SECURE TECHNOLOGY ALLIANCE

The webinar will begin shortly

SECURE TECHNOLOGY ALLIANCE

IoT Security: Mitigating Security Risks in Smart Connected Environments

IoT Security Council Webinar

October 11, 2018

Who we are

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

- Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

SECURE TECHNOLOGY ALLIANCE

Our Focus

- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

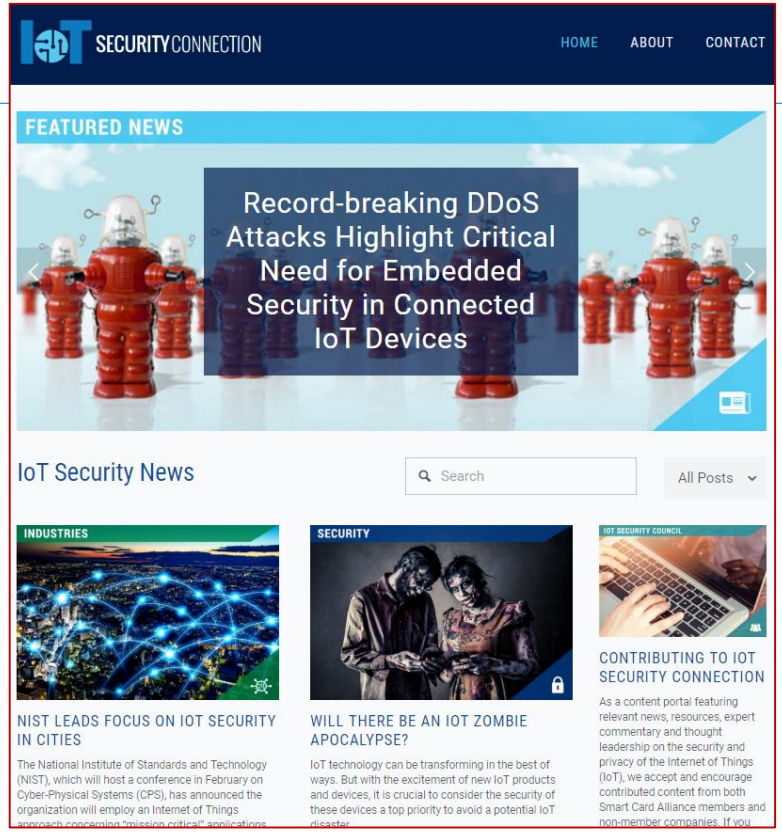
Member Benefits

- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

IoT Security Resources

IOT SECURITY COUNCIL PRIORITIES

- Accelerate market adoption of secure IoT architectures that incorporate embedded security and privacy
- Provide a forum for intra-industry and cross-industry collaboration on secure IoT architectures
- Provide a business-focused organization to discuss best practices and implementation of IoT architectures using embedded security and privacy
- Provide a single organization where all industry stakeholders can network, share implementation experiences, and discuss applications and security approaches
- Identify and collaborate with other industry organizations to define and promote standards for secure IoT architectures using technologies that provide embedded security and privacy



Publications – Internet of Things (IoT)

- Blockchain and Smart Card Technology
- Embedded Hardware Security for IoT Applications
- Implementation Considerations for Contactless Payment-Enabled Wearables
- IoT and Payments: Current Market Landscape

Today's IoT Security Webinar Presenters

Randy Vanderhoof (Moderator)
Executive Director, Secure Technology Alliance

Sri Ramachandran
VP, IOT & Solutions, G+D Mobile Security

Steve Hanna
Senior Principal, Infineon Technologies

John Neal
Business Development & Government Affairs, NXP

Josh Jabs
VP OCTO,GM IOT Solutions, Entrust Datacard

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

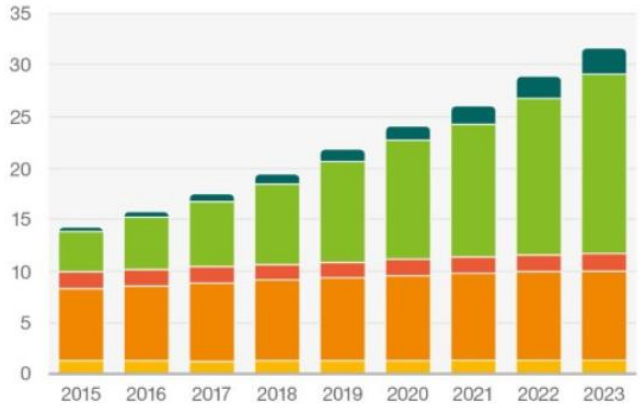
Intro to Security 101 for IoT

Sri Ramachandran,
Vice President IOT Solutions

G+D Mobile Security

The digital transformation challenge – Major increase in connected devices

Connected devices (billion)



	2017	2023	CAGR
Wide-area IoT	0.6	2.4	26%
Short-range IoT	6.4	17.4	18%
PC/laptop/tablet	1.6	1.7	0%
Mobile phones	7.5	8.8	3%
Fixed phones	1.4	1.3	0%
	17.5 billion	31.6 billion	

Ericsson Mobility Report November 2017

New devices

New services and use cases

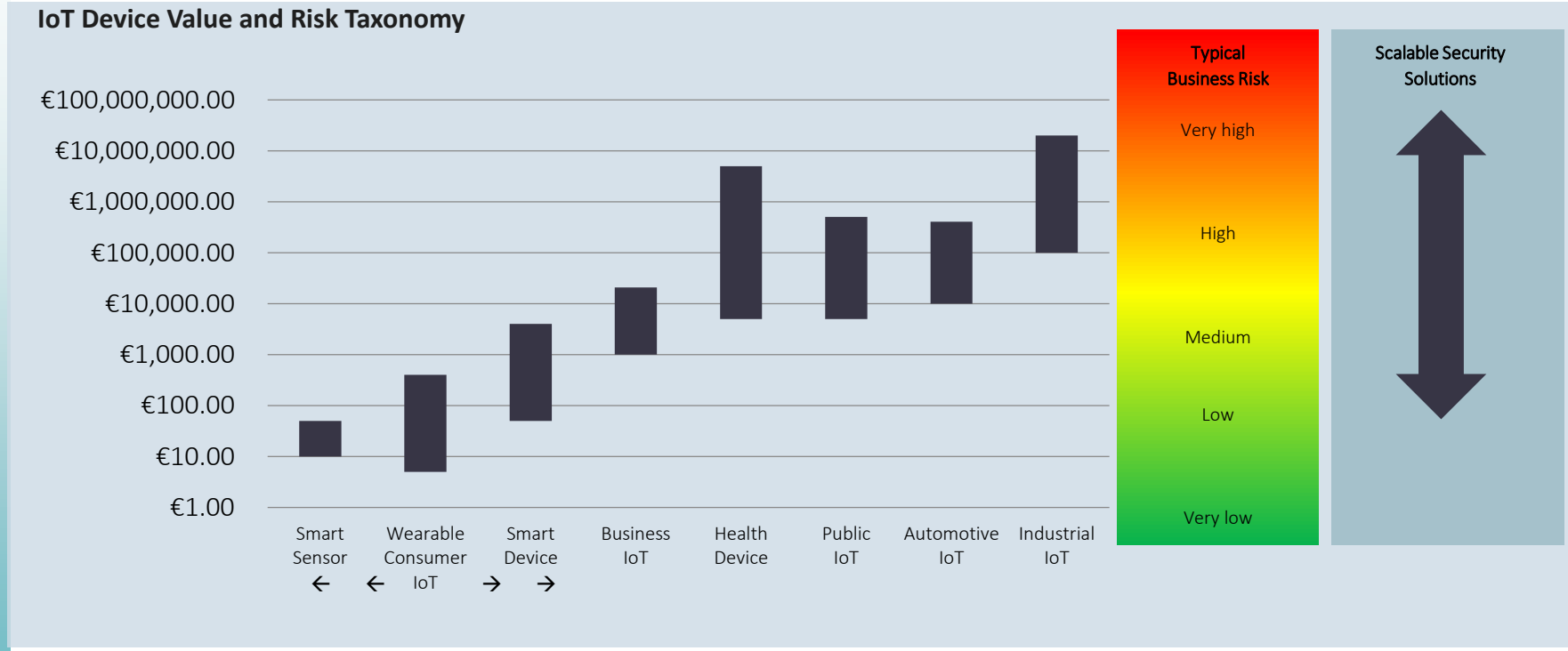
New business models

New security threats

SECURE TECHNOLOGY ALLIANCE

G+D Mobile Security

Internet of Things – Wide range of device values and risk



Poll Question

A connected baby monitor costs about $100. What do you think is the risk of that being compromised?

A) Low

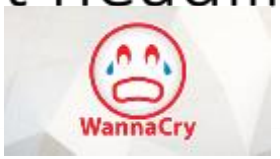
B) Medium

C) High

SECURE TECHNOLOGY ALLIANCE

Recent headlines

April 07, 2017



ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

BrickerBot malware attacks and destroys unsecure IoT devices

February 15, 2017

Attacks up in Q4, Akamai

Target Ignored Data Breach Alarms

Target's security team reviewed -- and ignored -- urgent warnings from threat-detection tool about unknown malware spotted on the network.

The German federal cyber agency, BSI, on Monday said it was aware of additional German institutions affected by the WannaCry "ransomware" cyber attack beyond those companies already known, and it expected additional variants of the virus to surface.

However, while the Mirai botnet continues to be a major source of attacks, the Akamai report had this warning: "The Mirai botnet continued as one of the largest threats in the fourth quarter, but it is not the only Internet of Things (IoT)-based botnet. At least two other major IoT-based botnets are in use."

SECURE TECHNOLOGY ALLIANCE

G+D Mobile Security

But wait, there's more…

JUL 27, 2017 @ 05:00 PM 3,146 12 Stock

Criminals Hacked A Fish Tank To Steal Data From A Casino

Security and IoT: Most I… Open to Hacking

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

Home › Internet of Things (IoT) › Security a… …ices are Unsecured and Open to Hacking and Malware

By Dick Weisinger

80 percent of all Internet of Things (IoT) devices have security flaws and are vulnerable to an attack, according to a Ponemon study made earlier this year.

SECURE TECHNOLOGY ALLIANCE

G+D Mobile Security

Poll Question

Do you think your company is adequately protected against cyberattacks?

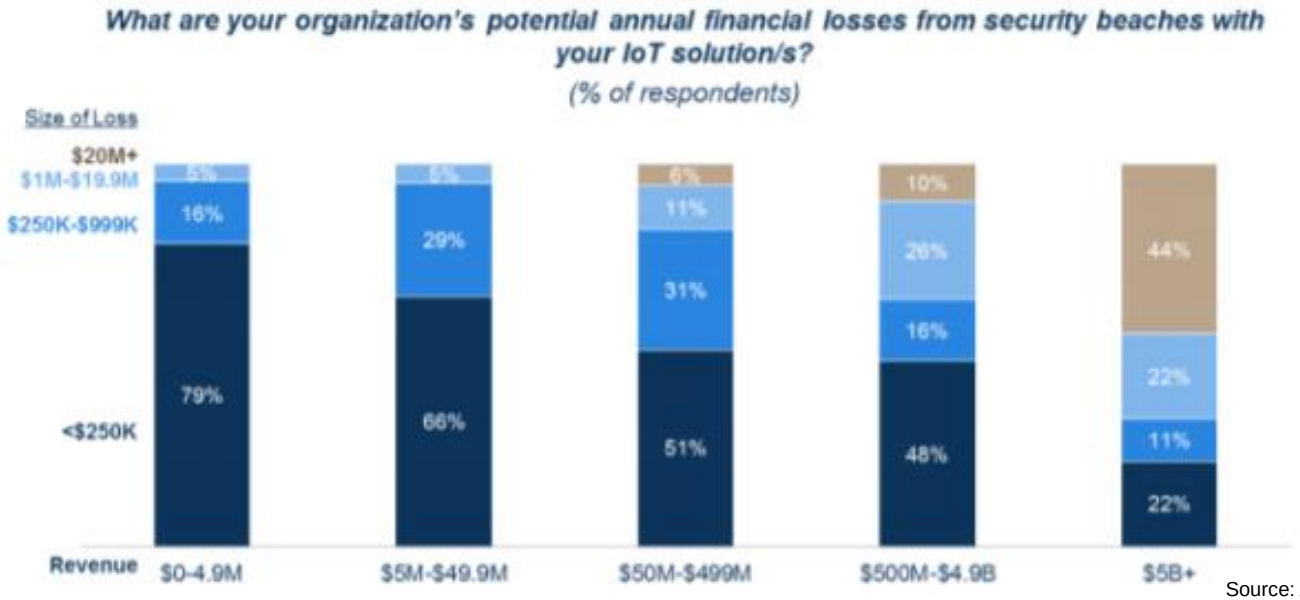
A) No, not at all

B) Yes, but we need more protection

C) Yes! We are Fort Knox against cyberattacks

Costs of security breaches are tremendous

*Companies with **less than $5M** in company revenue report potential **losses of $255K** on average, were they to experience a breach.*



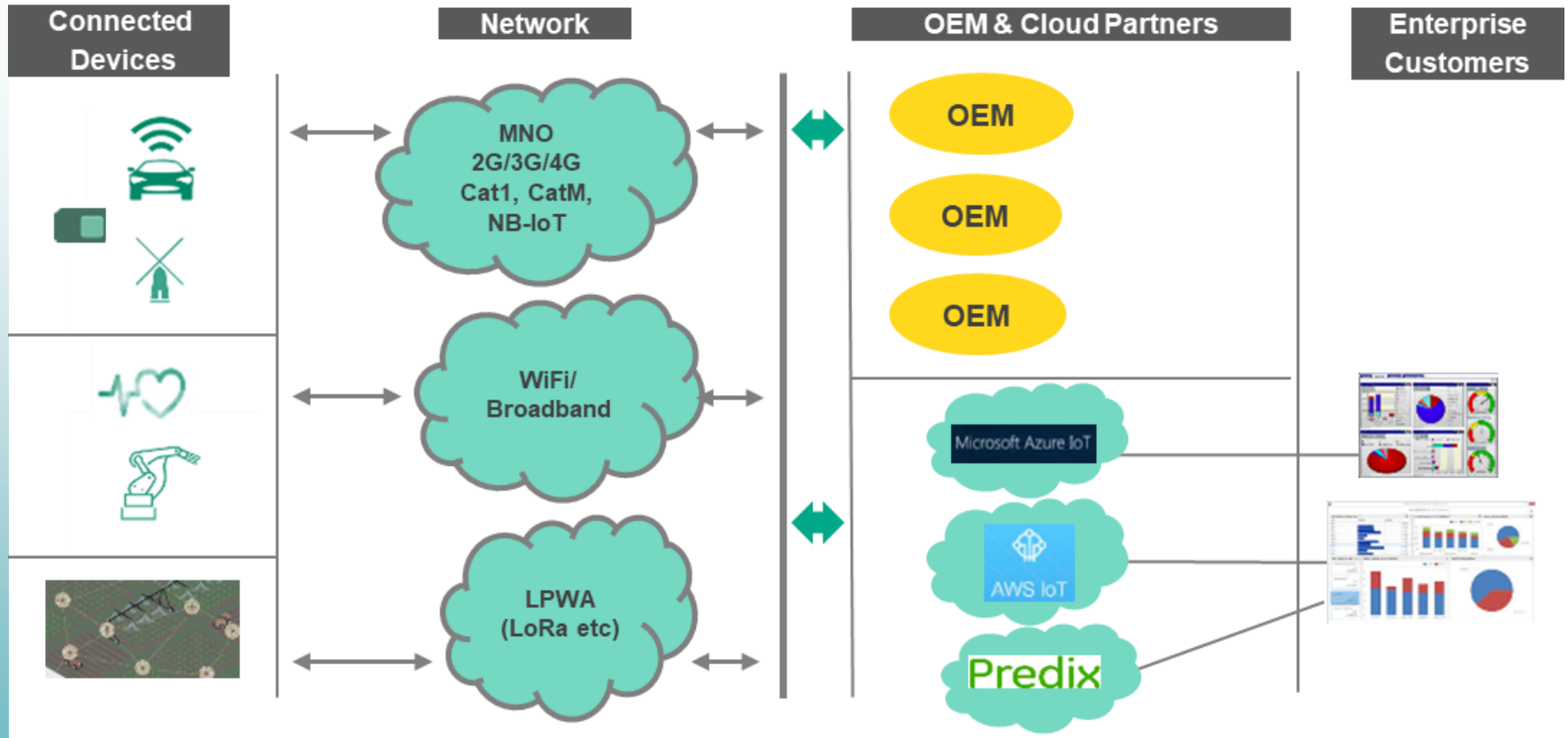
Source: Altman Vilandrie & Company

That lack of security in many IoT devices is causing a major concern among organizations that are using or plan to use IoT in the near future. So much so, that a follow up survey by Ponemon of businesses found that 76 percent expected that they would experience a serious attack within the next two years, and 94 percent said that an attack could be catastrophic for their business.

G+D Mobile Security

SECURE TECHNOLOGY ALLIANCE

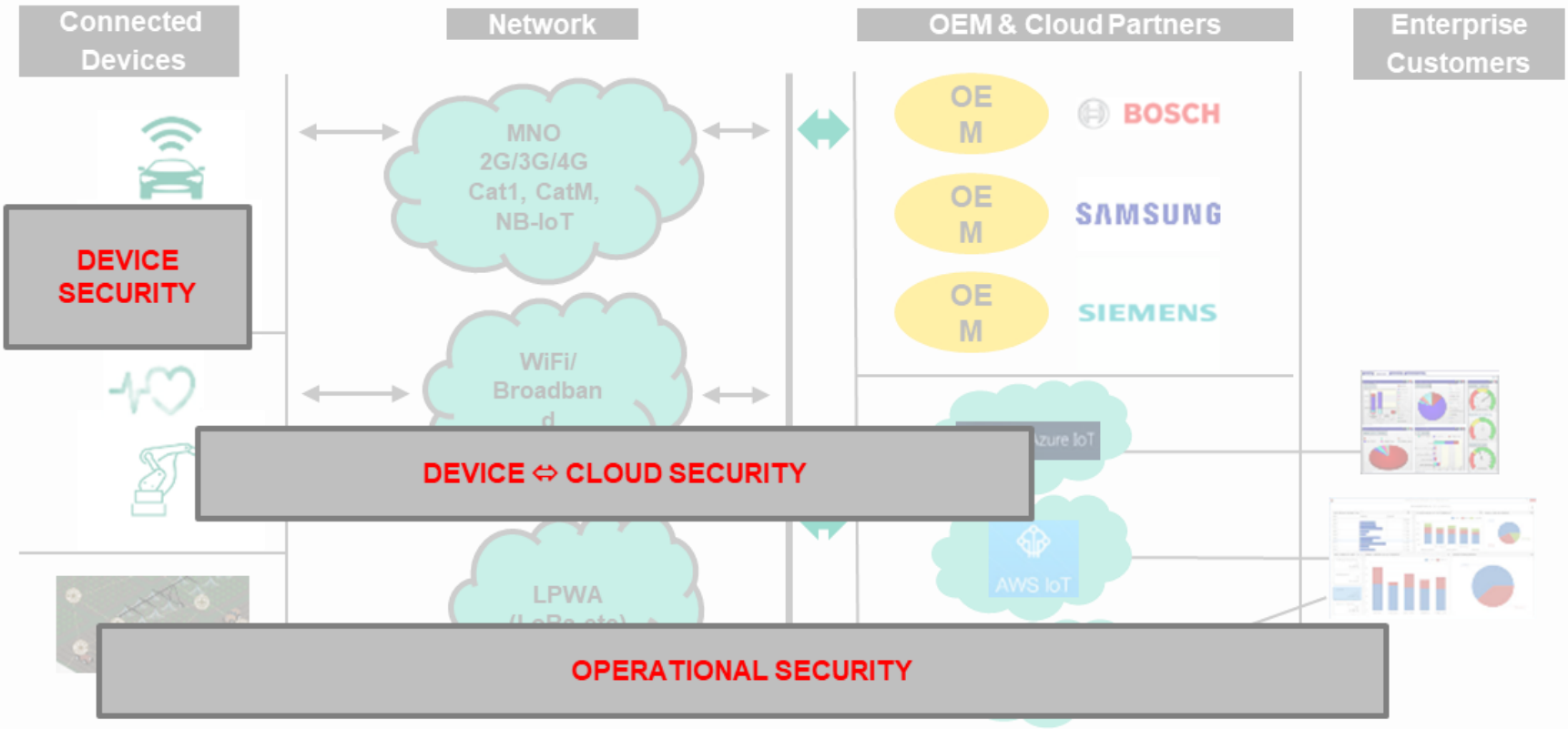
What we know: IoT is complex



SECURE TECHNOLOGY ALLIANCE

G+D Mobile Security

Challenges of IoT security



Challenges of IoT Device security…

Challenges of IoT Device security…

→ Identify every Device in the system
- Unique Identity
- Independent of network access

→ Device integrity
- Ensure Device is operating as planned

→ Data protection
- Data gathering as well as secure transport of data

→ Secure management and monitoring throughout life cycle
- Device is protected at all times - including secure firmware and configuration updates

→ Differential access control
- Differentiate among privileged and regular operations

G+D Mobile Security

SECURE TECHNOLOGY ALLIANCE

The Three Problems of Device to Cloud Security

DEVICE IDENTITY

Devices tend to use network identifiers for their identity which are easily abused

MUTUAL AUTHENTICATION

Lack of username/passwords in IoT devices make traditional authentication methods impractical

ENCRYPTION OF CHANNEL

Segment by segment encryption is not secure enough and very hard to manage

SECURE TECHNOLOGY ALLIANCE

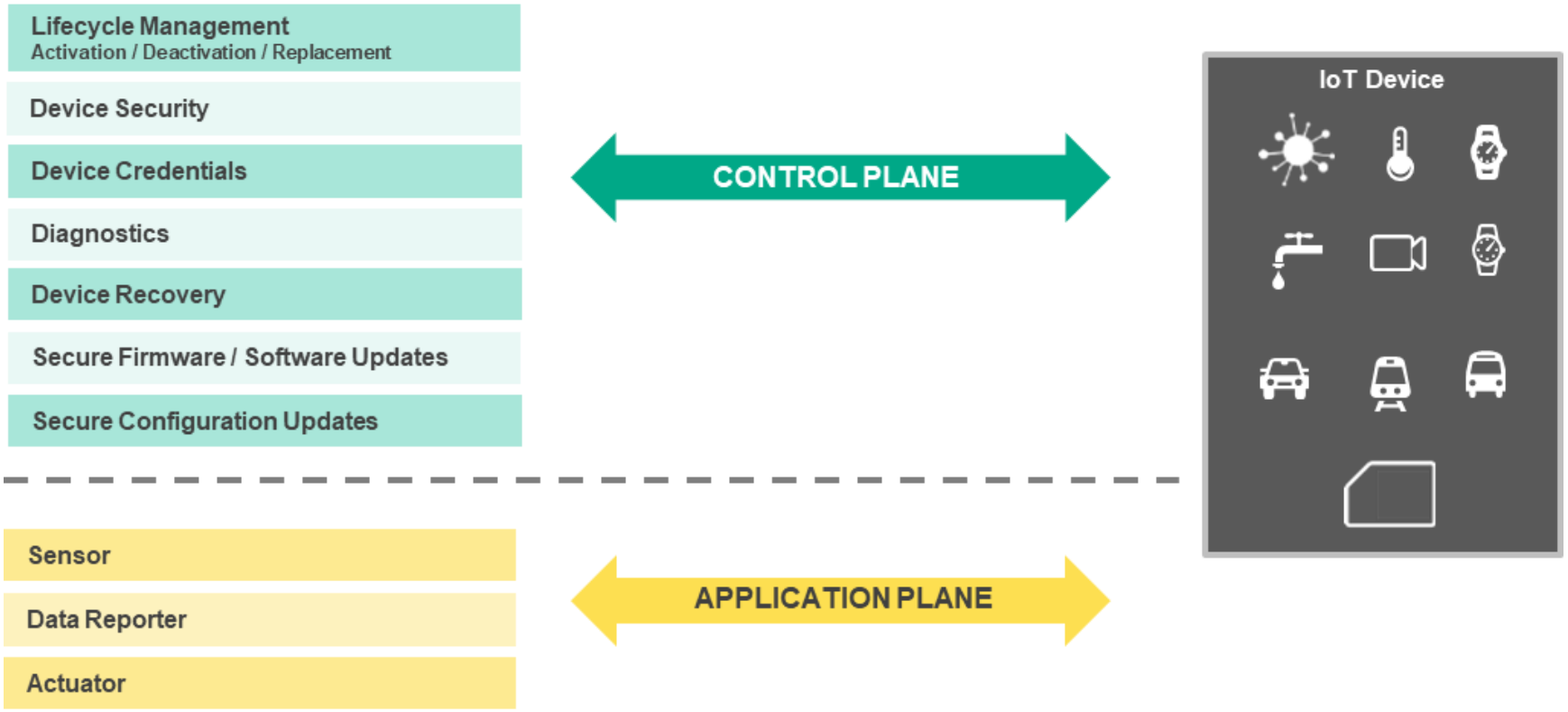
G+D Mobile Security

What we really need…

- **ROOT OF TRUST**
  providing irrefutable identity management
- **ALL DATA ENCRYPTED**
  between device and cloud
- **PREVENTION**
  of malware and rogue configurations
- **RECOVERY**
  of stranded devices

SECURE TECHNOLOGY ALLIANCE

Separation of functions in an IoT Device



SECURE TECHNOLOGY ALLIANCE

G+D Mobile Security

Secure Connectivity for IoT: Three building blocks

G+D Mobile Security

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Use Cases: Industrial and Financial IoT Security

Steve Hanna,
Senior Principal

Infineon

Poll Question

Which type of IoT are you securing?

A) Smart Car

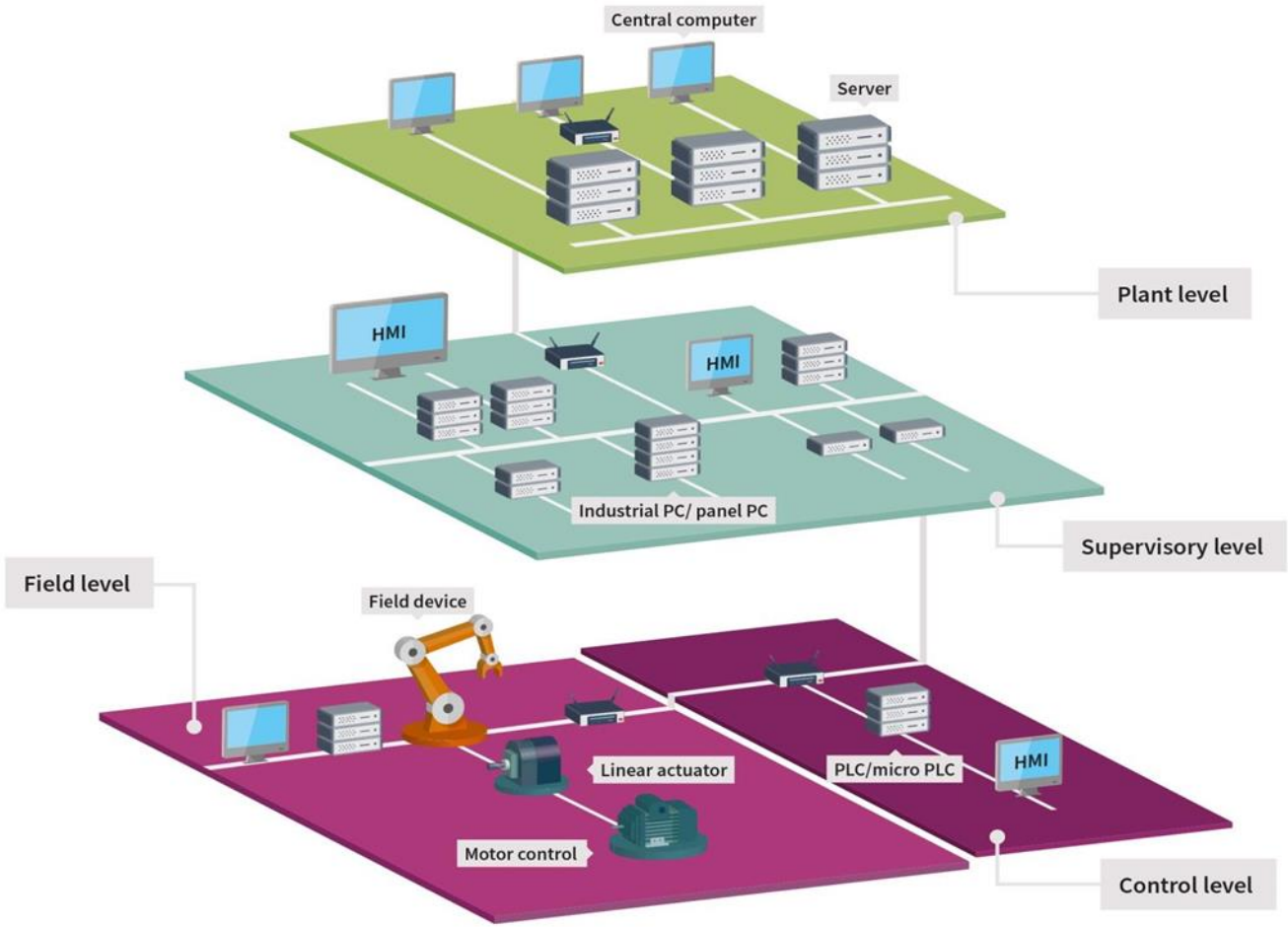
B) Smart City

C) Smart Home

D) Smart Factory

E) Other

Industrial IoT Connects Industrial Systems to the Cloud



Connectivity and intelligence drive innovation

Industrial IoT Innovations

- **"Lot size 1":** Ability to produce highly individualized products
- **Cloud services:** Data mining, deep learning, cost reductions
- **New Business Models:** Pay per use, predictive maintenance, continuous innovation

Enabled by

- Lightweight sensors
- Ubiquitous communications
- Cloud intelligence
- Smart equipment
- Remote software update

Finances are also being revolutionized

More IoT devices are used for financial transactions

Connected devices will initiate more than

$1 trillion

in transactions by 2020

http://www.electran.org/publication/transactiontrends/the-internet-of-payments/

Different Security Levels for Different Threats

Security Level 0

No security

Security Level 1

Protects against accidental errors

Security Level 2

Protects against intentional attacks with **simple** means and **low** resources and knowledge (e.g. PC virus)

Security Level 3

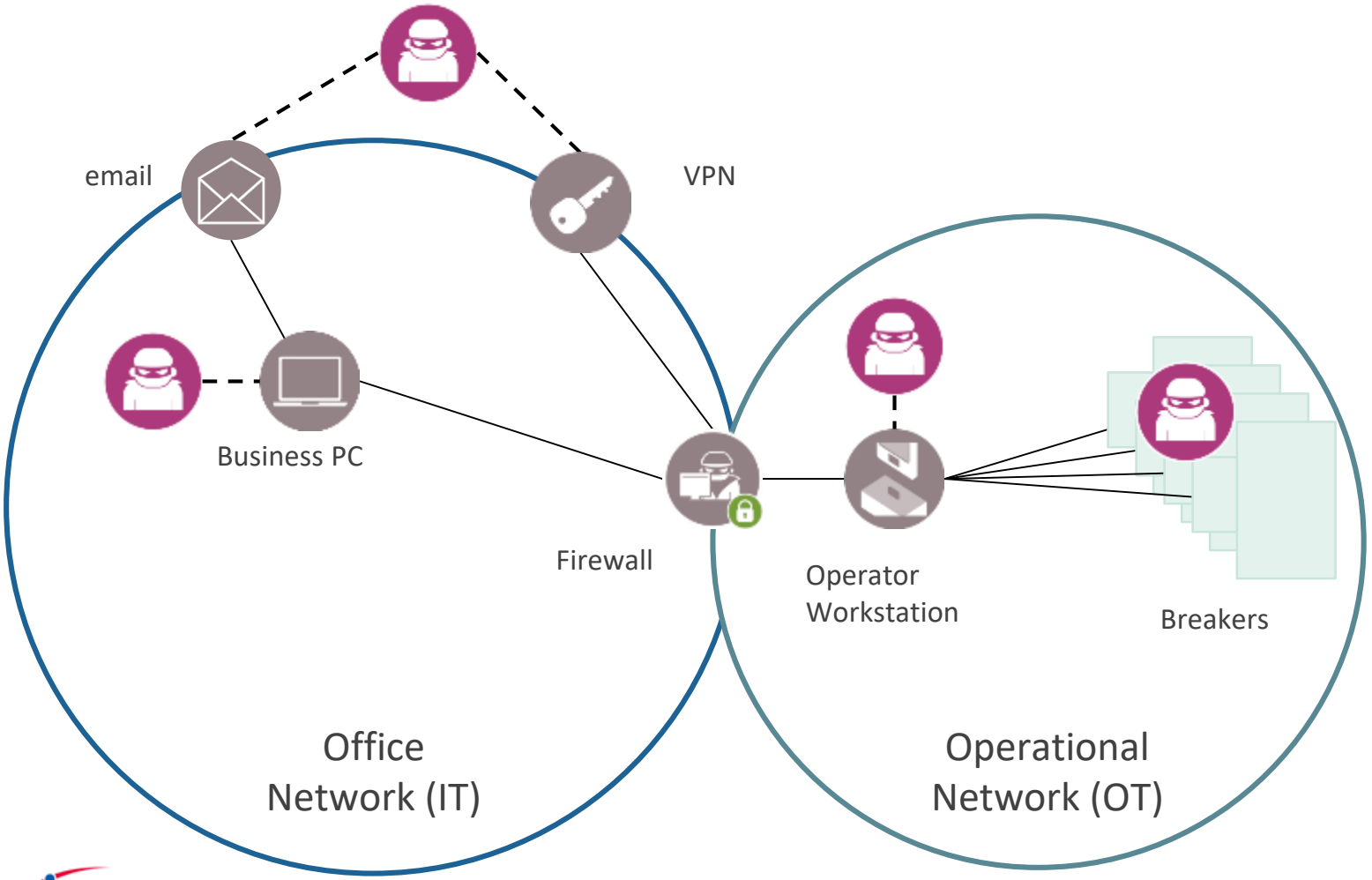
Protects against intentional attacks with **sophisticated** means and **moderate** resources and knowledge (e.g. ICS knowledgeable attacker)

Security Level 4

Protects against intentional attacks with **sophisticated** means and **high** resources and knowledge (e.g. nation state)

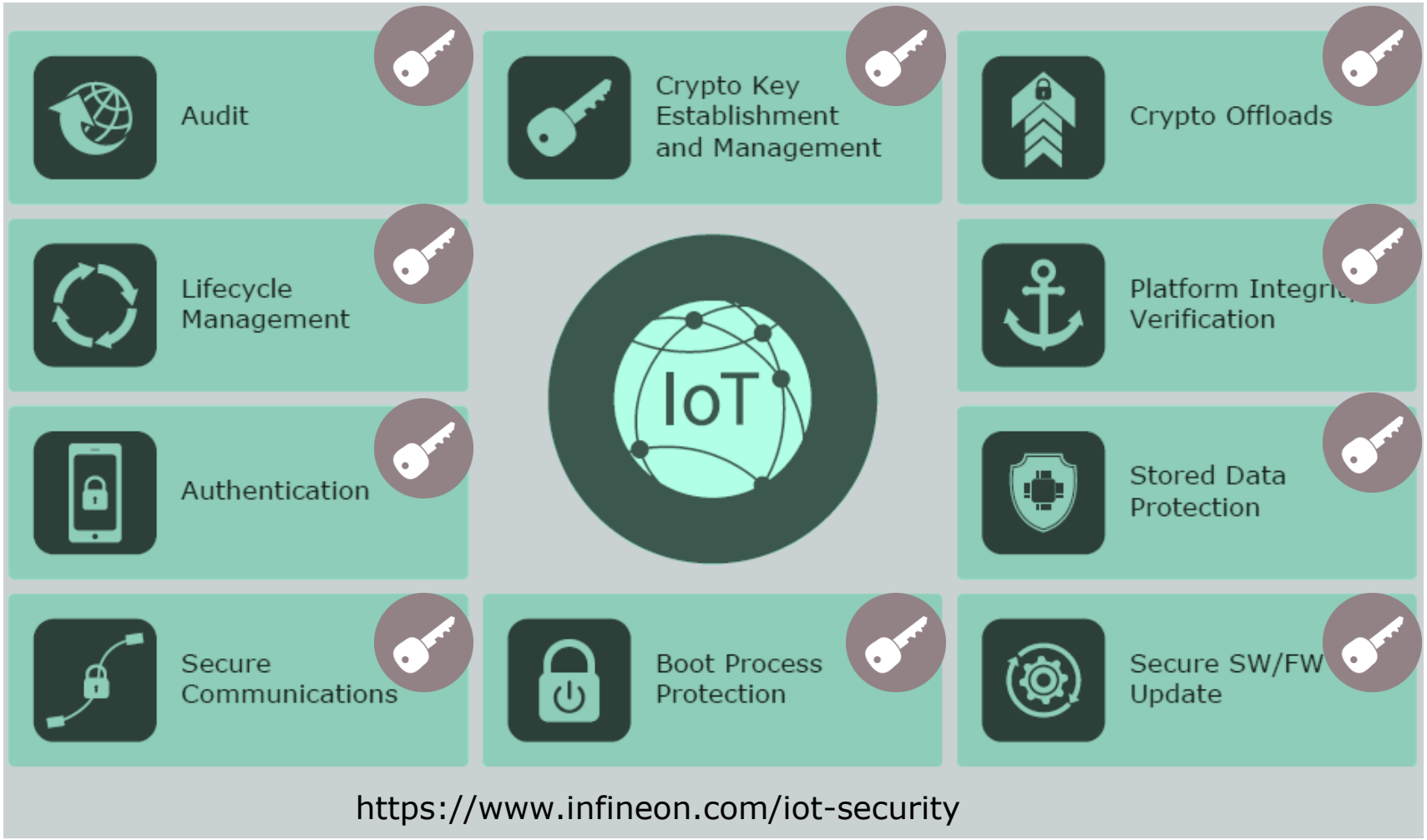
Source: IEC 62443-3-3 - Industrial communication networks – Network and system security

Ukrainian Power Grid Attack

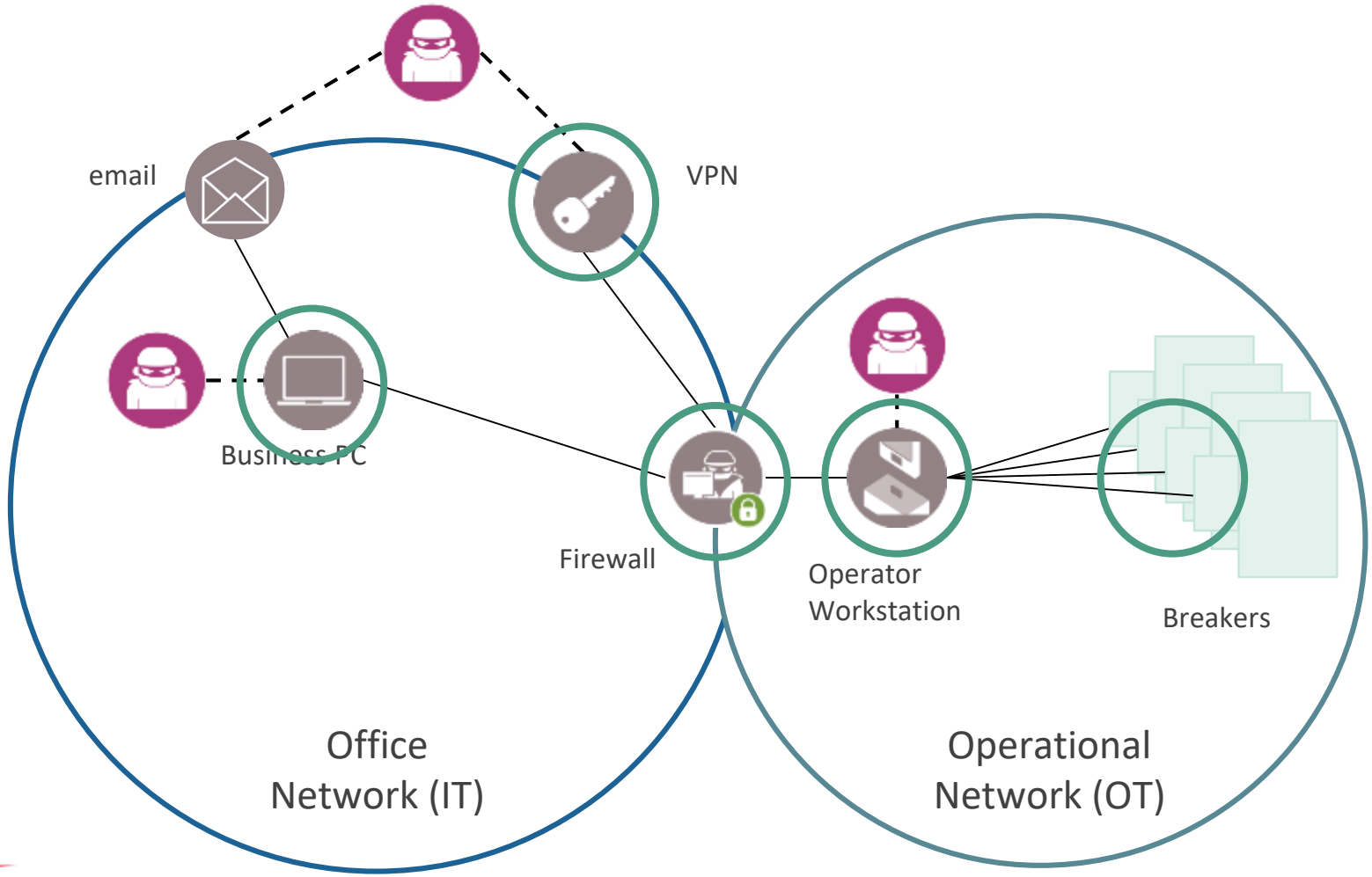


Source: Analysis of the Cyber Attack on the Ukrainian Power Grid, SANS & E-ISAC, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Cryptographic Keys – The Foundation of Cybersecurity



Stopping the Ukrainian Power Grid Attack

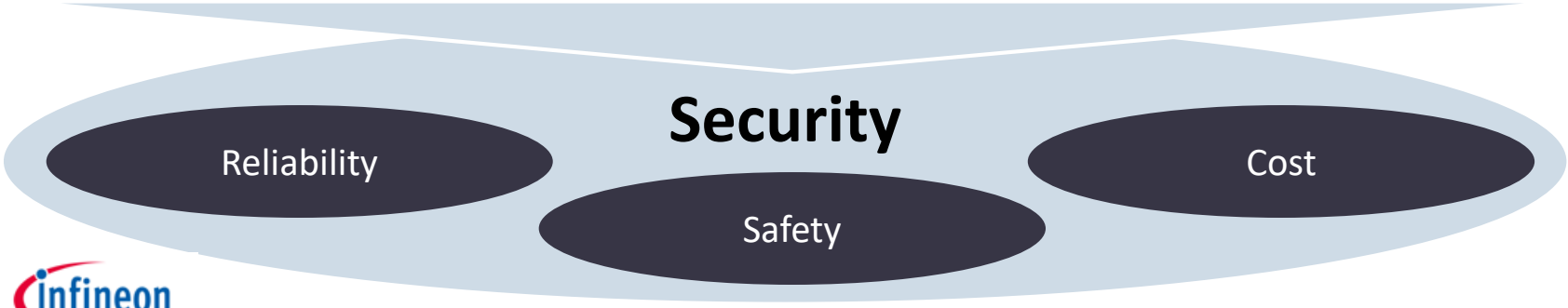


Value Proposition for IoT Security

- Maximize uptime, reliability, and quality
- Ensure customer satisfaction
- Reduce support costs

- Promote safety and reduce risk
- Protect private and confidential data
- Avoid damage to brand

- Maintain steady course
- Enable innovation
- Differentiate from competition



SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Use Cases: Connected Cars & Parking

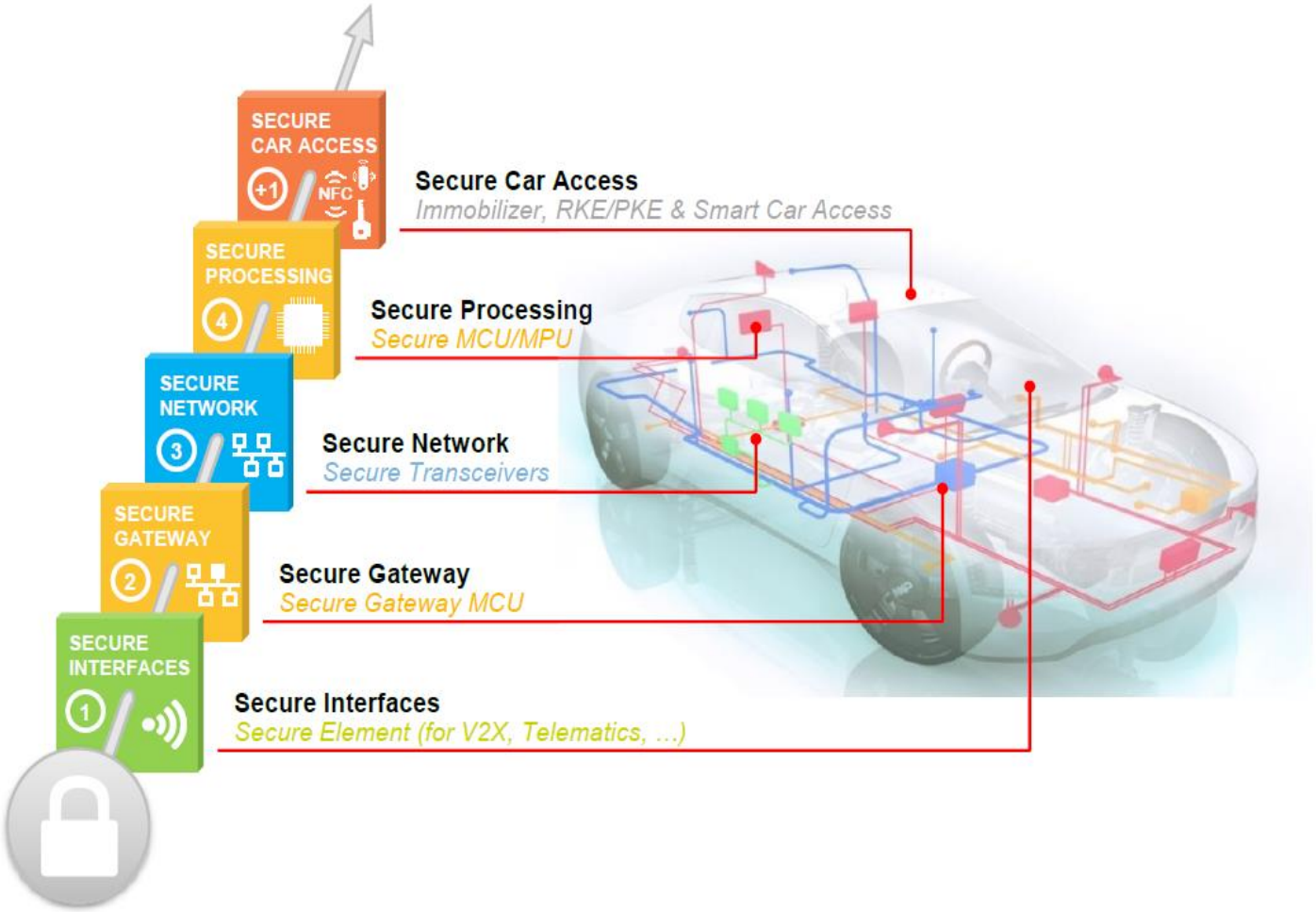
John Neal,
Business Development and Government Affairs

NXP

Connected Cars

- 1970's car electronics - unconnected
- Today's car contains hundreds of millions of lines of code run in hundreds of processors linked to sensors, actuators and other components.
- Smart cards on wheels
  - Payment
- Navigation, infotainment and software updates.
- Autonomous vehicles will require even more connectivity to safely and seamlessly interact with their surrounding environment
- Security features must include:
  - Physical access
  - Secure PII and confidential information
  - Critical safety systems
- The increasingly interconnected nature of a vehicle's control modules means there is no safety without security.

4+1 Layer Security Framework

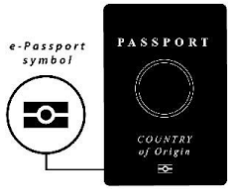


Root of Trust and Secure Boot Functions

- Hardware root of trust helps users incorporate security at the design phase
- Secure boot, for example, is an un-bypassable mechanism for developers to lock down their code
- developers cryptographically sign their software.
- Each time the system boots, the NXP processor validates the digital signature.
  - Only proven authentic software can execute.
- Software update/patching

Long Range RFID and Contactless Parking Solutions

- NXP's long-standing experience in contactless authentication, payment and rewards support the advancement of smart mobility.
- Secure long range UHF RFID tags integrated in license plates make automatic vehicle identification easier for governments and road users
  - Tolling, parking, payment
  - Security Secure cryptographic authentication
    - Banking, ePassport
    - GDPR requirements
    - Customizable for service providers
    - Supports BYOD



Poll Questions

Has your company been affected by regulation such as GDPR?

A) Yes

B) No

Does your company see a need to advocate for baseline policy for securing the IoT in the United States and abroad?

A) Yes

B) No

IoT Charter of Trust

- Currently there is no basic level, or “level zero”, defined for security and privacy of smart, connected devices.
  - Hacks going up, companies misusing customer data in a non-transparent fashion
  - Result: Consumers are becoming more and more reluctant to invest in smart technologies
- Goal: Increase trust in IoT
  - To better protect the ecosystem: baseline security standards and principles must be valid across the entire life cycle of IoT products
  - design process through the supply chain to field life and decommissioning
- Initiative of industry, government and public key actors engaging the key players in a joint mission to establish baseline standards and mandatory requirements for the security and privacy of connected devices.
  - Munich Security Conference
  - 16 companies: Siemens, NXP, IBM, Cisco, Airbus, Allianz, Dell, Total
    - Energy, IT, telecom, transportation, financial services
- Floor or ceiling – Reputational risk

SECURE TECHNOLOGY ALLIANCE

Maintaining Security For a Lifetime

Josh Jabs
VP OCTO,GM IOT Solutions

Entrust Datacard™

SECURE TECHNOLOGY ALLIANCE

Trustworthiness is the degree of confidence one has that the system performs as expected in respect to all the key system characteristics (security, safety, reliability, resilience and privacy) in the face of environmental disruptions, human errors, system faults and attacks.

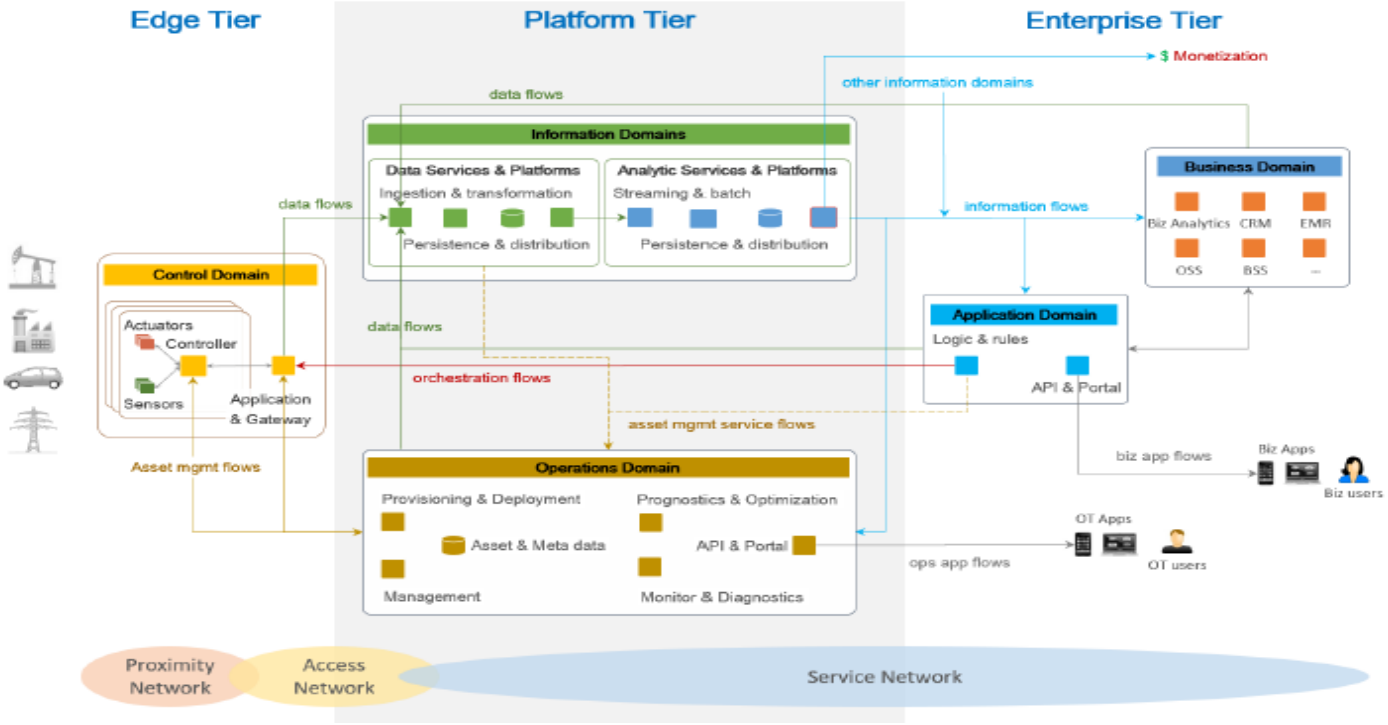
From IT to IOT – A Mix of Existing and New Challenges

NEW RISKS AS A RESULT OF CONNECTING, MANAGING, AND CONTROLLING THE OPERATIONAL ENVIRONMENT

- Changing the physical environment
- Scale and Ecosystem Complexity
- New architectures
- Safety, Resilience, Real-time and security
- Evolving Standards
- LOB vs Security processes and lack of skills
- Greenfield vs brownfield
- Supply chain

Key IOT Architectural Characteristics

- Sense and/or control
- Data and command flows
- Device classes and environments
- Platform considerations



Vulnerabilities

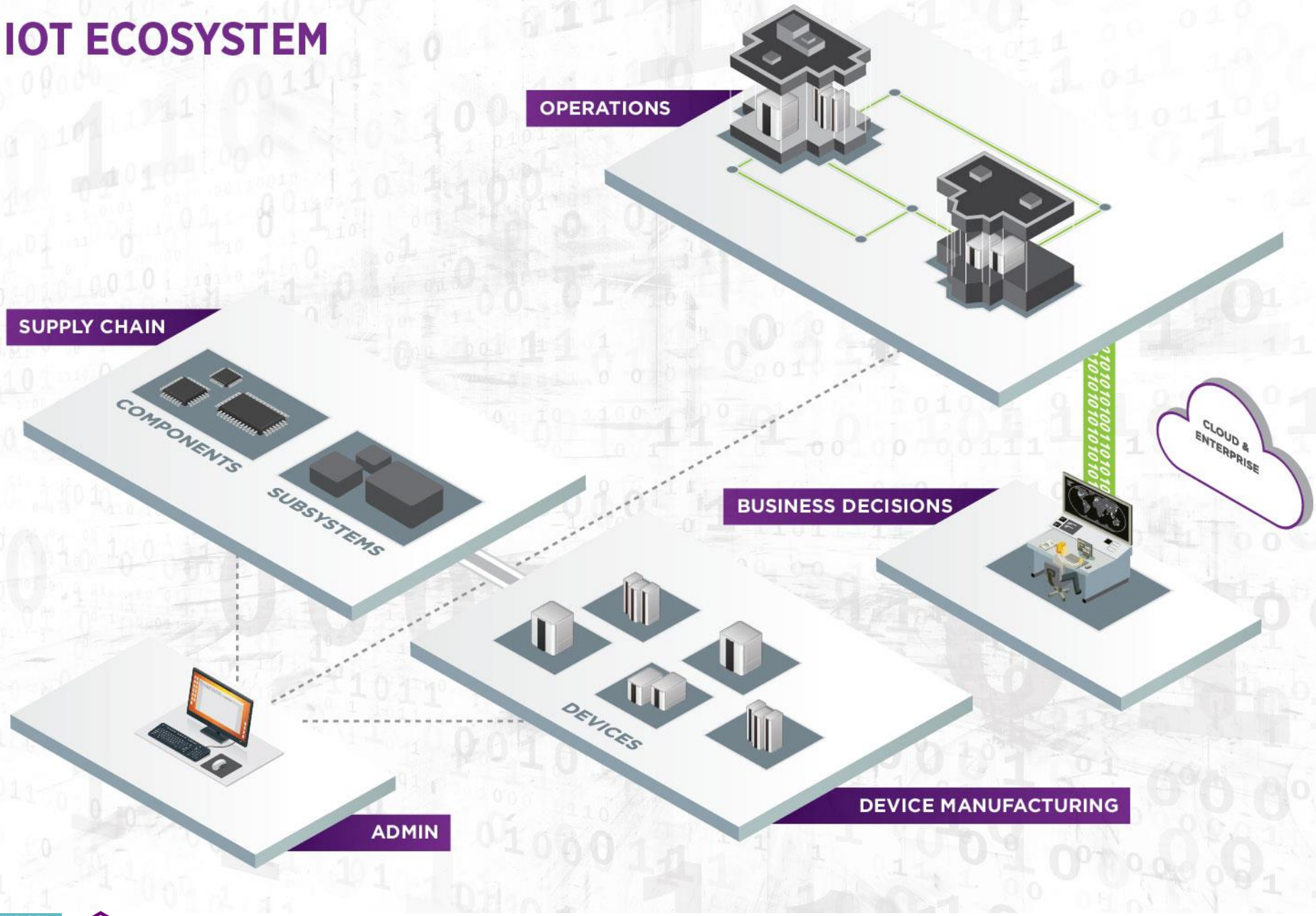
OWASP IOT Top 10 Vulnerability Categories

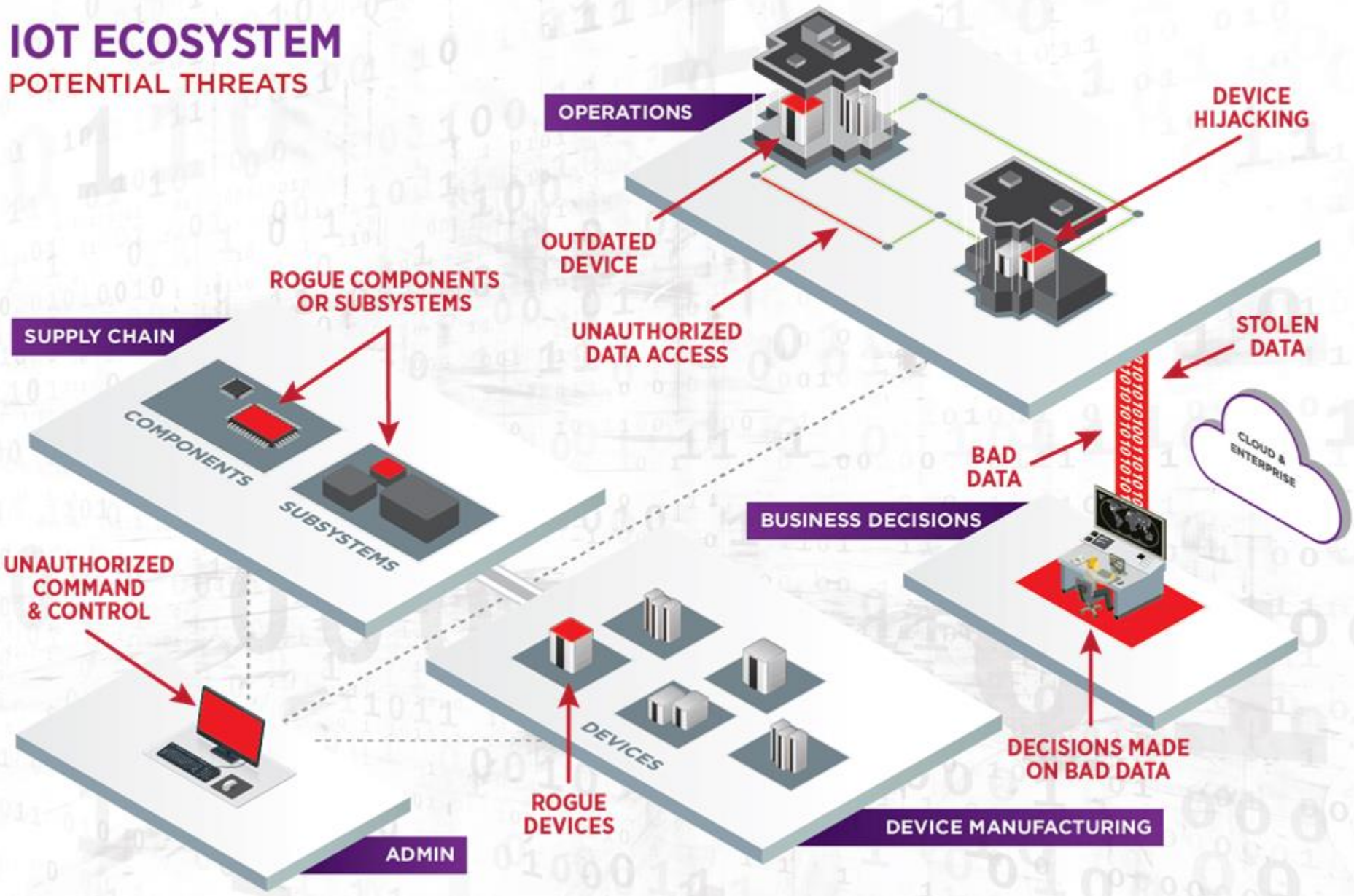
1. Insecure web interface (IOT Device Admin Interfaces)
2. Insufficient authentication/authorization (All Device Interfaces and Services)
3. Insecure network services (All services – device, cloud, web, and mobile)
4. Lack of transport encryption (All services – device, cloud, web, and mobile)
5. Privacy concerns (All system components)
6. Insecure cloud interface (Cloud API and/or web interfaces)
7. Insecure mobile interface
8. Insufficient security configurability (IOT Device)
9. Insecure software/firmware (IOT Device)
10. Poor physical security (IOT Devices)

OWASP Internet of Things Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

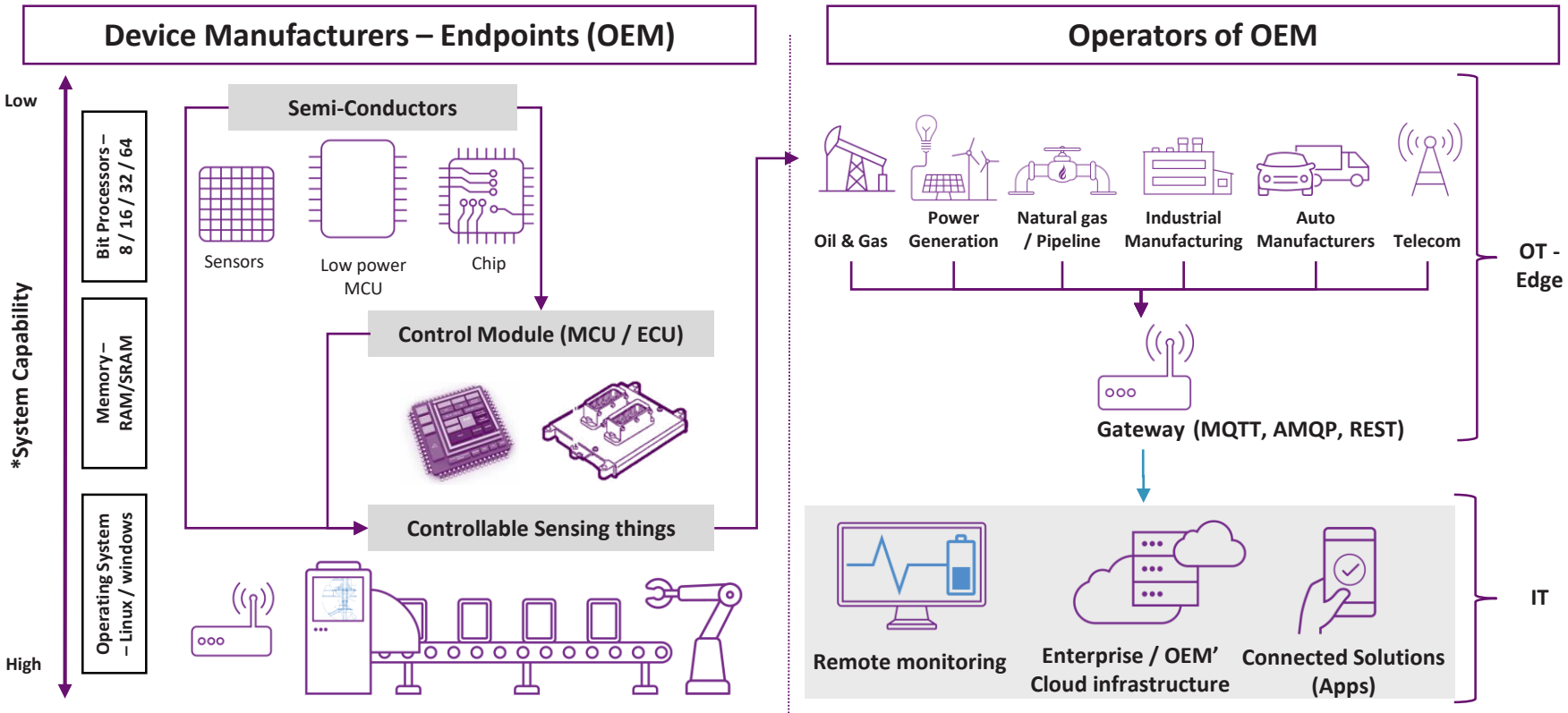
- Assess Industry specific information
- Review existing organizational threat models

IOT ECOSYSTEM




IOT ECOSYSTEM
POTENTIAL THREATS
OPERATIONS
DEVICE HIJACKING
OUTDATED DEVICE
UNAUTHORIZED DATA ACCESS
ROGUE COMPONENTS OR SUBSYSTEMS
SUPPLY CHAIN
COMPONENTS
SUBSYSTEMS
STOLEN DATA
CLOUD & ENTERPRISE
BAD DATA
BUSINESS DECISIONS
UNAUTHORIZED COMMAND & CONTROL
DEVICES
DECISIONS MADE ON BAD DATA
ROGUE DEVICES
DEVICE MANUFACTURING
ADMIN

Device Lifecycle in IoT



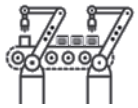
Security

- Establishing Root-of-Trust
- Addition of Device attributes & bootstrap certificate / token
- HSM, TPM, eSIM, SE, TEE
- Key Management
- Ownership transfer
- Discovery
- Device Authentication
- Provisioning & Authorization
- Policy - Data, Communication, & Lifecyle changes
- Integrity
- Device Update – Firmware, Credential and Ownership

Entrust Datacard

SECURE TECHNOLOGY ALLIANCE

Key IoT Roles



ENSURING SUPPLY CHAIN INTEGRITY FROM CHIP TO DEVICE

- Unique Device Identity and Key Management
- Secured Firmware and Software Delivery
- Geo/Contract Mfg License Enforcement
- Transfer of Ownership
- Manufacturing Execution System Support

SECURING DATA OPERATIONS AND ENABLING A TRUSTED INFRASTRUCTURE

- Secured Device Provisioning and Enrollment
- Protect Data at Rest and in Motion
- Control Access at the Edge with Brownfield Support
- Secure Updates and Lifecycle Management

Many device manufacturers will also be operators providing provisioning, predictive maintenance, remote monitoring, and product as a subscription offerings

Getting Started

Gartner

G00325538

"Don't Let Your IoT Projects Fail: Use the Right IoT Security Pattern to Protect Them"

- Recommendations for SRM leaders
- Key project characteristics
- Mapping of controls

industrial internet CONSORTIUM

IIC G1 and G4

"IIC Reference Architecture" and "IIC Security Framework"

- Guidance on IOT system architecture and principles
- Security framework for the IIRA
- Vertically focused on industrial

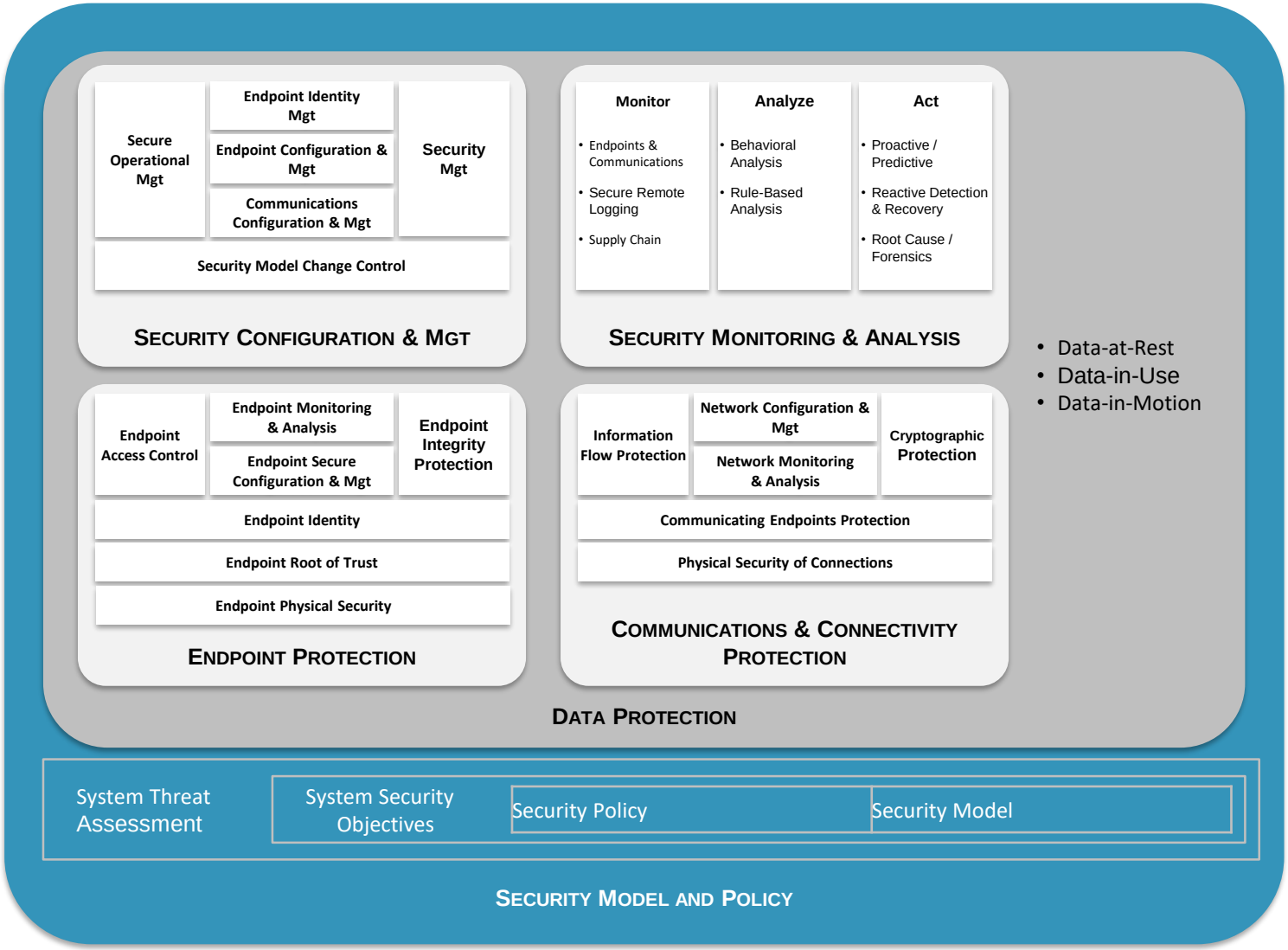
NIST

NISTIR 8200 (DRAFT)

"Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)"

- General IOT security Principles
- Industry examples
- Related Regulations

IIC Security Framework



Summary Considerations

- IT security processes don't typically address supply chain as a critical element
- Device environments are heterogenous, with a wide-variety of lifecycles, and brownfield vs greenfield considerations
- Automation of the onboarding process becomes critical at scale and reduce costs
- Multiple identities and transfer of ownership will be common
- Edge requirements and reliability/safety vs security tradeoffs are new

The physical / operational characteristics of IOT bring new risk and requirements

Use a framework to get started – they're capturing best practices

Consider IOT specific solutions as they reflect these unique needs and can help reduce costs / timelines

SECURE TECHNOLOGY ALLIANCE

Q&A

Selected Secure Technology Alliance Resources

- **Secure Technology Alliance Knowledge Center** - https://www.securetechalliance.org/knowledge-center/
  - Blockchain and Smart Card Technology
  - Embedded Hardware Security for IoT Applications
  - Implementation Considerations for Contactless Payment-Enabled Wearables
  - IoT and Payments: Current Market Landscape
- **IoTSecurityConnection.com** portal
- **IoT Security Council**
- **Securing Digital ID 2018**, December 4-5, 2018, Washington, DC - http://securingdigitalid.com/?utm=STA-Next-Event

SECURE TECHNOLOGY ALLIANCE

Contact Information

- Randy Vanderhoof, rvanderhoof@securetechalliance.org
- Sri Ramachandran, sri.ramachandran@gi-de.com
- Steve Hanna, Steve.Hanna@infineon.com
- John Neal, john.neal@nxp.com
- Josh Jabs, Josh.Jabs@entrustdatacard.com

SECURE
TECHNOLOGY
ALLIANCE