# How to Build Secure, Highly Reliable Critical Systems and Networks for the IoT

Trusted Computing Group
Seminar at IoT SWC 2017

©2017 Trusted Computing Group

# Agenda

| | |
|---|---|
| 0930 | Check-in, Networking, and Demos |
| 1000 | TCG Welcome and Overview |
| 1005 | Key Concepts of Trust and Application for IoT Security |
| 1040 | A Foundation for Trust in the IoT |
| 1110 | Industrial IoT Security: a New TCG Approach |
| 1135 | Q&A with the Speakers |
| 1200 | Networking and Demos |

©2017 Trusted Computing Group

# TCG OVERVIEW

©2017 Trusted Computing Group

# Who is the Trusted Computing Group?

The Trusted Computing Group (TCG) is an international industry standards group focused on Trusted Computing since its founding in 2003.



- You may know TCG for our technical specs & guidance such as:
  - Trusted Platform Module (TPM 2.0)
  - Self Encrypting Drive (SED)
  - Trusted Network Communications (TNC)

©2017 Trusted Computing Group

# What is a Trusted Platform Module (TPM)?




- **Standard Security Module**
  - Supports TPM standards
- **Features**
  - Authentication
  - Encryption
  - Attestation
- **Benefits**
  - Foundation for secure software
  - Resistant to attacks/hacks
  - Built-in virtual smart card

ISO/ IEC 11889

©2017 Trusted Computing Group

# What is a Self-Encrypting Drive (SED)?



- **Standard Secure Storage Device**
  - Supports SED standards
- **Features**
  - Encryption
- **Benefits**
  - Always on encryption
  - No performance impact
  - Protection against Physical Attacks, loss and theft
  - Cryptographic instant erase/Wipe

Works with SCSI and SATA

©2017 Trusted Computing Group

# What is Trusted Network Communications (TNC)?



- **Security Automation Standards**
- **Features**
  - Manage Network Endpoints
  - Enable New Capabilities
- **Benefits**
  - Automation for All Phases of Cybersecurity
    - Preparation
    - Detection
    - Analysis
    - Response

IETF NEA & SACM

©2017 Trusted Computing Group

# KEY CONCEPTS OF TRUST AND APPLICATION FOR IOT SECURITY

©2017 Trusted Computing Group

# Today's Speakers



Steve Hanna
Infineon Technologies



Monty Wiseman
General Electric Company



Lee Wilson
Onboard Security



Dennis Mattoon
Microsoft

©2017 Trusted Computing Group

# Key Concepts of Trust and Applications for IoT Security

Steve Hanna, Infineon Technologies
Monty Wiseman, General Electric Company
Lee Wilson OnBoard Security

©2017 Trusted Computing Group

# A Foundation for Trust in the Internet of Things

Dennis Mattoon, Microsoft

©2017 Trusted Computing Group

# INTRODUCTION

- Today's cyber-attackers are sophisticated and relentless in their continual efforts to seek out and exploit vulnerabilities.
- At the same time, market segments like IoT are driving architectures and solutions with challenging power, security, resource, and other constraints.

©2017 Trusted Computing Group

# INTRODUCTION

- To effectively address these challenges a security architecture must be:
  - Free or very cheap, and not just in BOM cost
  - Adaptable, with minimal silicon requirements
  - Scalable to millions of endpoints per solution
  - Standards-based, i.e., interoperable
- And most importantly, it takes a combination of hardware support and software techniques

©2017 Trusted Computing Group

# WHY HARDWARE SUPPORT?

- There are problems with software-only solutions
- Device Identity
  - If a bug leads to disclosure of Device Identity secret then how do we securely (and remotely) recover and re-provision a device?
- Device State and Attestation
  - Cannot trust software to report its own health
- Roots of Trust, data encryption, entropy, etc.
  - How do we securely extend trust chain, store keys, etc.?

©2017 Trusted Computing Group

# BEWARE SIMPLISTIC HW SOLUTIONS

- Why not just store Device Identity key/secrets in fuses?
  - If malware can manage to read the fused key then you are no better off than with a software-based key
- TPMs are great but, especially in IoT solutions, systems and components probably won't have TPMs or similar silicon-based capabilities (cost, complexity, physical space on the MCU/SoC)
- We need something different

©2017 Trusted Computing Group

# DICE AND RIOT

- Device Identifier Composition Engine (DICE, TCG)
- Robust, Resilient, Recoverable IoT (RIoT, MSFT)
- New specification from the Root of Trust for Measurement subgroup in the Trusted Computing Group (TCG)
- Foundational security for IoT at near zero cost
- Simple hardware requirements mean DICE is adaptable to most any system or component
- Provides HW-based identity and attestation, and a foundation for sealing, data integrity, device recovery and update

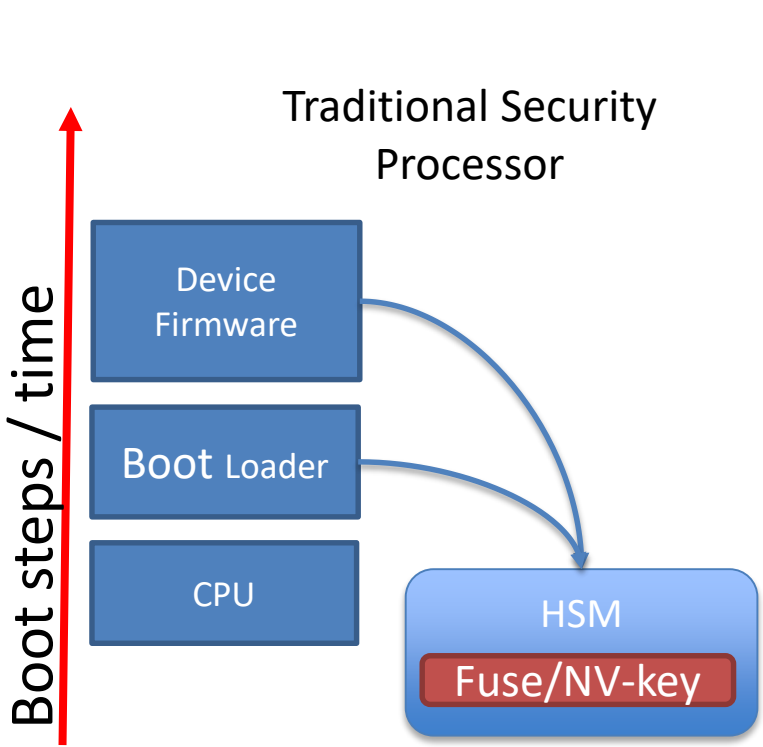
©2017 Trusted Computing Group

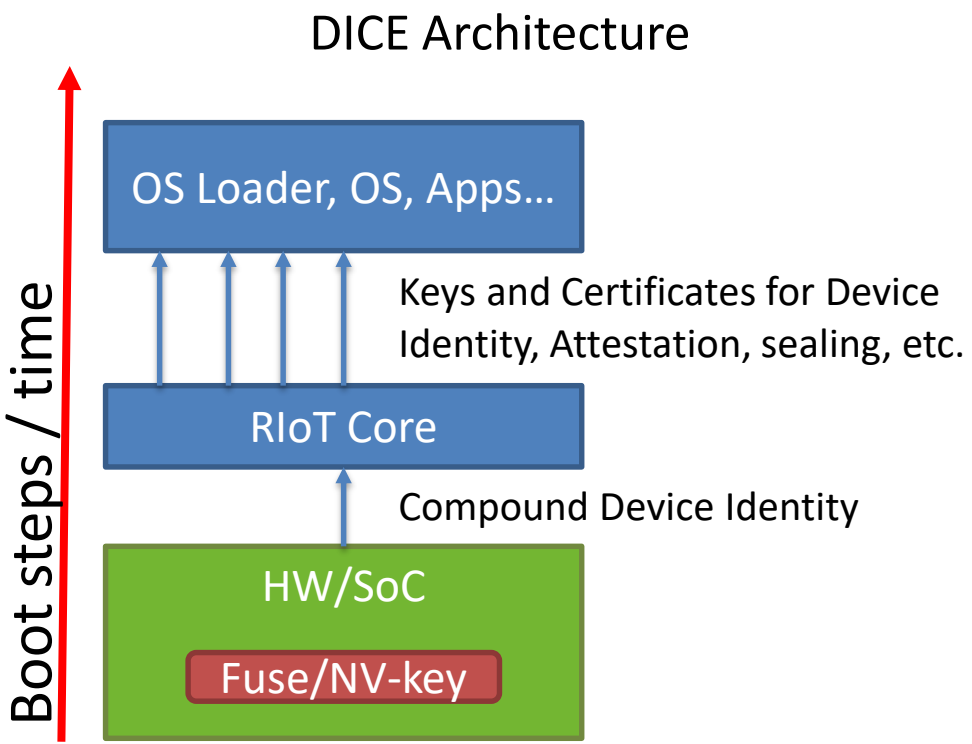
# THE DICE MODEL

- In a DICE Architecture device startup (boot) is layered
- Beginning with a Unique Device Secret (UDS), secrets/keys are created that are unique to the device and each layer and configuration
- This derivation method means that if different code or configuration is booted, secrets are different
- If a vulnerability exists and a secret is disclosed, patching the code automatically re-keys the device

©2017 Trusted Computing Group

# THE DICE MODEL

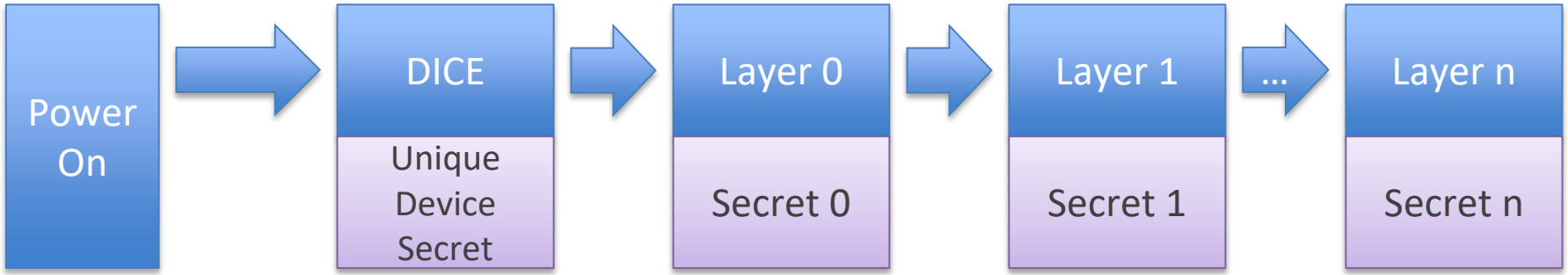



©2017 Trusted Computing Group

# THE DICE MODEL

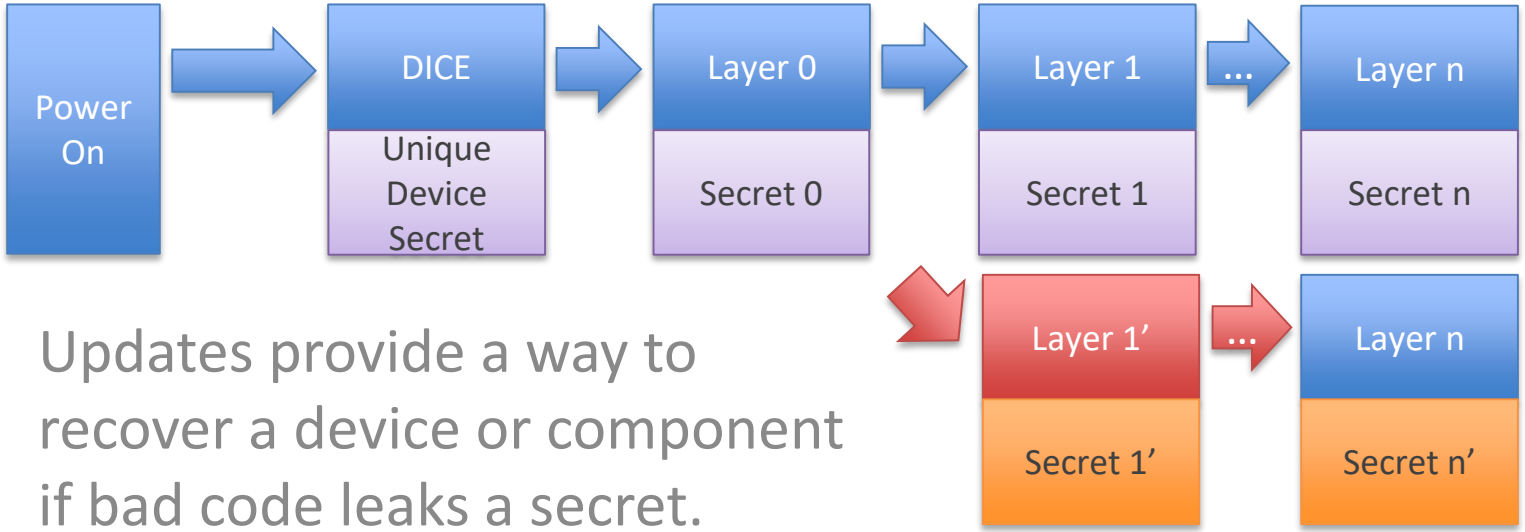
- Power-on (reset) unconditionally starts the DICE
- DICE has exclusive access to the UDS
- Each layer computes the secret for next layer (via OWF)
- In this derivation chain, each layer must protect the secret it receives




©2017 Trusted Computing Group

# WHEN SOMETHING CHANGES

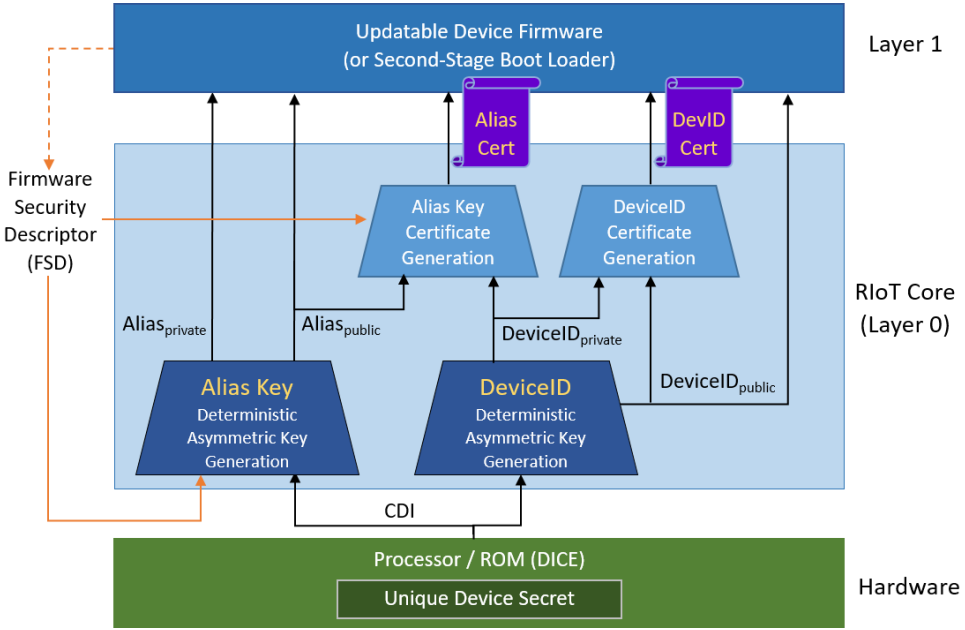
- The branch illustrates the result of a code/config change




- Updates provide a way to recover a device or component if bad code leaks a secret.

©2017 Trusted Computing Group

# A DICE ARCHITECTURE (RIOT)




- Underlying architecture for HW-based Device Identity and Attestation (Azure)
- DeviceID – Stable and well protected long term identifier for a device or component
- Alias Key – Derived from combination of unique device identity (HW) and identity of Device Firmware (SW)
- Integrates DICE-enabled HW with existing infrastructure

©2017 Trusted Computing Group

# BUT THAT'S JUST ONE EXAMPLE

- We can build on DICE to enable many high-value scenarios
- Secure remote device recovery (Cyber Resilient Platform Initiative)
  - Recover unresponsive (i.e., p0wned, hung, etc.) devices
  - Greatly reduced cost: no need for physical device interaction
- Supply chain management
  - Several recent damaging cyber-attacks were the result of malware introduced in the supply chain
  - DICE attestation lets end-customers trust far less of the supply-chain, e.g., just the storage-subsystem or flash vendor
- Component identity, authenticity, licensing, and many more

©2017 Trusted Computing Group

# DICE TAKEAWAYS

- Flexible security framework, not one size fits all
- Minimal silicon requirements, low barrier to entry
- Foundation for strong cryptographic HW-based device identity and attestation, data at rest protection (sealing), and secure device update and recovery
- Public announcements from SoC, MCU, and flash memory vendors so far with more on the way
- Represents the ongoing work of the DICE Architectures Workgroup (DiceArch WG) in TCG.  Come join us!

©2017 Trusted Computing Group

# REFERENCES

- Device Identifier Composition Engine (DICE) specification
- DICE Architectures Workgroup (TCG)
- RIoT – A Foundation for Trust in the Internet of Things
- Cyber-Resilient Platform Initiative
- Partners and Demos:
  - Microchip CEC1702 and SecureIoT1702
  - Micron Authenta
  - Sequitur Labs (i.MX6, SAMA5D2)
  - STMicroelectronics (STM32L4xx)
- Azure IoT:
  - Strengthening IoT Security
  - Zero-Touch Provisioning with Azure IoT

©2017 Trusted Computing Group

# Industrial IoT Security: Overview of a New TCG Approach

Monty Wiseman, General Electric Company

©2017 Trusted Computing Group

# Agenda

- Introduction to Industrial Security
- TCG and Industrial Security Today
- New Industrial Sub Group
- Call to Action

©2017 Trusted Computing Group

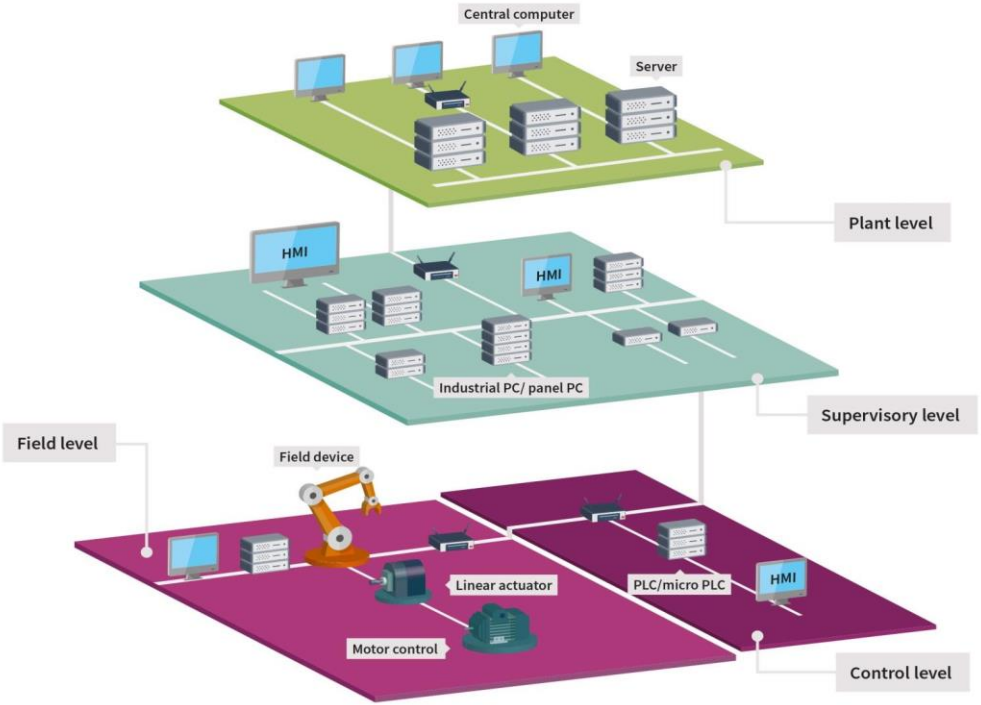
# IoT Attacks Growing



# Introduction to Industrial Security

©2017 Trusted Computing Group

# Industrial Automation




©2017 Trusted Computing Group

# Industrial IoT Brings Changes

## Smart Factories / Industrial IoT / Industry 4.0

- **"Lot size 1":** Ability to produce highly individualized products
- **Cloud analysis:** Enabling data mining, deep learning and cost reduction
- **Predictive maintenance:** Based on sensor data gathered and analyzed as big data

## Implications

- Greater communication within the plant and beyond
- Reconfigurable, smart manufacturing equipment
- New business models and opportunities
- New security risks

©2017 Trusted Computing Group

# Security Effects of Industrial IoT

## New security paradigms

- "Closed shop floor" paradigm not applicable anymore
- Security risks touch all machines with greater potential impact
- Industrial security is becoming part of corporate strategies

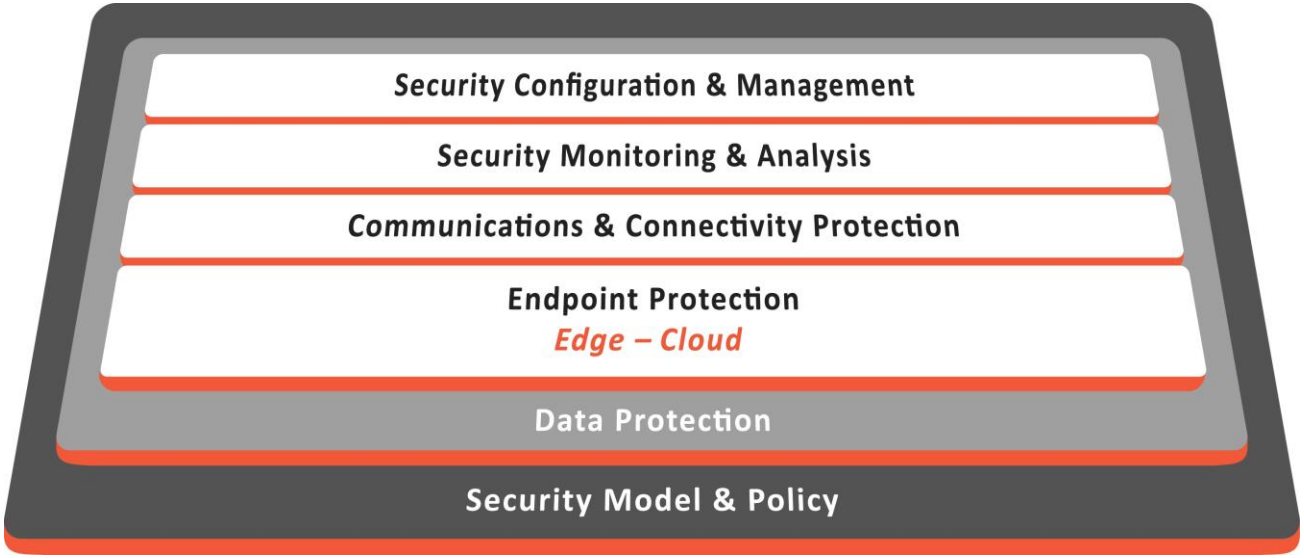


## Implications

- Strong protection required
- Availability has higher priority than Confidential or Integrity
- System-wide security approach required

©2017 Trusted Computing Group

# Industrial IoT Countermeasures




Source: Industrial Internet Security Framework
https://www.iiconsortium.org/IISF.htm
graphics are courtesy of Industrial Internet Consortium

©2017 Trusted Computing Group

# TCG and Industrial Security Today

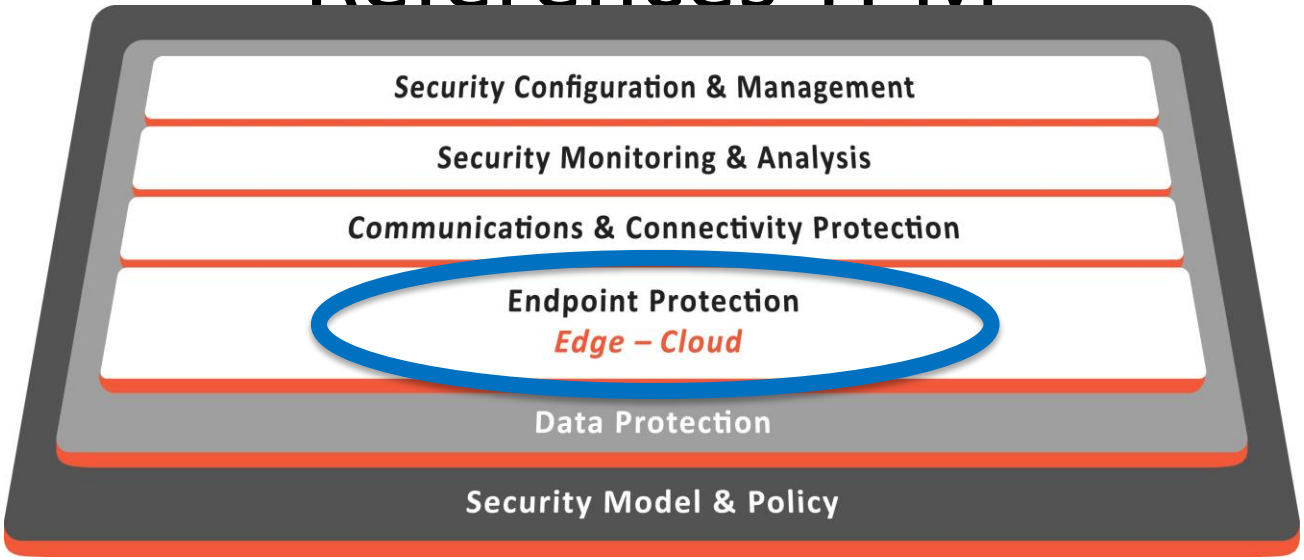
©2017 Trusted Computing Group

# TCG Industrial IoT Security Resources

- TCG IoT Architect's Guide: http://bit.ly/1RzLRa6
- TCG Guidance for Securing IoT: http://bit.ly/2f8RYkK
- TNC IF-MAP Metadata for ICS Security https://trustedcomputinggroup.org/tnc-if-map-metadata-ics-security/
- Architects Guide: ICS Security Using TNC Technology https://trustedcomputinggroup.org/architects-guide-ics-security-using-tnc-technology/
- Industrial Internet Security Framework: https://www.iiconsortium.org/IISF.htm

©2017 Trusted Computing Group

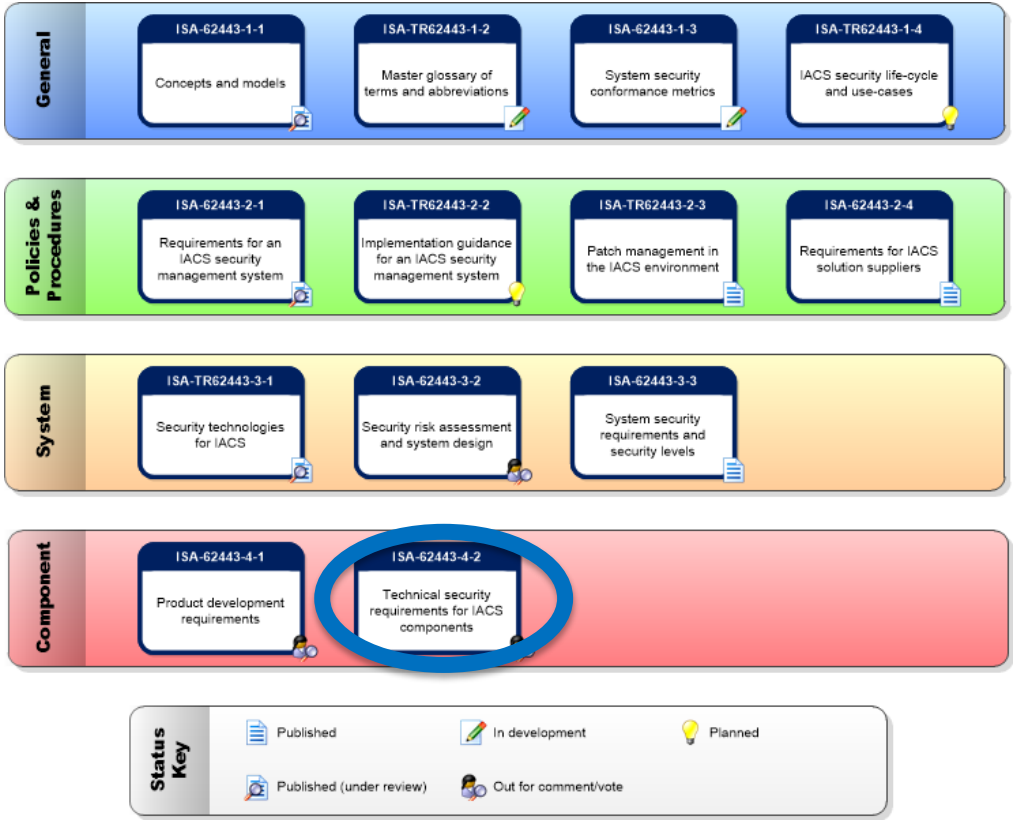
# Industrial Internet Consortium's IISF References TPM




Source: Industrial Internet Security Framework
https://www.iiconsortium.org/IISF.htm
graphics are courtesy of Industrial Internet Consortium

©2017 Trusted Computing Group

# IEC/ISA 62443 References TPM




©2017 Trusted Computing Group

# TCG’s New Industrial Sub Group

©2017 Trusted Computing Group

# Purpose of Industrial SG

- Provide specifications and guidance to implementers and users regarding the use of Trusted Computing technologies for Industrial applications
- Deliver:
  - Reference Documents
    - Guidance, …
  - TCG Specifications
    - Industrial Platform Firmware Profile,
    - TPM Profile?,
    - …
  - Marketing and Educational Materials
    - Architects Guides
    - Webinars

©2017 Trusted Computing Group

# Which TCG Technologies?

- TPM
- TNC
- OPAL
- Etc.

©2017 Trusted Computing Group

# Call to Action

1. Join TCG and then Industrial Sub Group
   - https://trustedcomputinggroup.org/membership

2. Help Create Deliverables
   - Guidance for Securing Industrial Equipment
   - Platform Firmware Profile

For more information, email
admin@trustedcomputinggroup.org

©2017 Trusted Computing Group

# Q&A with Our Speakers



Steve Hanna
Infineon Technologies



Monty Wiseman
General Electric Company



Lee Wilson
Onboard Security



Dennis Mattoon
Microsoft

©2017 Trusted Computing Group

# Networking and Demos with





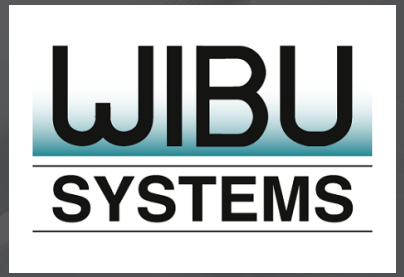













©2017 Trusted Computing Group

# Thank You For Joining Us Today
# Learn More at
# www.trustedcomputinggroup.org

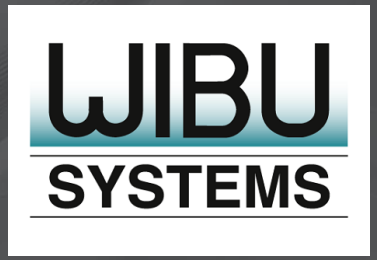











©2017 Trusted Computing Group