



IIC World Tour - Turin: Security Working Group Briefing



Nisarg Desai

Product Manager, GlobalSign





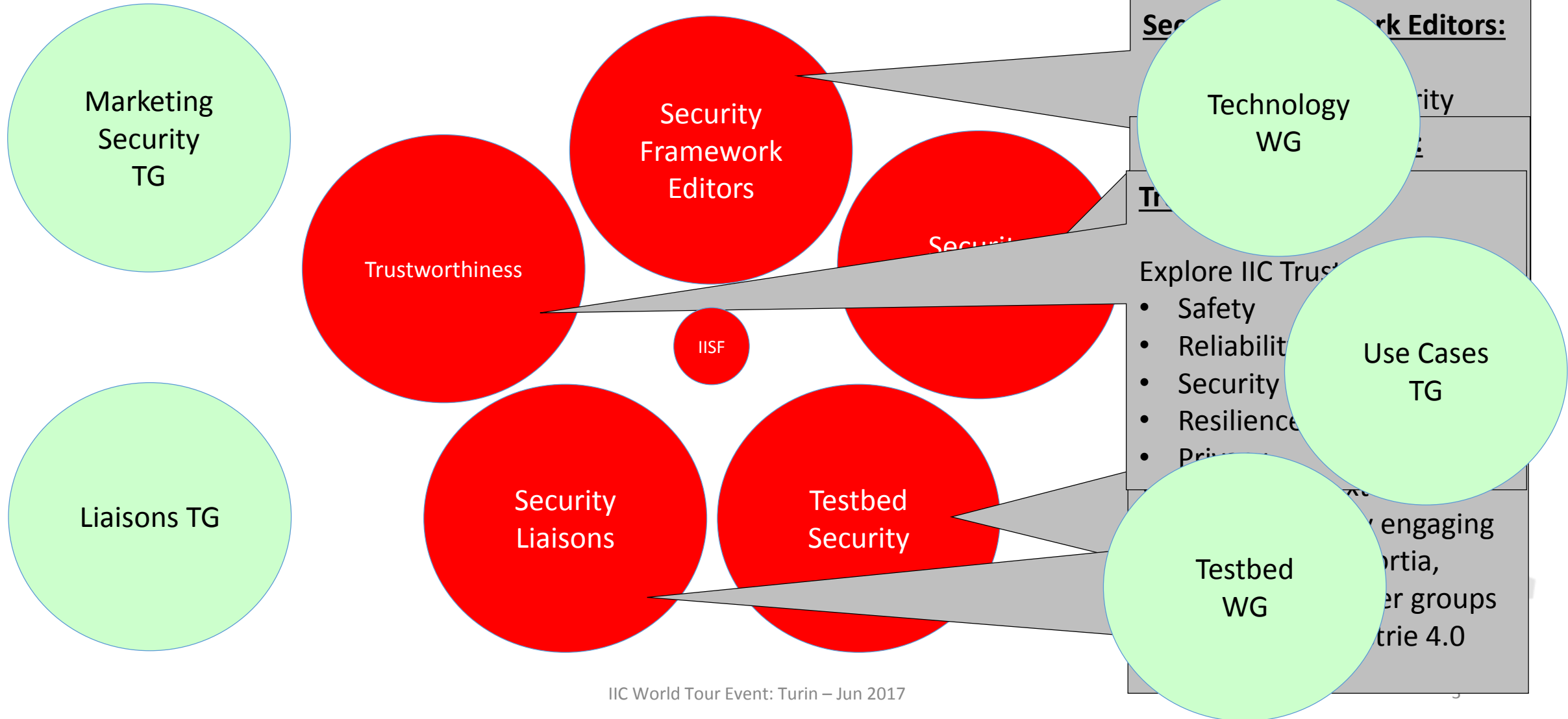
Security Working Group Charter

Group Mission	The purpose of the Security Working Group, is to address the <u>trustworthiness</u> of the IIoT ecosystem, driving the vision on safety, reliability, resilience, security, and privacy.
Scope	<p>The domain is broken down into subcategories to address individual aspects relevant to IIoT:</p> <ul style="list-style-type: none">• maintain the document library for IIoT, specifically evolving framework documents and creating support documents• guide practical implementation by working with IIC Testbeds, providing public-facing technology demonstrations, and provide thought leadership for the industry• identify gaps and construct requirements to engage with external consortia, standards bodies, and industry groups• apply the breadth of industry understanding through maturity models, use cases, case studies, norms and best practices <p>This promotes IIoT business adoption of trustworthy technology, interoperability, best practices and models</p>



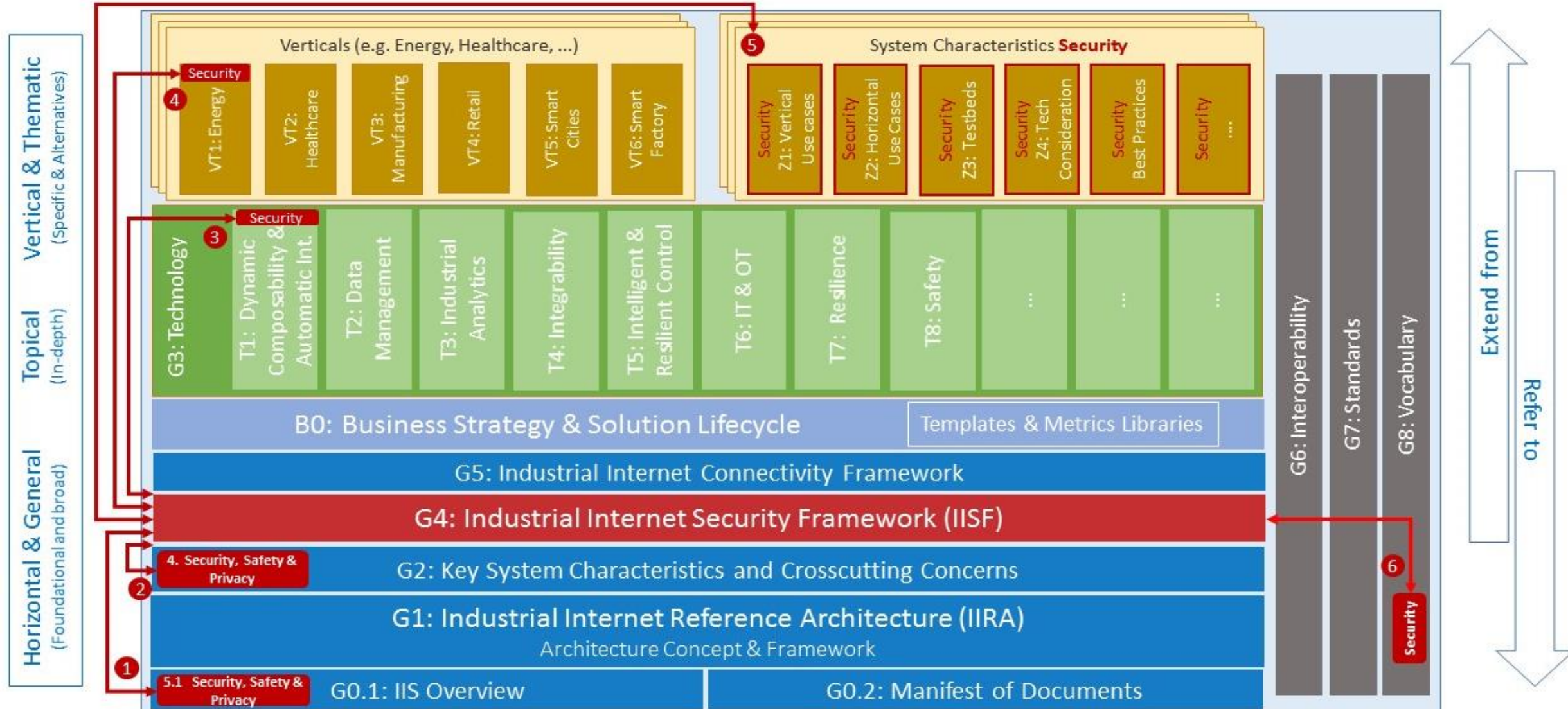


Security Working Group Organization





The IIC Library of Knowledge + Security





The IIC has published the Industrial Internet Security Framework (IISF)

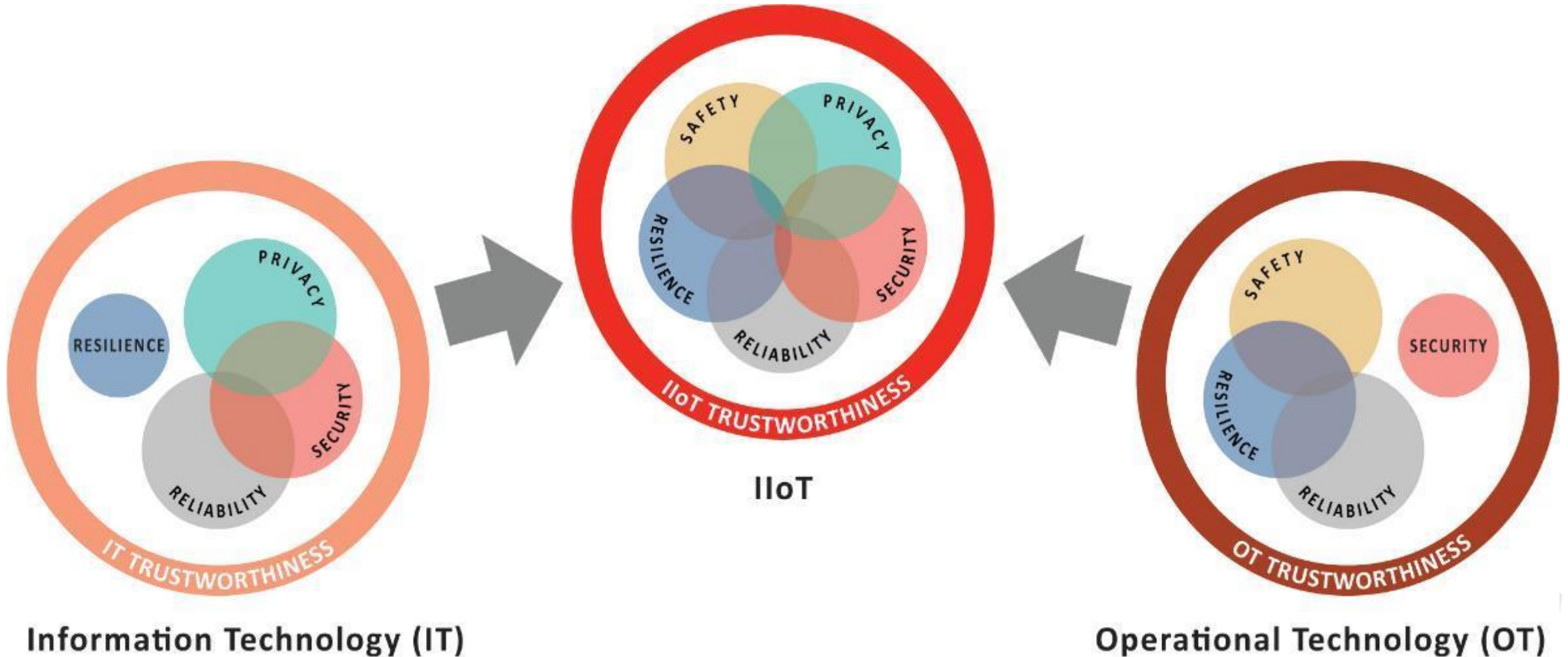
- 174 pages
- 12 chapters
- 7 Annexes
- 18 pages of reference lists
- 177 individual references
- 142 individual acronyms
- 37 figures
- 7 tables
- All references hyperlinked (Description & Download)
- Fully Indexed
- Table of contents
- Table of figures
- All hi-res (EPS) vector graphics
- 800+ comments over the lifetime of the document
- 15 version updates in one day (mid-July)

<http://www.iiconsortium.org/IISF.htm>





IIoT Trustworthiness: OT/IT Convergence



Information Technology (IT)

Operational Technology (OT)





Trustworthiness: Basis for Industry Adoption of IIoT

- Industrial Business Benefits from IIoT Trustworthiness
- Leverage Trustworthiness to Manage Risk:
 - increase likelihood of correct business decisions
- Permeation of Trust:

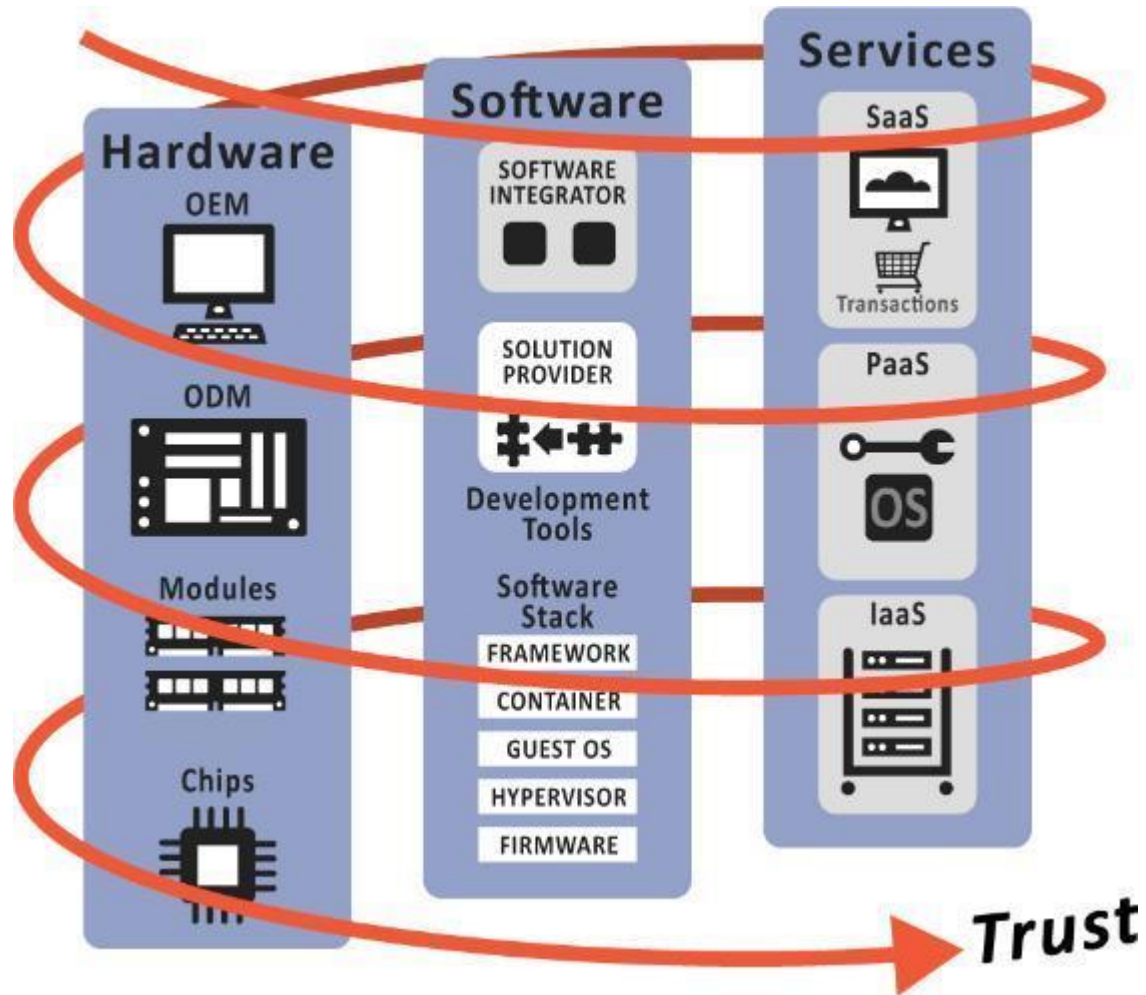
Assure Trust across the entire Industrial System

- Component Builders
- System Builders
- Operational Users





Assurance of the Permeation of Trust



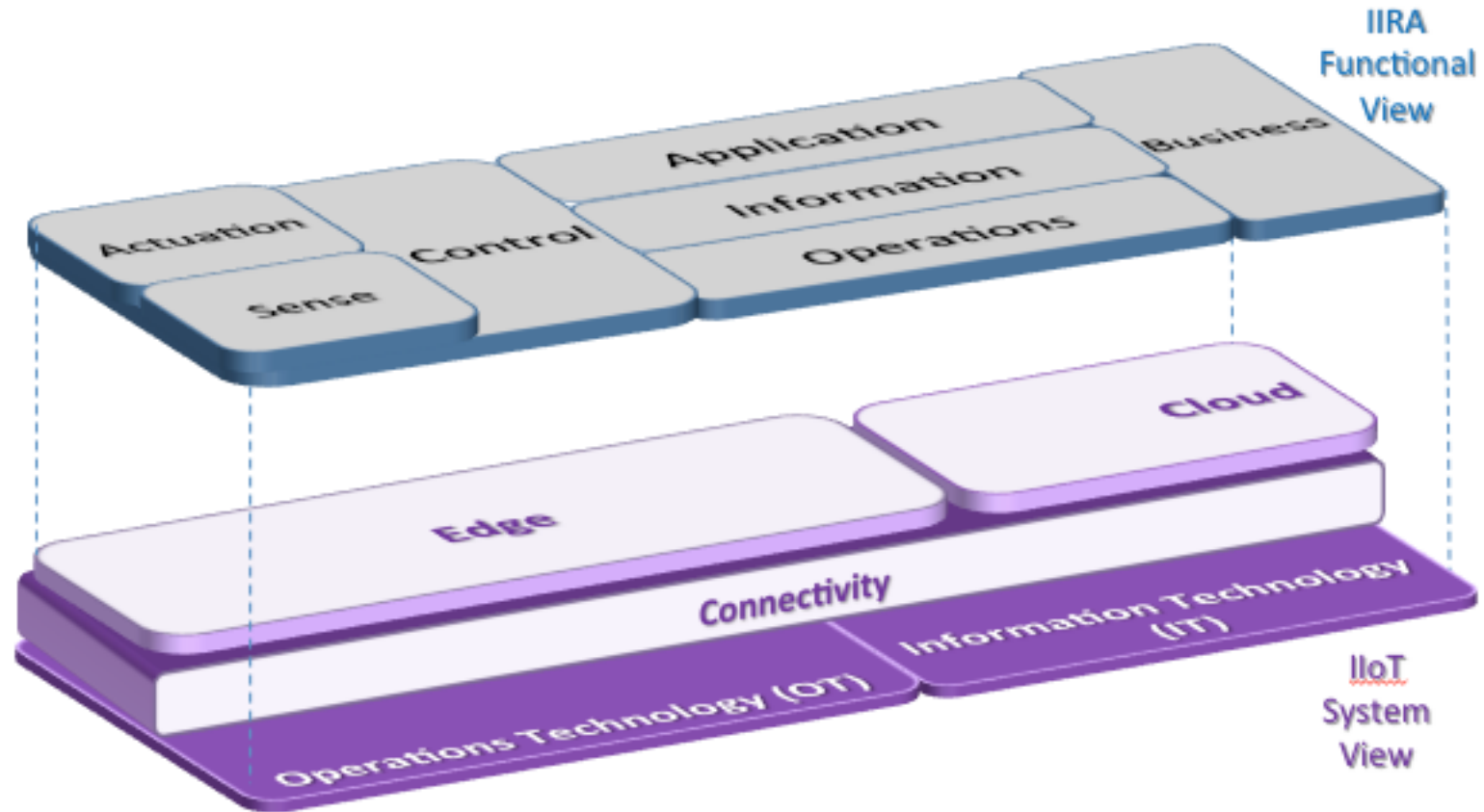
Permeation of Trust

trust in all of the system elements, how these elements are integrated and how they interact with each other.



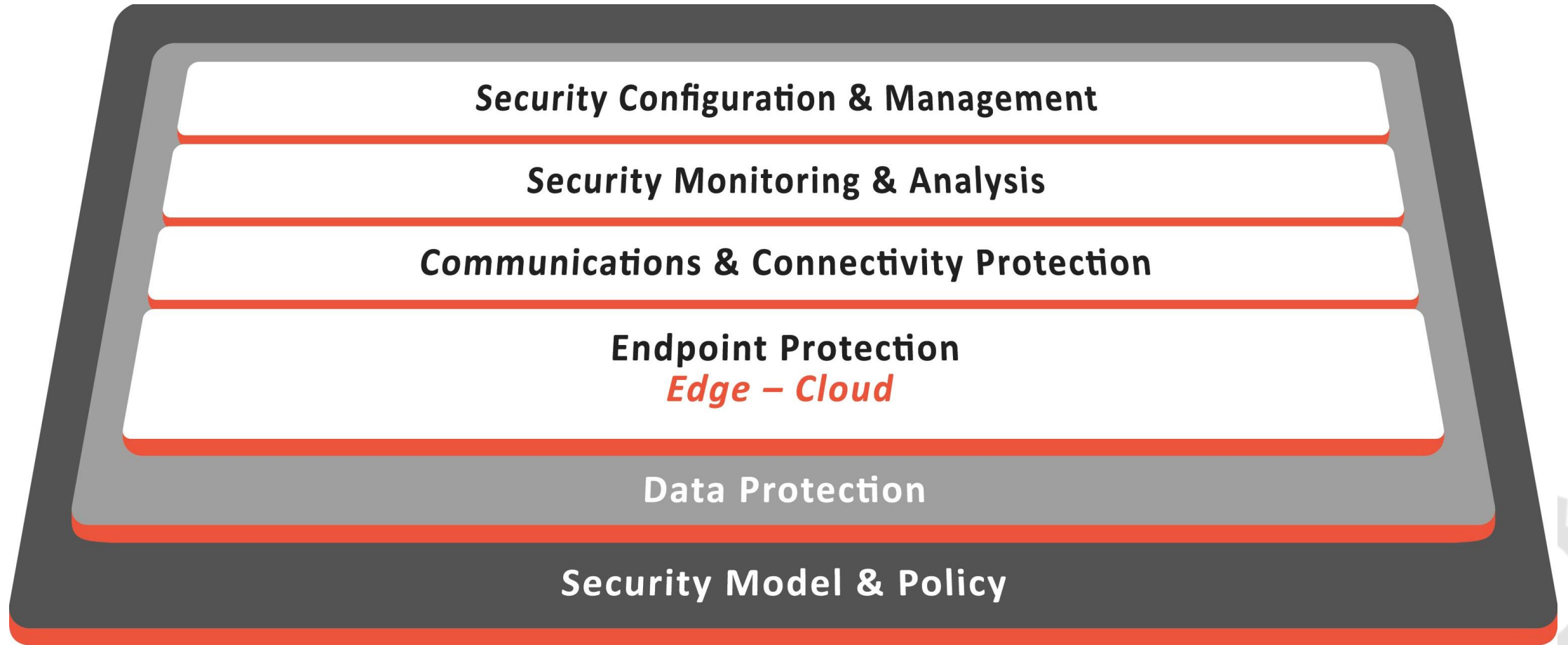


Perception of IIoT



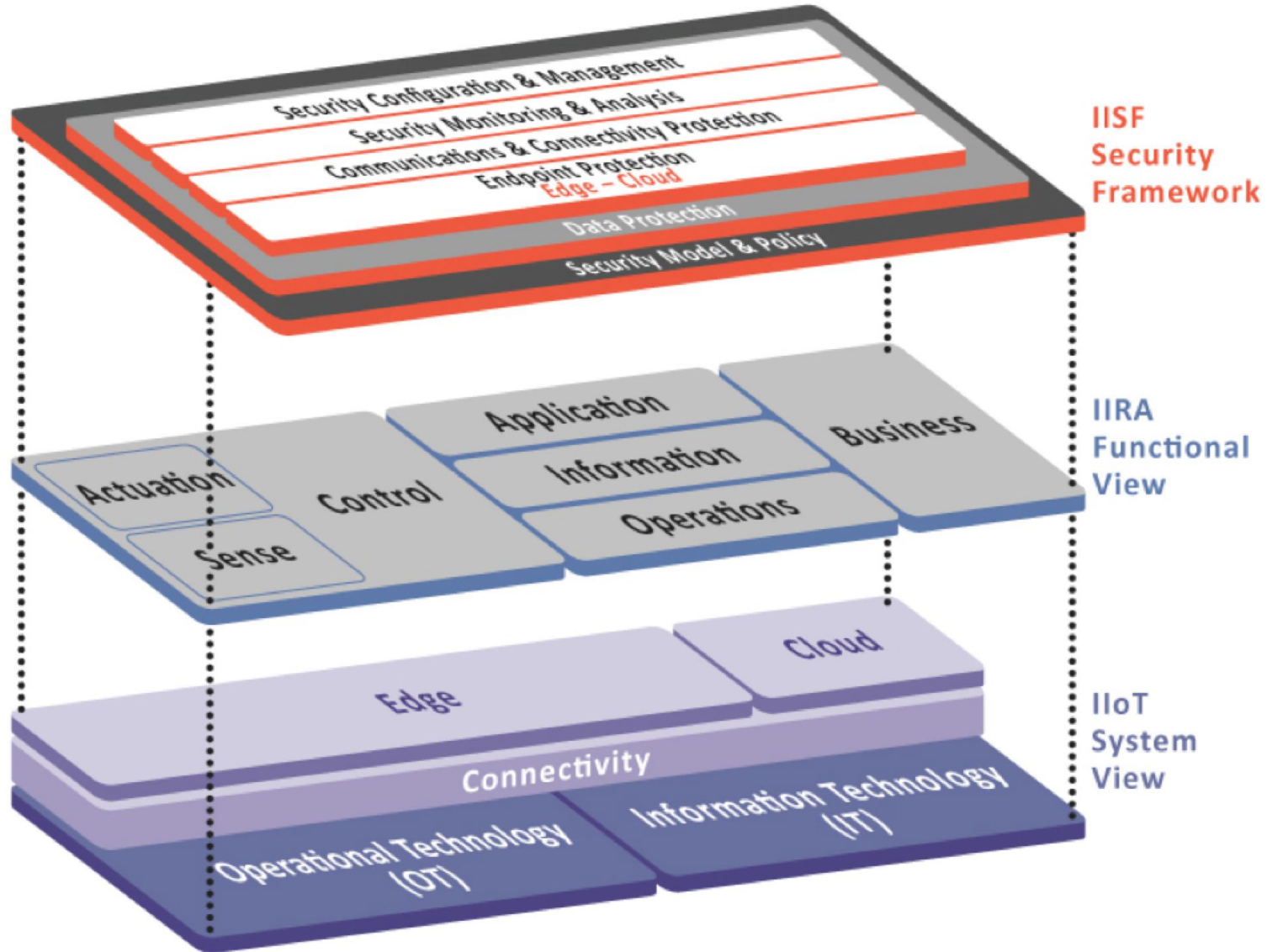


IIoT Security Building Blocks and Techniques





IIoT Security Application





Industrial Internet Security Framework Summary

- Addresses Industrial Internet security issues
- Delivers the adoption model to apply IIoT security techniques
- Unifies Industrial characteristics in terms of trustworthiness
 - Security to enable: safety, reliability, resilience and privacy
- Provides system-wide, top-to-bottom assurance of Trustworthiness
- Applies techniques spanning: endpoints, communications, monitoring, and management
- Tracks future security trends to bring into Industrial Internet when mature



IIoT Thought Leadership

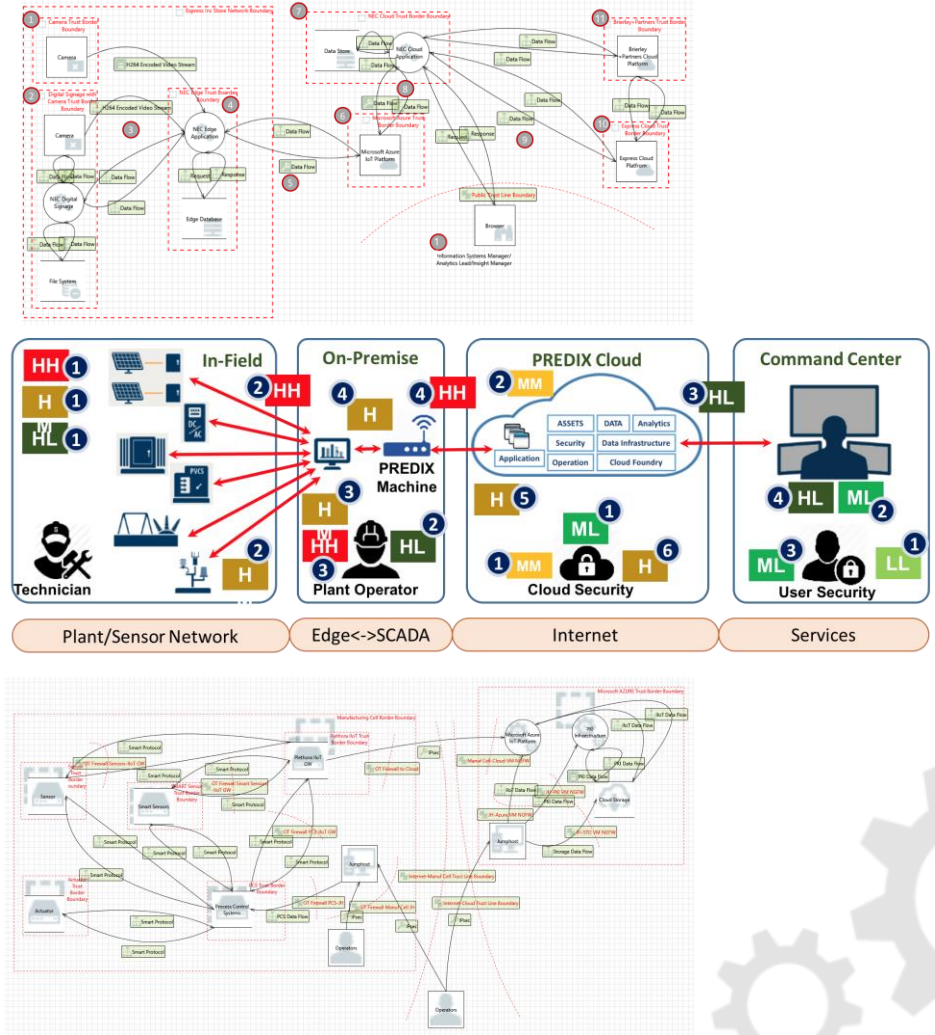
- Industrial Internet Consortium
- Industrie 4.0
- National Institute of Standards and Technology (NIST)



NIST

IIC Testbed Security Profile

- Retail Video Analytics
 - First testbed evaluated
 - STRIDE for threat assessment
 - Privacy issues
- Digital Solar Panel Testbed
 - Focus on reliability and safety
 - IoT Gateway
- Smart factory Machine Learning
 - Focus on reliability and safety
 - Threat Model using STRIDE
 - IoT gateway
 - Honeypots





Security Maturity Model

Hierarchical structure

3 Business functions

- 3 Domains for each Business function
- - 2 Security Practices for each Domain

18 Practices in total provided with a description

- 4 Basic Components of the Model
 - 4.1 Model Maturity Domains
 - 4.1.1 Security strategy and Governance
 - 4.1.1.1 Security Program Management
 - 4.1.1.2 Compliance Management
 - 4.1.2 Threat Modeling and Risk Assessment
 - 4.1.2.1 Threat Modeling
 - 4.1.2.2 Risk Attitude
 - 4.1.3 Supply Chain and External Dependencies Management
 - 4.1.3.1 Supply Chain Risk Management
 - 4.1.3.2 Third-Party Dependencies Management
 - 4.1.4 Identity and Access Management
 - 4.1.4.1 Establishing and Maintaining Identities
 - 4.1.4.2 Authorization (of users and devices)
 - 4.1.5 Asset, Change and Configuration Management
 - 4.1.5.1 Asset Management
 - 4.1.5.2 Change and Configuration Management
 - 4.1.6 Data Protection
 - 4.1.6.1 Security Model and Policy for Data
 - 4.1.6.2 Implementation of Data Protection Controls
 - 4.1.7 Vulnerability and Patch Management
 - 4.1.7.1 Vulnerability assessment
 - 4.1.7.2 Patch management
 - 4.1.8 Situational Awareness
 - 4.1.8.1 Auditing
 - 4.1.8.2 Information Sharing and Communication
 - 4.1.9 Event and Incident Response, Continuity of Operations
 - 4.1.9.1 Event Detection and Response Plan
 - 4.1.9.2 Remediation, Recovery and Continuity of Operations





Endpoint Security Document

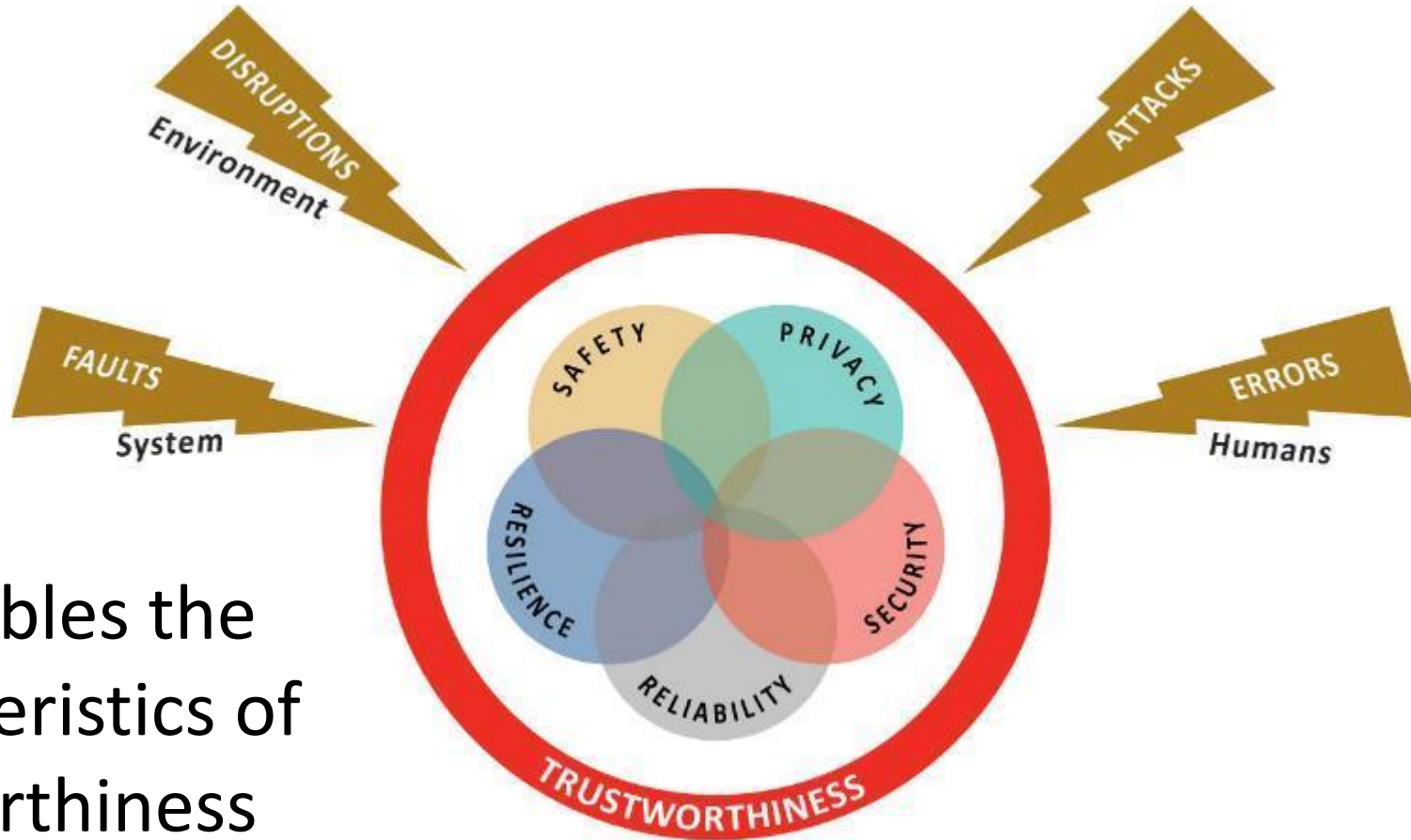
Lay out a set of recommended best practices for endpoint security in industrial applications

- Security levels to address different levels of security needed
- Provide for each level, a list of recommendations
- Establish a series of items that can be verified by a third party





Whitepaper on IIoT Trustworthiness



Security enables the other characteristics of IIoT Trustworthiness



THANK YOU

Security Working Group co-chairs:

Sven Schrecker, Intel

Jesus Molina, Fujitsu

Hamed Soroush, RTI



Nisarg Desai

Product Manager, GlobalSign

nisarg.desai@globalsign.com

