"Who Watches the Watchmen?": A Critical Analysis of British Standards Concerning Security and Trust in The Cyber Domain

Group 4

19th February 2021

1 BS 10754–1:2018 or: How The British Standards Institution Learned to Stop Worrying and Copy NIST's Homework

The Cybersecurity Framework, published by the US Department of Commerce's (DoC) National Institute of Standards and Technology (NIST), is internationally–recognised as the benchmark standard for cybersecurity policy development. Originally published in 2014, the framework categorises cybersecurity risk management under five broad functions: identify, protect, detect, respond and recover. A revised version, the NIST Cybersecurity Framework 1.1 was published in 2018, shortly after the publication of the Information Technology–Systems Trustworthiness Part 1: Governance and Management Specification document (BS 10754–1:2018) by the British Standards Institution (BSI) in the same year. The following blog post will observe the commonalities between the two documents while critically assessing the risk management approach of BS 01754–1:2018, in the context of the security use case of cyber–physical systems (CPS). For the purpose of this piece, CPS are defined as "smart systems that include engineered interacting networks of physical and computational components", as per the NIST Framework for Cyber–Physical Systems Special Publication (NIST SP 1500–201).

It is important, when discussing any kind of security, to clarify terminology and two core concepts for cybersecurity, trust and composition, are crucial to define for the context of this piece. The sociological definition of trust, which has been widely adopted by the cybersecurity community, is the reliance on an entity to behave as expected, despite its capacity to defy expectations. In the context of this piece, if a system were to behave as expected, only expected kinds of processing would occur. Composition is the primary engineering approach to construct complex systems by composing preexisting components in layered designs. While the properties of individual components may be understood, the same properties of a combined system may be more difficult to ascertain, potentially resulting in unexpected behaviours.

BS 10754–1:2018 categorises risk assessment as "Understanding general risks" (6.3.2) and "Understanding trustworthiness risks" (6.3.3), though one may argue if the two are mutually exclusive in the context of cybersecurity. The first section, "Understanding general risks", outlines steps to assess system composition, which is consistent with the NIST Cybersecurity Framework (ID.RA) and Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (NIST SP 800–53 Rev.

4). To "assess the risk to trustworthiness", identifying and enumerating assets and their respective threats and vulnerabilities, which collectively manifest risks, is asserted as sound methodology. This is consistent with the "Identify" section of the NIST Cybersecurity Framework, specifically subsections ID.AM, ID.R–3 and ID.R–1, respectively. The techniques listed to understand "general risks" may be considered vague and lacking technical specificity, which could infer a lack of stakeholder engagement with the technical community.

The second section, "Understanding trustworthiness risks", outlines a threat intelligence framework to identify threats and vulnerabilities, utilising common security resources such as the Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) databases. While these are important resources for intelligence–gathering, this might be described as a "minimum viable framework" for threat intelligence. Indeed, it omits common intelligence–gathering methods for cybersecurity, such as monitoring activity on threat actor strongholds such as darkweb forums and internet relay chat (IRC) channels. Additionally, in the context of CPS, monitoring and analysing data collected from the Shodan search engine and network telescopes is common. This information is omitted in the document, further indicating a lack of critical stakeholder engagement. Again, all of the proposed steps are consistent with the NIST Cybersecurity Framework (ID.RA–2) and NIST SP 800–53 Rev. 4.

BS 10754–1:2018 categorises risk management as "Controls" (6.4), under the subheadings of personnel (6.4.2), physical (6.4.3), procedural (6.4.4) and technical (6.4.5). It would be impossible to enumerate all of the recommendations in this piece, however several particularly egregious recommendations bear scrutiny. The recommendation for a "single accountable owner of people risk" (PE.03.10) would create a single point of failure, meaning if the owner were compromised, it may impact trust across the entire workforce. The final category, Technical Controls, contains the most problematic content. One example, "Selection of appropriate programming languages, considering known vulnerabilities" (TE.02.10), may be considered an ill–informed statement as most modern programming languages are Turing–complete, meaning they can approximately simulate the computational processes of any other programming language. Other recommendations such as "Select appropriate algorithms" (TE.04.30) and "Integrate and configure components" (TE.07.50) offer no particular insight, which may increase doubt regarding the author(s)' technical knowledge. Recommendations such as removing "unused functions, macros, formats, codes, etc." (TE07.70) and "temporary files / logs" (TE.08.55), and storing source code with an escrow service (TE.11.10) may produce deleterious outcomes, including destroying forensic evidence and recovery data, and increasing attack vectors.

On the balance of evidence, we assert that BS 10754–1:2018 provides little meaningful value over and above the NIST Cybersecurity Framework, of which it appears largely derivative. Its content reflects lack of stakeholder engagement, particularly with the technical community, and although it is intended as a high–level document, its recommendations are generally reductive and lack technical specificity to such a degree that it impacts the document's credibility. As such, we find BS 10754–1:2018 to be inadequate with regards to providing effective recommendations for ensuring the trustworthiness of information and communication technology (ICT) systems, including CPS.

2 Managing The Risks of Composition

In this section, we will critically analyse two risk assessment methods proposed in the Risk Management – Risk Assessment Techniques standard (IEC 31010:2019), published by the International Electrotechnical Commission (IEC) in 2019. We have selected checklists, classifications and taxonomies (B.2.2), and [method], as they are salient to assessing security issues concerning system composition (See **SECTION 1**).

IEC 31010:2019's proposed risk assessment methods concerning checklists, classifications and taxonomies (B.2.2) advocates primarily for the use of checklists, however, we posit that taxonomies are of greater value for effective risk assessment of ICT systems. IEC 31010:2019 characterises taxonomies as "bottom–up" classification schemes that are intended to be mutually exclusive and exhaustive, with the goal to eliminate overlaps. Furthermore, it asserts that risk classifications may focus on isolating risk categories for scrutiny. We dispute the validity of these assertions, given the composite architecture of ICT systems (See **SECTION 1**). Indeed, if individual components are assessed in isolation, with the potential risks of a combined system omitted, we assert that such an approach might lead to deleterious consequences.

We propose cross–layer analysis as a more viable method for establishing risk taxonomies. Widely utilised by both security engineers and threat actors, cross–layer analysis is a empirical approach to risk assessment whereby statistical values of system layers are systematically collated and analysed. A typical analysis might identify and enumerate attack vectors, individual components and their trust relationships, and data flows between layers. By understanding the interactions and relationships between the system's layers at a granular level, mechanisms for unexpected behaviours can be identified and debugged. By doing this, vulnerabilities that might be exploited by threat actors can be patched.

A common theme in IEC 31010:2019's list of risk assessment methods is stakeholder engagement. However, one might argue there is a critical flaw in the approaches enumerated: all proposed stakeholders are good faith actors. A root cause of exploitation may be described as a fundamental disparity between the trust assumptions of a system designer, a user / implementer and a threat actor. To demonstrate the unexpected limits of a system's functionality, thus exposing the true taxonomy of risks, we assert the need for penetration testing by ethical exploit programmers as a crucial risk assessment method for ICT systems.