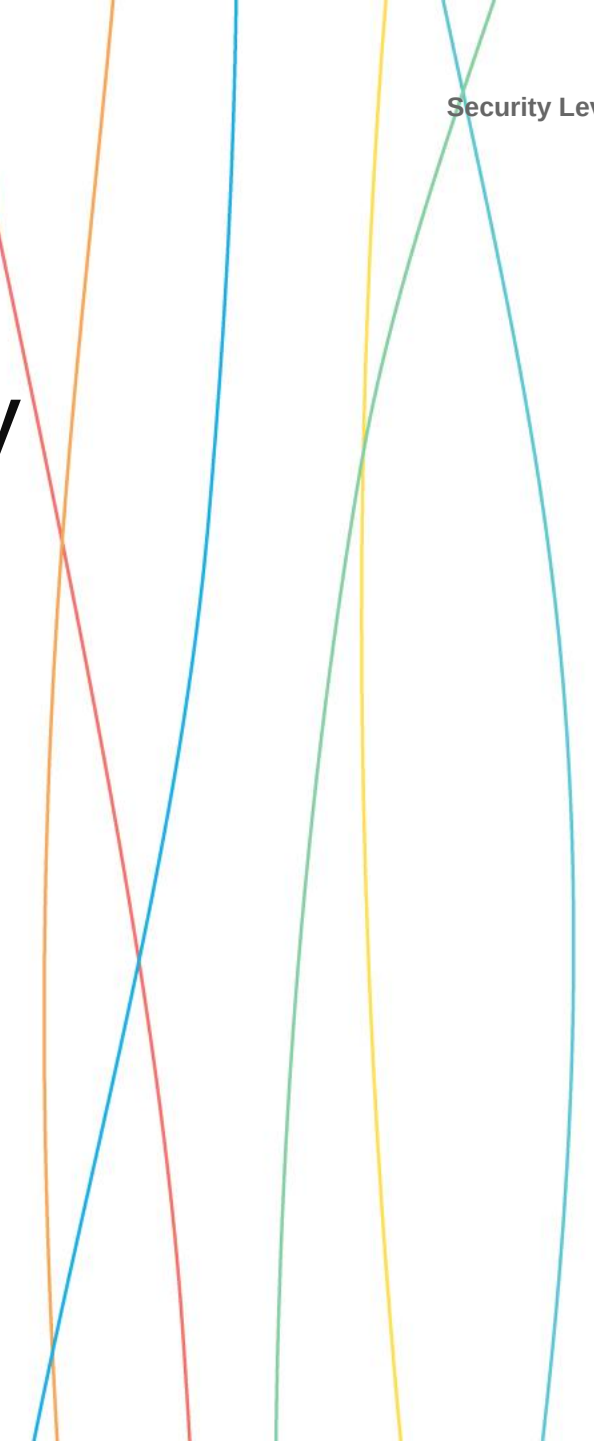
Security Level:

15 / 05 / 2018

Industry 4.0 from an IoT security standpoint

Dr. Evangelos Gazis
Chief Architect IoT Security
ENISA IoTSec Expert Group



Key questions for today's session

Industrie 4.0 connects humans, machines, processes, and the flow of goods along value chains

- Which security requirements do we expect for this infrastructure and how can such an infrastructure be established?
- How can we assure a high trust level along the value creation network

Security by design has to be the superior principle

- How can security-by-design be accomplished for the complete life cycle?
- How does a road map for an Industrie 4.0 security ecosystem look like?

[1] ENISA Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015)

Is security really and issue for the value chain?

~ 80% of data breaches have a supply chain origin

~ 45% of data breaches leveraged components of a (current or past) partner

~ 70% of companies lack visibility in their supply chain

~ 60% of companies lack an appraisal process for the cybersecurity of its partners

~ 40% of companies surveyed suffered a data breach in the last 12 months

~ 40% of companies surveyed had financial losses 1-10 MUSD

[1] SANS Institute, “Combatting Cyber Risks in the Supply Chain”
[2] “Deloitte, “Cyber risk in Advanced Manufacturing”

Challenges and drivers to security in Industrial IoT

Challenges

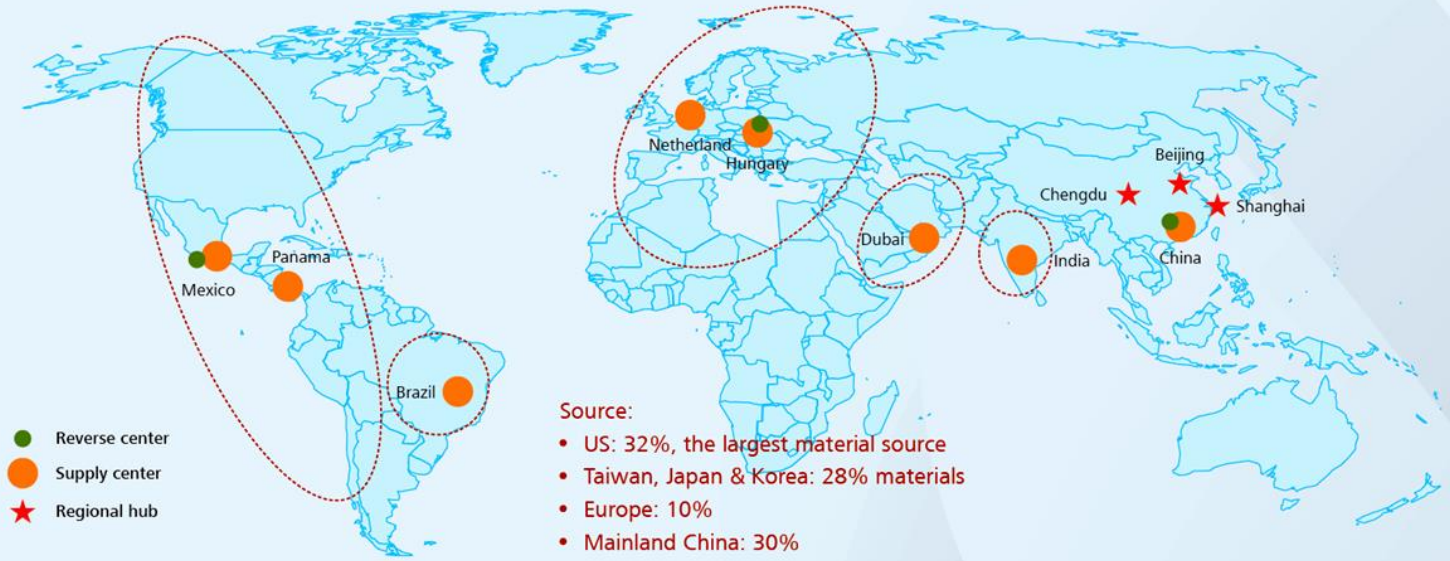
- Lack of visibility
- Lack of transparency
- Lack of alignment
- Lack of controls

Drivers

- Internet of Things (instrumentation and interconnection
- Digitization (code as the innovation engine)
- 3-D Printing (fine-grain embedment)

Huawei’s supply chain situation

Huawei Global Supply Network



Source:

- US: 32%, the largest material source
- Taiwan, Japan & Korea: 28% materials
- Europe: 10%
- Mainland China: 30%

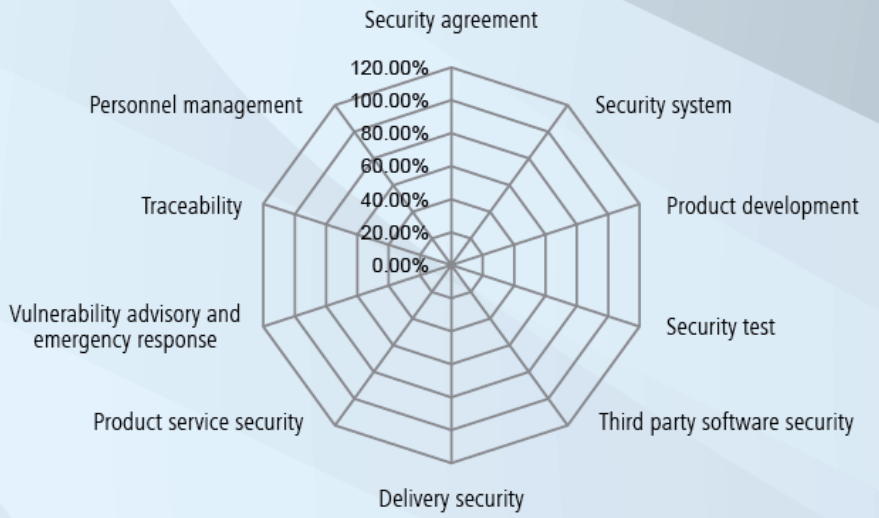
Supply Center	Reverse Center	Local EMS
• China (Delivery for the globe) • Europe (Delivery for West Europe & North Africa) • Latin America (Delivery for America, except Brazil) • Brazil (Delivery for Brazil) • India (Delivery for India) • Dubai (Delivery for Middle East)	• China • Mexico • Europe	• Brazil, Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery

Huawei’s approach to supply chain security

Supplier Name		Audit Date	
Audited Location		Contact Person & Title	
Lead Auditor		Auditor	

No.	Item	Weight	Percentage	Weighted Score	Remarks
1	Security agreement	7%			
2	Security system	12%			
3	Product development	18%			
4	Security test	20%			
5	Third party software security	6%			
6	Delivery security	5%			
7	Product service security	5%			
8	Vulnerability advisory and emergency response	16%			
9	Traceability	5%			
10	Personnel management	6%			
Total					
Grade					

This audit checklist includes 10 items and 49 questions, each of which weights 5% to 15% of the total score. There are 1 to 10 questions in each item to evaluate the supplier's cyber security.



Weighted Score	Grade	Risk Level
< 70%	D Failed	High risk
≥ 70%	C Normal	Medium risk
≥ 80%	B Good	Low risk
≥ 90%	A Excellent	Benchmark

Key supply chain aspects of security

Risk management aspects

- Secure environment
- Secure development

Authenticity

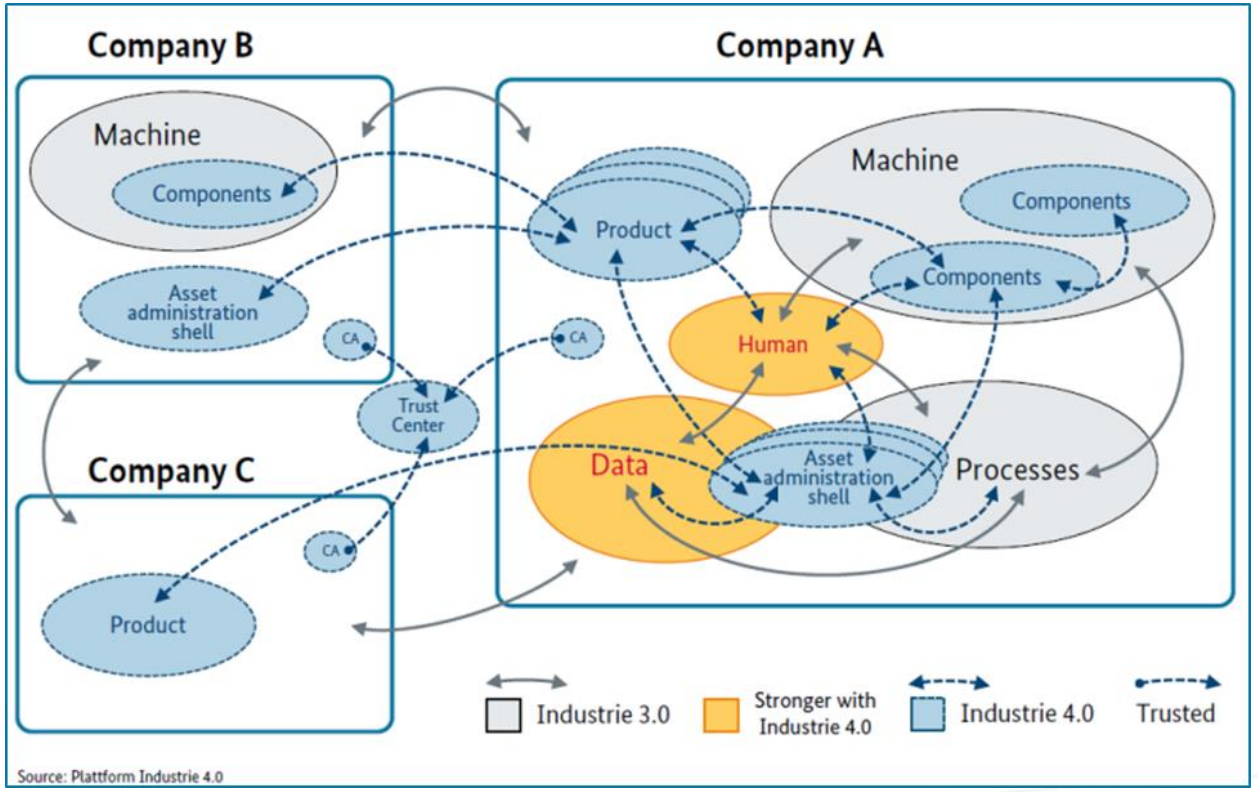
- Component (i.e. asset)
- Supplier (i.e. stakeholder)
- Interaction (i.e. trust in the supply chain)

[1] ENISA Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015)

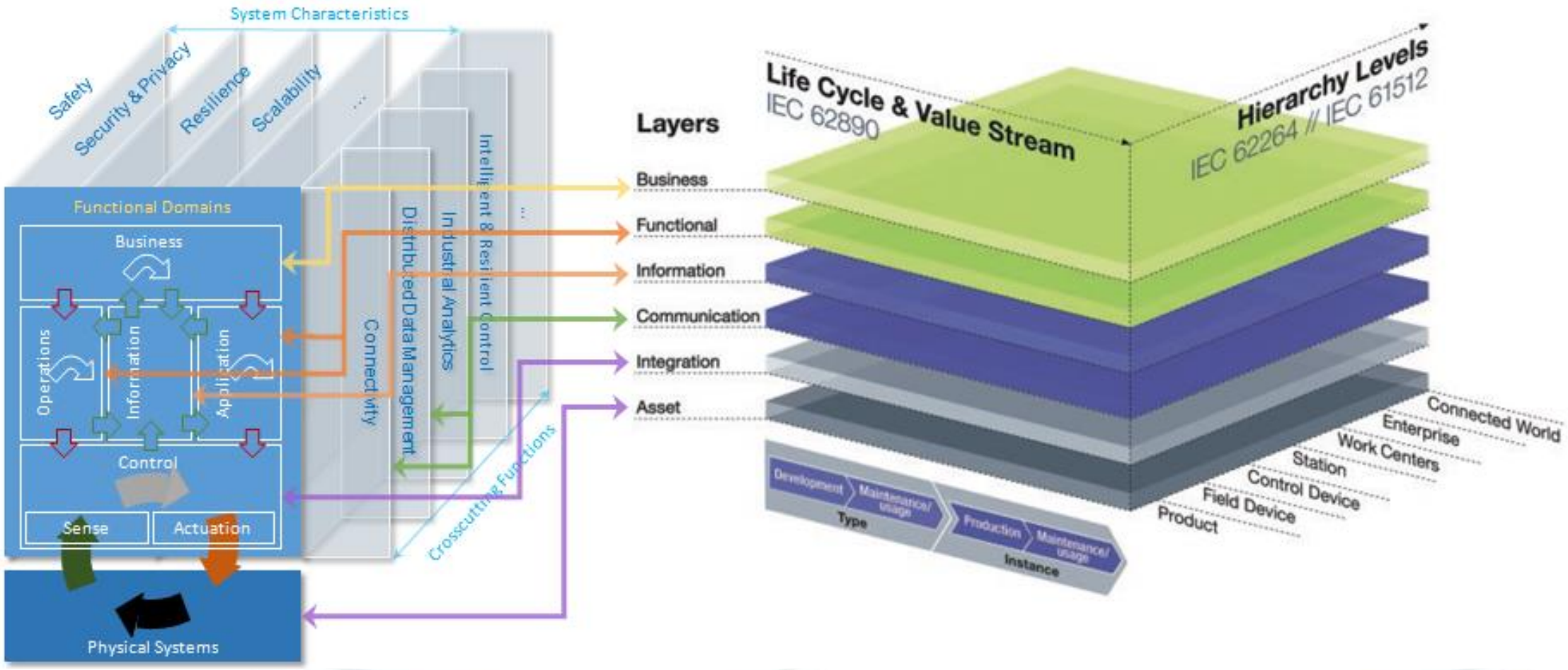
Industrie 4.0 vision

Dynamic online/semi-online system

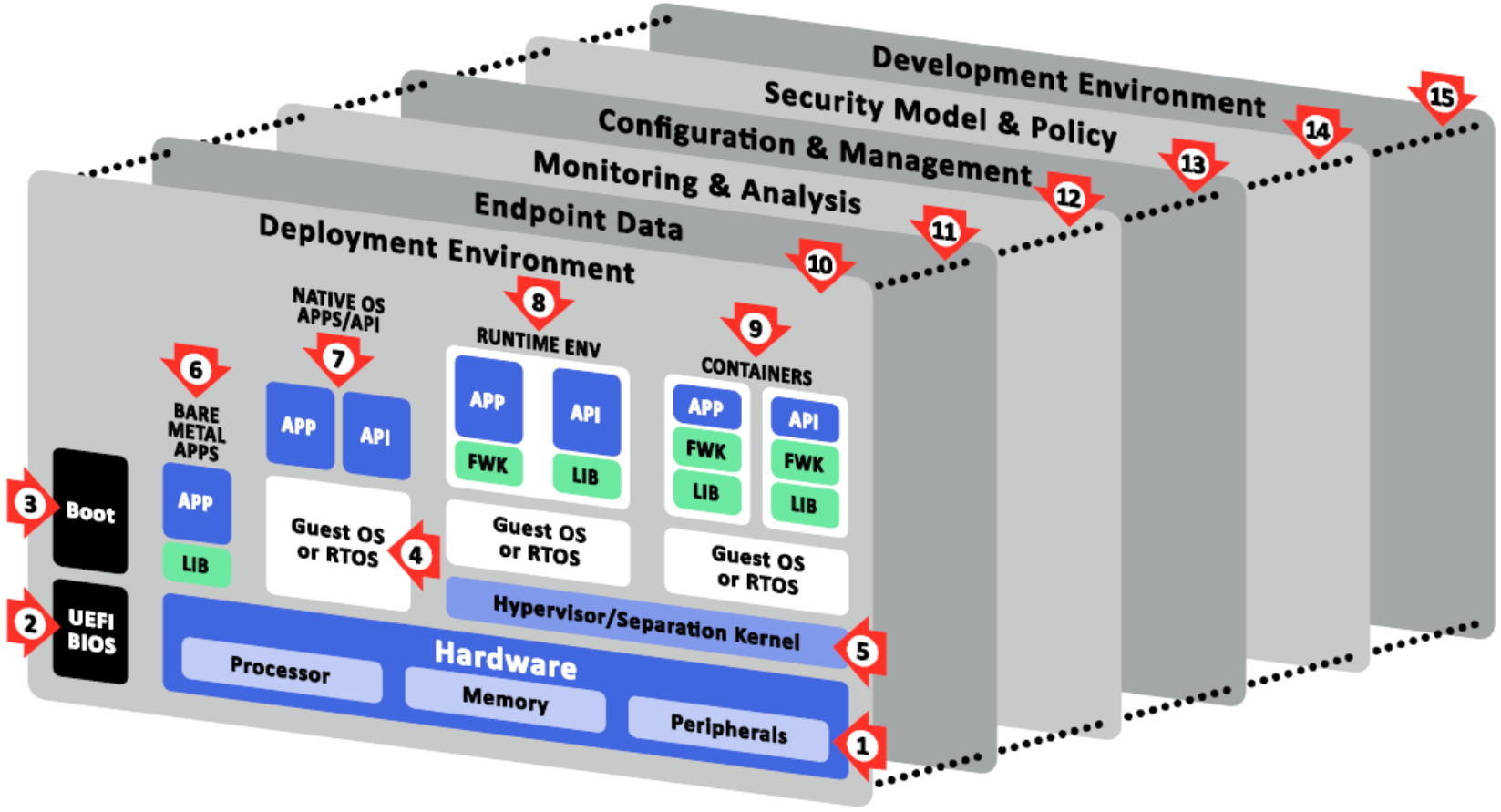
- Trust
  - Suppliers
  - Partners
- Trustworthiness
- Identification
  - Across organizations
- Interactions
  - Business purpose & relevance



Industrie 4.0 reference model



Industrial Internet Consortium threat model



Principles of security design for industrial IoT

Online trust management

- Identity management system
- Certificate management system
- Key management system

Online policy enforcement

- Policy provision (e.g. authentication, access control, etc.)
- Policy enforcement

Online intelligence management

- Knowledge management on threat and vulnerabilities

Online adaptation

- Statistical analysis at multiple levels
- Online model learning

Pillars of security architecture for industrial IoT

Security-by-design

- Security aspects MUST be integrated in requirements management

Secure defaults

- Consideration of secure defaults in system/process design

Reliable asset identification

- Tamper-proof identification framework
- Interoperable identity schemes

Compartmentalization of infrastructure

- Segregation and isolation

Policy enforcement

- Monitoring and analysis of asset interactions (e.g., DPI)
- Enforcement of policy (e.g. hardening, configuration templates, etc.)

Testing and validation

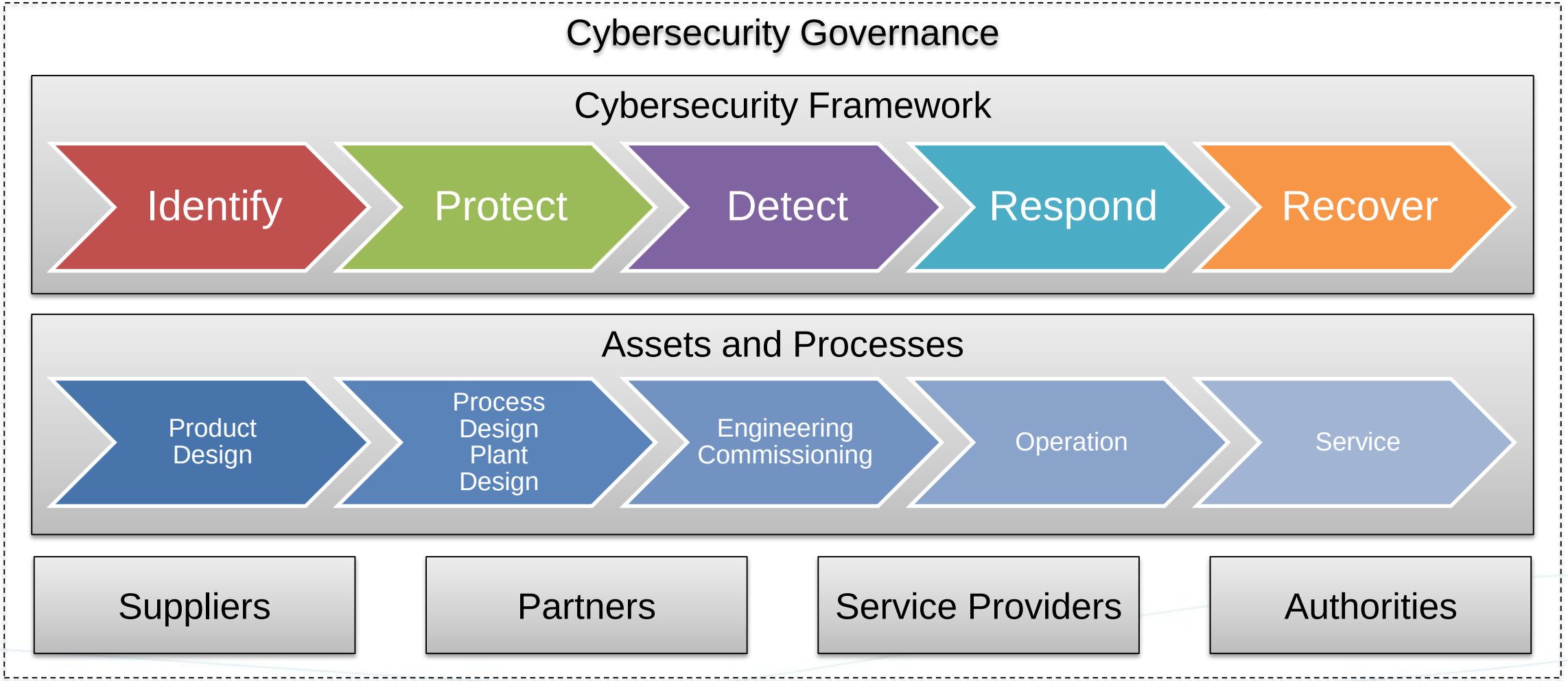
- Internal assessments (e.g. penetration tests, etc.)
- Independent assessments (e.g., reviews, audits, etc.)

Secure development throughout lifecycle processes

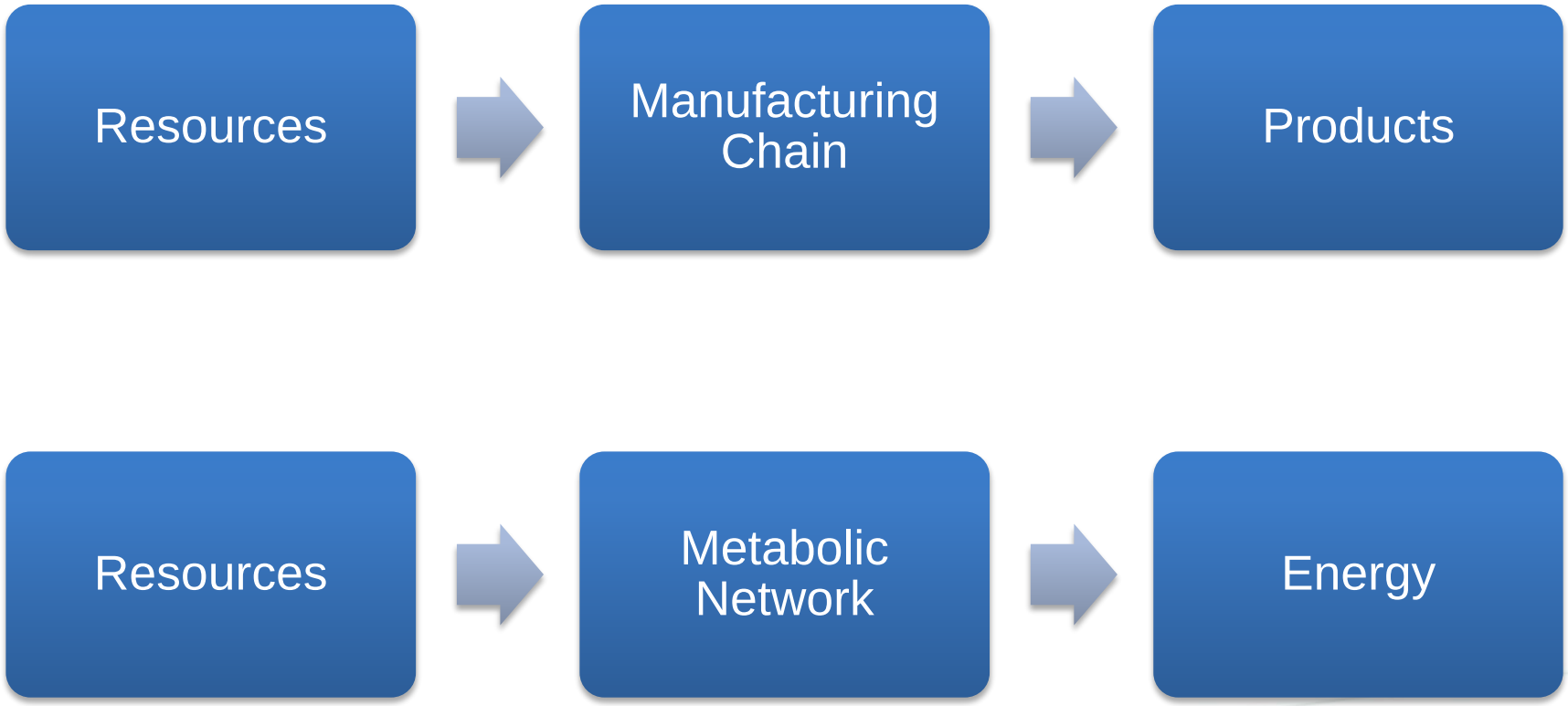
Primary Lifecycle	Supporting Lifecycle	Organizational
• Acquisition • Supply • Development • Operation • Maintenance	• Audit • Configuration Management • Joint Review • Documentation • Quality Assurance • Problem Solving • Verification • Validation	• Management • Infrastructure • Improvement • Training

[1] ENISA Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015)

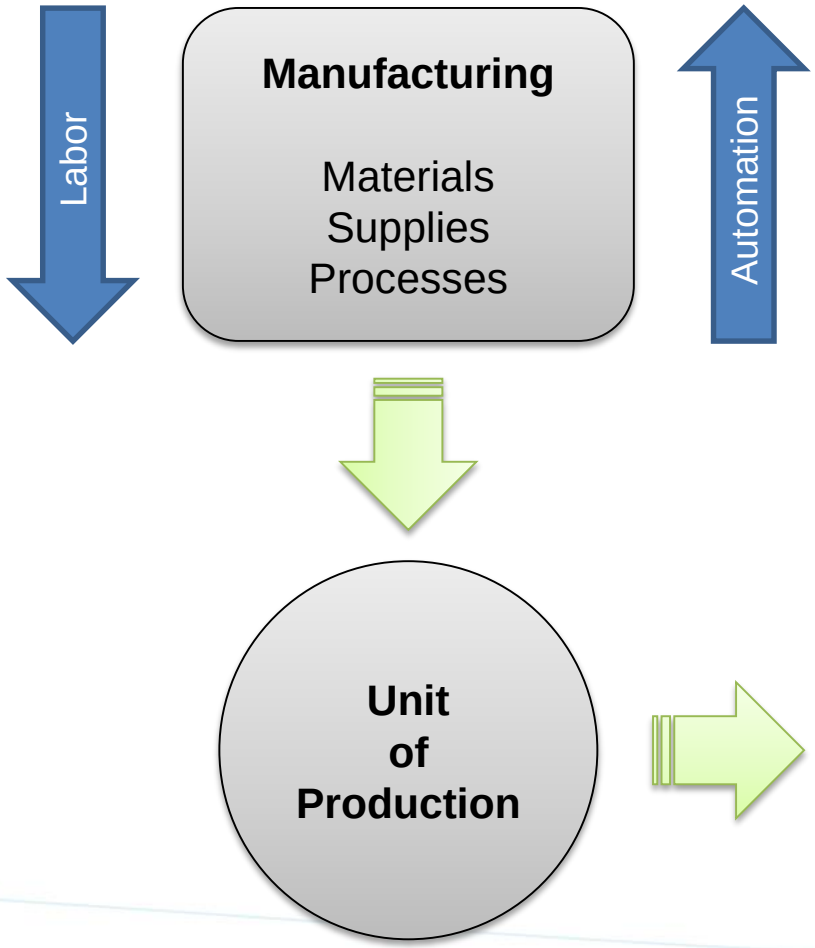
Industrial value chain design vis-à-vis security design

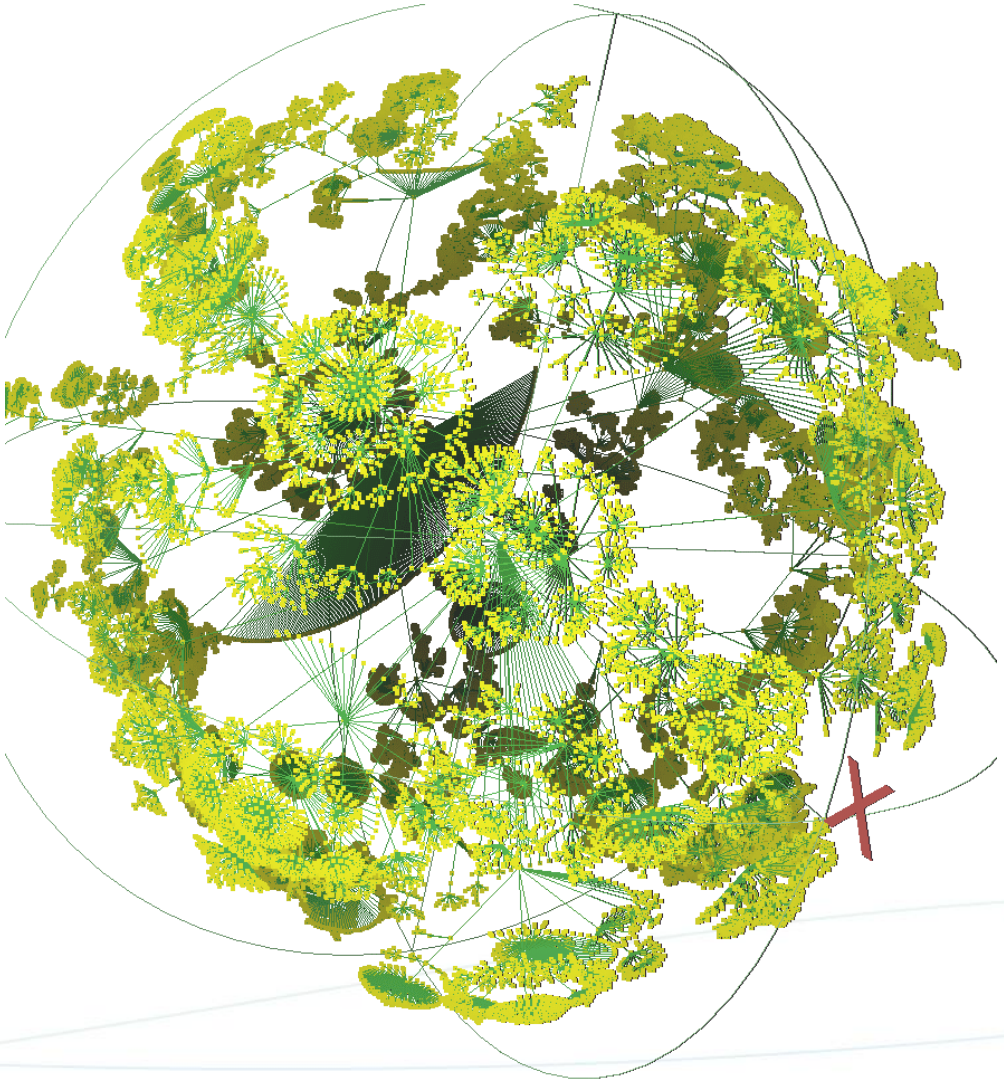


From static chains to self-balancing networks of value

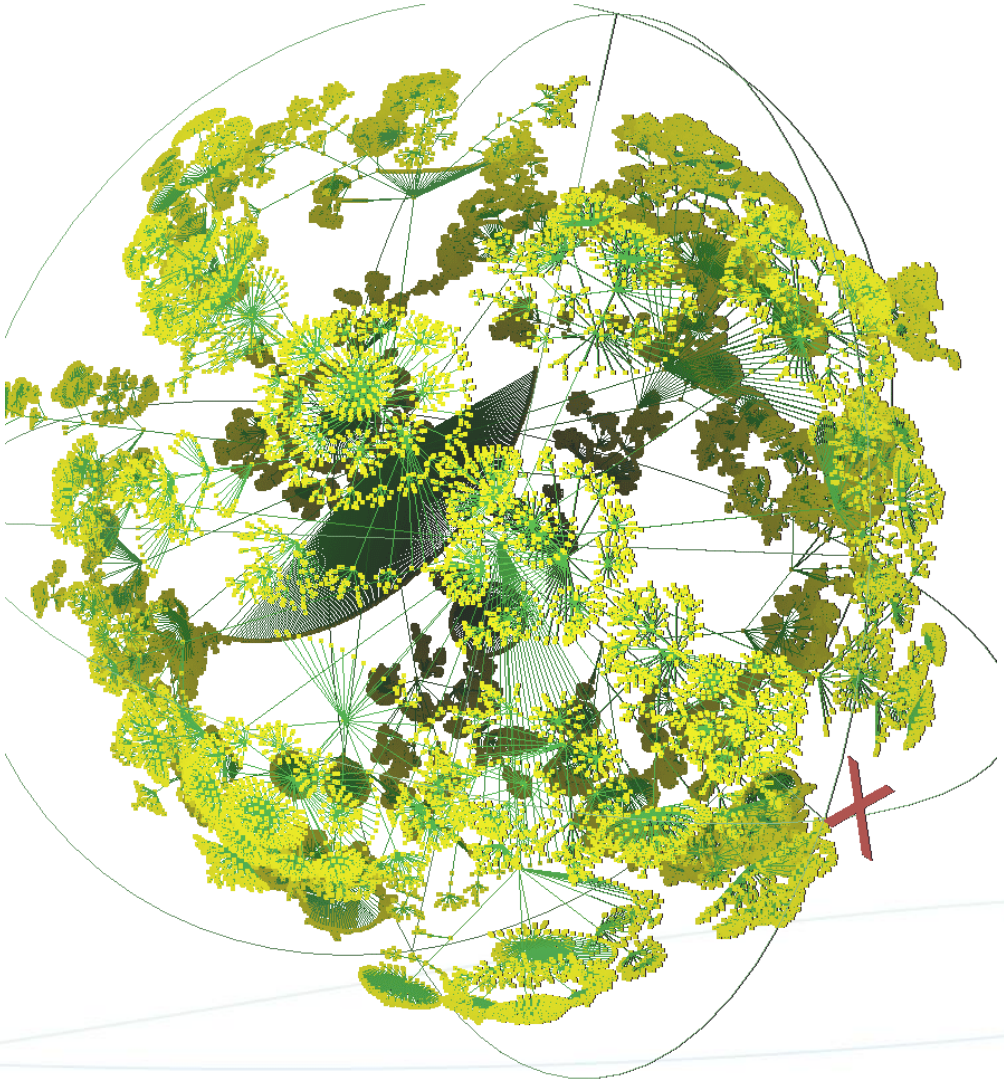


From static chains to self-balancing networks of value





How do we securely get from here to there?



Possible roadmap for ecosystem security

Establish joint initiative vehicle to drive security

- Driven by participation across the value chain
- Business enablement for value-at-risk decisions

Establish governance framework

- Decision structures
- Collaboration enablers
- Operating processes

Deploy security integration architecture

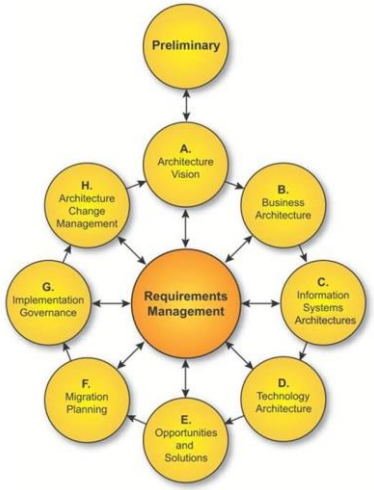
- Foundation and distribution of trust
- Standard and interoperable identity schemes
- Identity resolution and mapping services
- Services for online security management

Alignment and compliance framework

- Measures of adoption and alignment
- Acceleration of lighthouse innovation

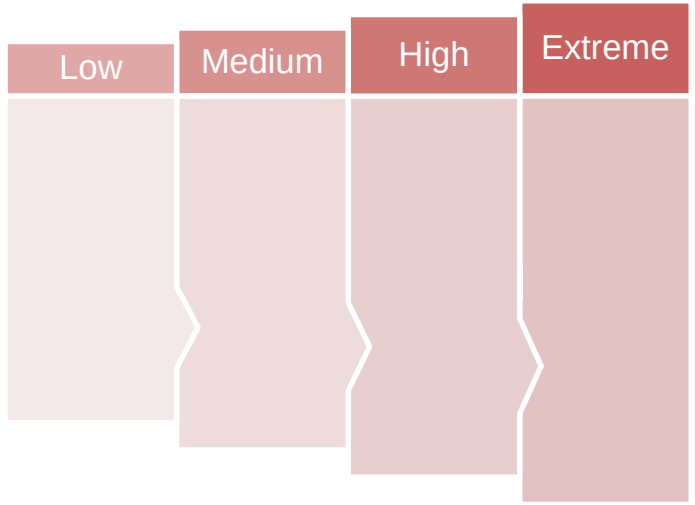
Iterative development of a security roadmap

Architecture Development Method



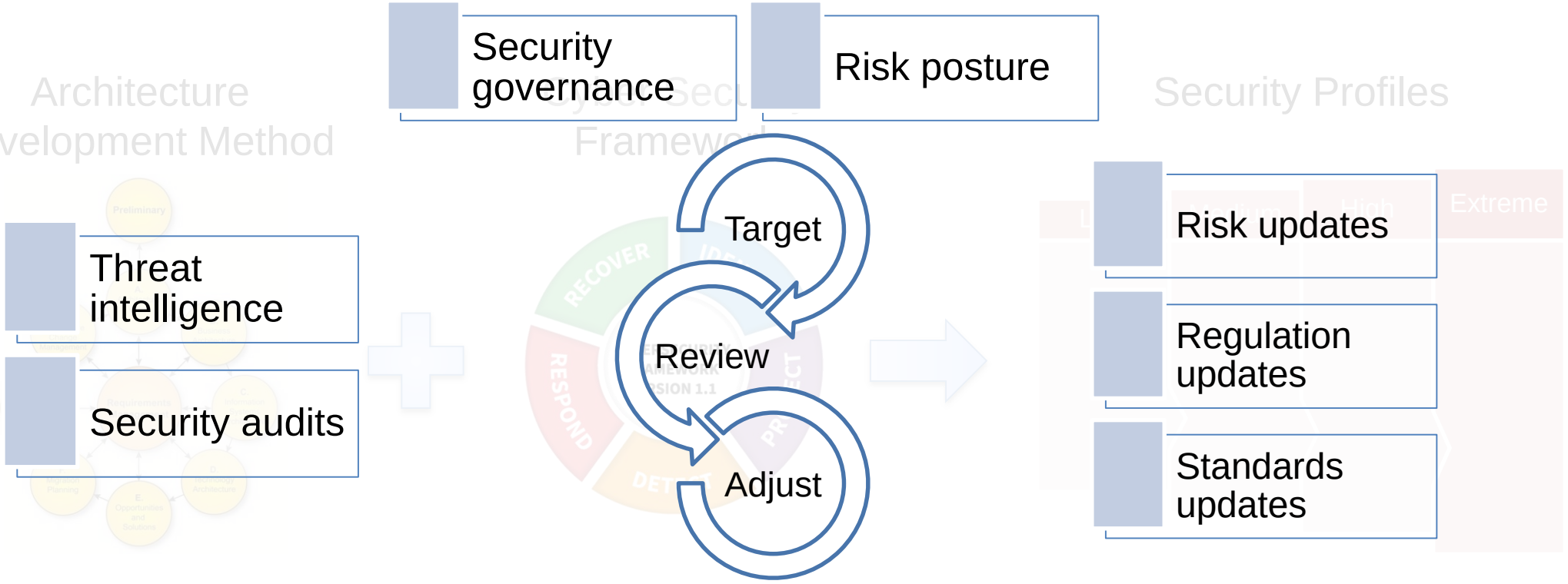
Cyber Security Framework

Security Profiles



Assets and Processes

Iterative development of a security roadmap



Assets and Processes

Product Design → Process Design Plant Design → Engineering Commissioning → Operation → Service

Thank You.