IoT Trustworthiness is a Journey and NOT a Project

Author:
Bassam Zarkout
CEO
IGnPower
bzarkout@ignpower.com

INTRODUCTION

Confidence that an IoT system will operate in conformance with requirements[1] results from assurance that several characteristics of the system are compliant with these requirements despite environmental disturbances, human errors, system faults and attacks. These characteristics – security, safety, reliability, resilience and privacy – have been identified by ISO/IEC (JTC SC41)[2][3], National Institute of Standards and Technology (NIST)[4] and the Industrial Internet Consortium (IIC) (Industrial Internet Security Framework (IISF), Section 3)[5] as defining trustworthiness [6] of a system. These characteristics manifest themselves in operational, organizational, commercial, budgetary, architectural and security areas.

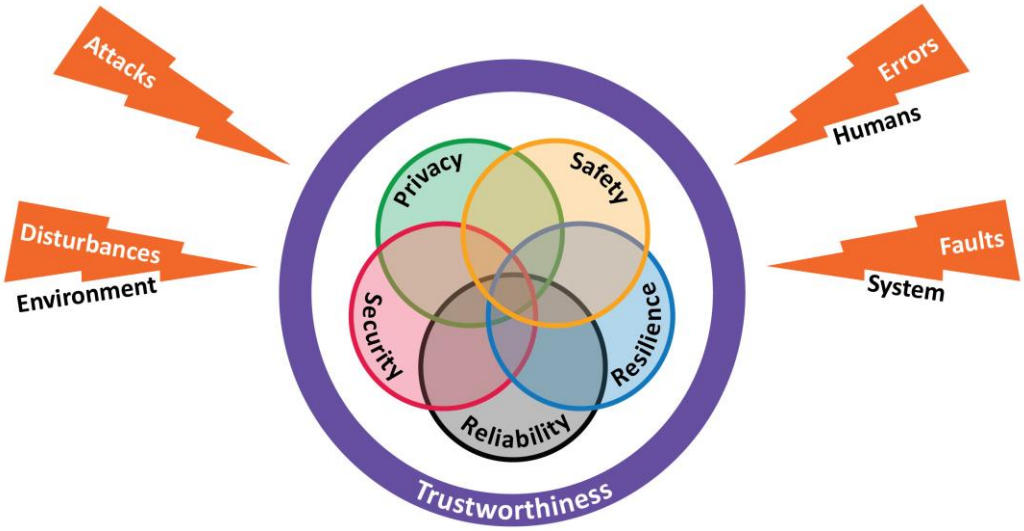

Figure 1: IoT Trustworthiness - IIC Industrial Internet Security Framework - source IIC IISF

An IoT system is trustworthy if it meets the minimum requirements for security, safety, reliability, resilience and privacy, as defined by laws, regulations, standards and industry best-practices. The OSHA 29 CFR 1910 is an example of such regulation[7].

In a sense, IoT Trustworthiness is a binary function.

1 Example business objectives, design objectives, risk management objectives, legal and regulatory requirements, standards, industry best practices, etc.

2 www.iec.ch/dyn/www/f?p=103:30:31458742125318::::FSP_ORG_ID,FSP_LANG_ID:20486,25

3 www.itu.int/en/ITU-T/Workshops-and-Seminars/20180604/Documents/Francois_Coallier_P_V2.pdf

4 www.nist.gov/news-events/events/2016/08/exploring-dimensions-trustworthiness-challenges-and-opportunities

5 www.iiconsortium.org/IISF.htm

6 www.iiconsortium.org/vocab/index.htm - definition of IoT Trustworthiness

7 www.osha.gov/laws-regs/regulations/standardnumber/1910

Failure to meet the minimum requirements can lead to significant consequences, such as industrial accidents, data breaches and operational interruptions. These consequences can, in turn, result in personnel injury, capital equipment damage, litigation costs and reputational damage.

Compliance with the minimum requirements of trustworthiness is not only about avoidance of negative outcomes. It can lead also to better outcomes, such as:

- Align the operation of the IoT System with Corporate Business Objectives
- Improve the visibility of Operational Risks throughout the lifecycle
- Mitigate the impact of fluctuations in Trustworthiness levels during the lifecycle

Furthermore, senior management within the organization may choose to exceed the minimum requirements of trustworthiness. The reasons could be to enhance the strategic positioning vis-à-vis competitors or perhaps to align the work on trustworthiness with other ongoing quality initiatives within the organization. It may be also to proactively achieve compliance ahead of anticipated changes in laws and regulations.

The efforts to establish and maintain trustworthiness in IoT systems must cover the full lifecycle of these systems. These lifecycles can be decades long in some cases; examples, a pipeline oil leak monitoring system, a pumping sub-system in a power plant, etc.

During these long lifecycles, the trustworthiness requirements may change and fluctuate:

- New legal and/or regulatory frameworks may add new requirements or significantly change existing ones
- Changes in corporate strategies and roadmaps may add new requirements or fundamentally change existing ones
- Achieved levels of trustworthiness may fluctuate and decay over time due to system and human errors, lapses, cyberattacks, malicious activities, etc.

Therefore, establishing IoT Trustworthiness in a system is not a point-in-time project. It is an effort that must be maintained systematically throughout the lifecycle journey of the system.

IoT Systems Have Long Lifecycles

The IIC Industrial Internet Reference Architecture[8] (section 3) asserts that the concerns about the architecture of the IoT system cover the full lifecycle of that system.

Equally, concerns about trustworthiness also cover the full lifecycle of IoT systems. These lifecycles can be very long due to the nature of industrial systems. As mentioned in the example in the Introduction section, the lifecycle of power plants and some of their major systems such as turbine cooling pumping system may be measured in decades. During such long lifecycles,

[8] www.iiconsortium.org/IIRA.htm

some of the internal systems and sub-systems of the plant may be upgraded, IoT-enabled, and in some cases totally replaced.

Moreover, some of the IoT data produced and consumed by the IoT systems at the plants may themselves have long lifecycles. For instance, data may be needed for predictive maintenance analytics or may become evidence in the case of industrial accidents and thus become subject to Electronic Discovery (eDiscovery) and legal holds.

Electronic Discovery[9] [10] is the process of identifying, preserving, collecting, processing, searching, reviewing and producing Electronically Stored Information[11] that may be relevant to a civil, criminal or regulatory matter, and legal holds.

Figure 2 illustrates an example of the lifecycle of an IoT system:

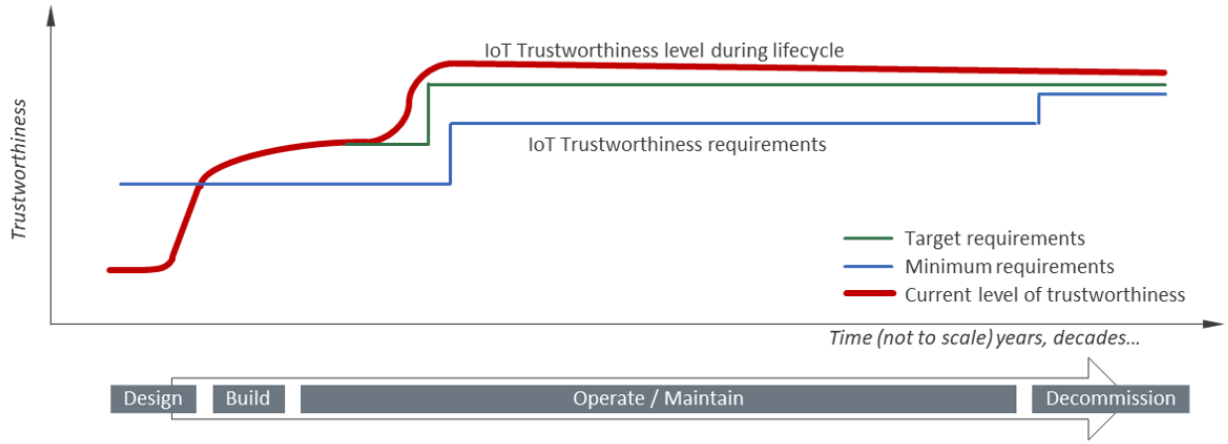

Figure 2: Trustworthiness during the lifecycle of an IoT system

The lines in this diagram represent the Current, Minimum and Target states of IoT Trustworthiness as they progress during that lifecycle. These states are described in detail in the next section.

Once these states are assessed and defined, the organization can implement methods and processes that can raise the Current level of trustworthiness to reach the Minimum level. They can, if so purposed and planned, exceed it to reach the Target State.

Concerns about trustworthiness continue throughout the full lifecycle of the system:

- The minimum requirements may increase over time
  - Legal and regulatory frameworks may change and/or become more stringent
  - New industry standards may come into effect

[9] www.edrm.net/glossary/electronic-discovery-e-discovery/

[10] www.law.cornell.edu/rules/frcp The Federal Rules of Civil Procedure (amended December 1st, 2016) Rules 26 and 34

[11] www.edrm.net/glossary/esi-electronically-stored-information/

  - The functional and technical evolution of the system may affect its trustworthiness requirements
  - Corporate mandates and roadmaps may change direction and pace
  - M&A activities may impact strategies and priorities
- The current trustworthiness levels may fluctuate over time
  - Normally, this level starts at a point below the required level
  - As trustworthiness-focused methods and processes are deployed, this level will rise
  - Organizations may need to raise the level of trustworthiness again later in the lifecycle due to future changes in the requirements
  - The current levels of trustworthiness may decay over time, due to system and human errors, lapses, cyberattacks, malicious activities, etc.
  - During the decommissioning stage, additional requirements may arise; example, how to decommission a nuclear facility and how to handle hazardous materials

IoT Trustworthiness States

The previous section has highlighted the importance of maintaining a system lifecycle perspective about IoT Trustworthiness. The path that trustworthiness should take during the lifecycle (red line in Figure 2) is planned/charted based on considerations such as:

- Required levels of IoT Trustworthiness and the timeframes for compliance with them,
- Corporate objectives and roadmaps,
- Risk management considerations,
- Budgetary and Return on Investment (ROI) considerations
- and many others.

In general, trustworthiness has three milestone states:

Figure 3: The states of IoT Trustworthiness

Current State

This is the actual "trustworthiness" status of an IoT system, based on the system as it is currently designed, implemented and operating:

- Current state of safety processes

- Current levels of reliability and resilience
- Current state of data protection and security, as well as data privacy controls

The Current State evolves over time as the methods and processes put in place to address the trustworthiness requirements take effect and as factors such as system and human errors, lapses, cyberattacks, malicious activities and external influences begin to negatively impact the level of trustworthiness of the system.

Minimum State

This is a non-negotiable level of trustworthiness mandated by external authorities and parties; example, legal, regulatory and standards bodies, as well as industry best practices.

- To determine the Minimum State level, it will be important to assess applicable laws, regulations, best practices and standards, and evaluate their impact
- In situations where these requirements may conflict with each other, the organization's Risk Management and Legal teams may need to be involved to provide opinions and guidance regarding the course of action.

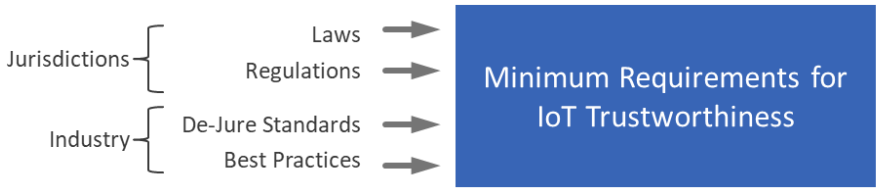

Figure 4: Minimum Requirements defined by external parties

The IIC Industrial Internet Security Framework (section 4.3) discusses some of the legal and regulatory requirements as they relate to Information Technology (IT) and Operational Technology (OT). Another example is the OSHA 29 CFR 1910 which covers occupational safety and health standards.

In addition to the above, requirements can have jurisdictional implications and in some cases actually boundaries (Data Residency[12]). In these cases, the methods and processes implemented to empower the trustworthiness of the IoT system must have jurisdictional variations.

[12] www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf

The EU General Data Protection Directive[13] (GDPR) data privacy law came into effect on May 25th, 2018. It applies to Personal Data created and consumed within the EU jurisdictions as well as Personal Data belonging to EU residents anywhere in the world. The law imposes a wide range of restrictions[14] on organizations (Data Controllers[15] and Data Processors[16]) that handle personal data. Personal data may be produced and consumed by an IoT system. Therefore the IoT Trustworthiness calculus must take into account the restrictions imposed by this law.

Other privacy law examples that apply within specific jurisdictions include the California Consumer Privacy Act of 2018 (CCPA)[17] and the Personal Information Protection and Electronic Documents Act in Canada[18].

Target State

This third state represents trustworthiness levels that exceed the Minimum requirements, based on additional internally-defined and self-imposed drivers and objectives (business and technical):

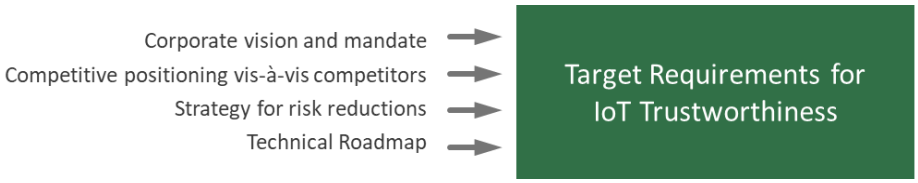

Figure 5: Target Requirements defined internally

IOT TRUSTWORTHINESS CHARACTERISTICS

The trustworthiness of an IoT system is defined by five main characteristics: security, safety, reliability, resilience and privacy. These characteristics have also been identified by ISO/IEC JTC SC41[19], NIST and the IIC IoT Vocabulary and the IIC IISF. Each characteristic will typically have its own Current, Minimum and Target milestone states. The overall assessment of a system's trustworthiness must be based on the aggregate assessment of each of these characteristics.

13 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1473816357502&from=en and http://data.europa.eu/eli/reg/2016/679/oj

14 Example: prior consent before data capture, data retention, jurisdiction where data is stored, etc.

15 Party which determines purposes and means of the processing of personal data

16 Party which processes personal data on behalf of the controller

17 https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf

18 https://www.priv.gc.ca/leg_c/leg_c_p_e.asp

19 www.iec.ch/functionalsafety/

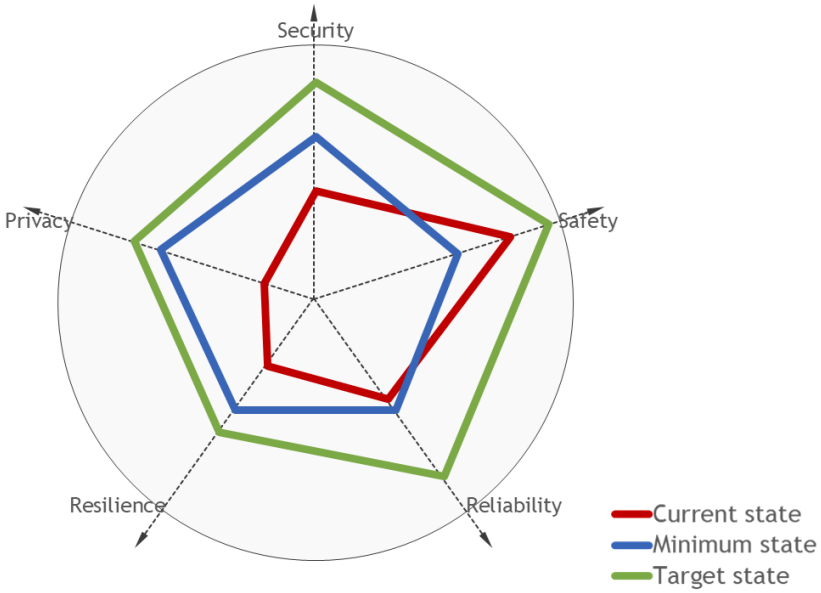

Figure 6: IoT Trustworthiness Radar Diagram - source IIC Trustworthiness Task Group

The diagram in Figure 6 provides an example of the five IoT Trustworthiness characteristics (and their states) for a particular system.

In this example, the Safety characteristic for this system already meets (in fact exceeds) the Minimum requirements. Therefore, in principle, no efforts are required to improve safety, except if necessary to meet the target state based on additional internally-defined and self-imposed drivers and objectives (business and technical).

The remaining four characteristics (Security, Reliability, Resilience and Privacy) do not meet the Minimum levels, and thus efforts are needed to make these system characteristics compliant with the minimum requirements.

It is important to note that each of the trustworthiness characteristics will have its own set of legal and regulatory requirements, standards, processes and best practices to comply with. Also these requirements may be specific to vertical application and use cases.

Some interdependencies may exist between the five characteristics, which in turn may lead to potential adverse effects; example, delaying Security updates in order to maintain Reliability levels can be detrimental to Safety.

Another example is the recommendation by some standards such as IEC 61508[20] [21] to separate between Control and Safety systems. “The EUC (equipment under control) control system shall

[20] www.iec.ch/functionalsafety/

[21] https://www.iiconsortium.org/pdf/Industrial_Internet_of_Things_Volume_G2-Key_System_Concerns_2018_08_07.pdf - IIC Industrial IoT - Key System Concerns G2 section 3

be separate and independent from the Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related system, other technologies safety-related systems and external risk reduction facilities."

This standard is used by the British Health and Safety Executive[22] (HSE) as a measure of "whether a safety-critical system has reduced risk As Low As Reasonably Practicable (ALARP), a requirement of English law."[23]

The main point here is that the interdependencies between the characteristics of trustworthiness must be considered and catered to in the analysis and definition of trustworthiness requirements.

IoT Trustworthiness Journey

Concerns about establishing confidence that an IoT system meets the expectations of trustworthiness[24] cover and permeate the whole lifecycle of the system. This means that IoT Trustworthiness is more than just a project with a finite start and end. It is a Journey that must be piloted via an established program.

The diagram in Figure 7 expands on the example lifecycle depicted in Figure 2.

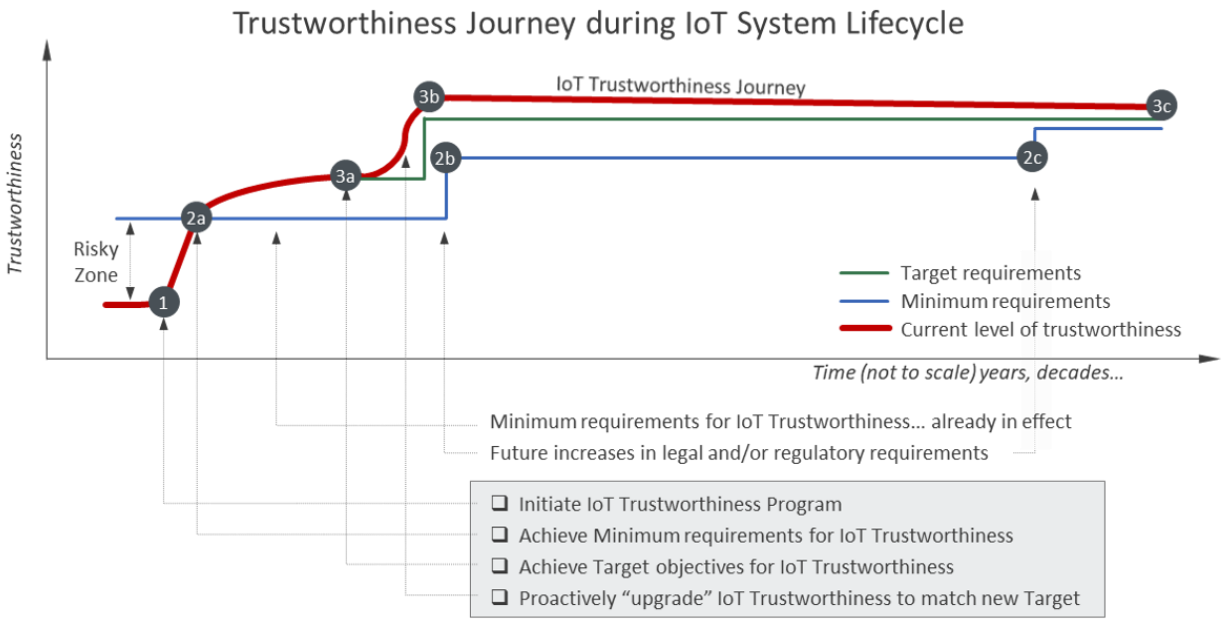

Figure 7: The IoT Trustworthiness Journey

[22] www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm

[23] https://pdfs.semanticscholar.org/e280/319e13657c0b5516b66429085e79f6ca2672.pdf

[24] The Minimum and Target levels described in the *IoT Trustworthiness States* section.

In this diagram, the path of the Current State (red line) navigates around (and above) the minimum compliant level requirements, their timelines, the corporate strategic mandates, and the implementation resources that made available for this effort. The path has multiple distinct segments, which will be explored in the next sub-sections.

Become Compliant… [1] - [2a]

This segment of the journey starts with the initiation of the IoT trustworthiness effort and ends when the Minimum mandatory requirements are met.

Following the assessment of current and minimum states of trustworthiness, the organization may determine that it is at risk of non-compliance with its mandatory minimum requirements. It must now implement a project with an accelerated schedule to raise the level of trustworthiness of a system to become compliant with these minimum requirements:

- The vertical distance between points [1] and [2a] in the diagram represents the gap in trustworthiness to be covered
- The horizontal distance between these points represents the expected project timeline to achieve this level of compliance

In this segment of the journey, the ROI may not be the primary concern. However, the organization will want to aim at reaching point [2a] in the most effective and cost-efficient way.

Meet Internal Mandates… [2a] - [3a]

Once point [2a] in the journey is reached, the organization may decide to continue its effort to raise the levels of trustworthiness to [3a]. The drivers for this segment are internally-defined and self-imposed:

- The corporate vision may mandate higher standards for trustworthiness
- The product/marketing group may want to better position its offering vis-à-vis its competition
- The risk management and legal groups may set higher standards for trustworthiness
- The technical roadmap may dictate alignment and timeline requirements for this segment

In this segment of the journey, ROI should be one of the primary concerns. In other words, the internally-defined drivers must have sound financial justification.

Comply with Upcoming Requirements… [3a] - [3b]

In anticipation of upcoming changes to the requirements[25] [2b], the organization may proactively raise the level of trustworthiness of its IoT system to [3b] to meet these new requirements. As

[25] Example: changes in regulations.

with segment [1] - [2a], the ROI may not be the primary concern. However with appropriate planning, the organization can ensure that point [3b] is reached in the most effective and cost-efficient manner.

Cruise to End of Life (EoL)… [3b] - [3c]

In the example depicted in Figure 7, the organization should set trustworthiness level [3b] in such a way to cater to the expected fluctuations and decay in trustworthiness levels over time. This is represented in the diagram by the slow downwards slope of the red line. The organization should also cater to future potential increases in trustworthiness requirements [2c]:

- This would allow the journey to continue in cruise mode all the way to the EoL point
- The organization must also monitor the level of decay in trustworthiness and position itself to intervene tactically to mitigate and redress such decay
- Depending on the nature of the system, the decommissioning of the system may require specific requirements

The ROI and costs efficiency calculations must take into consideration the overall trustworthiness efforts throughout the lifecycle and the agility with which the organization can intervene to address unexpected hurdles along the journey path.

IOT TRUSTWORTHINESS PROGRAMS

As stated earlier, IoT Trustworthiness is NOT a project. It is a journey that is piloted by a Program.

The IoT Trustworthiness Program is a framework for organizing, directing, implementing and maintaining Trustworthiness of an IoT System throughout its lifecycle, and in accordance with established Corporate Business Objectives. The domain and discipline of IoT Trustworthiness is emerging and it can be characterized with the following:

- Levels of awareness and maturity about trustworthiness are emerging
- Discipline requires the involvement of multiple groups in the organization
- Technical complexities are involved: IT, OT, Operation, Safety, Design, etc.
- Underdeveloped execution strategy
- Lack of effective executive sponsorship… who is in charge

Upon the initiation of such a program (point [1] in Figure 7), the organization must establish a top-down view for the program as well as a bottom-up perspective, as depicted in Figure 8:

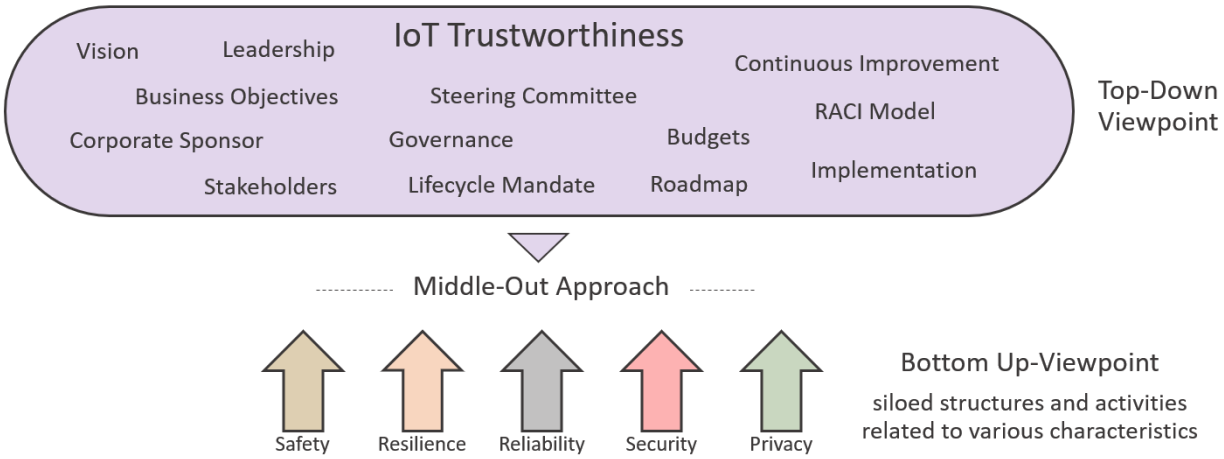

Figure 8: IoT Trustworthiness Top-down versus Bottom-up Views

Corporate Sponsorship

IoT Trustworthiness is a cross-functional discipline that involves stakeholders from the IT and OT side, as well as stakeholders from other functions such as the business, corporate and legal. These stakeholders tend to have divergent perspectives on trustworthiness:

- IT is concerned with security
- Operations (and OT in particular) are interested in safety, reliability and resilience
- Compliance and legal are concerned with the risks of non-compliance
- Corporate is interested in the strategic vision for the IoT solution
- The business is interested in achieving the business outcomes

For such a multi-disciplinary and cross-functional effort to succeed, the program MUST have a senior corporate sponsor whose mission is to define the objectives of trustworthiness and empower the organization to achieve them and maintain them throughout the lifecycle of the system. The objectives can be any mix of business, technical, operational and even reputational objectives. The type of vertical domain and use case will determine who that person is and the level of his or her seniority.

IoT Trustworthiness Program Tsar

The cross-functional nature of trustworthiness poses another challenge. The program must have a clear leader who is empowered and mandated by the Corporate Sponsor to steer this cross-functional program and achieve its objectives.

The IoT Trustworthiness domain is still in its early stages of development. It is not clear yet who in the organization should assume this leadership role, what his or her profile should be, and where he/she fits within the organization chart.

Information Governance (IG) is also a cross-functional function. It addresses the need to manage corporate information in a manner that balances between the legal and compliant use of information, security, operational transparency and reduced legal costs.

When IG emerged a decade ago, it faced similar challenges regarding its leadership. Gartner started calling for the creation of a new C-level title in the organization to own this function. One of these publications is G00254671, the "Business Case for the Chief Data Officer (CDO)."[26]

In a 2015 survey of 3000 executives, Forrester Research reported that 45% of respondents stated that their organizations had CDOs[27].

Figure 9 provides suggestions about the responsibilities, profile, reporting structure and budget sources for the IoT Trustworthiness leadership role:

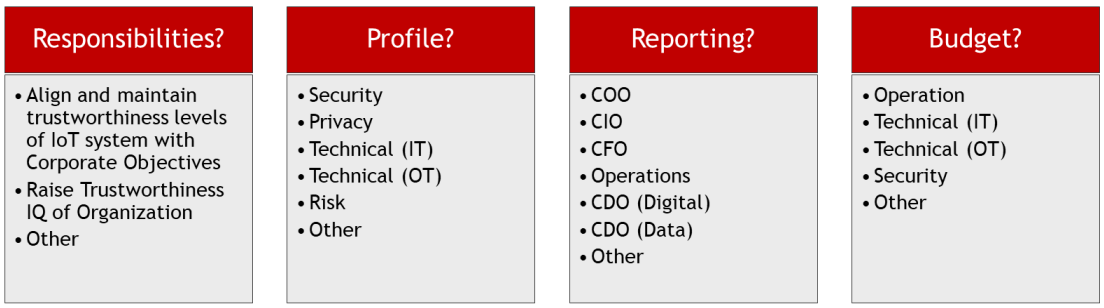

Figure 9: Who will be the IoT Trustworthiness Tsar?

Whether the IoT Trustworthiness leadership role will be assigned to an existing senior executive in the organization or a totally new title will be created for that function will depend on the vertical domain, the use case and the prominence of the IoT-focused business activities within the Digital Transformation strategy.

Steering Committee for the Stakeholders

A functional and effective Steering Committee is another element of the IoT Trustworthiness Program and is key to its governance and success. The members of this committee must have representation from the communities that correspond to the five characteristics of trustworthiness, security, safety, reliability, resilience and privacy.

[26] www.gartner.com/doc/2876417/business-case-chief-data-officer

[27] www.forrester.com/report/Top+Performers+Appoint+Chief+Data+Officers/-/E-RES123064

Exploring the Dimensions of Trustworthiness: Challenges and Opportunities Workshop[28] (NIST August 2016): In the NIST Cyber-Physical Systems CPS Framework, trustworthiness is captured as a high-level and critical concern encompassing safety, security, privacy, resilience and reliability. These system characteristics are typically considered separately and in isolation, resulting in work, intended to address one of these concerns, adversely impacting work to address one or more of the others.

The titles of the members of the IoT Trustworthiness Program steering committee will vary depending on the vertical domain and use case within that vertical. For example, the Security characteristic may be represented by a senior person in the CISO organization whereas the Resilience characteristics may be represented by Operations.

It is in this committee where the top-down perspective of IoT Trustworthiness and the bottom-up perspectives of the individual characteristics of IoT Trustworthiness mesh and integrate. This is referred to in Figure 8 as the Middle Out approach.

The Steering Committee must also create a Responsible-Accountable-Consulted-Informed Matrix (RACI) for the program. This matrix should identify the individual tasks involved in the program, the parties involved in these tasks and the responsibilities of these parties for each task:

- Responsible
- Accountable (or Approver)
- Consulted
- Informed

Characteristic	Corporate	Legal	Finance	Security	Business	IT	OT	Operations	Other
Security	I	C	I	R/A	I	R	R	R	Tbd
Safety	I	I	I	C	C	I	R	R/A	Tbd
Reliability	I	I	I	C	I	I	R/A	R	Tbd
Resilience	I	I	I	C	C	I	R/A	R	Tbd
Privacy	I	R/A	I	R	C	R	I	C	Tbd

RACI = Responsible, Accountable (or Approver), Consulted, Informed

- Rows can have multiple R's (should not have more than necessary)
- Each row must have -o-n-e- A
- Rows can have multiple C's (having too many leads to analysis-paralysis)
- Rows can have multiple I's

Figure 10: Example RACI Matrix for IoT Trustworthiness Program

[28] www.nist.gov/news-events/events/2016/08/exploring-dimensions-trustworthiness-challenges-and-opportunities

Value Delivered by Program

Above all, the IoT Trustworthiness Program must deliver value to the organization. This value must take the form of better outcomes that are expressed and communicated to the various groups within the organization in terms they relate to and appreciate and in a manner that addresses the issues at the various layers and viewpoints described in the Industrial Internet Reference Architecture, Section 3.5

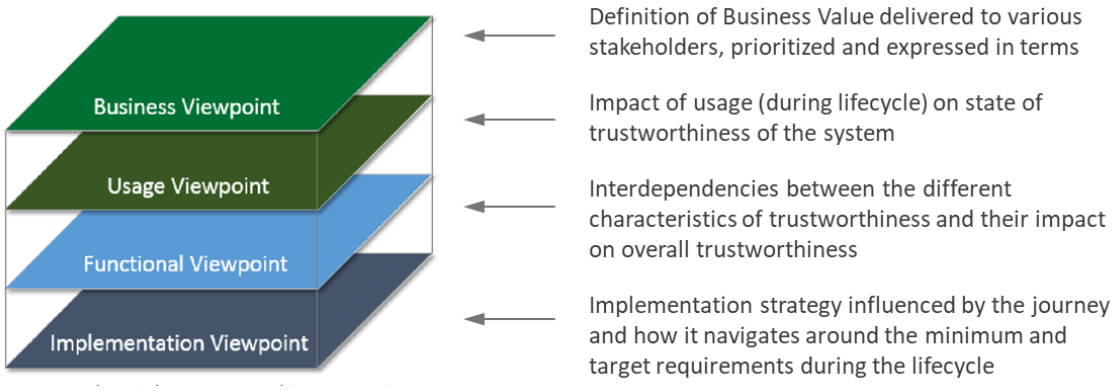

Figure 11 - Industrial Internet Viewpoints - source IIC IIRA Section 3.5

The table below provides examples of such better outcomes:

Group	Value Delivered
Corporate	Support ability to meet vision
Legal	Reduce legal risks and litigation cost
Risk	Provide a better visibility of risks
Finance	Reduce unplanned costs
Security	Achieve a better understanding and appreciation of the impact of security on other characteristics of trustworthiness, and consequently the ability of the IoT system to deliver the overall business value
Business	Improve quality of service and decision making
IT	Achieve a better alignment with OT and a better understanding of the architectural impacts the IoT system will have on the IT infrastructure
OT	Achieve a better alignment with IT
Operations	Achieve a better understanding of the impact Security and Privacy can have over availability of service
Other	TBD

The delivery of these better outcomes should be prioritized, based on corporate strategy, product strategy, available resources, available budgets, critical internal milestones, as well as industry and market milestones.

Roadmap Alignment

The mapping of the journey and its path during the lifecycle must consider the individual roadmaps of the characteristics of trustworthiness.

CONCLUSION

Establishing trustworthiness for an IoT system is one of the key factors to ensure that the system can deliver on its objectives. IoT Trustworthiness is a concern that must be addressed throughout the long lifecycle of the system. This effort must cater to the expected changes and fluctuations in the levels of trustworthiness (Minimum Required and Current sides).

In order to achieve this, IoT Trustworthiness cannot be treated as a project. It is a journey that covers the lifecycle of the system. This journey must be piloted by a formalized IoT Trustworthiness Program within the organization, with continuous evaluation, direction and monitoring.

➢ Return to IIC Journal of Innovation landing page for more articles and past editions.