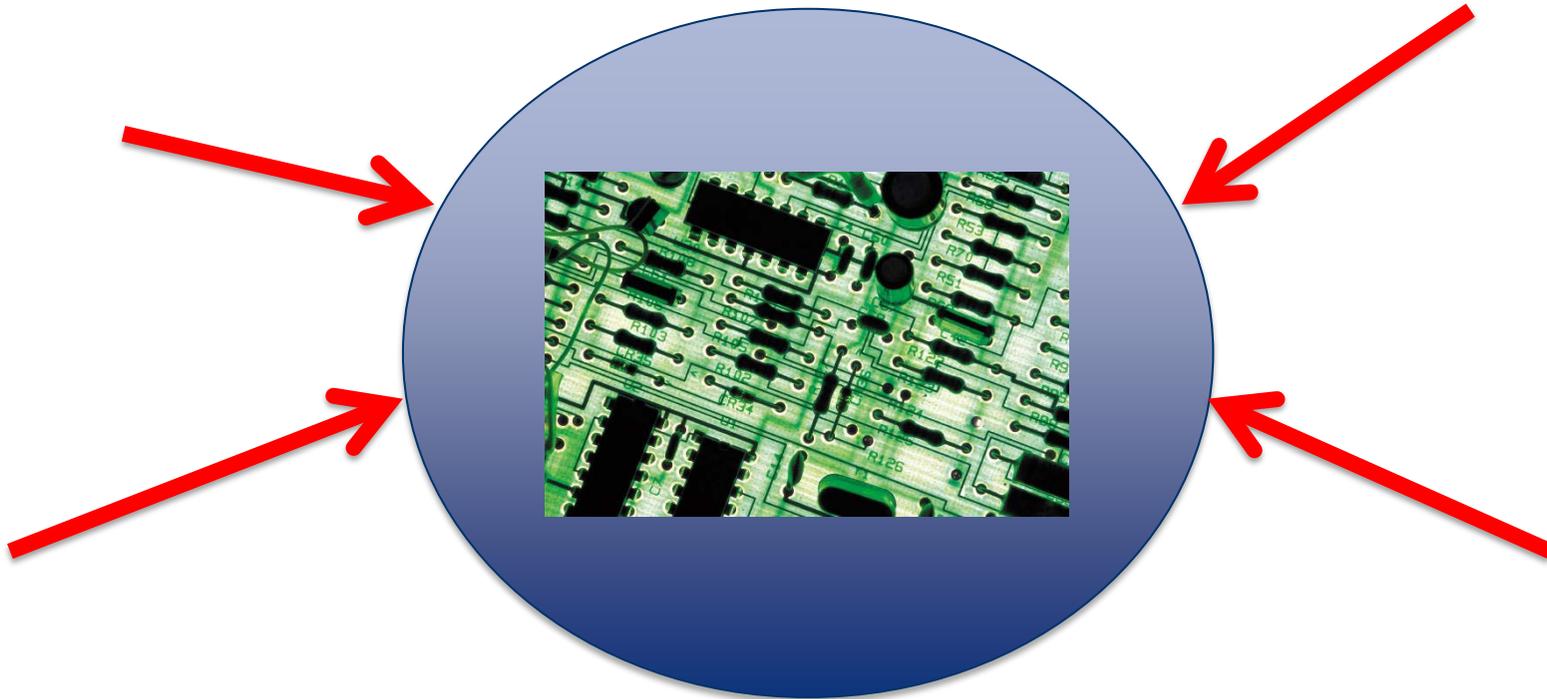
## Core Cybersecurity Principles

- The classic “CIA” triad of Confidentiality, Integrity, Availability
- How is this prioritized in ICS?



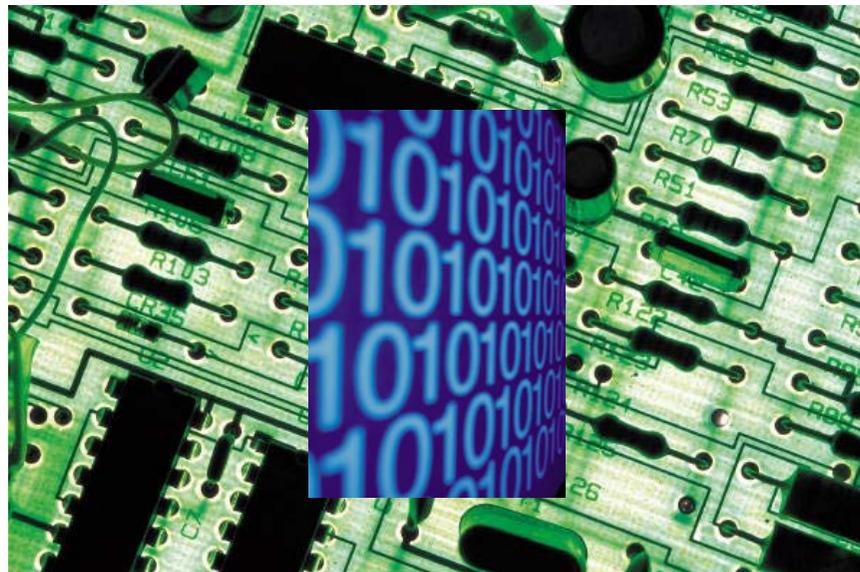
## Availability

- The system must always work no matter what.
- Ability to defend against any denial of service (DOS) attack.
- Robustness testing takes top billing.



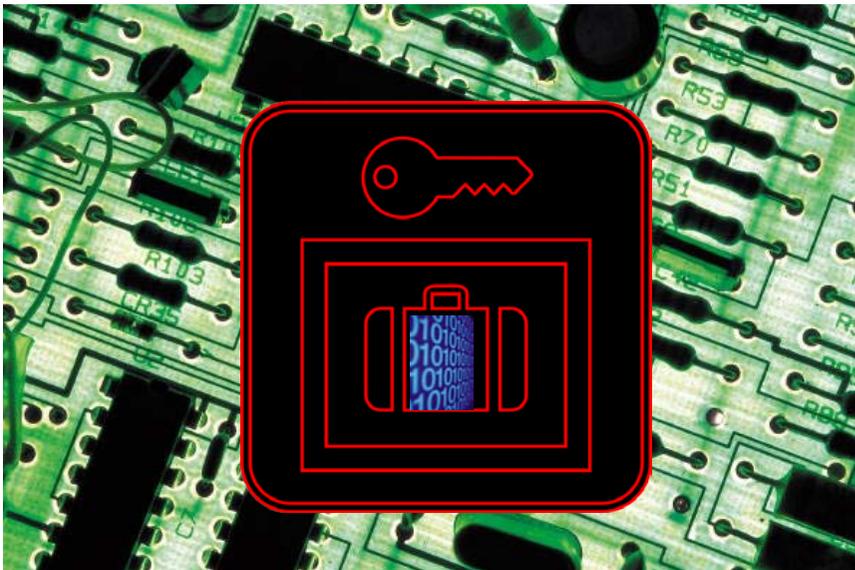
# Integrity

- Data must be correct
- Changes must be authorized



# Confidentiality

- Proprietary information kept secret.
- Where does confidentiality matter?
- Is privacy a concern?



## There Is A Bias

- **Availability** and **Integrity** are of paramount importance.
- **Confidentiality** is often a secondary concern in most ICS applications.
- **Confidentiality** is LEGALLY MANDATED in Health Care.

**Do regulatory considerations affect practical considerations?**

## Authentication and Availability

- Authentication can affect availability
- What happens if authentication fails?
  - Is there a “Plan B”?
  - How do you prevent “Plan B” from being misused?
- System constraints that need to be considered:
  - Power
  - Speed

## Authentication – Integrity and Confidentiality

- Authentication can help maintain integrity.
- It is important to know how the identity is attached to “authentic” data.
- Improperly implemented identity can be attached to the wrong data.
- Implementation flaws can lead to a system that can be made to ignore authentication.
- Authentication of user (person or system process) can insure confidentiality.
- Improperly implemented authentication/identity can allow a user to spoof another user.

# Encryption

- Encryption may affect availability.
- Encryption/Decryption requires additional resources (such as power and \$\$\$)
- The key must be stored in a secure environment.
- Is the key universal (break once, break everywhere)?
- Certificates/Keys require management systems.
- Revocation must also be managed.

## Intrusion Protection/Detection

- Can a traditional IPS be used on health care systems?
  - For networked large devices in hospitals – yes
  - For home health care systems – yes
  - For embedded/worn devices – no
- Embedded and worn devices need special consideration.
  - Embedded IPS at the device level
- Whitelisting?
  - For networked large systems – yes
  - Not easily accomplished on small RTOS based devices

## Data Diodes

- Can be quite beneficial for getting data out of a system where high security may be critical.
- Can protect integrity of connected critical care systems.
- Embedded and worn systems - ?

# Patching

- Patching affects availability
  - Patch can fail
  - Patching requires power
  - Managing patching of embedded devices is quite challenging
  
- FDA Regulatory Issues
  - Security patches are permitted
  - Changes in functionality, safety, effectiveness must be submitted
  - Rigorous validation required in all cases
  - Changes not submitted to FDA always present high risk to device manufacturers

## Opportunities To Address Health Care Security

- Similarities between ICS and Health Care security challenges mean we have a great opportunity to offer expertise to an industry that is in need of assistance.
- Vendors of IPS systems can design systems to address vulnerabilities specific to health care environments.
- ICS security experts can provide training to health care organizations and device manufacturers.
- Tools used to build secure ICS systems can be modified to build secure Health Care Systems and Devices.

## Questions ?



Mike Ahmadi –  
[Mahmadi@Wurldtech.com](mailto:Mahmadi@Wurldtech.com)  
925-413-4365

**Wurldtech Security Technologies**

Suite 1000 – 1090 West Georgia Street

Vancouver BC Canada V6E 3V7

T 604 669 6674

F 604 669 2902

[info@wurldtech.com](mailto:info@wurldtech.com)

**Wurldtech Security BV**

Parkstraat 83

Den Haag, The Netherlands 2514 JG

T +31 70 3538 177

F +31 70 3538 299

