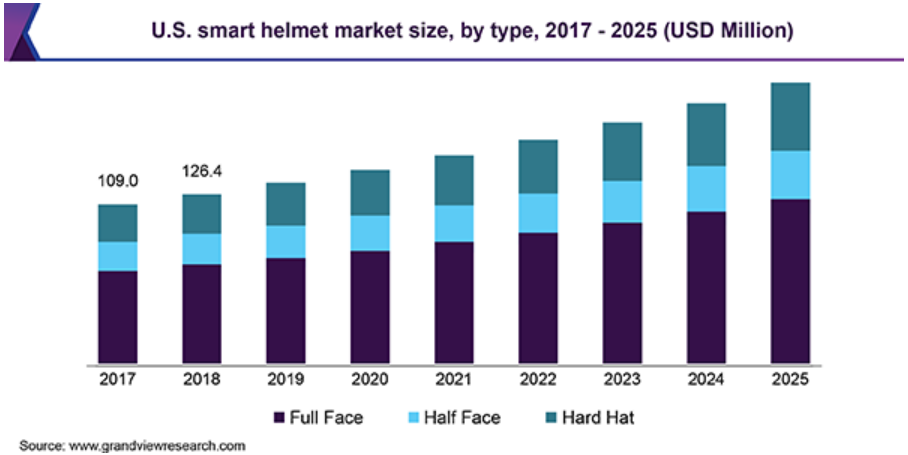
Conference: Shaping a globally secure Industrie 4.0 Ecosystem

Approaching industrial IoT trustworthiness in international standards and guidelines

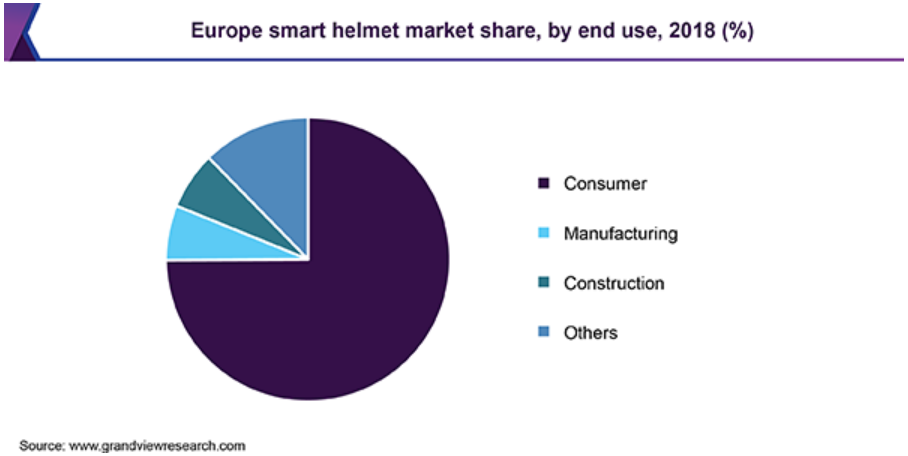
Ekaterina Rudina and
Vyacheslav Zolotnikov

Kaspersky ICS CERT

kaspersky

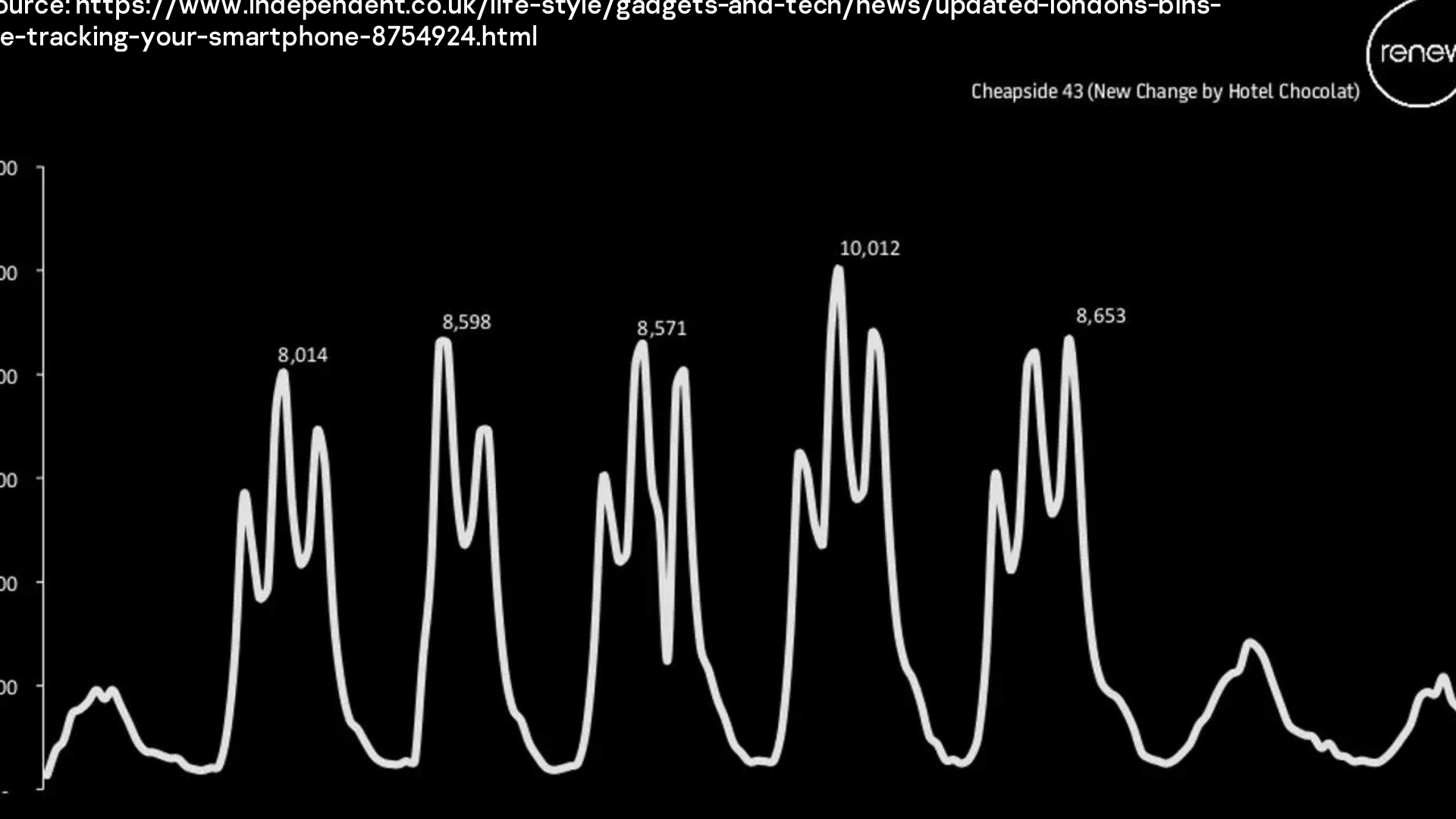


Source: ww.grandviewresearch.com/industry-analysis/smart-helmet-market




London Underground
Good Service
Good Service
Good Service
Good Service
Good Service
Good Service
Good Service
Good Service
Part Suspended
Good Service
Good Service
Good Service
Good Service

ource: https://www.independent.co.uk/life-style/gadgets-and-tech/news/updated-londons-bins-
e-tracking-your-smartphone-8754924.html



What

What trustworthiness is for the IIoT

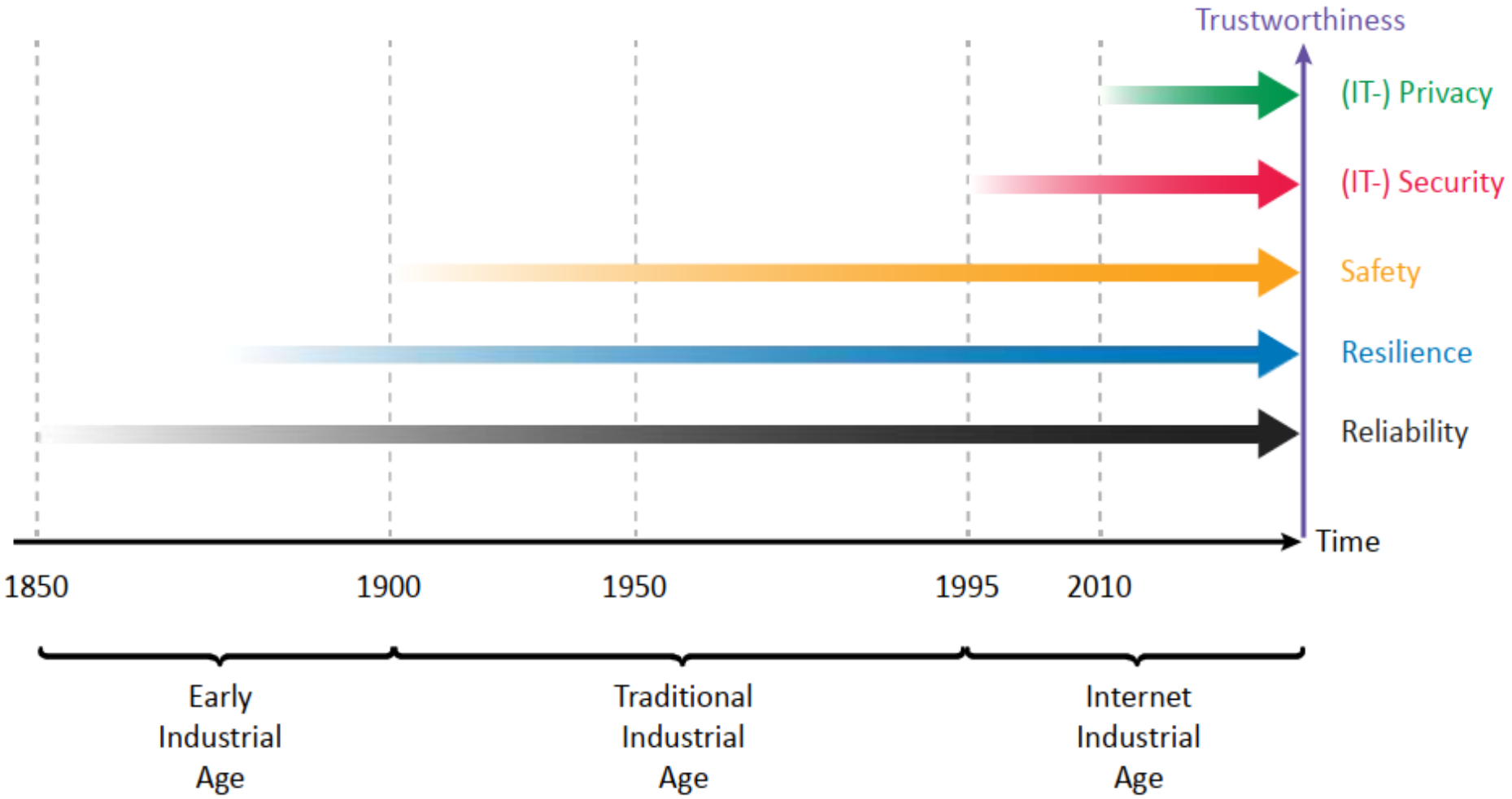
Trustworthiness

In the context of an industrial system or a component used for an industrial system, trustworthiness means that a subject deserves trust or is able to be trusted.

Trust

Assurance

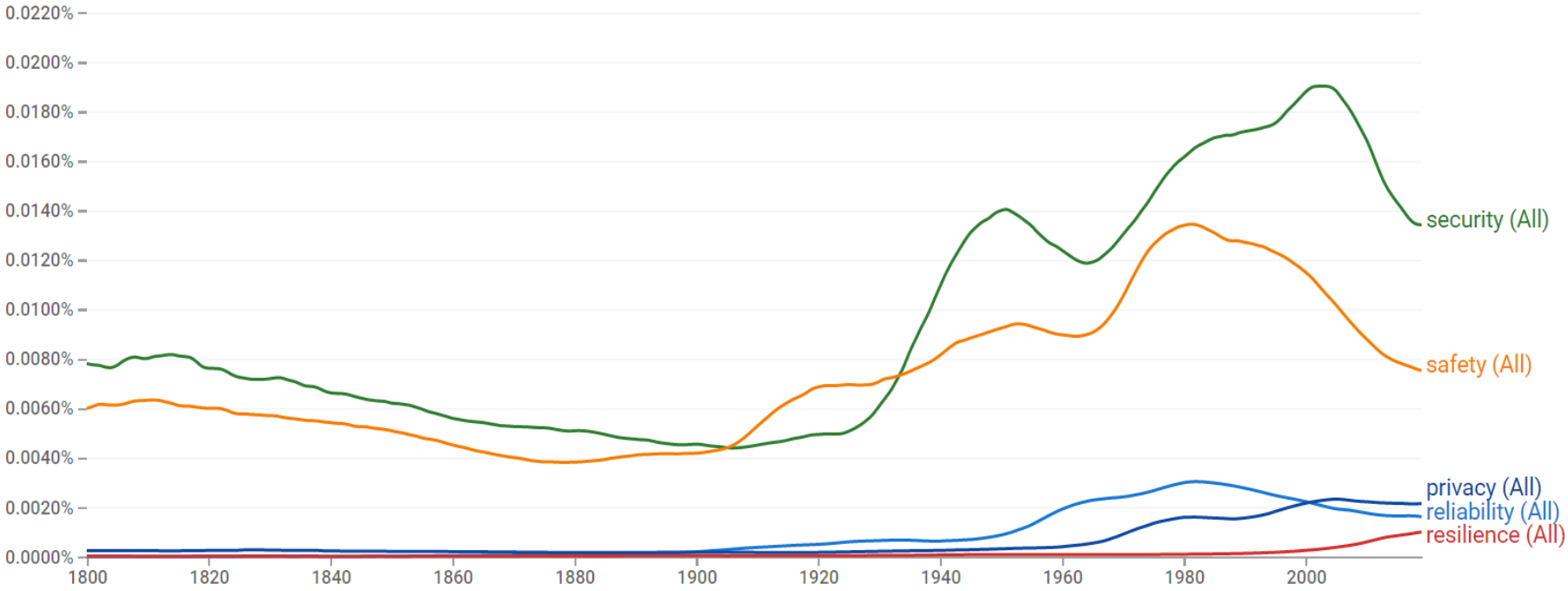
Trustworthiness

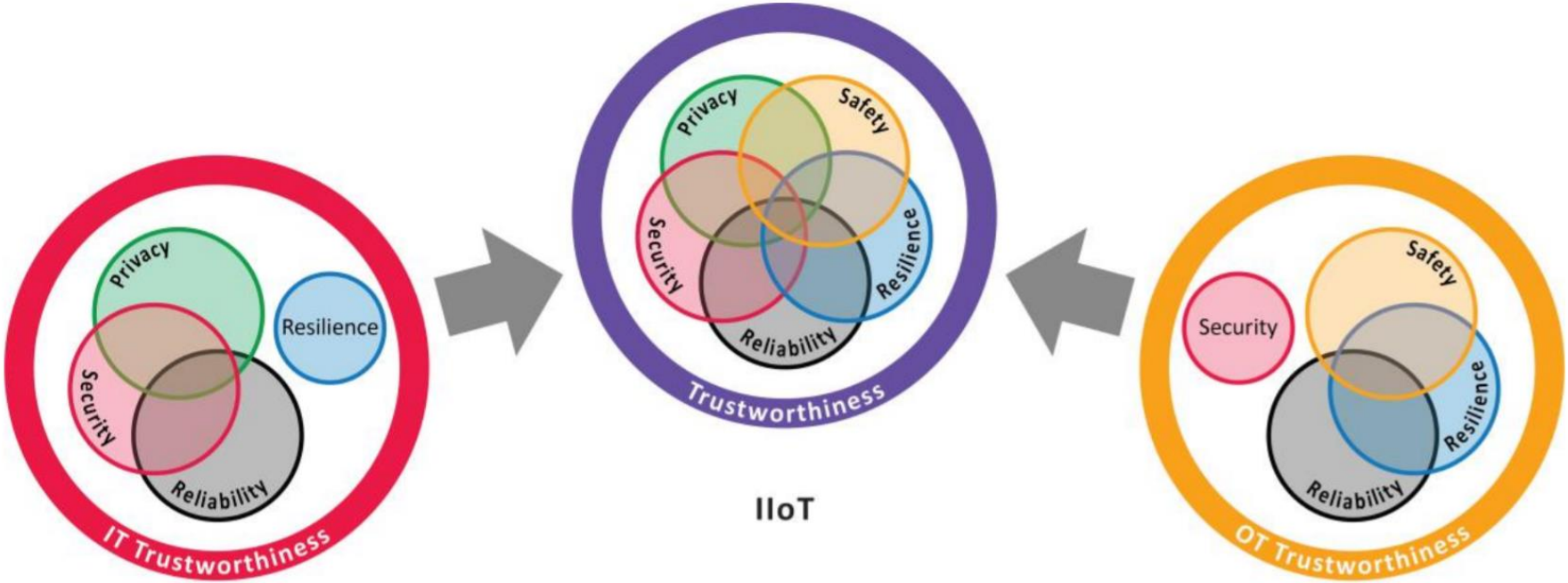

Trustworthiness
(IT-) Privacy
(IT-) Security
Safety
Resilience
Reliability
Time
1850
1900
1950
1995
2010
Early Industrial Age
Traditional Industrial Age
Internet Industrial Age

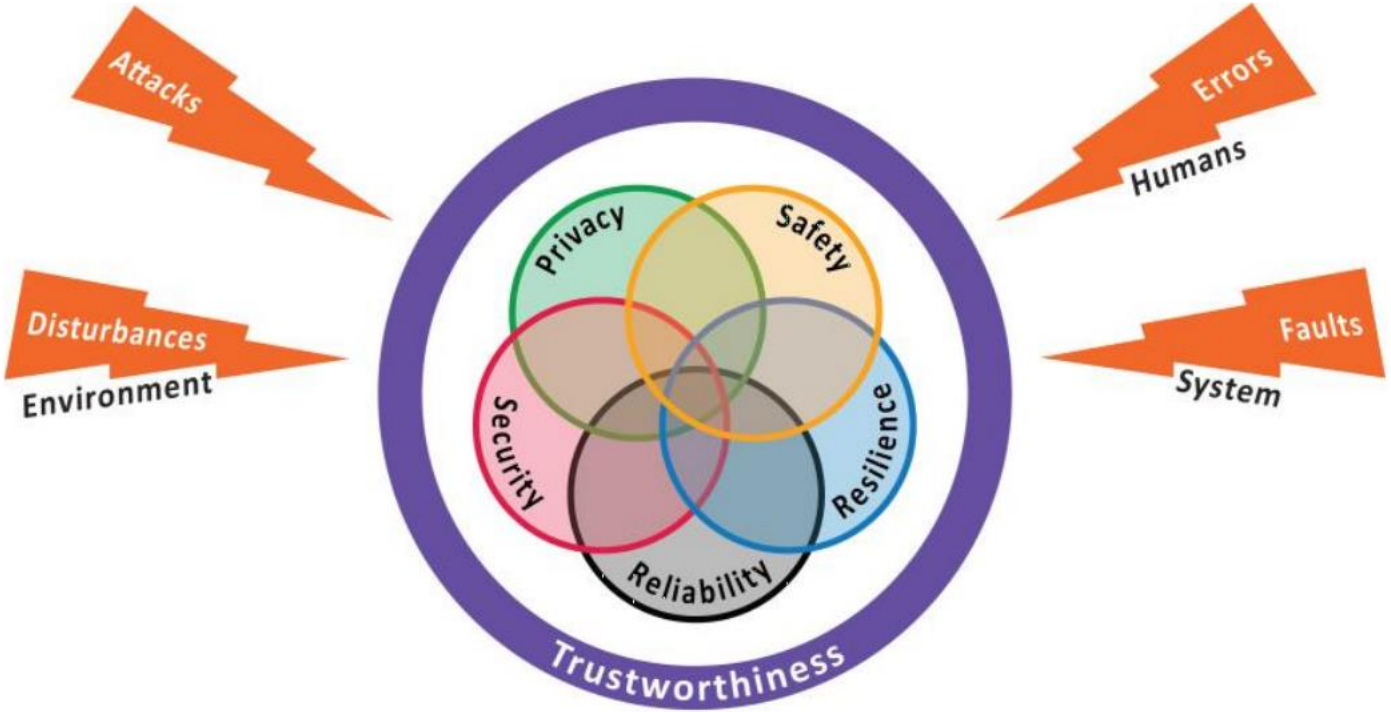
reliability,resilience,security,safety,privacy

1800 - 2019 | English (2019) | Case-Insensitive | Smoothing of 6

Google Books Ngram Viewer

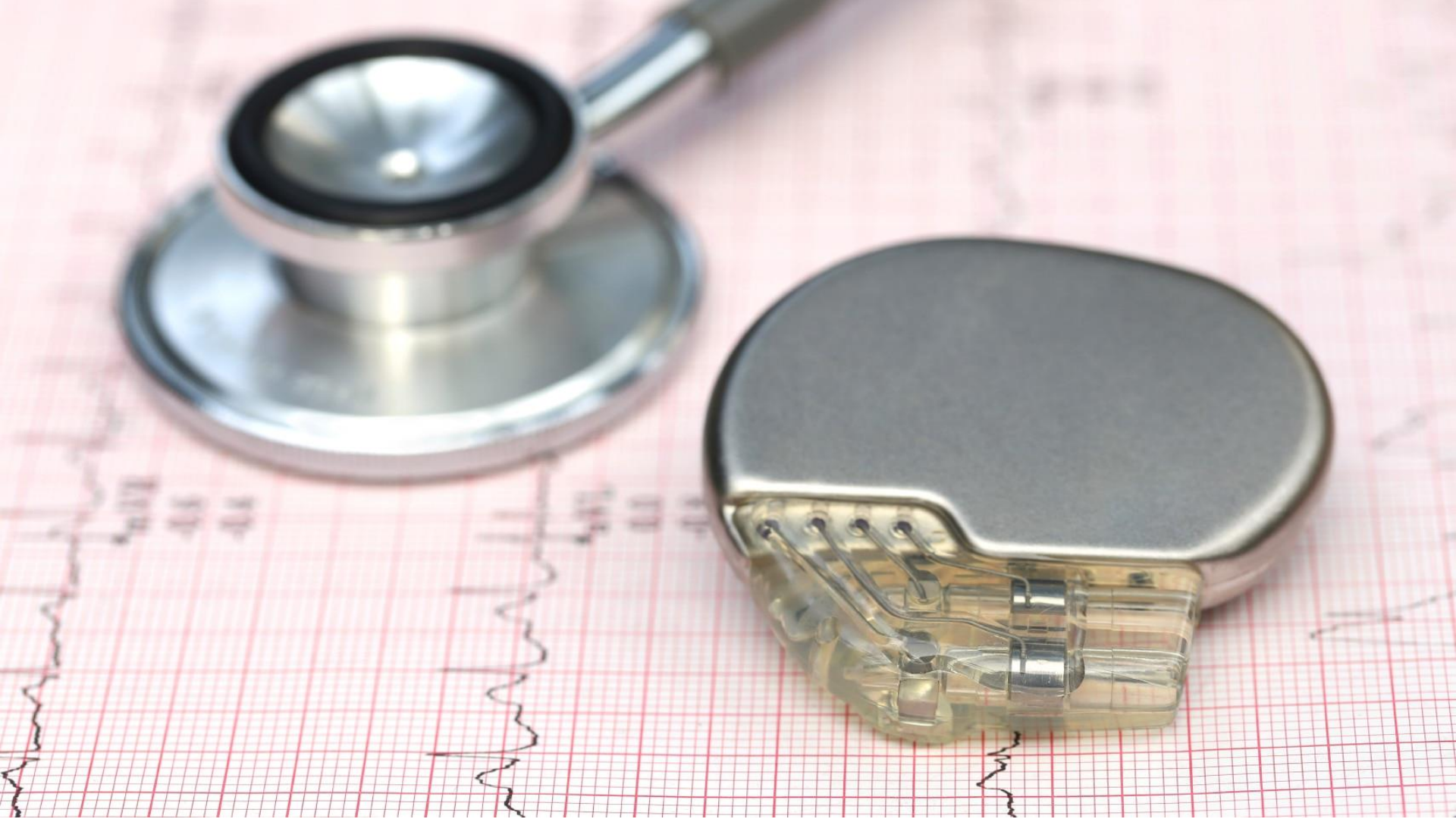



Privacy
Resilience
Security
Reliability
IT Trustworthiness
Privacy
Safety
Security
Resilience
Reliability
Trustworthiness
IIoT
Safety
Security
Resilience
Reliability
OT Trustworthiness


Attacks
Errors
Humans
Disturbances
Environment
Faults
System
Privacy
Safety
Security
Resilience
Reliability
Trustworthiness

Why

Why trustworthiness is not just a set of characteristics



Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.8 HIGH **Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

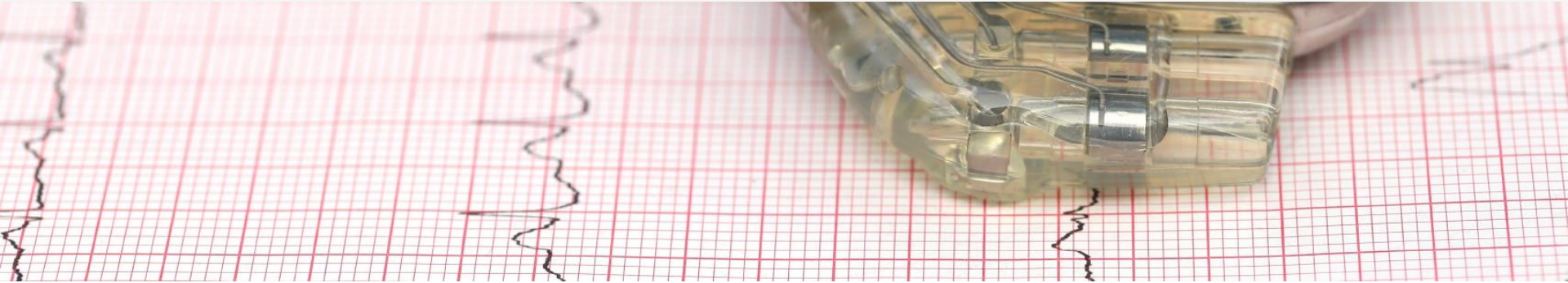
NIST: NVD **Base Score:** 8.8 HIGH **Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.8 HIGH **Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

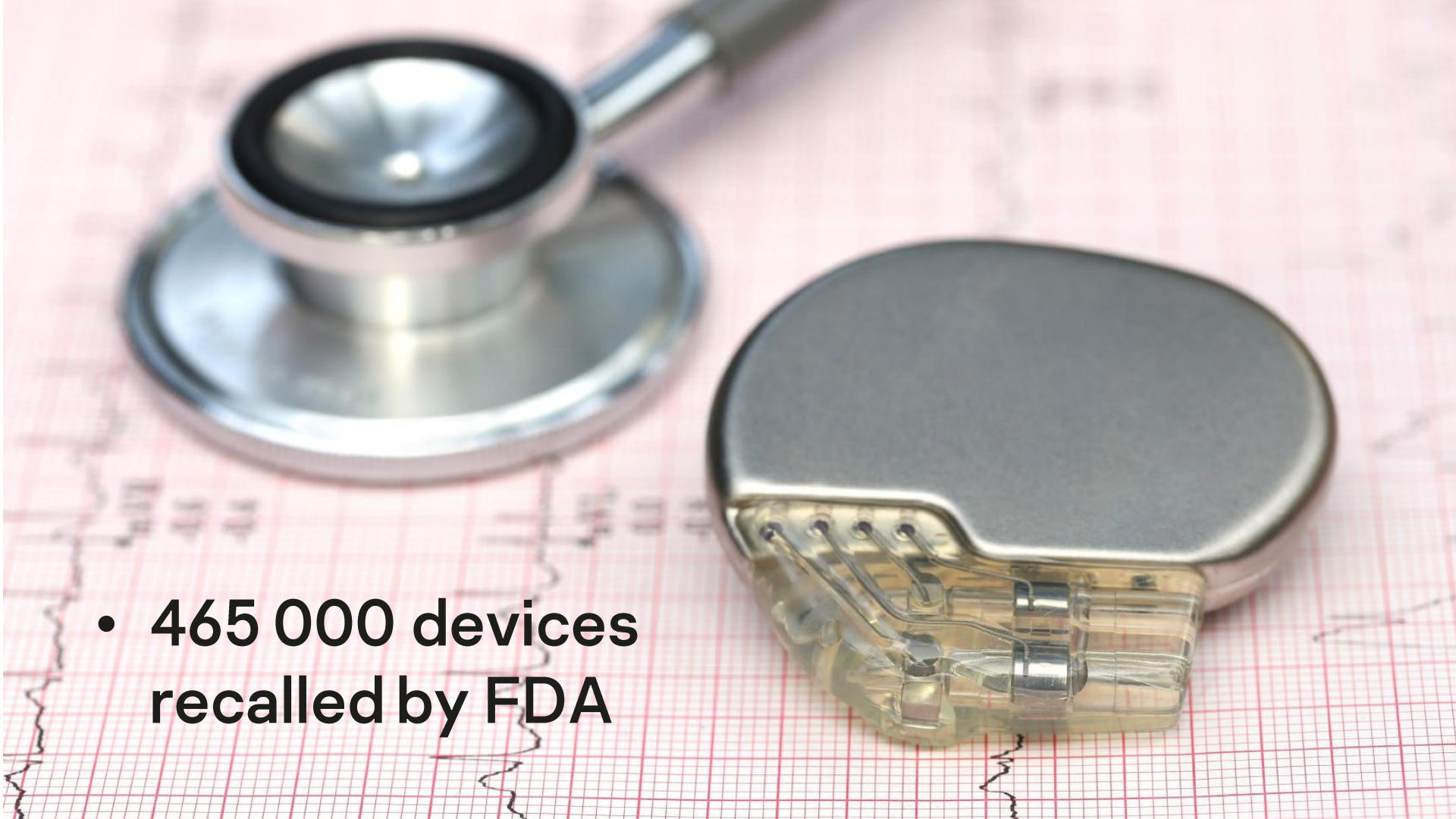
NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



- 465 000 devices recalled by FDA

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE ID	CVSS v3 base score	CVSS vector string	Can affect safety if exploited
CVE-2017-12712	8.8	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	yes
CVE-2017-12714	6.5	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	yes
CVE-2017-12716	6.5	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	no
CVE-2017-12701	6.5	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	no

IEC 60601-1

General Requirements for Safety of Medical Electrical Equipment

_____ main required for the certification of medical devices

_____ nationally adopted in the USA, European countries, Canada, Russia

_____ used for risk management

The standard indicates that in the risk management process for medical electrical products and systems not only the hazards that are addressed in this standard, but also all other hazards, associated risks and risk control measures should be determined.

— IEC 60601-1

The standard also specifies that in the event that the requirements of this standard relate to the prevention of unacceptable risk, the acceptability or unacceptability of this type of risk should be determined by the manufacturer in accordance with his accepted principles for determining the acceptable risk.

— IEC 60601-1

What are the risks?

What are the incentives for the manufacturer to manage the risks from cyberattacks?

_____ the manufacturer defines the principles for identifying and assessing safety risks associated with cyberattacks on medical equipment.

_____ This violates the fair application of separation of duties and does not facilitate the improvement of the whole situation with a possible impact of cyberattacks on safety.

How

This is addressed in discussions within the working groups of IIC and ISO/IEC

Main issues

For standards and guidelines on trustworthiness

Align the objectives for security, safety, resilience, privacy and reliability

Resolve the conflicts of assumptions

Combine the methods of trustworthy design and proper assurance already provided for the aspects

(and not forget their relationships)

1. Problem structuring

Guidelines and standards approach the trustworthiness as a whole and try to decompose it to different aspects, address these aspects both separately and in their relationships for the given industry or sector.

The set of aspects may follow the characteristics proposed by IIC or be different depending on the specific requirements of the industry and authority issuing the recommendations.

— Examples: IIC trustworthiness characteristics, set of “–ilities”, CIA, etc.

2. Hazard identification and structuring

Tasks of this group are usually solved based on hierarchical (or even structured) representation of the factors which are considered as the direct issues for trustworthiness or related characteristics (safety, security, etc.).
These issues may have different names (threats, hazards, etc.). Vulnerabilities are also considered in some cases.
Everything that “can happen to the system”

Examples: attack trees, fault trees, HAZOP, bow-tie, STRIDE, CVSS, OWASP Top 10, CAPEC, MITRE Att&ck etc.

3. Risk evaluation

Risk evaluating methods are mostly oriented on the likelihood and impact assessment but other approaches exist as well.

It is important that there is no “trustworthiness risk”, risk evaluating models usually work at the level of safety, security and so on because the risks for these aspects usually have significantly different nature.

Examples: DREAD, Automotive HEAVENS, Risk evaluation through severity (or cost) and likelihood, Mean time to failure (MTTF), linear and non-linear hazard model (reliability), stress-dependent hazard models

4. System design approaches and best practices

Rational (method based)
Participative (stakeholder based)
Heuristic (lessons learned)
Normative (solution based)

Examples: (two of each kind) PKI, MILS architectural approach, V-cycle adopted by ISO 26262, MS SDLC based on STRIDE, Saltzer and Schroeder principles, KISS principle, Prevention through design

5. System assurance

This may cover a variety of methods from simple testing to model checking approach and behavior verification and other run-time methods.

Assurances approaches relate to the hazard identification and risk evaluation and may change depending on the methods of trustworthy system design.

Examples: Common Criteria, Structured Assurance Case Metamodel

6. Maturity models

that are aiming to cover the gaps in processes of development, configuration and maintenance of (not only) IoT solutions thus indirectly contributing to the quality of code, in-time discovery of vulnerabilities and patching those of vulnerabilities that may have and impact on trustworthy solution functioning.

Examples: OWASP Software Assurance Maturity Model (OWASP SAMM), IIC IoT Security Maturity Model (IIC IoT SMM), Capability Maturity Model Integration (CMMI), Automotive SPICE, Lockheed Martin Cyber Resilience Level™ (CRL™), Cyber Resilience Review methodology by the US Homeland Security

Trustworthiness principles (1)

- related to the system and context

- **Trustworthy system should reflect the real-world (business or mission) trust relationships.**
- **Trustworthy system should clearly set up the priorities for the trustworthiness aspects**
- **Trustworthy system should implement the fail-safe design at least for the for the prioritized aspects.**

Trustworthiness principles (2)

- **related to the methods and methodologies**

- **Rational (method-based) approach** in design, implementation, configuration and maintenance of trustworthy system **has a preference over the heuristic (lessons learned) approach**
- **Normative (solution-based) approach** in regulatory, design, implementation, configuration and maintenance **has a preference over the voluntary approach**

Trustworthiness principles (3)

- related to the process

- **Participative (stakeholder-based) approach** to attain trustworthiness **has a preference over the unilateral** (e.g., compliance-based only) **approach**
- Trustworthiness assurance processes should enforce the **separation of duties principle** in implementation and assurance procedures for trustworthiness aspects
- **Established (standardized) protocols**, procedures and methods to attain trustworthiness **have a preference over the ad-hoc approach**

Ongoing work and published papers

Industrial Internet Consortium

ISO/IEC JTC 1/SC 41
Internet of Things and related technologies

- WG3
- WG13

ISO/IEC JTC 1/AG 8
Meta Reference Architecture and Reference Architecture for Systems Integration

ISO/IEC JTC 1/SC 41
Internet of Things and related technologies

WG3

ISO/IEC 30141 ED2 Working draft
Internet of Things (IoT) - Reference architecture
Trustworthiness viewpoint

ISO/IEC 30149 Working draft
Trustworthiness principles

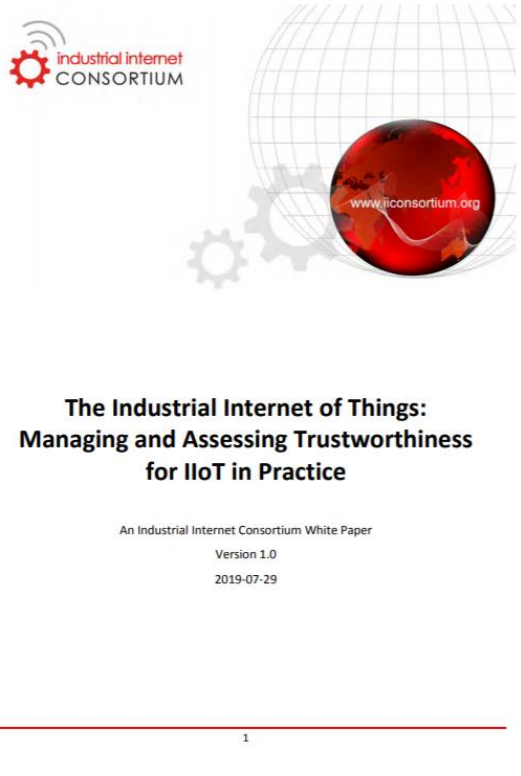
Trustworthiness Task Group
The Trustworthiness Task Group is chartered to explore aspects of trustworthiness relevant to IIoT and the IIC's vision of an IIoT ecosystem.

Papers and guidelines
Technical guidelines and whitepapers

Journal of Innovation
September 2018

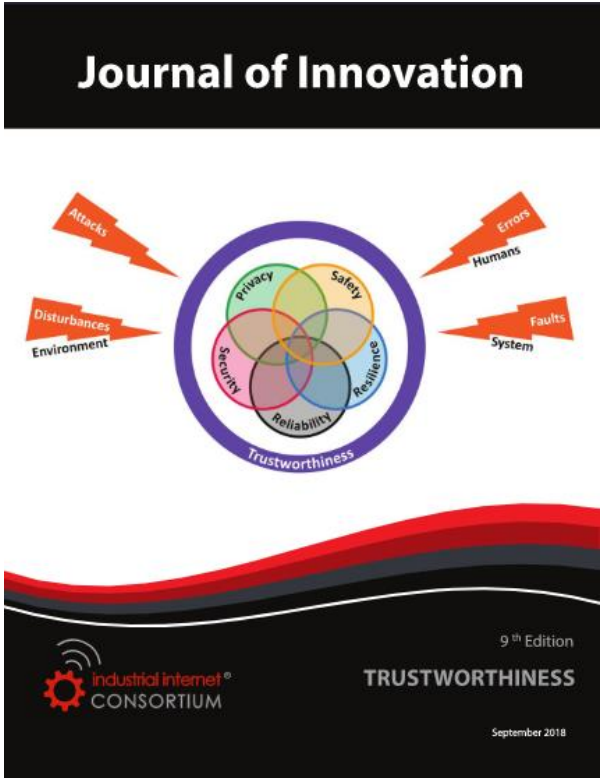
https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

https://www.iiconsortium.org/pdf/Key_Safety_Challenges_for_the_IIoT.pdf



https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf



Sincere thanks goes to this edition's editors and peer reviewers:

Mr. Mark Crawford, Standards Strategist, SAP Strategic IP Initiatives
Mr. Edy Liongosari, Chief Research Scientist, Accenture Labs
Ms. Enas Ashraf, Innovation Manager, Advancys ESC
Mr. Vincent Bemmel, Industry Technology Lead, Corlina
Mr. Bassam Zarkout, CEO, IGnPower
Mr. Dean Weber, CTO, Mocana
Mr. Sudhanshu Mittal, Director, Industry 4.0, NASSCOM CoE-IoT
Mr. Shyam Nath, Director, Enterprise Cloud Architect, Oracle
Mr. Saurabh Mishra, Product Management = IoT, SAS
Mr. Abhik Chaudhuri, Chevening Fellow (UK), FCSA (USA), Tata Consultancy Services
Mr. Jijun MA, Director of Industrial Internet, Wanxiang Group
Mr. Gavin Green, VP of Product, XMPro
Mr. Pieter van Schalkwyk, CEO, XMPro
Ms. Cheryl Rocheleau, Sr. Marketing Manager, Industrial Internet Consortium
Mr. Matt Sexton, Sr. Marketing Specialist, Industrial Internet Consortium

https://www.iiconsortium.org/news/joi-sept-18.htm

Q&A

Approaching industrial IoT trustworthiness in international standards and guidelines

Ekaterina Rudina

kaspersky ICS CERT