Measuring the Trustworthiness of Software

with ISO/IEC 5055

2022-07-27

Author

Bill Curtis, Ph.D,
Consortium for Information and Software Quality
curtis@it-cisq.org

CONTENTS

FIGURES

1 INTRODUCTION

The definition of Trustworthiness and its constituent characteristics focuses on the behavior of a system in operation and whether people can trust that it will perform as expected and according to its requirements. Consequently, many of the measures of Trustworthiness evaluate the operational behavior of a system or collection of linked devices.

These measures are post-hoc in that they measure failures that have already occurred rather than the engineering weaknesses that caused these failures. This paper focuses on software measures that can be calculated during development and testing in order that weaknesses be corrected before linked devices are placed in operation.

Until recently there has been no widely accepted way to measure the Trustworthiness of software from the actual source code product prior to placing it in operation. This article will discuss how the Industry IoT Consortium's (IIC) five Trustworthiness characteristics relate to the software quality model in the ISO 25000 series of standards.

It will discuss how ISO/IEC 5055:2021 (hereafter referred to as ISO 5055) supplements the ISO 25000 series to provide measures that can be used to assess the Trustworthiness of a software-intensive system at the level of the source code. It will show how detecting known weaknesses in the source code can be used to assess a software-intensive systems Trustworthiness prior to placing it into operation.

2 TRUSTWORTHINESS AND THE ISO/IEC SOFTWARE QUALITY MODEL

The IIC Trustworthiness Framework[1] decomposes trustworthiness into five characteristics —Safety, Security, Reliability, Resilience, and Privacy. These are the characteristics that should be measured independently since each is affected by a different ensemble of weaknesses.

The IIC Trustworthiness characteristics are similar to several quality characteristics and sub-characteristics in the ISO/IEC 25010:2011 software and system product quality model[2]. The importance of this relation is that the ISO 25000 series of quality standards provides one basis for measuring IIC's Trustworthiness characteristics.

The eight quality characteristics in ISO 25010 include Functional Suitability, Performance Efficiency, Compatibility, Usability, Reliability, Security, Maintainability, and Portability.

---

[1] M. Buchheit, F. Hirsh, R.A. Martin, V. Bemmel, A.J. Espinosa, B. Zarkout, C.F. Hart, & M. Tseng (2021). *The Industrial Internet of Things Trustworthiness Framework Foundations*. *https://www.iiconsortium.org/foundational-publications.htm*

[2] ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model. Geneva: International Organization for Standardization.

There are relations between these two models, but they are not perfectly mapped. ISO 25010's quality characteristics for Reliability and Security mirror similar characteristics in the IIC Trustworthiness model. However, IIC's Resilience is addressed by two sub-characteristics under ISO 25010's Reliability characteristic—Fault Tolerance and Recoverability.

IIC's Privacy characteristic is addressed by Confidentiality, a sub-characteristic under ISO 25010's Security characteristic. The current published version of ISO 25010 does not have a quality characteristic for Safety. ISO 25010 is currently being revised and will contain a ninth quality characteristic devoted to Safety in its next publication. Reliability and Security will remain largely identical to their construction in the 2011 publication.

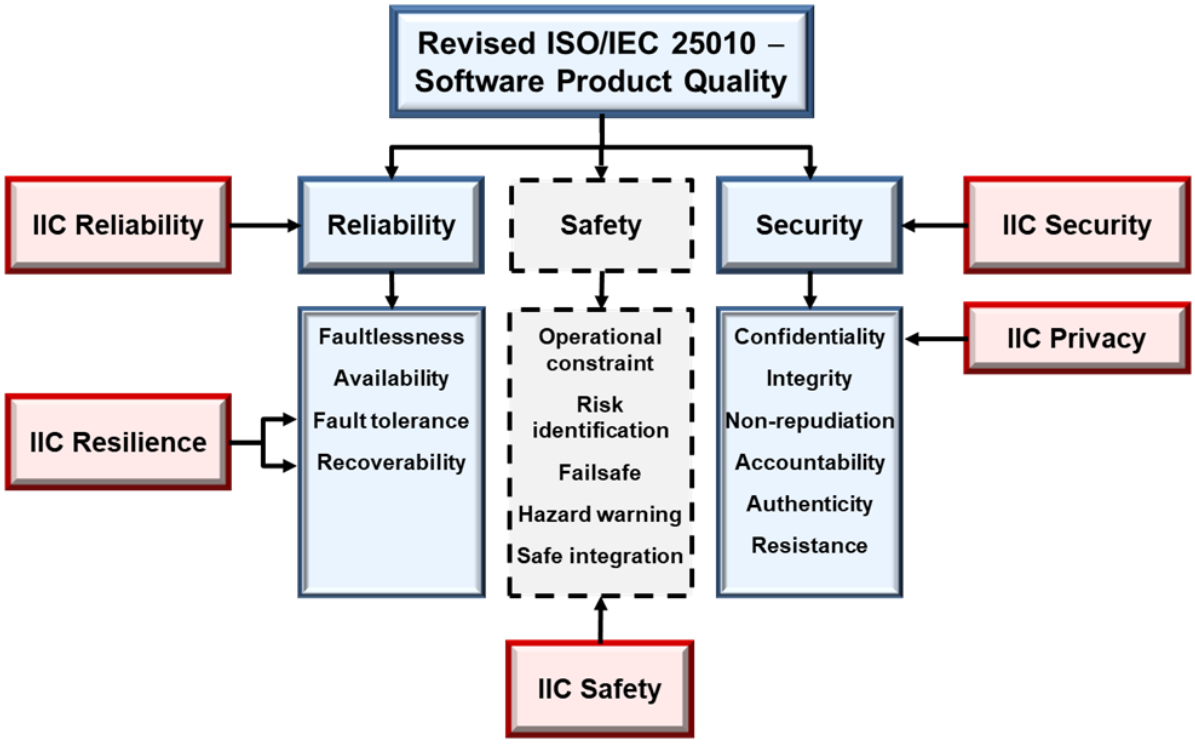

Figure 2-1. Relation of IIC Trustworthiness characteristics to the quality characteristics in the revised ISO/IEC 25010.

Figure 2-1 displays a partial representation of the revised ISO 25010 quality model with the relevant quality characteristics of Reliability and Security highlighted in light blue. The new Safety characteristic is highlighted in a dashed gray. The IIC Trustworthiness characteristics are presented in red with pointers to their related ISO 25010 characteristic or sub-characteristic.

ISO 25023[3] is the standard that defines measures for each of the characteristics and sub-characteristics in ISO 25010. However, virtually all of the measures in ISO 25023 evaluate the operational behavior of a system rather than the quality of its construction. With the exception of Safety, ISO 25023 defines measures that can be used to assess the operational aspects of Trustworthiness such as outages, security breaches, data theft, managing unexpected conditions, etc.

For instance, Reliability is measured by the amount of time the system is available rather than by assessing software flaws that will cause the system to crash. Consequently, there was a need to evaluate the engineering structure of a software system to assess its Trustworthiness characteristics before it was placed in operation.

3 ISO/IEC 5055:2021 AUTOMATED SOURCE CODE QUALITY MEASURES

To meet this need, last year ISO published ISO/IEC 5055:2021[4]. This standard was originally developed by the Consortium for Information and Software Quality (CISQ), a Special Interest Group managed by the Object Management Group (OMG). CISQ was co-founded by Paul Nielsen, CEO of the Software Engineering Institute (SEI) at Carnegie Mellon University and Richard Soley, CEO of the Object Management Group. CISQ was initially chartered to create standards for automating the measurement of software size and structural quality.

Over 80 senior software experts from 31 companies in North America, Europe, and Asia met several times over 18 months to develop standards for measuring 4 of the 8 quality characteristics in ISO 25010—Reliability, Security, Maintainability, and Performance Efficiency. The four standards were initially focused on business software applications.

These four measurement standards were eventually upgraded to add coverage for embedded software. All four updated measures were combined into one OMG standard—Automated Source Code Quality Measures. This consolidated standard was approved by OMG and submitted to ISO as a Publicly Available Standard. On March 31, 2021, it was approved and published by ISO as ISO/IEC 5055:2021.

The two measures related to Trustworthiness are Reliability and Security, and they also provide coverage for Resilience and Privacy. Currently ISO 5055 does not provide a measure to cover Safety. However, when the updated ISO 25010 with is published between 2023 and 2025, ISO 5055 will be updated to include a measure for Safety.

[3] ISO/IEC 25023:2016 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality.

[4] ISO/IEC 5055:2021 Information technology — Software measurement — Software quality measurement — Automated source code quality measures.

4 STRUCTURE AND CALCULATION OF ISO 5055 MEASURES

The two measures in ISO 5055 relevant to Trustworthiness, Reliability and Security, are developed from detecting and counting severe weaknesses in software that affect each of these quality characteristics. The international team of software experts sorted through a wide range of software weaknesses and selected the most severe ones for inclusion in ISO 5055 measures.

A weakness was considered severe if the majority of experts developing the measures believed that it had to be removed from the software to avoid damaging business operations or creating excessive IT costs. In the case of Trustworthiness this would be a weakness that, if triggered, would cause the system or device to behave in a way that caused the user to lose trust in its operation.

The measures are developed through static analysis of the software. Static analysis detects non-functional, structural flaws in both the architecture and coding of the software. Severe weaknesses related to the four quality characteristic measures are detected and counted. The base measure for each quality characteristic, such as Reliability or Security, is the total number of occurrences of each weakness included in the quality characteristic.

Occurrence counts of weaknesses can be transformed into normalized measures such as the density of weaknesses per thousand lines of source code or other size measure. Sigma levels can be computed by calculating the number of weaknesses per million parts, where agreement must be established on what constitutes a 'part' (e.g., a line of code, a computational element such as a command or variable reference, etc.).

They can also be transformed into compliance ratios comparing the number of potential occurrences of a weakness to the number of times the weakness was actually detected in the code. Compliance is most often calculated as a ratio comparing the number of times a structure was instantiated in the software system to the number of times one of the instantiations contained a weakness.

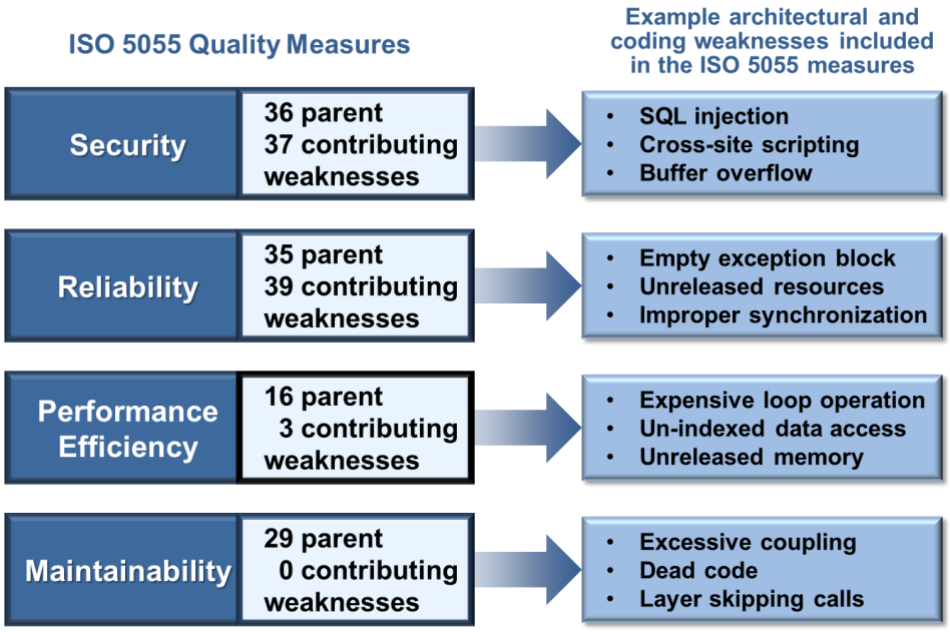

Figure 4-1. ISO 5055 structure and example weaknesses.

The four ISO 5055 measures are constructed from a list of 138 unique weaknesses, as presented in Figure 4-1with several example weaknesses from each measure. All 138 weaknesses are contained in the Common Weakness Enumeration (CWE) repository[5] maintained by MITRE Corp. and have been assigned unique CWE identification numbers. Weaknesses are divided between 92 parent weaknesses and 46 contributing weaknesses. Contributing weaknesses represent various structural patterns through which 13 of the parent weaknesses can be instantiated in source code.

Many weaknesses are included in more than one measure. The two quality characteristics with the most overlapping weaknesses are Reliability and Security with 42 overlaps. This overlap results because many of the weaknesses that will crash systems also provide opportunities for unauthorized access by hackers. For this reason, security cannot be separated from the overall structural quality of a system. The large number of overlaps is due to the large number of contributing weaknesses nested under the overlapping parent weaknesses.

To fully assess Trustworthiness, the search for severe weaknesses must be conducted across the entire stack of software technologies comprising a system, or across the ensemble of devices comprising an Internet of Things (IoT) application. ISO 5055 includes serious flaws at both the architectural and component levels to provide a full evaluation of the factors determining a system's Trustworthiness.

[5] R. A. Martin (2001). Managing vulnerabilities in networked systems. *IEEE Software*, vol. 34, no. 11, pp. 32-38, Nov. 2001. DOI: 10.1109/2.963441. *https://cwe.mitre.org*

For instance, *CWE-424: Improper Protection of Alternate Path* is an architectural weakness that violates Security and Privacy controls by allowing a path from the user interface directly to restricted functionality or resources such as a database without passing through access or user authentication controls. Similarly, *CWE-662: Improper Synchronization* is a Reliability weakness where two or more processes or threads interfere with each other when operating on shared resources causing the system to react in unpredictable ways.

5 USING ISO 5055

ISO/IEC 5055 measures can be used to set measurable targets for sustaining the Trustworthiness of a system of interconnected devices by setting targets for scores on the Reliability and Security measures (and Safety when it is added to the revised ISO 25010). These targets can be written into requests for proposal, statements of work, and contracts as acceptance criteria for software products delivered by system integrators, software vendors, and other third-party suppliers. Incentives can be written into contracts tied to achieving increasingly higher levels of Trustworthiness in delivered products.

Some of the most dangerous Security and Reliability weaknesses contained in ISO 5055 can be marked as 'unacceptable'. If these weaknesses are detected in delivered software, the vendor will be required to remove them at the vendor's expense before the delivery will be accepted. Software should not be put into operation until banned weaknesses have been removed.

ISO 5055 Reliability and Security measures can also be evaluated by internal development teams to establish release criteria and improvement targets. The targets should reflect the amount of risk the organization is willing to tolerate in each of IIC's 5 components of Trustworthiness. The level of risk on each component may vary across systems based on whether they are exposed to customers, contain confidential data, etc. The cost of detecting and repairing weaknesses becomes exponentially larger the closer to zero defects an organization sets a target. Therefore, the executive team must determine the tradeoff between cost and risk when setting measurable Trustworthiness targets.

The risk associated with a single instance of a weakness depends on the context of its position in a software system. In some contexts, a severe weakness can become less onerous, while a less severe weaknesses may become more dangerous. The weaknesses in ISO 5055 measures were selected because they expose systems to substantial operational and cost of ownership risk in most contexts. Nevertheless, the severity of individual weaknesses can be assessed using the Common Weakness Scoring System[6] to help prioritize corrective actions.

[6] MITRE Corp. (2014). Common Weakness Scoring System (CWSS). *https://cwe.mitre.org/cwss/cwss_v1.0.1.html*

ISO standards undergo a systematic review every 5 years. This provides ISO/IEC 5055 an opportunity to update the list of weaknesses in each measure. New classes of severe weaknesses can be added. Empirical evidence from operational and cost of ownership research can cause others to be removed. Thus, ISO/IEC 5055 will be periodically updated as computing technology, languages, and attack patterns evolve.

6 CONCLUSION

ISO 5055 offers an alternative for measuring 4 of the 5 characteristics of Trustworthiness. It will soon provide measures for all 5 characteristics in conjunction with revisions to the quality model in ISO 25010. The relevant measures—Reliability and Security—were developed from detecting and counting severe weaknesses that cause Trustworthiness problems. These measures can be used both with third party suppliers and with internal projects to sustain and improve the Trustworthiness of software systems and interconnected IoT devices.

7 ACKNOWLEDGEMENTS

The views expressed in the IIC Journal of Innovation are the author's views and do not necessarily represent the views of their respective employers nor those of the Industry IoT Consortium®.

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