Breakthroughs in Testing and Certification in Cybersecurity: Research Gaps and Open Problems

Said Daoudagh[1,*], Eda Marchetti[1]

[1]ISTI-CNR, Pisa, Italy

Abstract

Software and hardware systems are becoming increasingly complex and interconnected, making their testing and certification more challenging, considering cybersecurity aspects. The trustworthiness, security, and quality of these systems call for innovative approaches to testing and certifications. This paper provides an overview of some of the most promising research directions in software and hardware testing and certification in the cybersecurity area. It outlines some of the critical challenges and opportunities for future research. We discuss each approach's potential benefits and challenges, highlight some key research questions to be addressed in each area, and investigate how they can be used to promote "Full Quality – positive-sum, not zero-sum" in developing software and hardware systems.

Keywords

Certification, Cybersecurity, Open Problems, Research Gaps, Testing

1. Introduction

Information Technology (IT) is pervasive in both work and social sectors. Homes, industries, offices, cars, streets and public buildings are full of IT devices, systems apps, or electronic equipment. In our daily lives, under normal conditions, we are usually not worried about the technology around us. We are reasonably sure that our mobile phones, PC, refrigerator, electronic device, cars, or even apps, cannot damage our life, steal data, or cause security or safety issues, because they should have been built according to the required standards, properly tested and fully certified.

However, we have recently witnessed various examples of malfunctioning or issues like the following: Tesla had a failure in a flash memory device, causing a safety risk in more than 135,000 vehicles [1]; the New Jersey hospital vaccine scheduling system bug caused 10 to 11 thousand duplicate appointments [2]; the Zoom app suffered from security issues during the coronavirus pandemic in 2020 [3].

As reported in the recent Cybersecurity Act, "Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021" [4].

ITASEC 2023: The Italian Conference on CyberSecurity, May 03–05, 2023, Bari, Italy

*Corresponding author.

said.daoudagh@isti.cnr.it (S. Daoudagh); eda.marchetti@isti.cnr.it (E. Marchetti)

https://saiddao.github.io/ (S. Daoudagh);

https://www.isti.cnr.it/en/about/people/people-detail/223/Eda_Marchetti (E. Marchetti)

0000-0002-3073-6217 (S. Daoudagh); 0000-0003-4223-8036 (E. Marchetti)

Humans and society trust industries and the best practices they adopt in testing and certification processes. However, considering that the overall cost of testing is around 40% of the total development costs of a typical software project [5], if not stringent and without concrete safety risks, often verification, validation and assessment procedures are the first to be reduced or skipped to save cost and time. Additionally, pressure from the need to research new products, the time to market, and competition forces industries and developers towards massive widespread integration and the use of available third-party or open-source components that could surreptitiously increase the cybersecurity risks if not properly tested and certified.

In an IT world that is going to be more human-centric and focused on people's needs (such as the Internet of People (IoP) manifesto [6]), the presence of evidence of the testing and certification activity performed needs to become a common practice. We must increase awareness to avoid "poisoned" IT products as we do for poisoned food. Therefore, the assessed or certified quality level must be a label for each IT product to establish trust and reduce risks to security and privacy.

Thanks to the research activity, experience, and collaborations with several partners involved in the cybersecurity domain during different European and National projects (such as CyberSec4Europe [1], BIECO [2], and NESSoS [3]), we matured the awareness that the quality of digital products (combination of software and hardware) must become a guarantee label, in the same way as the label we find on the food we buy in supermarkets. In this paper, to share our multi-year experience and lesson learned, we go inside some of the main breakthroughs of testing and certification in cybersecurity. In particular, we identify practical research gaps and open problems and depict some challenging near-future research directions. To provide generic baseline knowledge about testing and certification in the context of cybersecurity, we let our analysis be guided by the following General Questions (GQs):

GQ 1: Which is the common perception about testing and certification? In particular, we investigate the impact of the lack of testing and certification processes on the trustworthiness and cybersecurity of products used by ordinary people, companies, organizations, and governments.

GQ 2: Which could be the consequences of a lack of testing and certification activities? In particular, we analyze the damage of an inadequate testing and certification process for IT products and technologies and the possible mitigation strategies.

GQ 3: What could be the worst scenario? We analyze the most famous disasters caused by a lack of testing and certification activity in cybersecurity, and we envision the possible ones.

GQ 4: What are the main research gaps? We explore recent research trends in cybersecurity testing and certification to identify the main gaps to be addressed to ensure the development of trustworthy, secure, and sustainable technology aligned with social and ethical values, inclusiveness, and legal requirements.

[1] CyberSec4Europe: https://cybersec4europe.eu/
[2] BIECO: https://www.bieco.org/
[3] NESSoS: https://cordis.europa.eu/project/id/256980

GQ 5: Which are the pressing research problems? We explore some cutting-edge research directions in software and hardware testing and each approach's potential benefits and challenges.

The reply to the above questions provides a set of research directions for advancing state of the art in software and hardware testing and certification in the cybersecurity domain. Additionally, the paper contributes to improving the general background knowledge and highlighting the challenges and opportunities for strengthening software and hardware systems' trustworthiness, security, and quality.

Outline. The remainder of this paper is organized as follows. Section 2 briefly discusses GQ 1 by providing an overview of who is expected to be affected by changes in cybersecurity testing and certification practices, and Section 3 discusses the potential impact of these changes (GQ 2). In Section 4, we examine GQ 3 and explore potential research gaps (GQ 4) in Section 5, whereas in Section 6, we highlight future research directions (GQ 5). Finally, Section 7 provides concluding remarks and outlines potential future work.

2. Which is the common perception about testing and certification?

The lack of testing and certification processes can affect everyone directly or indirectly using products or technologies. For instance, babies could be damaged by a toy going out of control; Generation Alpha or Zeta could be unconsciously deceived by appealing apps maliciously stealing their pictures; companies can be affected by ransomware hidden in useful plug-ins or libraries; organisations and governments can be subjected to cybersecurity attacks. Of course, testing and certification are not the only means of avoiding such critical situations. Everything has to be executed correctly at every phase of the development process. Significant progress has been made in the field of software system security since its early stages [7]. As evidenced by the several national and European initiatives and call-for-proposals (such as those belonging to the Cluster 3 Work Programme 2023 - 2024, for instance, and, in particular, the Increased cybersecurity), it is recognised the urgent necessity to respond to the challenges related to the increasing persistent security threats to fight with proper (digital) weapons against the cybercrime and the natural and artificial disasters, as well. Reliable techniques, tools and methodologies for conducting advanced analysis and verification, as well as dynamic testing of hardware and software components that may be vulnerable or insecure, necessitate the implementation of best practices for cybersecurity issues. Hence, it is crucial to focus on software development tools, IT security metrics, and guidelines to ensure the security of products and services throughout their entire lifecycle [4]. So far, various initiatives and frameworks have been developed to face those issues, such as NIST's Secure Software Development Framework [8], OWASP's Software Assurance Maturity Model [9], Microsoft's SDL [10], ETSI's standard 303 645 [11], and the Cybersecurity Body of Knowledge [12] [7].

[4]More information can be found at the following link: https://digital-strategy.ec.europa.eu/en/policies

However, conceiving and developing (by-design) quality products is crucial but insufficient per se to meet the final requirements: building the product right does not guarantee building the right product [13]. Testing and certification remain pivotal for trustworthiness and cybersecurity assurance and for guaranteeing that a product is designed and manufactured with quality as a primary objective. Therefore, as long as stakeholders (ordinary people, companies, organisations, and governments) do not firmly demand transparent, labelled, tested and certified products, the situation will hardly change, and cybersecurity risks will remain on the agenda.

3. Which could be the consequences of a lack of testing and certification activities?

What is the expected damage without an adequate testing and certification process? Unfortunately, there are many aspects to be considered:

Hardware/software failure: It has been estimated that nearly 80% of unexpected downtime can be ascribed to HW/SW failures and power outages. Proper storage backups can be an ad hoc solution in most cases, but preventing failure would be less costly and risky.

Natural disasters and emergencies: Lack of testing and certification of the processes and procedures for resuming operations/data and systems in case of (natural) disaster or emergencies can be extremely costly and cause the loss of business continuity.

Human factor: Even not intentionally, humans may inevitably cause mistakes or execution of unexpected procedures. Testing based on user profiles or exploiting machine learning approaches could avoid or predict possible misbehaviour or accidental situations. User-centred assessment processes and training programmes could be essential for minimising human damage and avoiding permanent losses.

Cybersecurity attack: Because society and organisations increasingly rely on digital information for daily operations, cybersecurity attacks can be more dangerous. Currently, 95% of companies invest in testing and certification activities only after a disaster and then actuate a recovery plan (reactive behaviour). Predicting vulnerabilities and providing solutions before a cybersecurity attack is mandatory (proactive behaviour). The penetration test is pivotal for avoiding and anticipating cyberattacks by hackers who are trying to exploit potential vulnerabilities to access company networks and steal confidential data or inject malicious codes.

High expectations: In our hyper-connected world, where IT products need to be available 24h7d without disruptions, failures and loss of services are costly disasters for companies and favour their competitors. Therefore, robust testing and certification processes, which can assure the quality of services and make it possible to establish a suitable recovery plan, are pivotal activities.

Trust or reputation damage: Loss of trust or damage to a reputation is mostly translated into a loss of customers, and hence a loss of revenue: trust and reputation are nearly

impossible to regain. Testing and certification are among the most effective means of avoiding this problem.

Compliance requirements: Nowadays, business continuity is not just a mere desire: it is becoming a requirement, especially for Operators of Essential Services (OESs) [14]. All of them must follow specific and strict regulations and standards. That means that adopting certification processes and maintaining their product certification is becoming a legal obligation and offers a competitive advantage within the reference market.

4. What could be the worst scenario?

Figuring out what could happen without testing and certification should not point to the future but simply to the past. Most worst-case scenarios have already been covered in the newspapers, the default reports and disaster documentation. The worst-case bugs history started as soon as the first computer was massively used and included:

- **The Ariane 5 Disaster**, 4th June, 1996. During the launch of the Ariane 5 spacecraft, 37 seconds after the first rocket ignited, it started flipping in the wrong direction, and less than two seconds later, the whole world observed its self-destruction. The problem was quickly identified as a software bug in the rocket's inertial reference system and, unfortunately, could have been easily solved with a trivial integration testing procedure [15].
- **The Mars Climate Orbiter**, 23rd September, 1999. During its descent into the Martian atmosphere, the Mars Climate Orbiter was reoriented to pass behind Mars and successfully enter its orbit. Unfortunately, this did not happen: the craft was not on the correct trajectory and was finally lost without a trace. The root cause analysis of this error yielded a long chain of wrong or unexpected events, which included: the incidental arrangement of solar panels on the craft due to the solar sail effect; the use of two different units in the Ground Control software (data provided using imperial units and pound-seconds on the sender side but expected in metric units on the receiver side); and finally, human errors in communications. Again, proper integration testing procedures and correct use of standards and assessment procedures would have avoided such a critical disaster [16].
- **Therac-25**. During the period from 1992 to 1998, reports about radiation overdoses caused by the 80's computer-controlled radiation therapy were published. In particular, six documented accidents occurred, resulting in deaths or severe injuries. The causes were identified as personnel's application of incorrect procedures and the weaknesses of the software used for assuring safety. In particular, all accidents involving software resulted from flawed software requirements. Application of certification processes and a proper system and acceptance testing process would have again avoided significant loss of life [17].
- **Knight Capital Group**. On 1st August 2012, during a software update of the production server, an incorrect configuration of an old (2003) system caused 97 email notifications and the execution of 4 million unexpected trades. That led to a $460 million loss and the risk of bankruptcy. The post-analysis highlighted that the program believed it was in a test

environment and executed trades as quickly as possible without worrying about losing the spread value. As in the previous cases, the testing process would have discovered that misbehaviour and avoided using obsoleted, not aligned software [18].

Past mistakes have likely been resolved, and lessons learnt, but challenges, vulnerabilities and new scenarios are constantly emerging. Who does not remember the Millennium bug [19]? Or the 2018 cyberattack that interrupted communications on the Midcontinent Independent System Operator? Or even the six/seven hours of the global unavailability of the social network Facebook and its subsidiaries in October 2021 [20]? Or the recent ransomware attacks on the IT network?

The smart and quick discovery and provision of new technologies, programming languages and systems obliges testing and certification to continuously jump **"Back to the Future"** and provide new means, strategies and processes to prevent future worst-case scenarios. Indeed, history teaches that the past can always turn into the future and *vice-versa*.

What is the worst that can happen? A life without testing and certification means lacking quality, efficiency and trust in every system and software package.

Indeed, testing and certification seek to mitigate the risks of safety, security and privacy loss or absence for anyone worldwide. Who would use a machine without it being tested? Who would be willing to set up a medical facility without being certified? Who could think to give a child toys that put their life at risk?

Unsafe, not secure or not trustable HW or SW products, elements, components, and libraries make the world dangerous: they can cause environmental disasters; they can play a role in the default or bankruptcy of companies, industries and even nations; they can impact essential services [14] (e.g., energy, transport, financial and banking, healthcare, drinking water supply & distribution, and digital infrastructures); they can compromise health systems or medical devices. The current international situation can also paint even more dramatic scenarios: HW/SW vulnerabilities and security threats could be exploited to allow terrorist attacks on nuclear power plants and military bases.

Luckily, in this catastrophic apocalyptic scenario, learning from the past and focusing on the future, research and industry are starting to understand the importance of strict collaboration in testing and certification to prevent disasters before they happen effectively.

5. What are the main research gaps?

Considering that "Program testing can be used to show the presence of bugs, but never to show their absence. (Dijkstra)" [21], exhaustive testing is usually impossible, and issues and problems in testing and certification are far from being exhausted. New challenges are continuously added in parallel with developing new technologies, features, languages, and application domains and discovering new vulnerabilities and threats. In particular, the following areas are recent trends in research activities, presented without any specific priority order.

5.1. Human-centred testing and certification

Supporting human-centred testing and certification approaches can guide, improve and assess technological development in line with social and ethical values, sustainability and trustworthiness. Additionally, increasing inclusiveness by supporting the gender and diversity balance of different stakeholders involved in the testing and certification approach can ensure trustworthy public awareness, the broad adoption of IT methods, and the adoption of standards to increase transparency and openness [22].

5.2. Integrated cybersecurity and functional safety certification

Besides interleaving and overlapping several aspects of cybersecurity and safety, a gap exists in providing a comprehensive framework and technical standards for their full integration. Indeed, safety assurance/certification cannot be achieved without considering the impact of cybersecurity vulnerabilities and threats on the system [23]. Thus, there is a need to provide a functional safety/cybersecurity assurance risk-based integrated approach [24].

5.3. Quantitative and qualitative testing and certification

Accountability and replicability are essential characteristics of cybersecurity modelling, testing and certification approaches and require methods and means for quantitative and qualitative collection and the analysis of results and data. Thus, the availability of open-source data sets and conformance test suites as the facilities for the setting up and execution of controlled experiments should be improved [25, 26]. In particular, challenges focus on the following:

1. Improving formal methods for quantitative security modelling and analysis and their application to risk management, enriching their data-driven aspects, e.g., synthesising and refining models from (possibly underspecified) attack scenarios and validating them concerning data from previous attacks.
2. Realisation of modelling, testing, and certification approaches driven by cybersecurity risks.
3. Making data collection, quantification approaches/tools, and result analysis more accessible to practitioners and open-access communities.
4. Improving the efficacy and efficiency of the testing and certification processes, making them more focused on qualitative properties.
5. Making testing and certification by design, guided by user stories, domain-specific needs requirements, and standards.
6. Providing metrics, guidelines, and approaches for securing products and services throughout their lifetime.

5.4. Automation of testing and certification

Testing and certification are complex, costly and time-consuming activities. Reducing the effort and mitigating the cybersecurity cost and risk is a significant challenge for attainable automation [27]. Important directions are:

1. Developing advanced techniques, finding innovative support procedures to (fully) automate the different activities, or providing metrics, guidelines and approaches applicable throughout the overall process lifetime.
2. Providing a holistic methodology that integrates runtime and design-time methods applicable at different specification levels—such as firmware, communication protocols, stacks, operating systems (OSs), and application programming interfaces (APIs)—and that considers the integration of software and hardware.
3. Specifying and developing manageable and human-centric KPIs, metrics, procedures, and tools for dynamic and automatic cybersecurity certification from chip to software and service levels.

5.5. Diversity, heterogeneity and flexibility of environments

Diversity, heterogeneity, and flexibility are challenging for testing and certification proposals. In particular, any approaches and solutions provided should move according to vertical and horizontal research levels. Indeed, ecosystems and systems of systems (SoSs) rely on the continuous integration of components, apps, and devices developed using different languages and operating systems and on combining and accessing thousands of device-browser-platform combinations simultaneously. To avoid the risk of becoming outdated, testing and certification need highly flexible and modular schemes that rapidly adapt to the changes and updates of the technological environment and elements at each horizontal or vertical level. Additionally, to follow the rapid and pervasive evolution of the different supply chain environments [28] (such as the Critical Infrastructures (CIs) [5]), and new technologies [29, 30, 31, 32] (such as the metaverses [6]), holistic, modular proposals are necessary, able to effectively and efficiently validate, verify and certify the different HW/SW elements under real user conditions and considering other interacting systems and application domains.

5.6. Including legal aspects inside testing and certification

The interplay between HW and SW elements in current systems promotes a new direction for cybersecurity testing and certification research: to include legal aspects in the verification, validation and assessment procedures [33]. The legal framework and technical standards must be considered necessary parameters during the development life cycle (for more details, we refer to [34]). Indeed, cybersecurity vulnerabilities may cause legal violations, especially in sensitive applications such as healthcare. The future direction is to ensure that cybersecurity, safety and legal requirements are tested and certified as inseparable aspects of the same process [34].

[5] Critical Infrastructures (CIs) are defined as essential large-scale systems or Systems of Systems (SoSs) that are crucial for the proper functioning of critical societal functions and the well-being of individuals, as stated by the relevant European Council Directive [28].

[6] The World Economic Forum [29], the Metaverses Standards Forum [30], the Open Metaverses Interoperability Group [31], and the Metaverses Interoperability Community Group at the W3C [32] are examples of metaverses initiatives and actions.

6. Which are the pressing research problems?

As the complexity and interconnectedness of software and hardware systems continue to grow, testing these systems effectively is becoming more challenging. To ensure the reliability, security, and quality of these systems, we advance to exploring innovative approaches to testing, from leveraging AI/ML/DL to gamification and crowd-sourced testing. In this section, we explore some of the cutting-edge research directions in software and hardware testing and the potential benefits and challenges of each approach.

Testing the unknown. SoSs continuously integrate various new devices and components; some of them could be untested and any intrinsic flaws will be inherited. The research should pave the way to new testing paradigms to achieve self-adaptive testing methodologies aiming at ensuring that unknown and untested components and devices are trustable and have good quality before they join the SoS. In other words, this research should promote "Full Quality – positive-sum, not zero-sum." [7]

Testing of AI/ML/DL. Provide testing methodologies and tools that can be suitable for revealing bugs in artificial intelligence (AI), machine learning (ML) or deep learning (DL) applications. The study should consider the following three main aspects: (1) the required conditions (correctness, robustness, security and privacy); (2) the AI, ML or DL items (e.g., the data, the learning program, or the framework used); and (3) the involved testing activities (test case generation, test oracle identification and definition, and test case adequacy criteria).

Using AI/ML/DL for testing. Provide AI/ML/DL-based methodologies and tools that can help perform most testing tasks, such as test-case generation, test-case classification, oracle derivation or mutation analysis, to cite a few. Therefore, this research aims to leverage state-of-the-art AI/ML/DL technologies to aid software and hardware testers in achieving the desired quality driven by testing data.

Understanding the testability of the metaverse. Improve the understanding of the challenges of testing the metaverse by considering three testing pillars: cybersecurity, aimed at security testing; API testing, crucial for guaranteeing interoperability, which is a fundamental characteristic of the meta experience; and interactive and immersive testing, which puts the human at the core of testing meta experiences.

We are all testers. Improve the understanding of the role of humans in the testing process. The research should provide theories, insights, and practical solutions for engaging people in the testing and assessment of digital products and services, considering different dimensions of (digital) ethnography. The starting point for this kind of research should be gamification, which aims to convert testing tasks to gameplay components, and crowd-sourced testing (also known as crowdtesting), which is an emerging approach for involving users and experts in testing activities.

[7] This term is inspired by the well-known privacy by design principle "Full functionality: positive-sum, not zero-sum" [35].

7. Conclusion and Future Work

In this paper, we summarized our research activity, experience, and awareness about testing and certification in cybersecurity matured during multi-year collaboration in different European and National projects. Focusing on complex and interconnected systems, we discussed the limitations of available approaches and highlighted innovative opportunities to improve modern software and hardware systems' trustworthiness, security, and quality. Guided by five general questions, we identified practical research gaps and open problems and depicted some challenging near-future directions. In particular, we presented several cutting-edge research directions, including testing the unknown, testing AI/ML/DL applications, using AI/ML/DL for testing, understanding the testability of the metaverse, and involving humans in the testing process. We discussed each approach's potential benefits and challenges and provided tangible examples of problems to motivate future research in these areas.

The analysis provided in this work highlighted that testing and certification still have an essential role in industries, companies, society, and individuals. The paper aimed to provide valuable insights and guidance for researchers and practitioners in software and hardware testing and certification and inspire further research in the areas.

The evidence collected in this paper evidence that complex and interconnected software and hardware systems still look for effective and efficient cybersecurity approaches and solutions for their testing and certification. Thus the analysis presented is a starting point for this future, and other open research questions can be conceived and addressed.

In our future work, we will exploit the lesson learned in this paper to investigate open new research directions. Thus our research activity will be devoted to improving the investigation of testing the unknown, i.e., new testing paradigms that can ensure the trustability and quality of unknown and untested components and devices. Similarly, in the area of testing AI/ML/DL applications, further work will be devoted to different paths, such as: i) analyze testing and certification methodologies and tools that can reveal bugs and ensure the correctness, robustness, security, and privacy of these applications; ii) investigate how AI/ML/DL can aid testing and certification activity to achieve the desired quality using testing data.

Additionally, in the emerging domain of the metaverse, further research will be devoted to analyzing specific cybersecurity challenges. Finally, in involving humans in the testing process, future work will be dedicated to emerging theories, insights, and practical solutions (such as gamification and crowd-sourced testing) for engaging people in the testing and certification of digital products and services.

Acknowledgments

This work was partially supported by the project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU, by the European pilot CyberSec4Europe H2020 Grant Agreement No. 830929 (https://cybersec4europe.eu/), and by BIECO H2020 Grant Agreement No. 952702 (www.bieco.org).

References

[1] National Highway Traffic Safety Administration, Part 573 safety recall report, https://static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V035-4682.PDF, 2021. [Accessed: 21 February 2023].

[2] J. Drees, Software bug in new jersey hospital's vaccine scheduling system causes thousands of duplicate appointments, https://www.beckershospitalreview.com/healthcare-information-technology/software-bug-in-new-jersey-hospital-thousands-of-duplicate-appointments.html, 2021. [Accessed: 02nd May 2023].

[3] 8 Zoom Security Issues You Need to Know About, 8 zoom security issues you need to know about, https://www.sigmundsoftware.com/blog/zoom-security-issues-coronavirus/, 2020. [Accessed: 21 February 2023].

[4] European Commission, Cyber resilience act, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act, 2022. [Accessed: 15 January 2023].

[5] V. Garousi, A. Rainer, P. Lauvås, A. Arcuri, Software-testing education: A systematic literature mapping, Journal of Systems and Software 165 (2020) 110570. URL: https://www.sciencedirect.com/science/article/pii/S0164121220300510. doi:https://doi.org/10.1016/j.jss.2020.110570.

[6] J. Miranda, N. Mäkitalo, J. Garcia-Alonso, J. Berrocal, T. Mikkonen, C. Canal, J. M. Murillo, From the internet of things to the internet of people, IEEE Internet Computing 19 (2015) 40–47. doi:10.1109/MIC.2015.24.

[7] G. McGraw, Software Security: Building Security In, Addison-Wesley Professional, 2006. doi:10.1109/ISSRE.2006.43.

[8] NIST, Secure software development framework, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf, 2018. [Accessed: 07 November 2022].

[9] O. SAMM, Software assurance maturity model, https://owaspsamm.org/model/, 2022. [Accessed: 07 November 2022].

[10] Microsoft, Microsoft sdl, https://www.microsoft.com/en-us/securityengineering/sdl/practices, 2016. [Accessed: 28 April 2023].

[11] ETSI, Etsi en 303 645, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf, 2020. [Accessed: 27 April 2022].

[12] CyBOK, The cyber security body of knowledge, https://www.cybok.org, 2021. [Accessed: 28 April 2022].

[13] I. Sommerville, Software engineering 10, Harlow: Pearson Education Limited (2016).

[14] E. Commission, Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union (NIS), https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 2016. [Accessed: 22 February 2023].

[15] E. Weyuker, Testing component-based software: a cautionary tale, IEEE Software 15 (1998) 54–59. doi:10.1109/52.714817.

[16] A. Harish, When nasa lost a spacecraft due to a metric math mistake, https://www.simscale.com/blog/nasa-mars-climate-orbiter-metric/, 2022. [Accessed: 21 February 2023].

[17] N. G. Leveson, The therac-25: 30 years later, Computer 50 (2017) 8–11. doi:10.1109/MC.

2017.4041349.

[18] N. Popper, Knight capital says trading glitch cost it $ 440 million, https://archive.nytimes.com/dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/, 2019. [Accessed: 21 February 2023].

[19] Year 2000 problem, Year 2000 problem, https://en.wikipedia.org/wiki/Year_2000_problem, 2023. [Accessed: 28 April 2023].

[20] J. Taylor, Facebook outage: what went wrong and why did it take so long to fix after social platform went down?, https://www.theguardian.com/technology/2021/oct/05/facebook-outage-what-went-wrong-and-why-did-it-take-so-long-to-fix, 2021. [Accessed: 19 April 2023].

[21] E. W. Dijkstra, et al., Notes on structured programming, Section 3 On The Reliability of Mechanisms, corollary at the end (1970).

[22] O.-M. Latvala, M. Cheminod, S. Pape, W. B. Tesfay, M. Beckerle, S. Fischer-Hübner, D. Preuveneers, A. Hassan, L. Pasquale, B. Kežmah, M. Kompara, J. G. Rodríguez, R. T. Moreno, C. Martinie, D3.16: Security requirements and risks conceptualization, https://cybersec4europe.eu/wp-content/uploads/2022/01/D3.16-Security-requirements-and-risks-conceptualization-v1.0_submitted.pdf, 2021. [Accessed: 24 April 2023].

[23] E. Fosch-Villaronga, T. Mahler, Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots, Computer Law & Security Review 41 (2021) 105528. URL: https://www.sciencedirect.com/science/article/pii/S0267364921000017. doi:https://doi.org/10.1016/j.clsr.2021.105528.

[24] D. Chastain-Knight, S. Dharmavaram, P. N. Lodal, Integrating cybersecurity into the risk-based process safety (rbps) program, Process Safety Progress 41 (2022) 721–727. URL: https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.12403. doi:https://doi.org/10.1002/prs.12403.

[25] R. Leszczyna, Choosing the right cybersecurity solution: A review of selection and evaluation criteria, ETHICOMP 2022 (2022) 418.

[26] M. M. Yamin, B. Katt, Modeling and executing cyber security exercise scenarios in cyber ranges, Computers & Security 116 (2022) 102635.

[27] E. Cioroaica, S. Daoudagh, E. Marchetti, Predictive simulation for building trust within service-based ecosystems, in: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom 2022 Workshops, Pisa, Italy, March 21-25, 2022, IEEE, 2022, pp. 34–37. URL: https://doi.org/10.1109/PerComWorkshops53856.2022.9767457. doi:10.1109/PerComWorkshops53856.2022.9767457.

[28] C. Directive, Council directive 2008/114/ec of 8 december 2008–on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union. L 345 (2008) 75–82.

[29] T. W. E. Forum, Defining and Building the Metaverse, Technical Report, weforum.org, 2022. [Accessed: 09 January 2023].

[30] metaverse standards.org, The Metaverse Standards Forum, Technical Report, metaverse-standards.org, 2022. [Accessed: 09 January 2023].

[31] OMIGroup, Open Metaverse Interoperability Group, Technical Report, OMI Group, 2022. [Accessed: 09 January 2023].
[32] W. C. D. Team, METAVERSE INTEROPERABILITY COMMUNITY GROUP, Technical Report, w3c.org, 2022. [Accessed: 09 January 2023].
[33] S. Daoudagh, E. Marchetti, The GDPR compliance and access control systems: Challenges and research opportunities, in: P. Mori, G. Lenzini, S. Furnell (Eds.), Proceedings of the 8th International Conference on Information Systems Security and Privacy, ICISSP 2022, Online Streaming, February 9-11, 2022, SCITEPRESS, 2022, pp. 571–578. URL: https://doi.org/10.5220/0010912300003120. doi:10.5220/0010912300003120.
[34] Versen, Manifesto on software research and education in the netherlands, https://www.versen.nl/assets/manifesto/digitalfolder.pdf, 2020. [Accessed: 21 February 2023].
[35] A. Cavoukian, et al., Privacy by design: The 7 foundational principles, Information and privacy commissioner of Ontario, Canada 5 (2009) 2009.