Cyber Security Framework for Manufacturing

Nancy Cam-Winget
Cisco Systems Inc.

October 14, 2015

Why A Security Framework?

Vulnerabilities published at the rate IoT devices are introduced:

http://www.pcworld.com/article/2472772/your-living-room-is-vulnerable-to-cyber-attacks.html

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

DHS: Industrial control systems subject to 200 attacks in 2012

Exclusive: FBI warns of 'destructive' malware in wake of Sony attack

How do I build a Secure Industrial System?

The Washington Times NEWS OPINION VIDEO SPORTS LIFE MEDIA

TRENDING: NFL AL QAEDA CONGRESS FOOTBALL GREEN BAY PACKERS

EDITORS' PICKS: Pilot reports UFO around London's Heathrow Airport

HOME ▸ NEWS ▸ NATIONAL RADIO LOG IN WEE

TARGET credit card theft swells to 40 million victims

COMMENT(S) SIZE: + / - PRINT

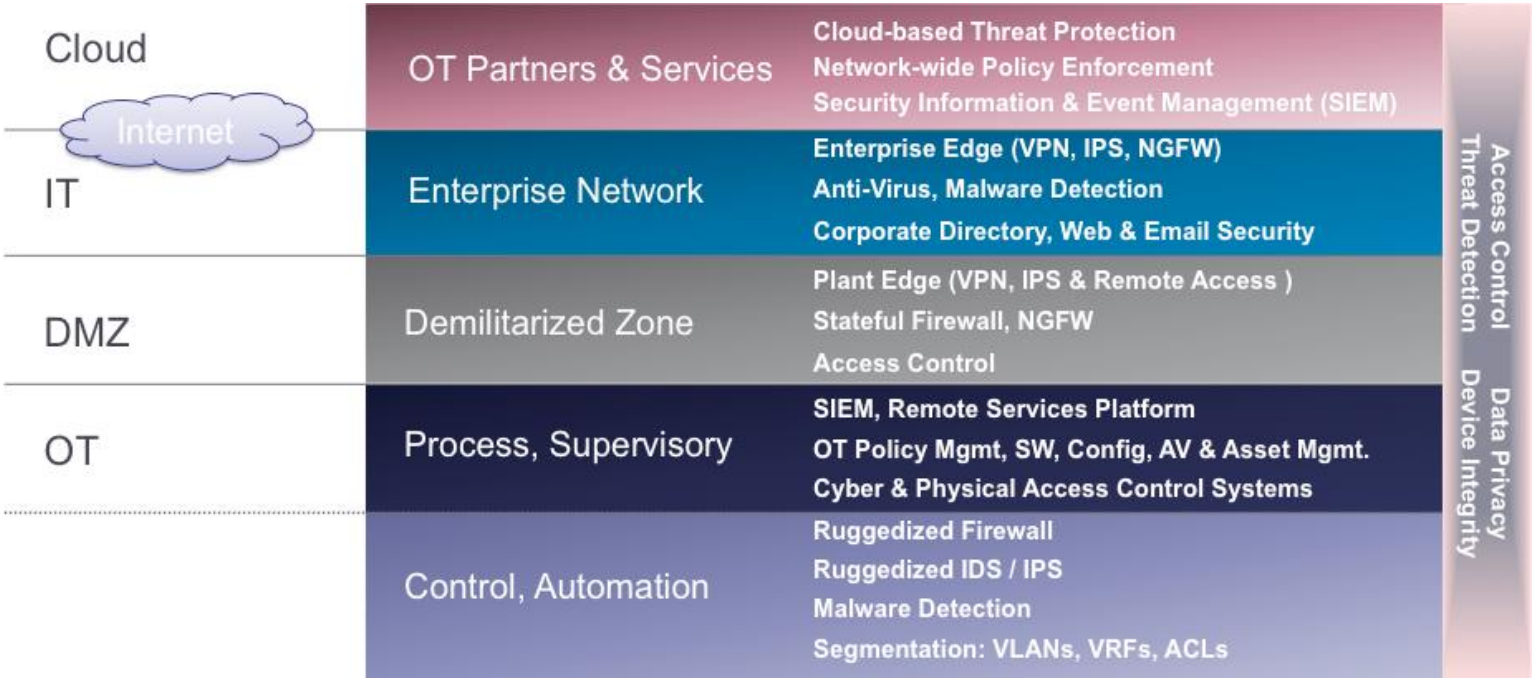
By Anne D'Innocenzio and Bree Fowler - Associated Press Friday, December 20, 2013

Cyber Physical Security Framework: Core Functions[1]

Identify	Protect	Detect	Respond	Recover
Risk Assessment	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Risk Management Strategy	Data Security	Security Continuous Monitoring	Analysis	Communications
Asset Management	Information Protection	Detection Process	Mitigation	Improvements
	Awareness & Training		Improvements	
	Protective Technologies			

[1] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

How do the Core Functions Map to an Industrial System?



How do the Core Functions Map to an Industrial System?

What about Trustworthiness?

What can we do to verify the hardware integrity of our products currently deployed in our network?

- DSTA Singapore

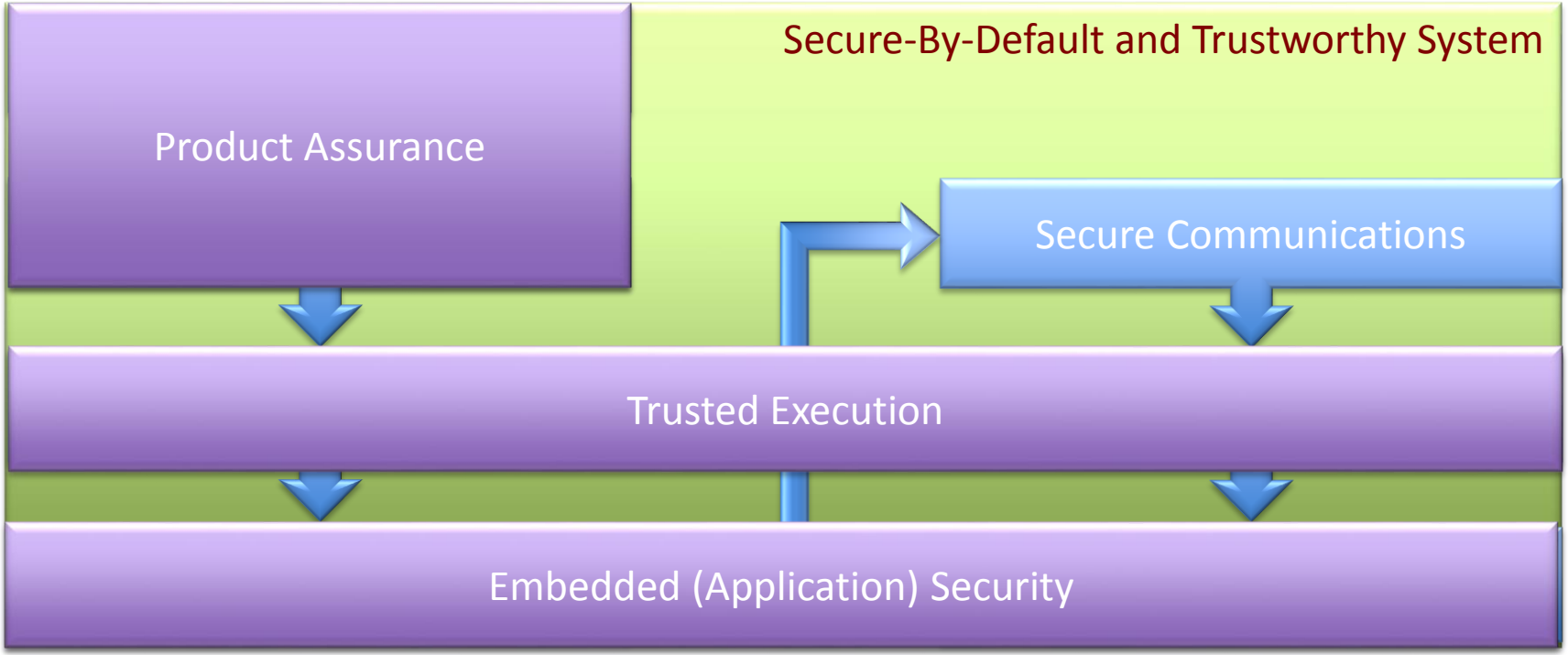
How do we trust devices?

How do I ensure our products can not be tampered?

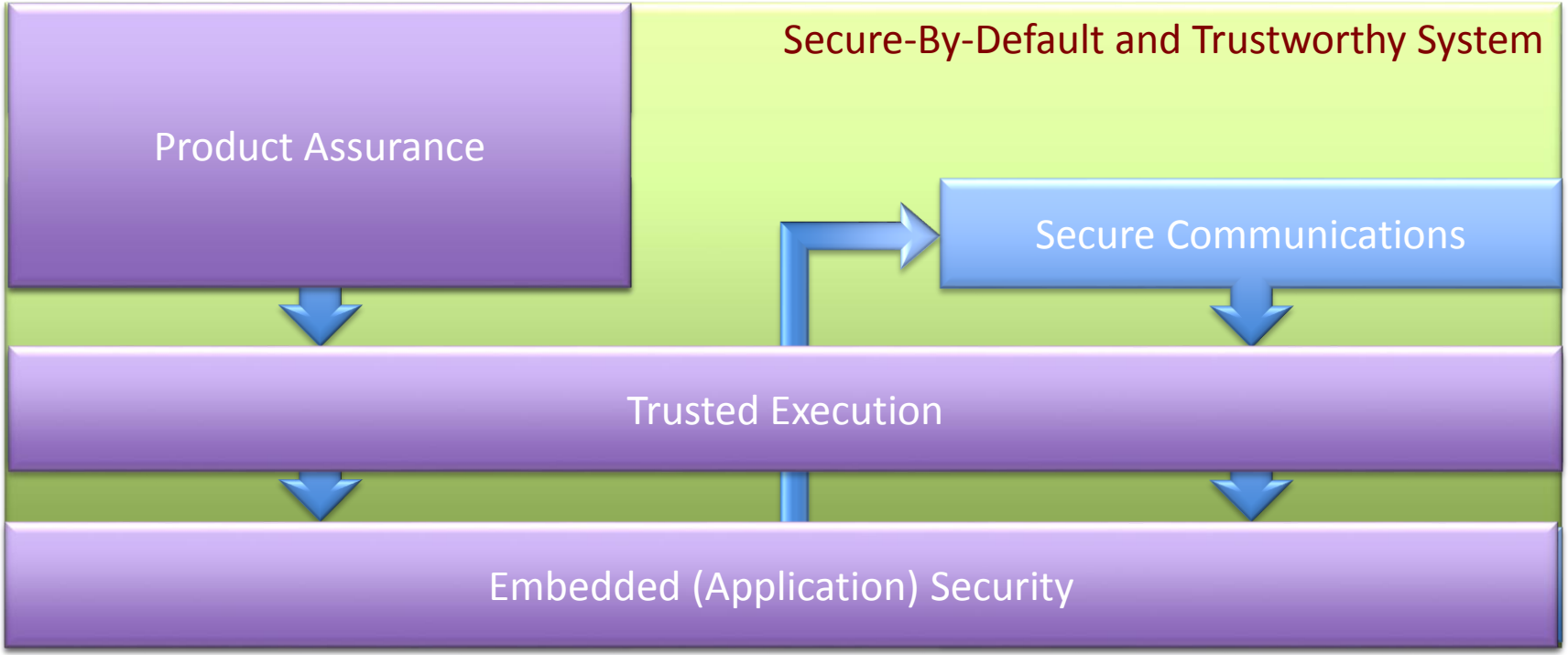
Is the software signed or integrity protected?

How do we ensure there are no back doors? ..

Trustworthy System Components



Trustworthy System Components



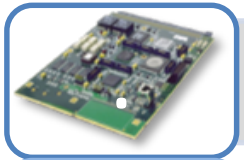
Trustworthy Components ➔ Trust Anchor Technologies

- Product Assurance

Hardware & Software Authenticity
Counterfeit & Illegal Upgrade Protection
Immutable Product Identity

- Trusted Execution

Boot-Time & Run-Time Integrity
Cyber Resiliency & Tamper Resistance
Strong Crypto & Certifiable Entropy



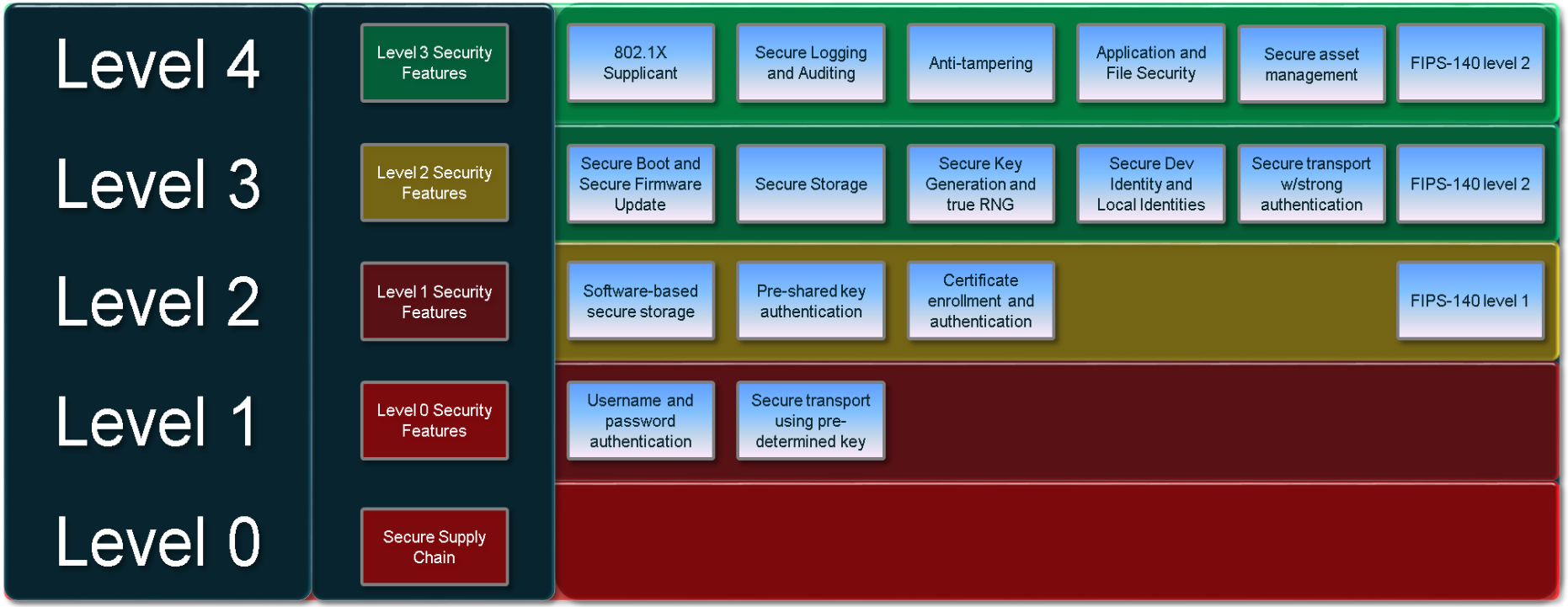
- Embedded Application Security

Secure (Application) Key Storage
Secure Crypto
IP & DRM Protection

- Secure-By-Default & Trustworthy Solutions

Strong Device/Network Authentication
Secure Communication
Customer Visible Trustworthy Status

Trustworthy Device Profiles



ODVA's role for Industrial Control Systems Cyber Security

- Expand ODVA's specification scope to include:
  - Continuation of Ethernet/IP security
  - Include CIP security
  - Define Security (Profile) Levels
  - Standardize a Security based Reference Architecture
  - Define Guidelines for secure network infrastructure deployment
  - Define Compliance and inter-operability requirements

11


ODVA
2015
INDUSTRY CONFERENCE
AND 17TH ANNUAL MEETING
ODVA'S 20TH ANNIVERSARY 1995–2015

THANK YOU