



HANNOVER MESSE 2024

No Digital Transformation without Cybersecurity

Ryan Dsouza

Principal Solutions Architect, AWS

Robert Andres

Chief Security Officer, Eurotech

Some security challenges in OT



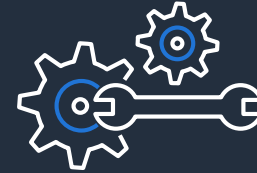
General lack of
cyber risk
mitigation



Inflexible change
control
procedures



Inconsistent
endpoint visibility



Security update
challenges



Insecure legacy
industrial
protocols

Safety and Availability

Stay secure while moving fast



Secure by
Design



Zero Trust



Security
Standards



Defense in
Depth

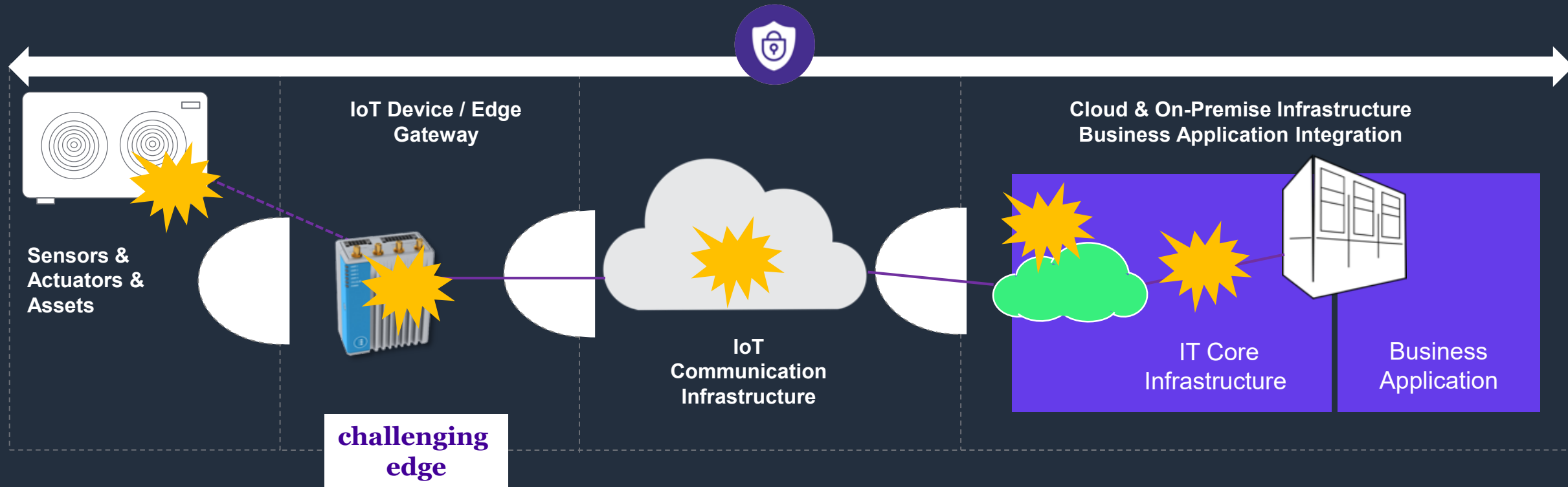
Secure by Design

1. Design for security from the start
2. Start with a cyber security risk assessment
3. Build security features into products and solutions
4. Implement security throughout a product's life-cycle
5. Use secure configurations by default



Secure by design

Security has to be a fundamental part of the overall architecture



- Design for security from the start of any digital transformation project
- Security needs to be built in (elements & systems) from ground up
- Use secure by default configurations

Zero Trust security principles

1. Follow zero trust security principles of never trust and always verify
2. Strong identity and least privilege access control
3. Continuous audit and monitoring

Zero Trust architecture

Apply Zero Trust security principles throughout the solution



system-level security

- Attack footprint minimized
- Encryption and Authentication
- Life-cycle-management

cloud-level security

- Integrated Certificate Management
- Validated Server Identity
- Role-based Access Control
- 2-factor Authentication

secure communication

- Encryption and Authentication
- Digitally Signed Messages
- Remote access, VPN

Security guidance & best practices

Designed to meet security standards

Continuous Monitoring & Improvement including Pen Tests

device-level security

- Unique Device Identity and Credentials
- Hardware Root of Trust
- Firewall, DDoS, IPS/IDS, Anti-Malware
- Encryption and Authentication
- TPM 2.0 and anti-tamper HW
- Secure Boot



Security Standards

1. Use security standards such as ISA/IEC 62443, PSA Level 1
2. Choose products which designed and certified to meet ISA/IEC 62443
3. Ensure a solid approach to device identities, leveraging standards like IEEE 802.1AR

Security Standards – Some Elements

PSA Level 1, IEC 62443-4-2

Secure Management

Secure audit and secure over-the-air updates for all components of the software on the device. Secure provisioning of device credentials and certificate management

System Integrity and Trusted Execution

Create a trusted execution environment by verifying software authenticity and integrity. File system integrity, Firewall, DDoS protection, IPS/IDS, malware protection, etc.

Device Attestation and Protected Data

Device Identity anchored to the hardware for secure attestation. Protected repository for sensitive data and keys at rest.

Platform Integrity

Secure and measured boot process with hardware attestation of the boot loader and OS kernel. Anti-tampering.

Certified cybersecurity approach

Holistic security requires holistic security standards



27001

— information security



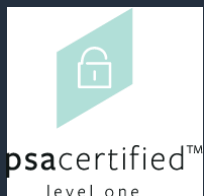
62443-4-1

— secure product development



62443-4-2

— certified secure programmable product



certified full
stack IoT
gateway



**operator /
asset owner**

**system
integrator**

**component
supplier**

policy & procedures

OT / IIoT solution
(IEC 62443-3-3)

subsystem

subsystem



product
(IEC 62443-4-2)

devices

programmable
edge

automation
components

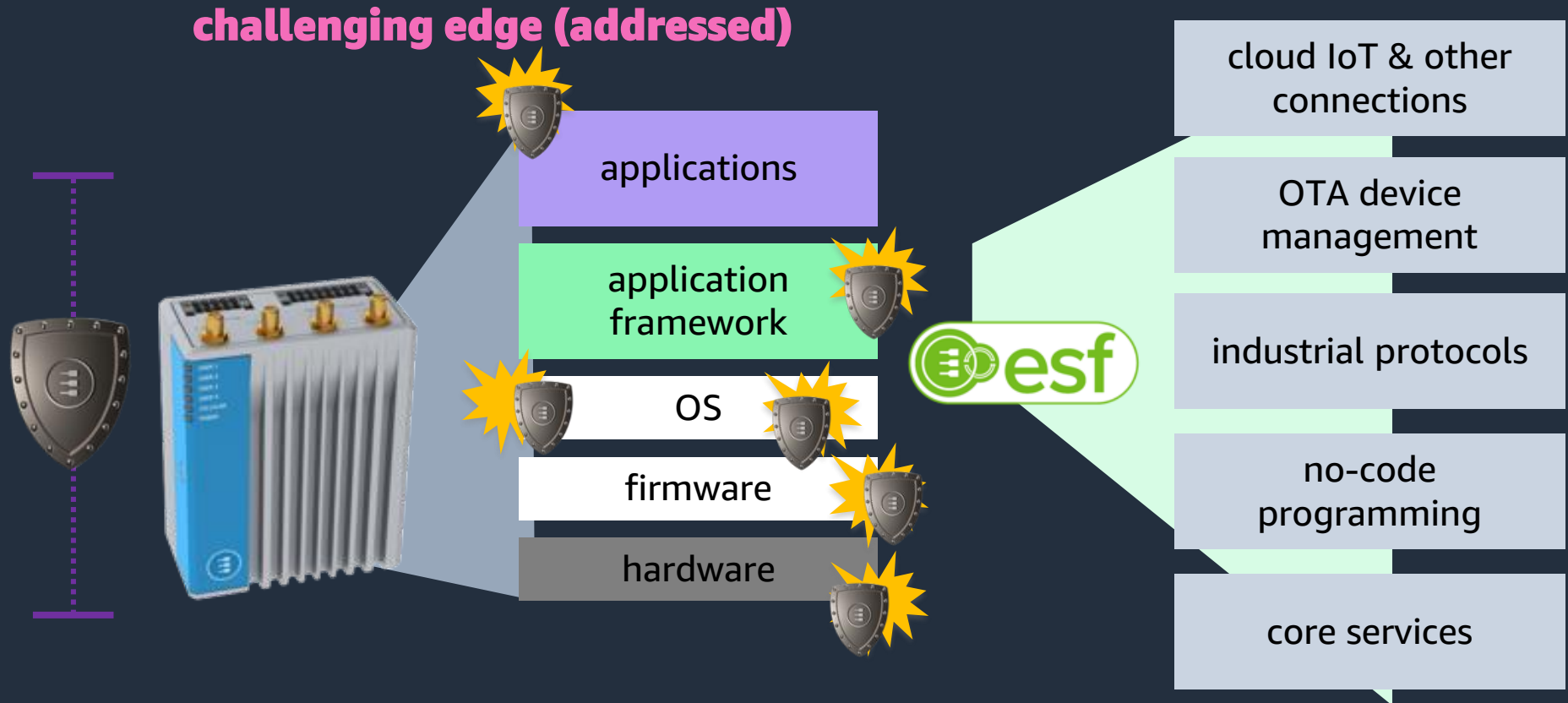
network
components

Certified cybersecurity approach using standards

Significantly Reduce Cost, Risk, Time, & Effort by “inheriting” product certification

**complete stack
optimized &
certified**

**IEC 62443-4-2
PSA Level 1**



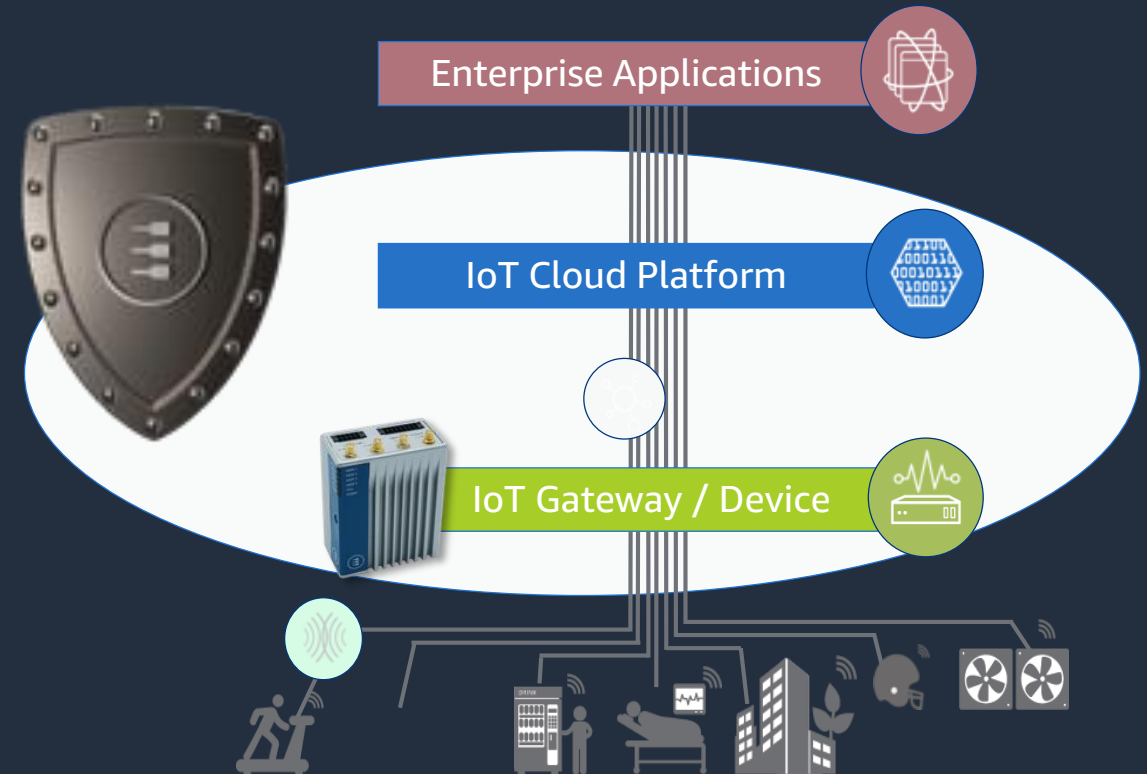
Defense in Depth

1. Implement multiple layers of defense using multiple security controls
2. Secure devices, networks, edge and cloud
3. Follow AWS's ten security golden rules for IIoT solutions
4. Secure device onboarding at scale, employing Zero-Touch Provisioning (ZTP)
5. Security related updates are essential – secure device management is essential

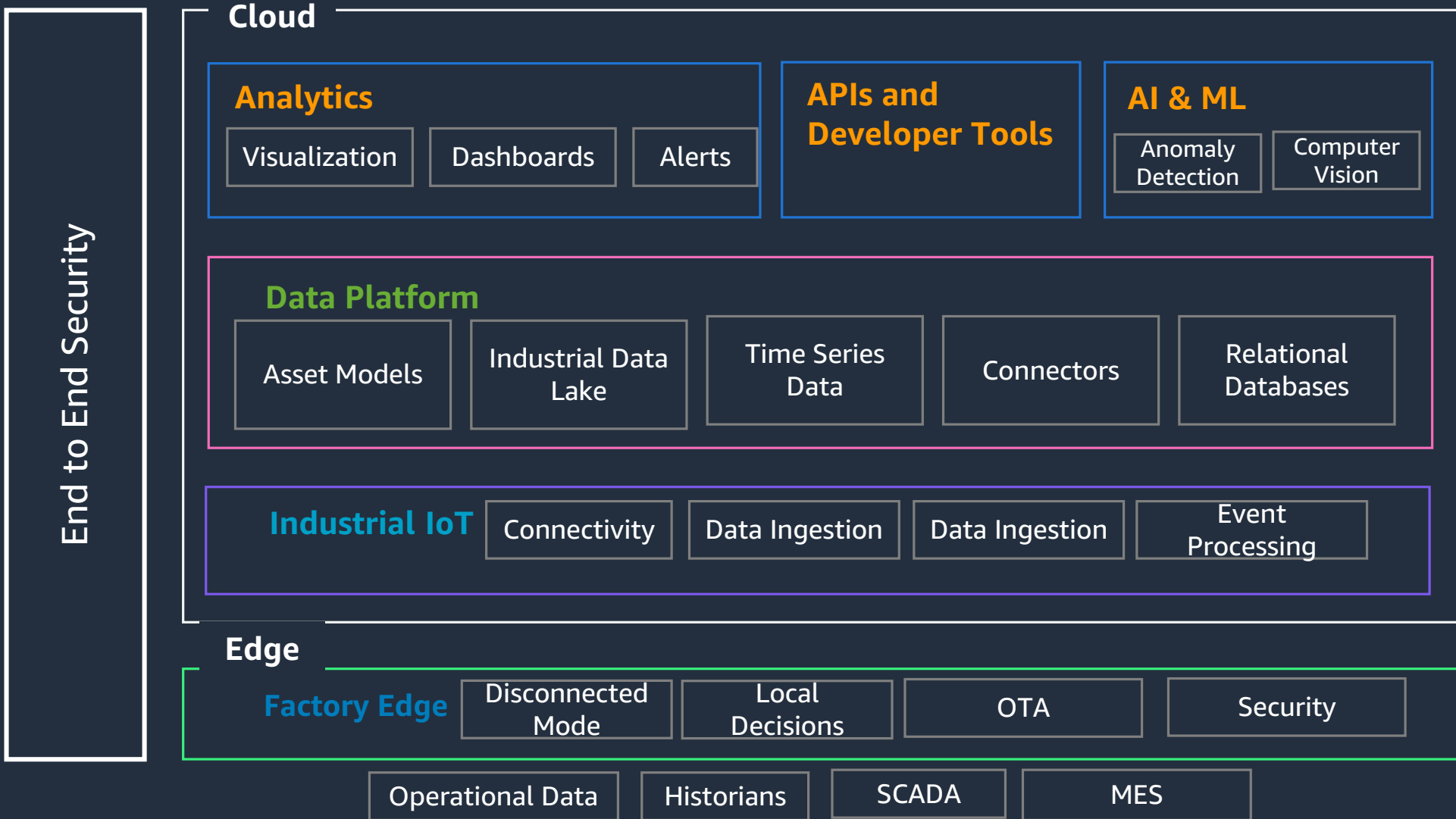
Defense in Depth

Designed to meet IT & OT Security Standards / Certifications

- Open and industry standards
- Proven security technologies
- Scalable and resilient
- Designed for OT demanding environments
- Continuous testing, auditing and enhancing
- Ten security golden rules



End-to-end capabilities for industrial digital transformation



Securely transform your industrial operations with AWS

Scalable, performant, secure and cost-effective services for industry

Foundational IoT and AI/ML services
for general purpose use cases



AWS IoT Core



Amazon SageMaker



Amazon Managed
Grafana



AWS IoT Greengrass



AWS IoT Device
Management



AWS IoT Device
Defender



Amazon Kinesis Video
Streams

Purpose-built IoT and AI/ML services for
industry use cases



AWS IoT SiteWise



AWS IoT TwinMaker



AWS IoT Events



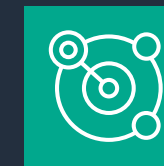
AWS IoT SiteWise
Edge



Amazon Monitron



Amazon Lookout for
Equipment

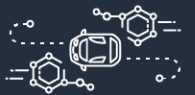


Amazon Lookout for
vision



Keys to secure digital transformation

1. Design for security from the start
2. Follow zero trust security principles
3. Use security standards such as ISA/IEC 62443
4. Implement defense in depth
5. Keep continuously improving



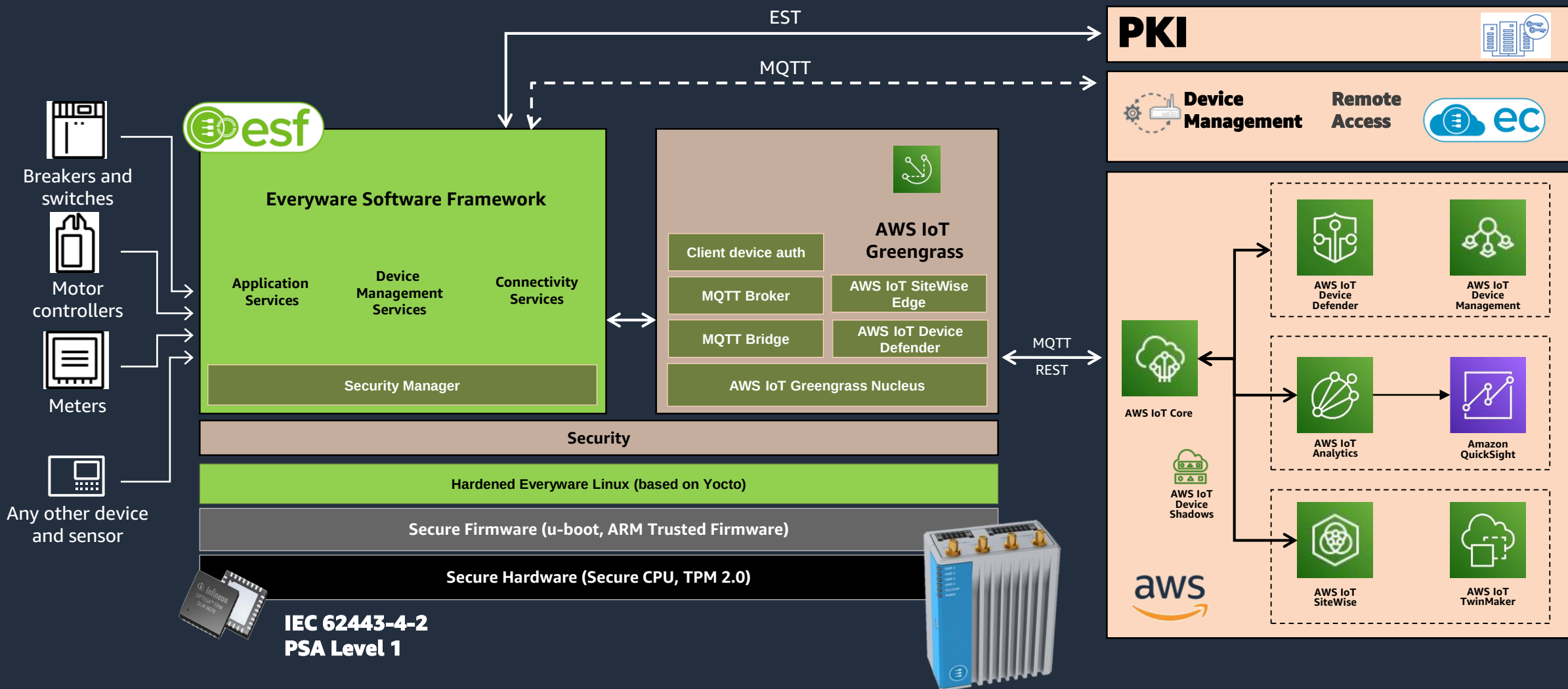
Eurotech and AWS collaboration

Helping companies accelerate secure industrial digital transformation

1. Bringing OT, edge and cloud capabilities together with integrations which accelerate time to value for customers
 - AWS IoT Core
 - AWS IoT Greengrass
 - AWS IoT SiteWise Edge
2. Eurotech Everyware GreenEdge
3. Unified customer billing experience



AWS IoT Greengrass / Eurotech ESF integration



Visit the AWS booth in Hall 15, Booth D76





Thank you!

Ryan Dsouza

rydsouza@amazon.com

Robert Andres

robert.andres@eurotech.com

Robert Hanuschke

AWS