industrial internet CONSORTIUM

IIC Global Event Series, Beijing 2018-Nov-16

IIoT Security under the Roof of Trustworthiness

Marcellus Buchheit
President and CEO, Wibu-Systems USA,
mabu@wibu.com

www.iiconsortium.org

From Security to Trustworthiness

What is *Security*?

- "Traditional" Security: Fences, Gates, Locks, Watchmen, Safes etc.
  - Well introduced in the industrial world since begin on
  - "don't steal our equipment"

- "Cyber" Security: protect from remote access via Internet
  - "don't steal our data, don't interrupt our operation, don't ruin our system"
  - Well introduced in Information Technology (IT)
  - Industrial world: so far not much internet, no cyber security
    - IIoT: The real *challenge*

# IIoT: based on IT and OT

IT = Information Technology
- Examples: PC, Mobile phone, server, Ethernet, internet, cloud
- Typical software: Standardized multitasking OS, GUI, data bases
- Security since „IT in internet" relatively well addressed

OT = Operational Technology
- Examples: sensors, control systems, robots
- Typical software: „homegrown", real-time OS
- High demand for safety
- Real-time behavior
- Internet-security typically *not* implemented

IIoT is the result of IT and OT Convergence
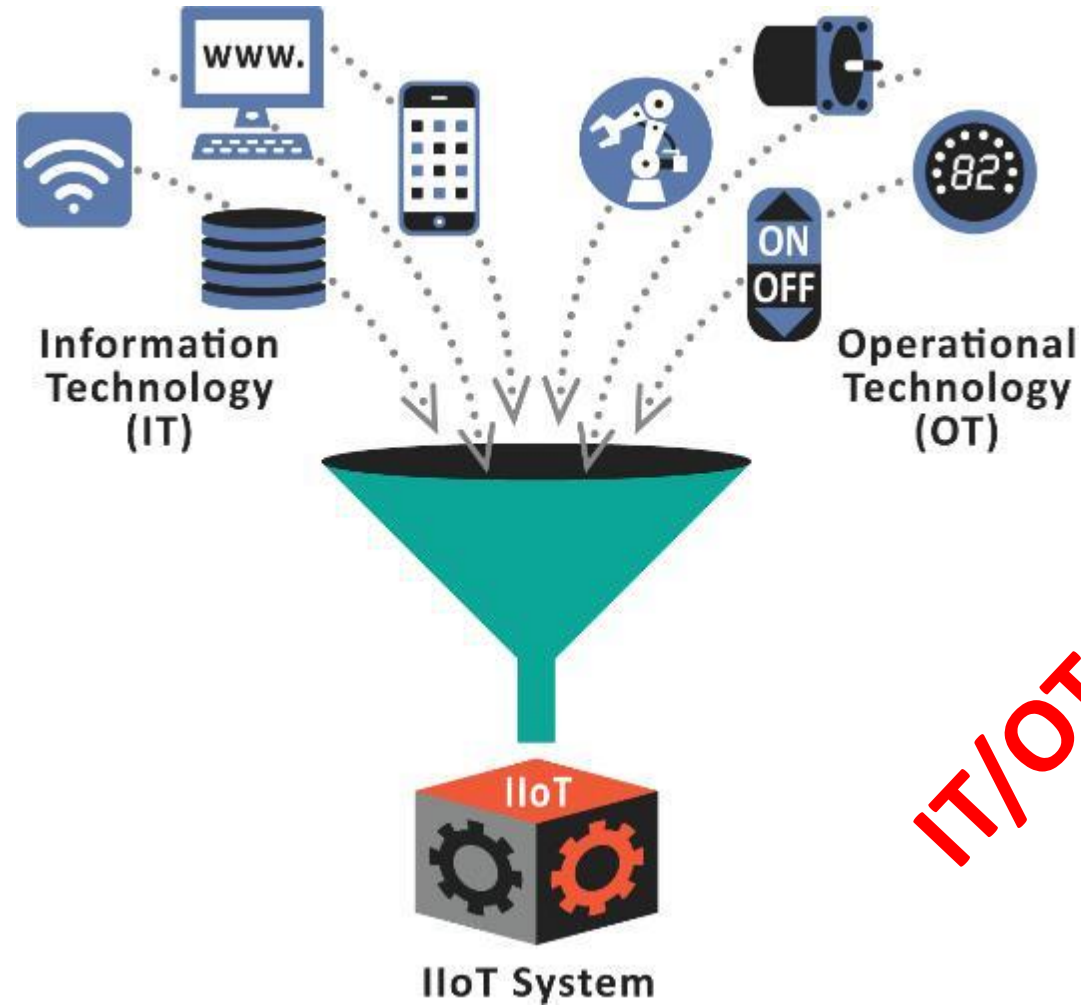
IT/OT Convergence

Principles differences of IT and OT

Security is demanded by **IT**

- Compromises are not accepted

Safety is demanded by **OT**

- Mostly unknown in IT world

Average age of OT structures: 19 years

- For comparison: average age of IT structures: 3 to 5 years

Conclusion:

The IT/OT convergence leads to *new* and *very complex* problems

Solution: Definition of Trustworthiness (IIC)

Trustworthiness is the degree of *confidence* one has that the *system* performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental *disturbances*, human *errors*, system *faults* and *attacks*.

Trustworthiness Characteristics

Trustworthiness Threats

IIC definition from IIC vocabulary version 2.1
https://www.iiconsortium.org/vocab (August 2018)

IIC Symbol of Trustworthiness
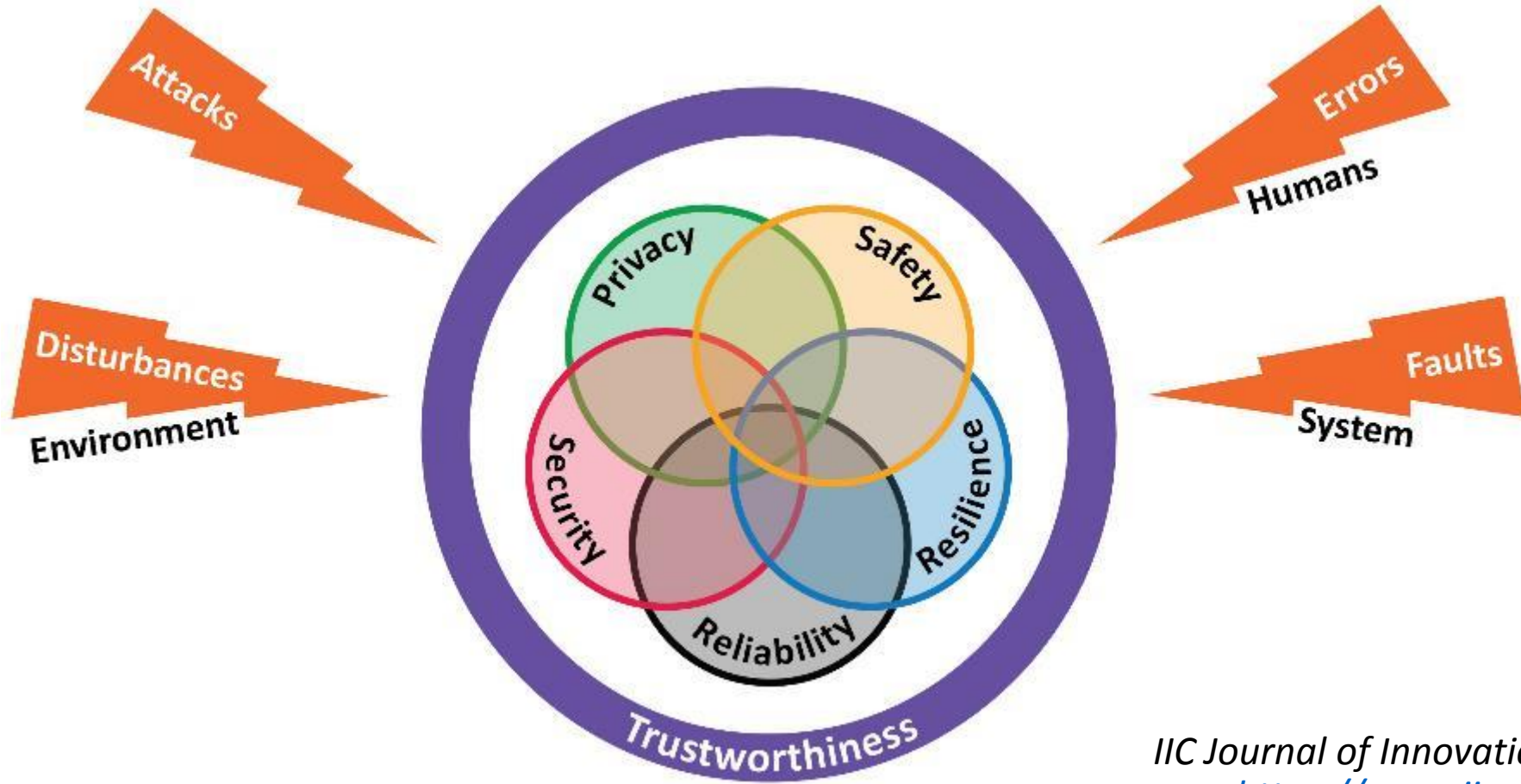
Explaining IT/OT Convergence with Trustworthiness

Information Technology (IT)

IIoT

Operational Technology (OT)
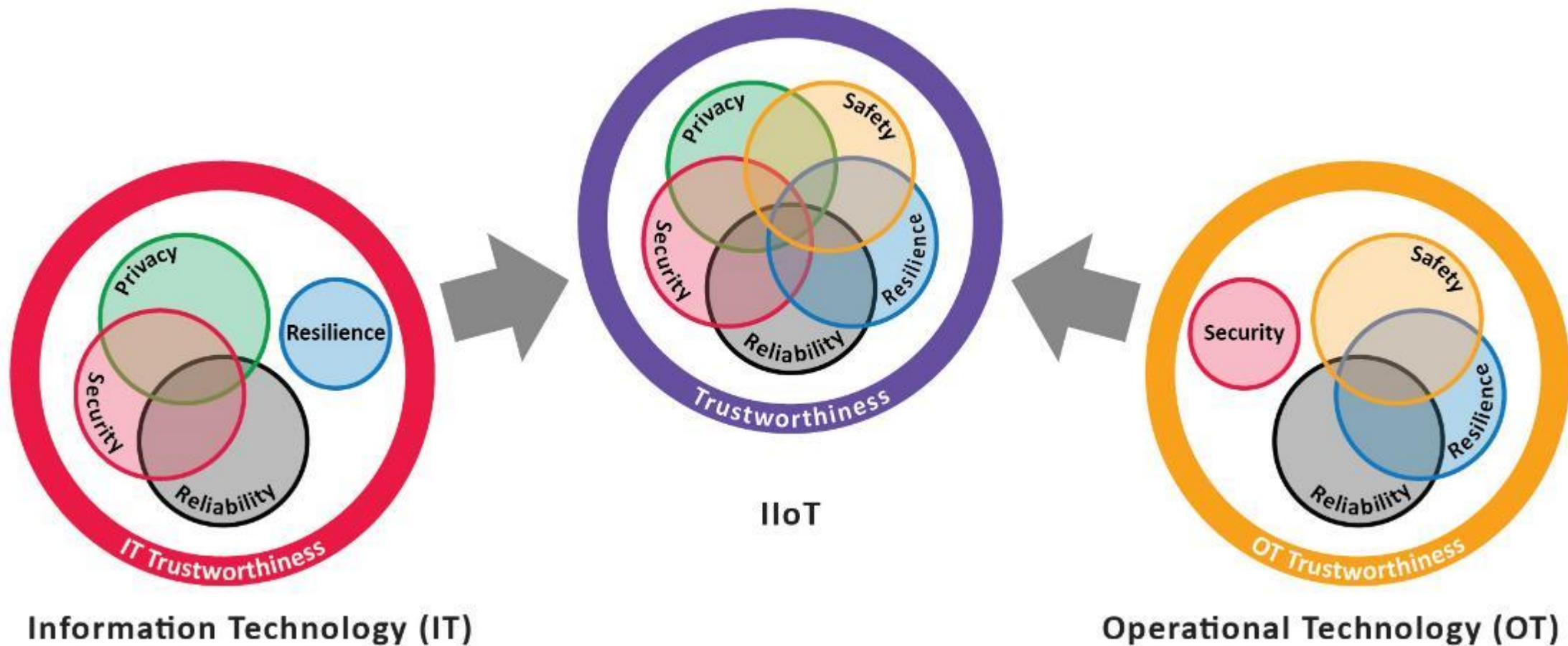
IISF – Security Framework Functional Building Blocks

Security Configuration & Management

Security Monitoring & Analysis

Communication & Connectivity Protection

Endpoint Protection
Edge – Cloud

Data Protection

Security Model & Policy

Industrial Internet Security Framework
https://www.iiconsortium.org/IISF.htm
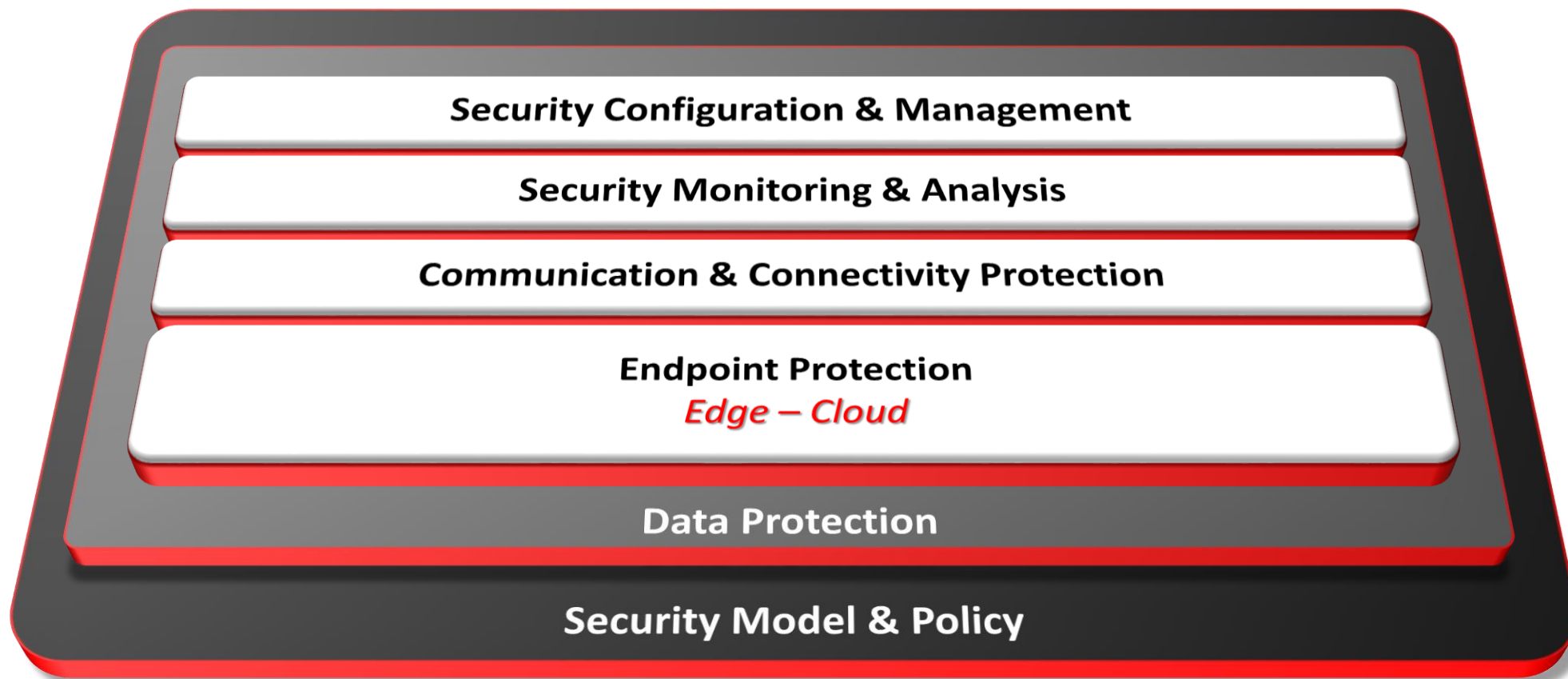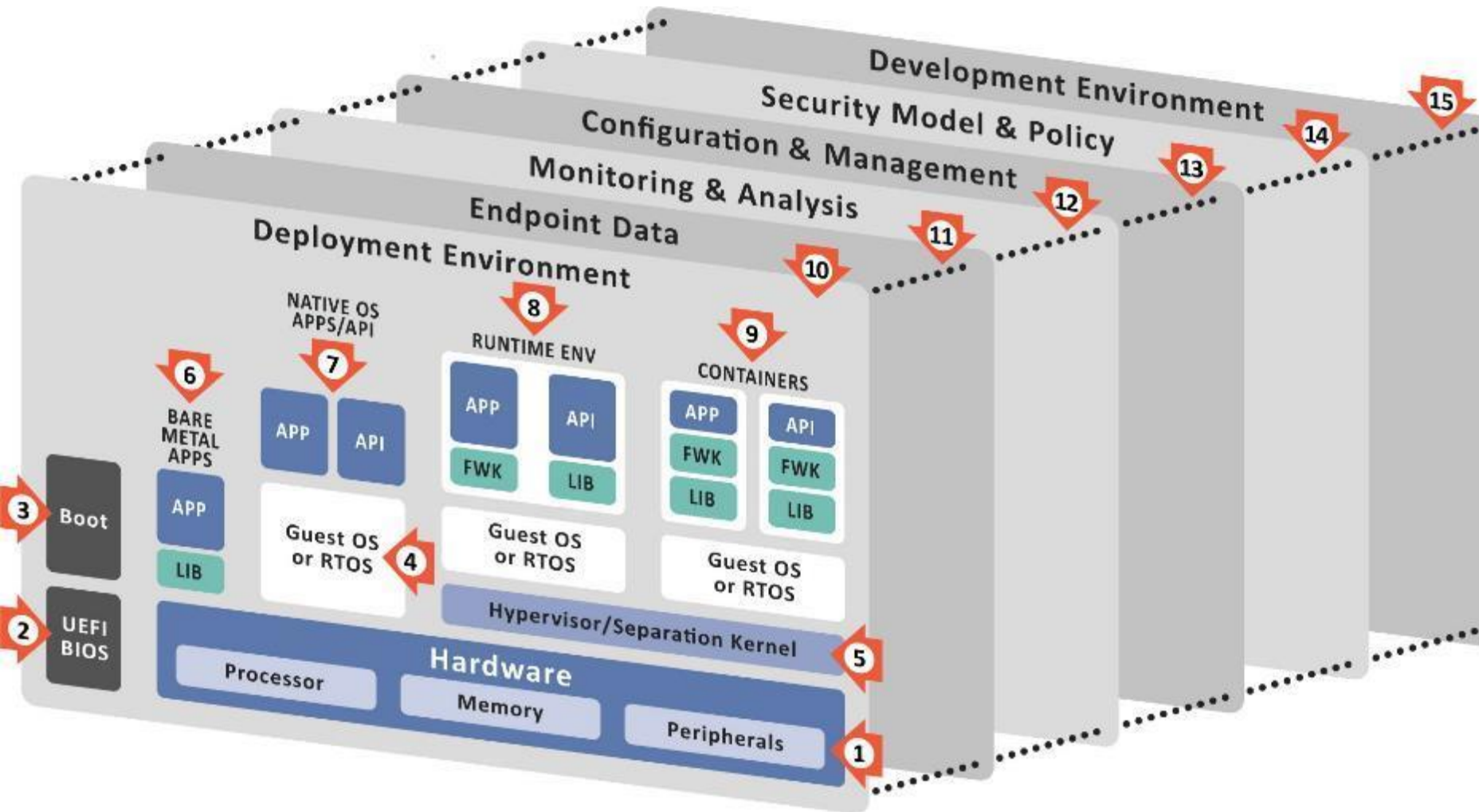
IISF – Endpoint Protection Model
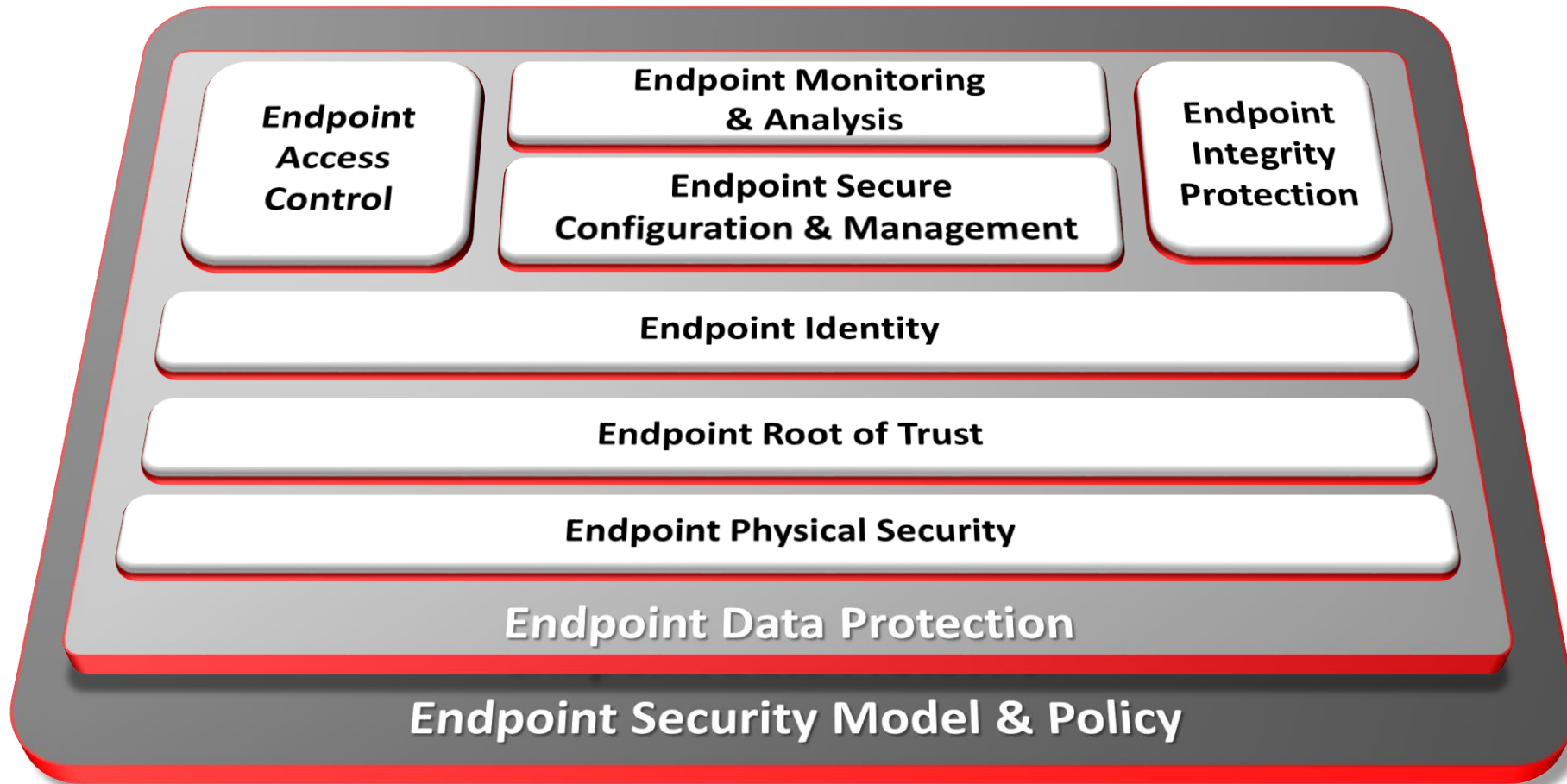
IISF – Threats and Vulnerabilities to an IIoT Endpoint

1. Hardware components
2/3. Boot process
4. Operating System
5. Hypervisor/Sep. Kernel
6. Non-OS Applications
7. Applications and their API
8. Runtime Environment
9. Containers
10. Deployment
11. Data at Rest, Data in Use
12. Monitoring/Analysis
13. Configuration/Management
14. Security Model/Policy
15. Development Environment