

A portrait of Ekaterina Rudina, a woman with long brown hair, looking directly at the camera. The portrait is set against a white background that is partially obscured by a teal geometric shape.

kaspersky



Kaspersky Industrial
Cybersecurity
Conference 2020

Екатерина Рудина

Руководитель группы аналитиков по
информационной безопасности,
АО «Лаборатория Касперского»

#KasperskyICS

Чат конференции: <https://kas.pr/kicscon>

kaspersky

Доверие в Интернете вещей



Kaspersky Industrial
Cybersecurity
Conference 2020

Екатерина Рудина
Лаборатория Касперского

On behalf of



industrial internet
CONSORTIUM

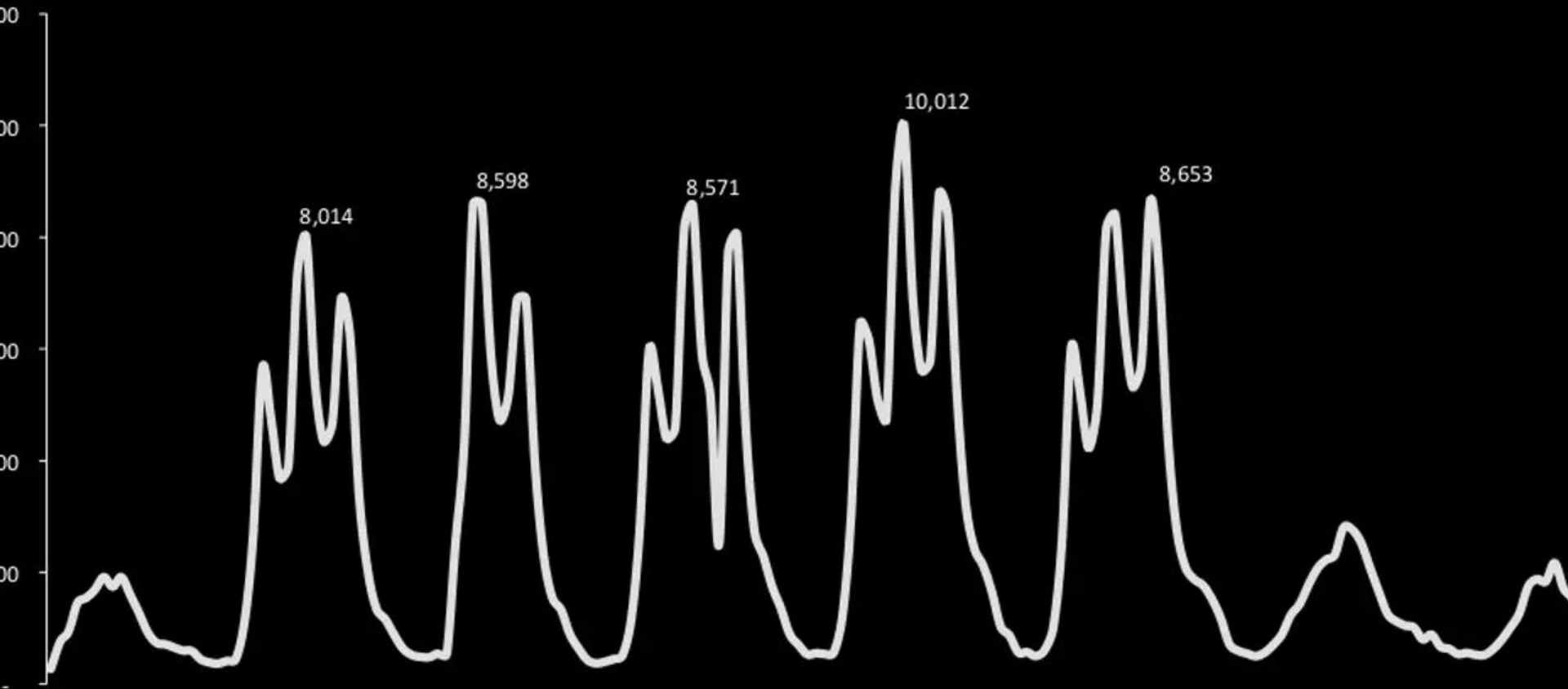


London Underground

Circle	Good Service
Central	Good Service
District	Good Service
Hammersmith	Good Service
Metropolitan	Good Service
Northern	Good Service
Piccadilly	Part Suspended
Victoria	Good Service
Waterloo & City	Good Service
Charing Cross	Good Service
Great Northern	Good Service

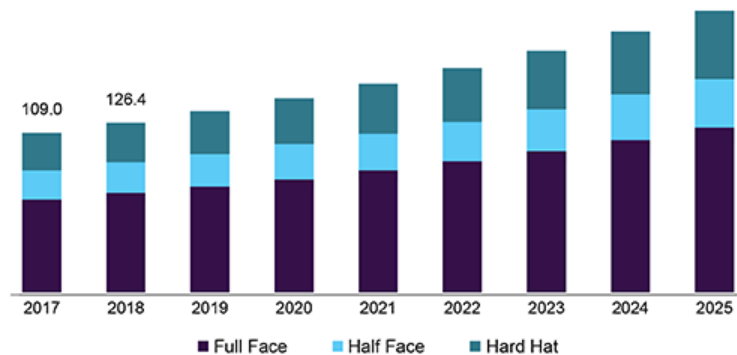
© 2013 TfL. All rights reserved.

Cheapside 43 (New Change by Hotel Chocolat)





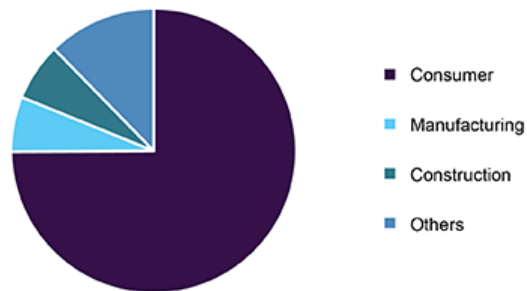
U.S. smart helmet market size, by type, 2017 - 2025 (USD Million)



Source: www.grandviewresearch.com

Источник:
<https://www.grandviewresearch.com/industry-analysis/smart-helmet-market>

Europe smart helmet market share, by end use, 2018 (%)



Source: www.grandviewresearch.com

Доверие

уверенность в
том, что
система
работает
должным
образом

Trust

Assurance

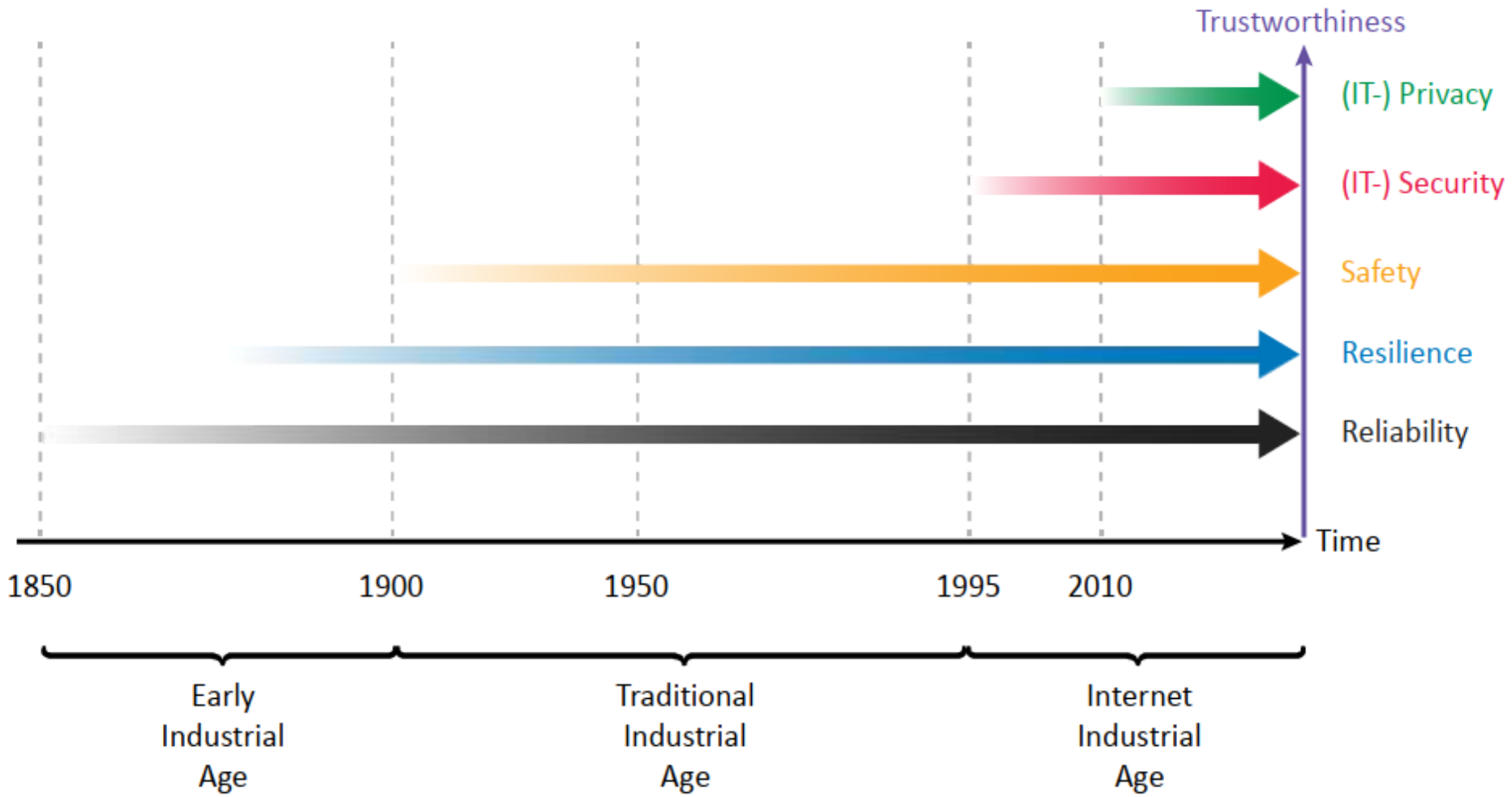
Trustworthiness

Что



Что определяет доверие

Нефункциональные характеристики системы





reliability,resilience,security,safety,privacy



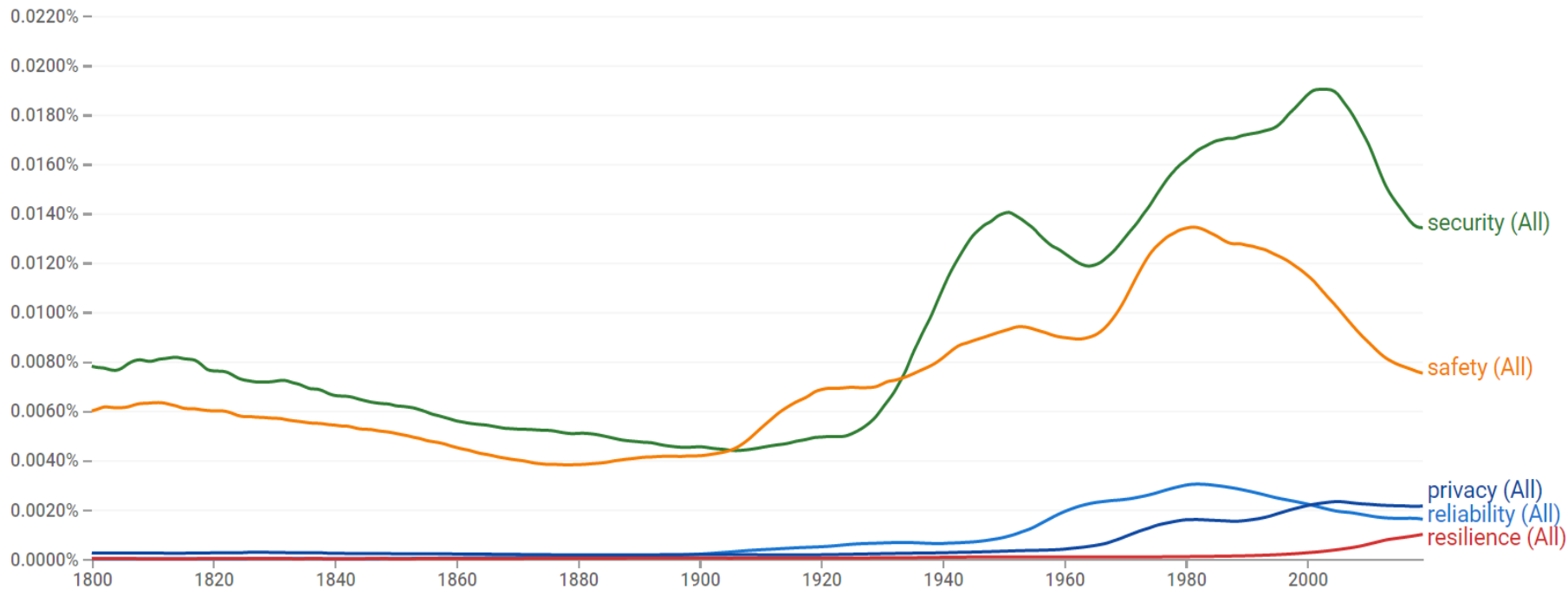
1800 - 2019

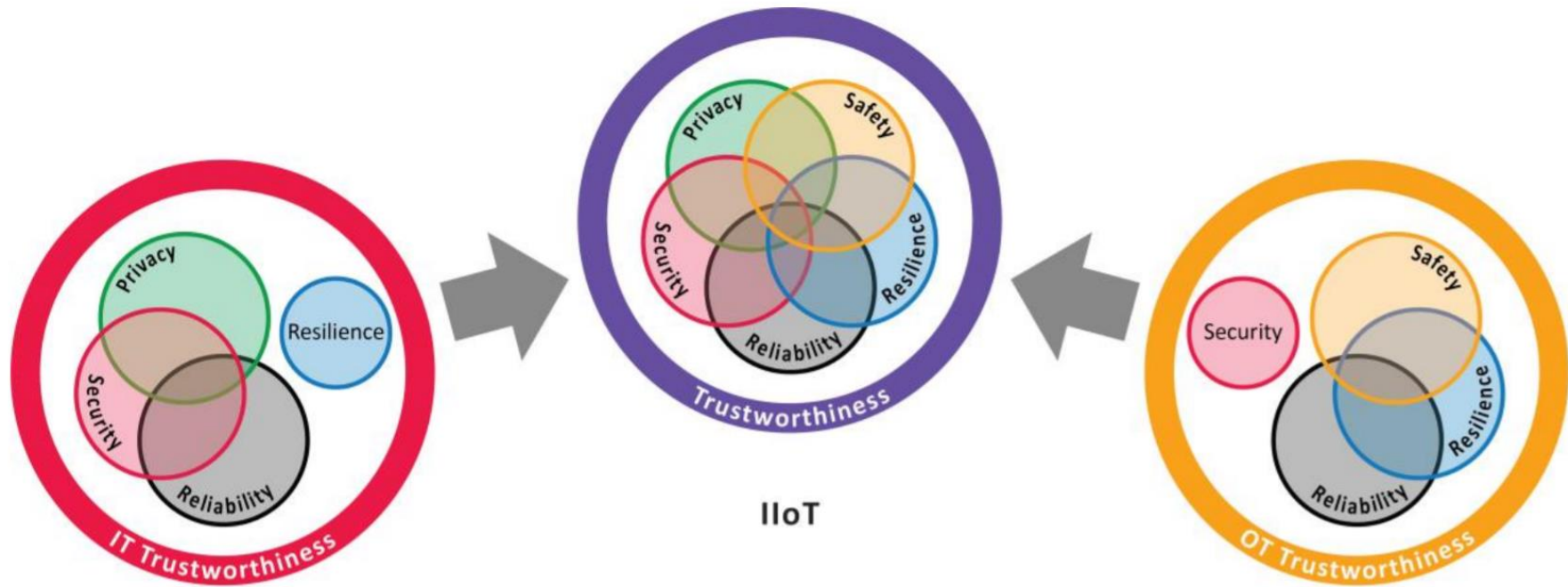
English (2019)

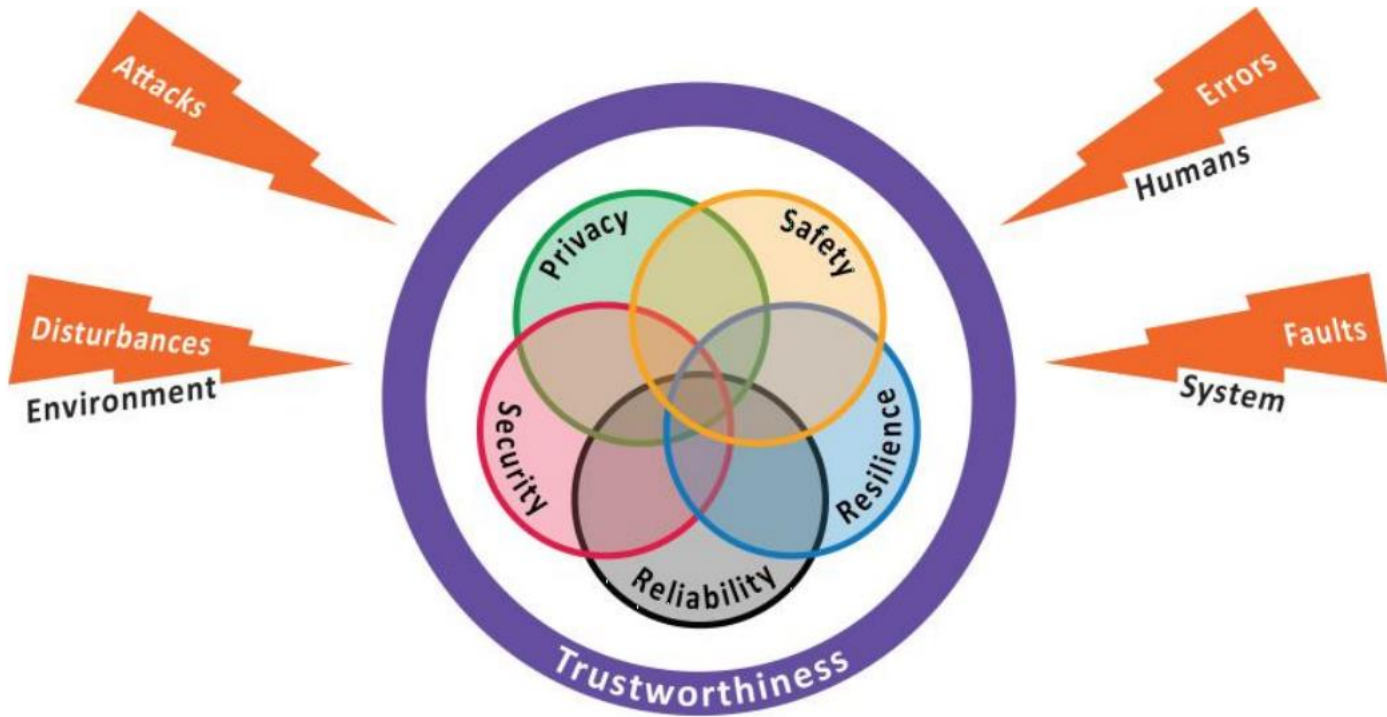
Case-Insensitive

Smoothing of 6

Google Books Ngram Viewer



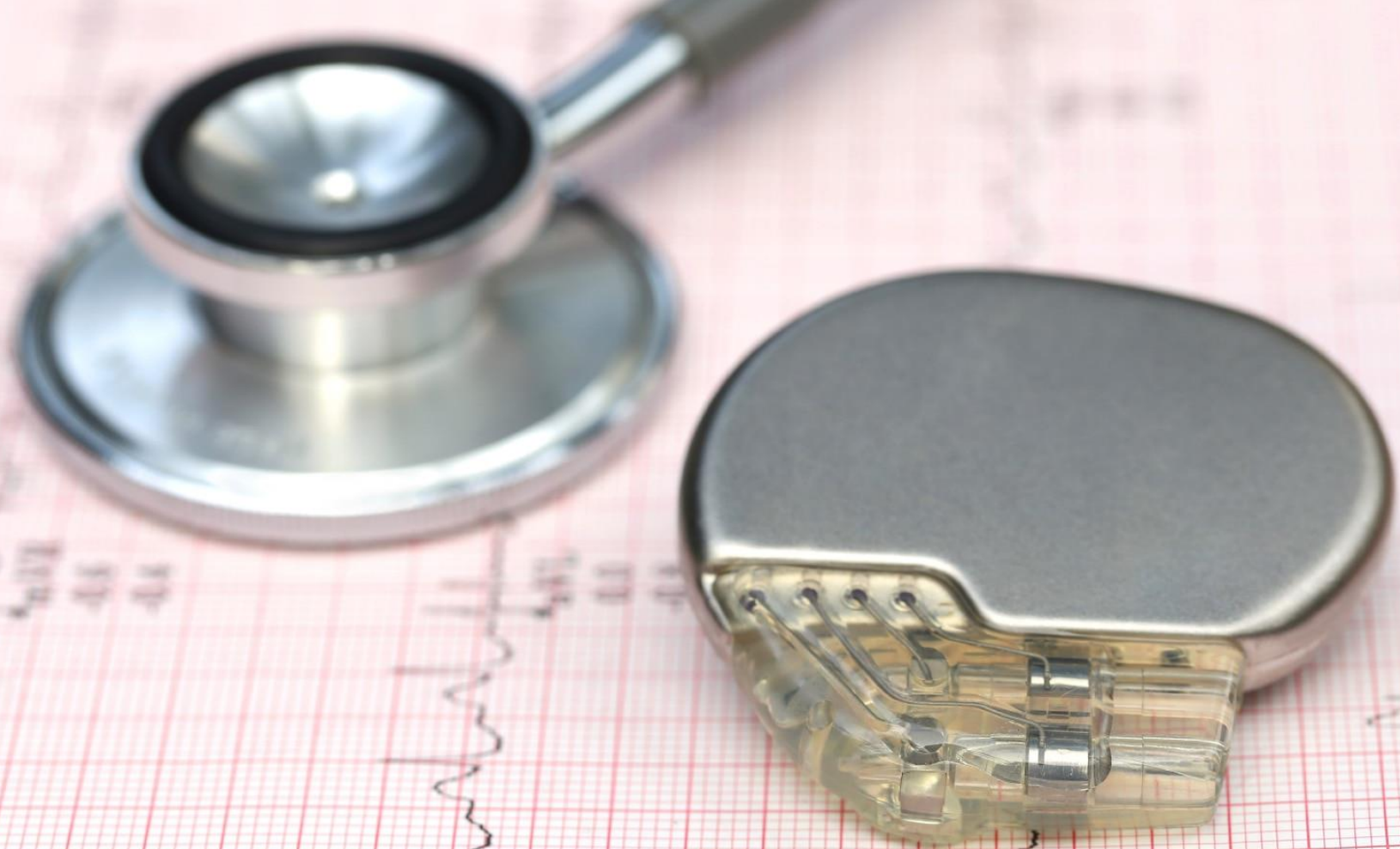




Зачем

The background is a detailed technical schematic of a piping system. It features numerous pipes, valves, pumps, and tanks. A large, dark teal, irregular shape is superimposed over the center of the diagram, partially obscuring some of the components. The overall color scheme is a gradient of teal and green.

Зачем рассматривать требования доверия совместно



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

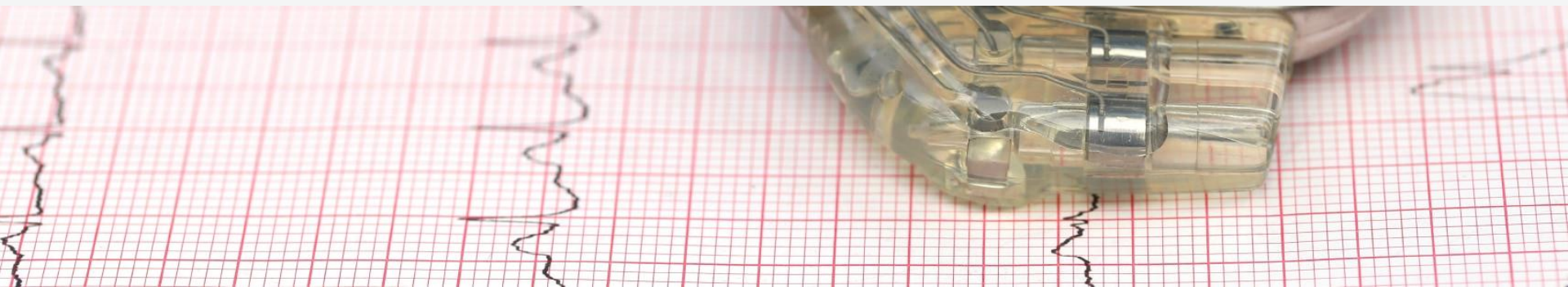
CVSS 3.x Severity and Metrics:



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

- 
- The image features a stethoscope on the left and a medical device on the right, both resting on a pink ECG grid. The stethoscope is silver and partially out of focus. The medical device is a small, oval-shaped device with a grey top and a clear bottom showing internal components. A black text overlay is positioned in the lower-left area of the image.
- **465 000 устройств
отозвано**



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

Уязвимость	CVSS v3 base score	CVSS vector string	Может ли повлиять на безопасность здоровья
CVE-2017-12712	8.8	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	да
CVE-2017-12714	6.5	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	да
CVE-2017-12716	6.5	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	нет
CVE-2017-12701	6.5	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	нет

Почему



Текущие схемы стандартизации и сертификации не решают проблему

IEC 60601-1

**General Requirements for Safety
of Medical Electrical Equipment**

основной для сертификации
медицинских устройств

на национальном уровне принят в
США, европейских странах, Канаде

В России принят как ГОСТ Р МЭК
60601-1-2010 и действует с 2011
года

В процессе менеджмента риска должны определяться не только те опасности, которые учитываются в настоящем стандарте, но и все другие опасности, связанные с ними риски и меры по управлению риском.

когда требования настоящего стандарта относятся к предотвращению недопустимого *риска*, приемлемость или неприемлемость данного вида *риска* должна определяться *изготовителем* в соответствии с принятыми им принципами определения допустимого *риска*.

От чего защищаемся?

Согласно стандарту

принципы идентификации и
оценки рисков
функциональной
безопасности, связанных с
кибератаками на
медицинское оборудование,
определяет производитель.

Как



Подходят к вопросам определения комплексного доверия в IIC и ISO/IEC

Основные задачи

Для технических комитетов по стандартизации

Определить доверие
Ограничиваться пятью аспектами? Добавить свои? Или дать общее определение?

Определить риски,
методы менеджмента рисков, критерии и приоритеты в работе с рисками

Не переборщить
У нас уже есть методики для обеспечения безопасности, надежности, устойчивости - нужно понять где «пусто» и работать адресно над проблемами

Что обсуждается

Стейкхолдеры и задачи

Кто имеет отношение к доверию, для кого оно имеет значение. Задачи, опасения, фокус внимания

Моделирование

А точнее виды моделирования – model kinds

Точки зрения

т.н. Viewpoints – бизнес, функции, реализация, использование, доверие

Что может быть заложено в архитектуру и дизайн

И как достигнуть гарантий



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

Основные задачи

Для консорциумов, альянсов, инициатив от индустрии

Определить доверие
И придерживаться этого определения

Определить риски,
методы менеджмента рисков,
критерии и приоритеты в
работе с рисками

Обмениваться опытом
У нас уже есть методики для
обеспечения безопасности,
надежности, устойчивости -
нужно понять где «пусто» и
работать адресно над
проблемами

Что обсуждается

Понятие доверия и приоритеты для бизнеса
Как объяснить, как монетизировать

Лучшие практики
Для достижения доверия в частных случаях ПО, аппаратной части, целой системы и инфраструктуры

Прикладные проблемы и технические кейсы
В основном рассматриваются в т.н. whitepapers

Что может быть заложено в архитектуру и дизайн
И как достигнуть гарантий – assurance cases



Trustworthiness Task Group

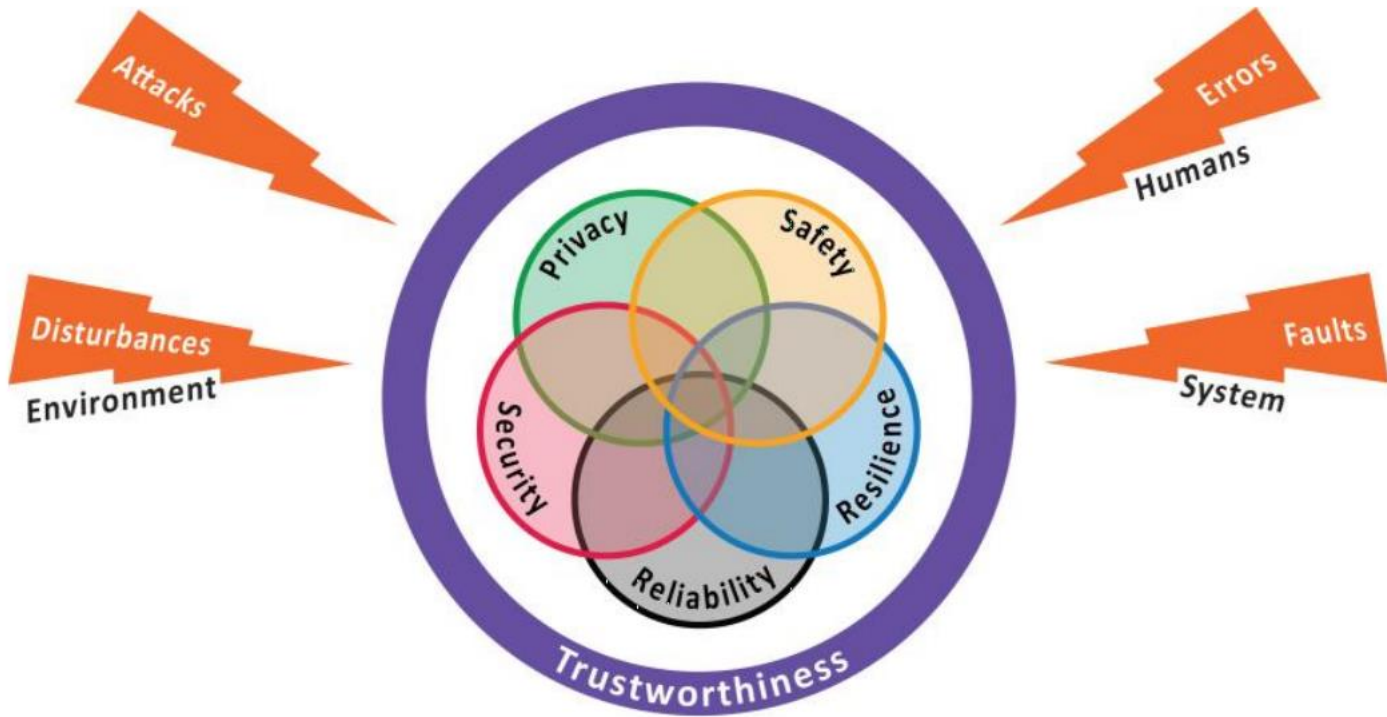
The Trustworthiness Task Group is chartered to explore aspects of trustworthiness relevant to IIoT and the IIC's vision of an IIoT ecosystem.

Papers and guidelines

Technical guidelines and whitepapers

Journal of Innovation

September 2018





Так что

Почитать



**Industrial Internet of Things
Volume G4: Security Framework**

IIC:PUB:G4:V1.0:PB:20160919



Key Safety Challenges for the IIoT

An Industrial Internet Consortium Technical White Paper

IIC:WHT:IN6:V1.0:PB:20171201

2017-12-01

Version 1.0

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

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



The Industrial Internet of Things: Managing and Assessing Trustworthiness for IIoT in Practice

An Industrial Internet Consortium White Paper
Version 1.0
2019-07-29



Software Trustworthiness Best Practices

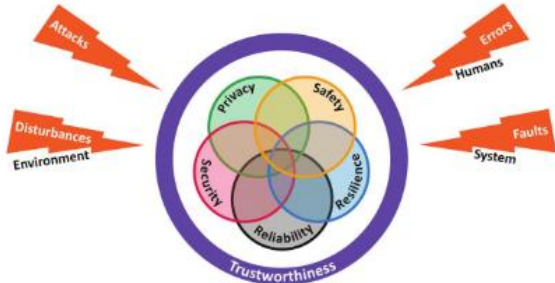
An Industrial Internet Consortium White Paper
Version 1.0 – 2020-03-23

Marcellus Buchheit (Wibu-Systems), Mark Hermeling (GammaTech), Frederick Hirsch (Fujitsu),
Bob Martin (MITRE), Simon Rix (Irdeto)

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

Journal of Innovation



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 Bommel, 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, XMPPro
Mr. Pieter van Schalkwyk, CEO, XMPPro
Ms. Cheryl Rocheleau, Sr. Marketing Manager, Industrial Internet Consortium
Mr. Matt Sexton, Sr. Marketing Specialist, Industrial Internet Consortium



9th Edition

TRUSTWORTHINESS

September 2018

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



Спасибо

Доверие в Интернете вещей

Екатерина Рудина

ICS CERT

On behalf of



kaspersky