

A methodology to derive security specifications for complex electronic systems

Sylvain Guilley*, Senior Member IEEE, Ritu Ranjan Shrivastwa*, Ville Yli-Mäyry*

* Secure-IC, a Cadence Company.

Abstract—Modern electronic systems are becoming increasingly complex and must satisfy demanding performance, power, and area (PPA) constraints. Consider for instance artificial intelligence chips, aiming at datacenters running LLMs or at automotive perception, which manipulate massive data streams. Beyond performance considerations, these systems must also provide increasingly strong security and dependability guarantees. Indeed, when electronic systems are based on chiplets, for instance, the supply chain gets longer and therefore brings a larger number of threats. Also, those systems are very versatile, in that they can run varied multi-tenant applications. Therefore, defining what security features are required in this context with numerous stakes is not trivial.

Existing scholarly research is very relevant when the security problem is well defined. The resulting scientific papers accordingly dig very deep: this *modus operandi* has proved productive in exploring new problems, and actually allowed to come up with innovative solutions. For instance, in the field of side-channel attacks, varied mitigations alongside with metrics to evaluate them have been devised. Increasing sophistication resulted from this research, as external considerations have been injected into the problem (typically, aspects such as attack order, impact of combinatorial glitches, etc.). Therefore, we face today the question of selecting the most suitable technology amongst the proliferation of state-of-the-art techniques.

In addition, in complex systems, we encounter another problem, namely that of defining the security problem(s). A fruitful approach in this respect is a risk based approach. Specifically, the application of a risk-oriented methodology allows to reason on the security rationale. It proceeds as follows. First, the system missions are listed. Then for each of them, the necessary assets are deduced. A threat analysis allows to identify how assets are threatened, and eventually, security requirements can be enunciated. At this stage, the task of matching relevant countermeasures becomes straightforward.

This paper illustrates the methodology by deriving security specifications for datacenter and automotive chiplets. The considered missions are (secure) provisioning, trimming, debugging, booting, and remote attestation.

Keywords—Risk analysis; Embedded Cybersecurity; AI-assisted security problem analysis; Cybersecurity requirements management; Maintenance of specifications.

I. INTRODUCTION

A. Increased complexity of electronic systems

Modern chips are empowered to manage always more sophisticated tasks. In particular, the management of artificial intelligence (AI) requires dealing with large workloads. Indeed, inference requires to pass each input through evolved models, hence a large number of processing operations per incoming data.

One way to measure the complexity is the so-called performance-power-area (PPA) metric. Performance is to be set high when the data rate is high. Of course, this comes at a price, in terms of implementation size. Indeed, performance

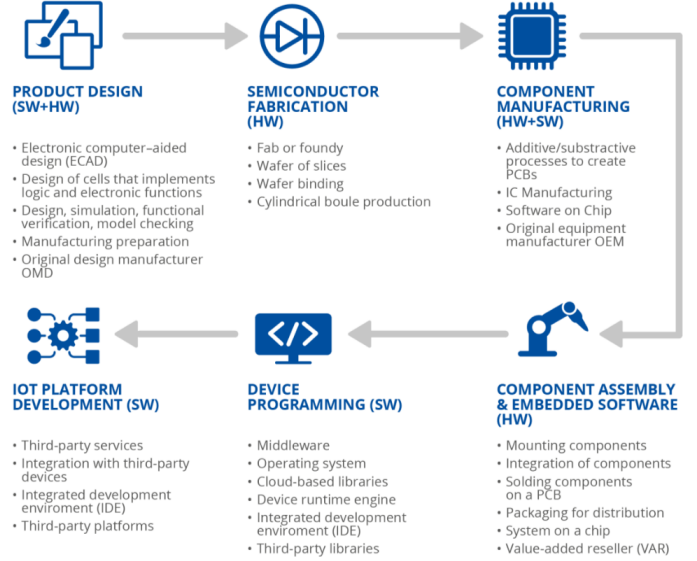


Figure 1: Mapping of the IoT supply chain (courtesy of [12, Fig. 2]).

can be obtained by turning sequential processing into pipelined ones. Pipelines can be seen as unrolling loops, hence an area that scales according to the number of iterations. Also, further performance can be obtained by the replication of some operators. Correlatively, the larger the area, the larger the power consumption.

Today's growth in silicon chips economy is driven by AI applications. They might concern markets such as datacenter or automotive. Datacenters are power hungry in compute, and must absorb massive input data. Automotive chips are fed by real-time data related to perception (cameras, radars, lidars, etc.), and shall derive from them a relevant navigation. One additional requirement for automotive systems (i.e., cars) is that inference shall happen real-time, as it is used for decision making regarding the car's actions.

B. Dangers applicable to chips

The semiconductor supply chain is long, global, and highly specialized (see Fig. 1). A modern chip may involve design in one country, IP blocks from several vendors, fabrication in another country, packaging elsewhere, and deployment worldwide. Security risks can therefore arise at many stages.

At design-time, an attacker can insert additional logic (hardware Trojan into a chip design) that remains dormant until a specific trigger occurs. Also third-party IPs (3PIP) represent risks. Indeed, modern SoCs may contain hundreds of reusable IP blocks, such as: cryptographic accelerators, CPUs,

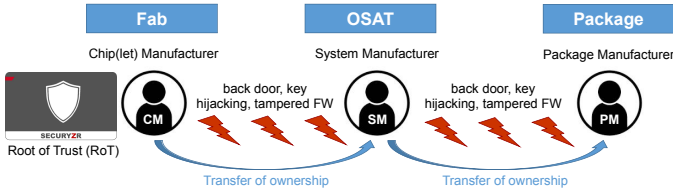


Figure 2: Chain of custody for chiplets and possible attacks.

memory controllers, and bus / interconnect networks. Risks typically include hidden backdoors, vulnerabilities in security protocols, insufficient isolation between security domains, and counterfeit IP with modified functionality. Additionally, the design flow depends heavily on Electronic Design Automation (EDA) tools. EDA tools themselves may also introduce similar threats. Further down the supply chain, the fabrication can also be hijacked, because foundries are not necessarily trusted. The Outsourced Semiconductor Assembly and Test (OSAT) actors can also disrupt the product. Indeed, production testing requires privileged access; hence an untrusted test site (which may be separate from the foundry) can exploit scan chains, JTAG interfaces, debug ports, and manufacturing test modes. Upon packaging and assembly, threats include chip substitution, counterfeit dies, package re-marking, and interposer modification (especially in advanced 2.5D/3D packaging [19]). For multi-chiplet systems, establishing trust becomes more complex because multiple dies may originate from different suppliers.

For example, the supply chain risks for chiplets is illustrated in Fig. 2. This chain involves at least one transfer of ownership. The trust is built from the silicon, leveraging a RoT – ownership is transferred along the chain of custody. This is typically described in OCP FCSA [4] and in the system-in-package Protection Profile [30].

C. Dependability of electronic systems

Now, modern systems increasingly derive their functionality, security, and reliability from integrated circuits. If the chips fail, are unavailable, or are compromised, the entire mission may fail. One problem is that chips concentrate critical elements; critical missions often depend on a small number of highly specialized components, hence the danger of single points of failures (SPOFs). This is all the more sensitive as:

- There is a supply-chain dependence: many critical systems rely on chips produced by a limited number of manufacturers.
- Critical systems often remain operational for decades; By contrast, semiconductor products may become obsolete within a few years.
- Modern chips are no longer isolated; As a result, the compromise of a chip can propagate through an entire system-of-systems architecture.
- Many mission-critical properties are directly tied to semiconductor technology. Small manufacturing changes can affect security.
- Foreign ownership, control, or influence (FOCI) risk is a critical factor, as it involves assessing the extent to which

foreign interests can control or influence a company and its supply chains.

II. STATE OF THE ART OF PROTECTION TECHNOLOGIES

The adequate selection of protections is important to strike a good balance between cost and security. Some frameworks exist, but at very early stages, such as MITRE EMB3D™ Threat Model [15], [23], and the very recent extension thereof called MITRE ESTM™ [21], [22]. MITRE EMB3D™ provides a cultivated knowledge base of cyber threats to embedded devices, providing a common understanding of these threats with security mechanisms to mitigate them. MITE ESTM™ provides a purpose-built framework to address embedded system vulnerabilities by offering a structured approach to analyzing and understanding potential adversarial behaviors targeting these systems. Although the ESTM does not currently offer specific mitigation guidance, it provides a common language and framework for cybersecurity professionals to analyze attacks, understand potential vulnerabilities, and collaborate on more effective defense strategies.

In this respect, the “security specification” activity is strategic. The specifications are sorted by types: functional, defense-in-depth, and normative. The three levels correspond to voluntary SFR, SAR, and mandated SFR & SAR. The SFRs (Security Functional Requirements [5]) consist in defining the protections to be instantiated. The SARs (Security Assurance Requirements [6]) further expresses the number of deployed protections, and the way they are piled up, to ensure security even in case of partially successful penetration. Eventually, the mandated SFR & SAR account for good practices that are imposed in order to enable a “checkbox” approach. The end result is a comprehensive security specification that encompasses all the aspects of cybersecurity.

A. Characterization of the existing protection techniques

We illustrate the panorama of protections against one threat: side-channel attacks. There are many possible derivations (the book [20] dates back from 2006 and lists only few of them), that unfortunately cannot be homogeneously compared. This intricate situation is exemplified in the rest of this section.

1) *Existing solutions:* At the chip level, protections against side-channel attacks are usually classified according to how they reduce the correlation between secret data and physical leakage (power consumption, EM emissions, timing, etc.). There is a proliferation of countermeasures, that can fall into the major categories listed below.

a) *Power Line Filtering:* includes those techniques:

- On-chip decoupling capacitors smooth current fluctuations;
- Integrated voltage regulators reduce correlation between internal activity and external power measurements;
- Power distribution network dense design minimizes observable switching signatures.

b) *Constant-Power Logic:* Special logic families attempt to make power consumption independent of processed data:

- Dual-Rail Precharge Logic [14];
- Wave Dynamic Differential Logic [32];
- Sense Amplifier Based Logic [31].

These balance switching activity so that every operation consumes approximately the same energy.

c) *Noise Generation*: Those heuristics consist of:

- Dedicated noise generators inject random current variations;
- Dummy circuits perform unrelated computations;
- Random clock modulation increases measurement difficulty.

2) *Multiple assessment methods*: On top of the great multiplicity of approaches to fight side-channel leakage, there are also multiple ways to appreciate the leakage. It happens that one finds an heterogeneous characterization situation.

One important aspect about countermeasures is to be able to compare them ideally apples-to-apples. The problem is that such a framework is unrealistic.

Let us give a partial overview of metrics:

a) *Leakage detection metrics*:

- Leakage detection metrics, such as Test Vector Leakage Assessment (TVLA), very easy to implement, but require collecting 2 datasets (e.g., fixed vs random key);
- χ^2 tests, Kolmogorov–Smirnov tests or Mutual Information (MI), are generalizations.

b) *Distinguishing metrics*:

- Signal-to-Noise Ratio (SNR [20, § 4.3.2, page 73]) and
- NICV (Normalized Inter-Class Variance [3]).

c) *Attack success metrics*: Those are typically the Success Rate (SR) or the Guessing Entropy (GE) [2].

d) *New trends*: Machine-learning metrics are getting increasingly important to analyze large datasets consisting of protected leakage traces. The typical metrics consist in classification accuracy, cross entropy, validation loss, top- k accuracy, guessing entropy, or success rate.

All in one, a designer is overwhelmed with the variety of countermeasures against side-channel attacks, and is also confused by the equally large variety of criteria of selection. The root cause of this unsatisfactory situation is the lack of systemic risk analysis.

B. Missing systemic approach

Mapping protections to risks is a classic risk-treatment or assurance-case exercise. In semiconductor security, the goal is to show that every identified threat is mitigated by one or more controls, and that every control can be justified by a threat.

Though, a common mistake is to start from available protections (“we use secure boot, encryption, PUFs, ...”) rather than from risks. The better approach is:

Asset → Threat → Risk → Protection → Residual Risk .

It is illustrated in greater details in Fig. 3. The question is: “Which techniques to use for what purpose?”

1) *Example of Post-Quantum Cryptography (PQC)*: The PQC ecosystem is very large, especially in terms of algorithms. Hence the need for an educated methodology to plan for the PQC strategy.

We give here-after in Fig. 4 an example of a PQC algorithms decision diagram. Use LMS or XMSS with SHA2 because CNSA 2.0 [25] does not recommend SHA3 for general purpose hashing. Thus SHA3 is only for use with lattice-based cryptography. Still, NIST SP 800-208 allows XMSS and LMS with either SHA-256 or SHAKE256 (SHA3 based) with 192- of 256-bit outputs.

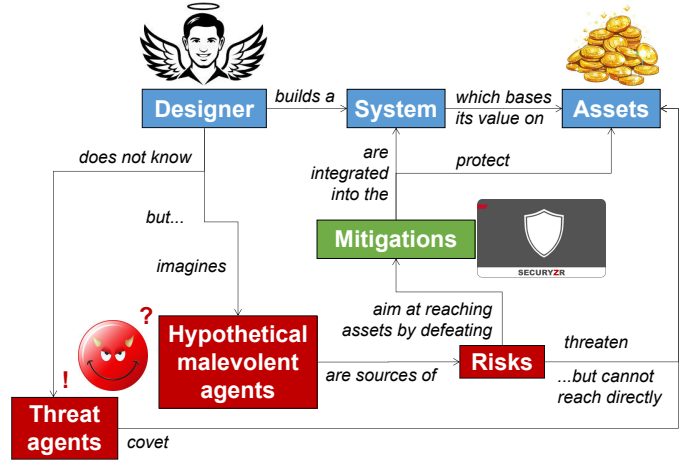


Figure 3: Risk analysis concept and application of mitigations as risk treatment.

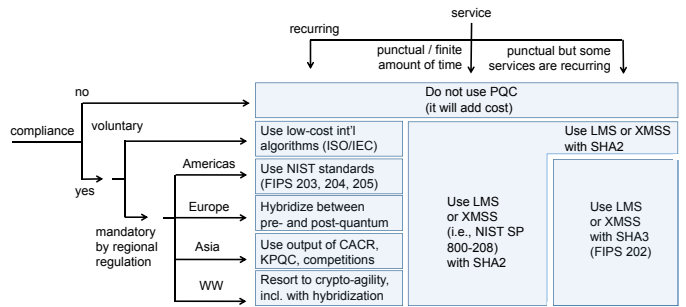


Figure 4: Strategy for Decision Making about the Algorithms.

The time when to start transitioning depends on the market vertical. We give an analysis in Fig. 5. The dates printed in red color are those getting close. The more dark the color is, the most imminent the required transition. It can be seen that governmental projects are the most important to transition as early as possible.

2) *Maturity measurement through TRL*: A solution is all the more robust as it is defined as a response to risks. Notion of TRL has been introduced in this respect. It is acclaimed by the industry hence has been standardized [17] for

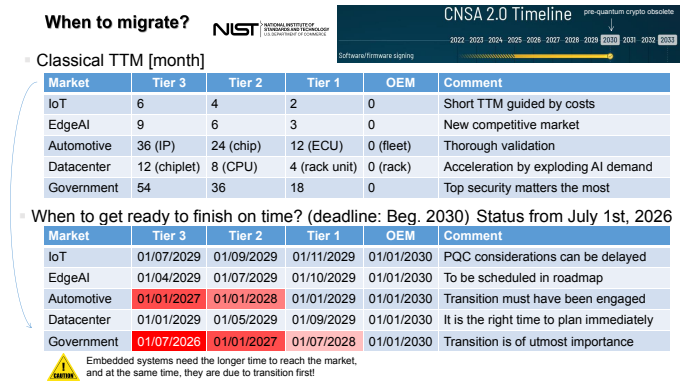


Figure 5: Timeline for decision when to switch to PQC.

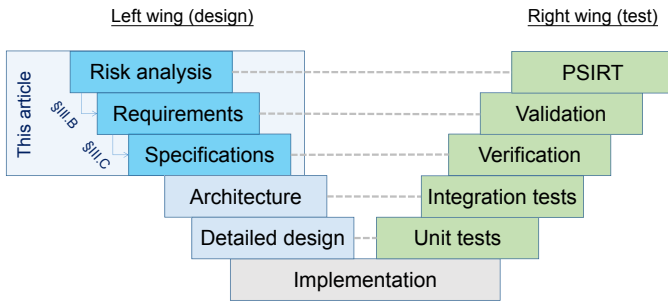


Figure 6: Security V-cycle stemming from a risk analysis.

space applications, and generalized by EU for any technology in [11].

In terms of cybersecurity, reaching the highest maturity, namely TRL 9, mandates that the system be designed and tested according to the most general framework capturing attacks. Namely, this is “risk analysis”. This approach is overarching because it makes shortcut reasoning nor assumptions, and instead reasons on the comprehensive array that can be mobilized by malevolent actors.

III. RISK ANALYSIS AS A CORNER STONE FOR ANALYSIS

A key action is to define the security problem(s). A fruitful approach in this respect is a risk based approach. Specifically, the application of a risk-oriented methodology allows to reason on the security rationale. Without surprise, some cybersecurity regulation, say the EU CRA [10] now mandates that all digital products placed on the European market comprise a risk analysis. It shall be reported to the authorities (here, the ENISA) as a declaration of conformity.

SPD5 is a USA policy directive on space that also requires a risk analysis [28, Sec. 4a].

A. Steps for the methodology

It proceeds as follows. First, the system missions are listed. Then for each of them, the necessary assets are deduced. A threat analysis allows to identify how assets are threatened, and eventually, security requirements can be enunciated. At this stage, the task of matching relevant countermeasures becomes straightforward.

Those steps are placed in the context of a V-cycle in Fig. 6. Notice that:

- risk analysis is verified by a Product Security Incident Response Team (PSIRT [13]);
- security requirements are subject to validation (e.g., system-level test);
- security specifications are verified by tests (e.g., deliverables ATE in Common Criteria [8]).

B. 1st step: Derivation of the requirements

Several risk analysis methods exist, such as EBIOS (“*Expression des Besoins et Identification des Objectifs de Sécurité*” in French, meaning “Expression of Needs and Identification of Security Objectives” in English) in France [1], that of UK [24], and RMF in the USA [26]. The steps we describe proceed along the lines of the five EBIOS workshops:

- 1) System description, and assets inventory

- Goal: capture the infrastructure and identify assets
- Deliverable: system description, in all its dimensions (manufacturing, lifecycle, elements, users)

2) Risk origin / target objective pair

- Goal: Risks enumeration and categorization
- Deliverable: Threat analysis (why assets are coveted)

3) Strategic scenarios

- Goal: Explain possible exposures
- Deliverable: Threat strategies, as analyzed from market insights

4) Operational scenarios

- Goal: Analyze likely attacks
- Deliverable: methods of attack that are likely to be used by the risk origins to carry out the strategic scenarios

5) Risk scenarios and Treatment

- Goal: State system requirements to mitigate risks
- Deliverable: Risk Analysis Report including security requirements and mitigations recommendations

The first four steps of EBIOS make up a risk assessment [7]. Indeed, they are observing and analysing the system, as is. The fifth step is the actually proposing fixes, and is thus a decisional aspect of risk management.

C. 2nd step: Deductive determination of specifications

The steps proceed as follows:

1) Functional security specification:

- Goal: Establish the mapping between the technology options and mitigations prescribed by the risk analysis
- Deliverable: configuration file (and its validation)

2) Specifications refinement regarding defense-in-depth:

- Goal: Map the level of risk to the multiplicity of the protections (e.g., leveraging an attack/defense tree for reasoning); For instance: number & placement of sensors, protection order against side-channel attacks, rate of redundancy against perturbation hazards & attacks, etc.
- Deliverable: Quantitative inputs to a system configuration (say of YAML format) file when the system is already legacy, or otherwise specifications of a system to be designed from scratch

3) Specification refinement based on compliance and regulatory requirements:

- Goal: Inject in the requirements external requirements originating from compliance (FIPS 140 [27], functional safety) and regulation (NIST SP 800-193 [29], memory safety from EO 14028 [34], etc.)
- Deliverable: State of the art of mandatory compliance, and resulting (cumulative) requirements

D. Discussion

Some specifications might seem overkill, but:

- 1) this may result from a defense-in-depth strategy; indeed, to attain a given security level, several mitigations can be piled up, which is called the “shift-left” approach;

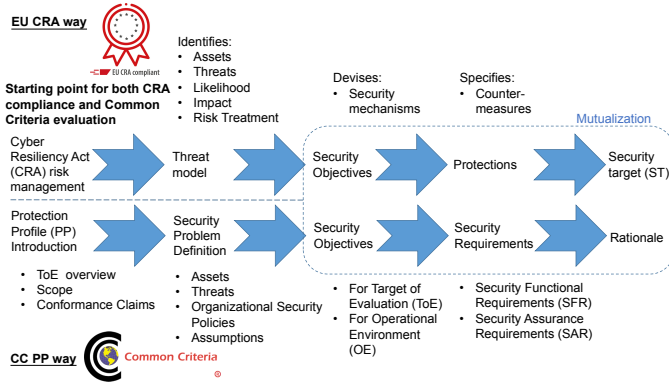


Figure 7: Risk analyses, as required by EU CRA and as practiced by the PP normative methodology.

- 2) good discipline also forces to analyse the security problem from all angles, thereby increasing its trustworthiness.

The methodology scales from unitary systems to systems-of-systems (SoS). Notice that the cybersecurity of SoS is currently a hot topic of standardization [18]. Besides, MITRE also develops PIVOT [36] to reason about risk analysis of SoS; the approach is top-down, with a decomposition of the risks according to natural fracture lines of the top-level system.

It shall be noted that the steps highlighted in a blue box in Fig. 6 (namely: risk analysis, requirements and specifications) are those pertaining to the *conceptual phases*. Those are the essence of the final product, and are created with the ingenuity of the designer; according so is the test strategy for those steps (namely: PSIRT, validation, verification). On the contrary, the downstream steps are rather belonging to a *practical phase*; they can be executed almost automatically, leveraging agentic genAI tools. Similarly, automated tests can be provided for those steps. In that sense, this paper tackles with seminal definition of the product, activity that cannot be delegated to an EDA toolchain.

E. Alignment with EU CRA

One obligation from the EU CRA is to not place on the market products with digital elements which would contain vulnerabilities. Now the vulnerabilities are precisely defined relatively to a risk analysis. Hence our methodology perfectly aligns with EU CRA.

One methodology to formally address risks on a class of products is that of the Protection Profiles (PP), as defined in CC [8, Part 3, §7]. It is thus natural that the ENISA (the EU cyber agency) is pushing for a notion of “presumption of conformity”. This means that a product certified compliant to a PP is presumed to meet the obligations from EU CRA.

This parallel is depicted in Fig. 7. The upstream task have different names, but the downstream ones converge and can be mutualized. This schematic aligns nicely with recent presentation at ICC 2026 [35].

Of course, the scope must be aligned, in that the application of the PP (i.e., the product Security Target) shall concern the actual use-case of the product when placed on the EU market.

But otherwise, there is no reason why not effectively consider a PP as an evidence for EU CRA obligations fulfilment.

The only hurdle might be though that the certification of compliance to a PP is requiring an evaluation by an independent laboratory, which incurs costs and delays. And within the short period of time between today (end of 2026) and the coming in force of the EU CRA (December 11, 2027), it can be doubted that laboratories will have the time to undertake and finish many parallel certifications with same timeliness.

IV. APPLICATION OF THE METHODOLOGY

We give the example of the security specifications for datacenter and automotive chiplets. The considered missions are (secure) provisioning, trimming, debugging, booting, and attestation.

A. Datacenter chips

The security in datacenter is still under consolidation of different approaches. Historically, the main risk has been a denial of service owing to existence of bugs, which can cause machines to fail operating properly (and typically reboot, which compromises the “availability” as an asset). Then the focus changed to the cyberattacks, whereby attackers were attempting to penetrate the datacenter leveraging misconfiguration of RBAC (Role-Based Access Control) or weaknesses in the high-level software. Today, we consider as well the hardware risks of Trojaned components. The approach adopted by OCP has been to ensure that a chain of trust stems from the datacenter chips, e.g., with mitigations such as remote attestation, starting in a silicon Unique Device Secret (UDS, root key of DICE [33]).

B. Automotive chips

The risk analysis is already well-established practice in automotive market. It is framed by UN ECE R.155 [9], which has been substantiated in ISO/SAE 21434 [16]. This international standard requires as a work product a Threat Analysis and Risk Assessment (TARA) evaluation. Hence the methodological framework is very mature already, and accounts for the high maturity of the automotive industry in terms of cybersecurity stance.

V. CONCLUSION

Security specifications need a traceable risk rationale. The system context determines the security problem; namely, missions, assets, supply-chain roles and lifecycle states establish the scope. Risk analysis justifies the requirements; Threat scenarios explain which protections are necessary and what residual risk remains. Specifications make the treatment implementable: it consists in selecting technologies, quantify defense-in-depth and include applicable compliance requirements.

Besides, assurance continues through the lifecycle; by connecting requirements and specifications to tests and validation, it is possible to extend to treat unexpected risks via a Product Security Incident Response Team (PSIRT) service. By enabling the capability to re-run a full V-cycle from its inception (risk phase), the system can be protected even post-market. The idea is to get a digital twin can that be re-assessed virtually before being sent back to the market, as a software patch.

ACKNOWLEDGMENTS

The authors would like to thank the audience of IEEE ICDV 2026 for their questions, Massimo Alioto for interesting discussions about the scalability of the method (composability, sustainment), and also Patrick Lejoly for his careful proofreading of the document.

REFERENCES

- [1] ANSSI. Methodology EBIOS Risk Manager, 2026. <https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/>.
- [2] Julien Béguinot, Olivier Rioul, Loïc Masure, François-Xavier Standaert, Wei Cheng, and Sylvain Guilley. Scalable Information Theoretic Evaluation of the Rank Statistics in Side-Channel Attacks. *IACR TCHES*, 2026(1):53–81, Jan. 2026.
- [3] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage. In *International Symposium on Electromagnetic Compatibility (EMC '14 / Tokyo)*. IEEE, May 12-16 2014.
- [4] Dominic Brown, Robin Emery, and Mark Knight. Foundation Chiplet System Architecture, February 12 2026. FCSA 1.0.0; <https://www.opencompute.org/wiki/Server/OCE/FCSA>.
- [5] Common Criteria for Information Technology. Security Evaluation. Part 2: Security functional components, November 2022. CC:2022, Revision 1, CCMB-2022-11-002, <https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART2R1.pdf>.
- [6] Common Criteria for Information Technology. Security Evaluation. Part 3: Security assurance components, November 2022. CC:2022, Revision 1, CCMB-2022-11-003, <https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART3R1.pdf>.
- [7] Computer Security Division Information Technology Laboratory. NIST Special Publication 800-30, revision 1: Guide for Conducting Risk Assessments, September 2012.
- [8] Common Criteria Consortium. Common Criteria (*aka* CC) for Information Technology Security Evaluation (ISO/IEC 15408), 2022. Website: <http://www.commoncriteriaportal.org/>.
- [9] ECE/TRANS/WP.29. UN Regulation No. 155 - Cyber security and cyber security management system, March 4 2021. E/ECE/TRANS/505/Rev.3/Add.154 - <https://unece.org/sites/default/files/2021-03/R155e.pdf>.
- [10] European Commission. European Cyber Resiliency Act (EU CRA), July 13 2023. <https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf>.
- [11] European Commission. Technology Readiness Levels, January 17 2024. <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq/2890>, consulted on Sept. 28, 2025.
- [12] European Union Agency for Cybersecurity (ENISA). Guidelines for Securing the Internet of Things, November 9 2020. Publication type: ENISA Reports; <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.
- [13] Forum of Incident Response and Security Teams, Inc. (FIRST). Product Security Incident Response Team (PSIRT) Services Framework, Spring 2020. Version 1.1, https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1.
- [14] Sylvain Guilley and Jean-Luc Danger. Chapter 13: Gate-Level Protection. pages 315–337. *Embedded Cryptography 2*; Wiley-ISTE (editors: Emmanuel Prouff, Guénaél Renault, Matthieu Rivain and Colin O’Flynn), February 2025.
- [15] Adam Hahn, Jack Cyprus, Dave Keppler, Marie Collins, Chris Harvey, Niyo Little Thunder Pearson, Wyatt Ford, Ang Cui, and Michael Locasto. The EMB3D™ Threat Model for Embedded Devices, September 2024. https://emb3d.mitre.org/assets/EMB3D_Paper_09-23-24.pdf.
- [16] International Organization for Standardization. ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering, 2021. Published (Edition 1), <https://www.iso.org/standard/70918.html>.
- [17] ISO. ISO 16290:2013 Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment, November 2013. <https://www.iso.org/standard/56064.html>, Edition 2024.
- [18] ISO/IEC JTC1/SC27/WG3. ISO/IEC CD TS 27115 Cybersecurity evaluation of complex systems, 2026.
- [19] Suny Li. *MicroSystem Based on SiP Technology*. Springer Singapore, 30 May 2023. Edition 1. Softcover. ISBN 978-981-19-0085-3. DOI: 10.1007/978-981-19-0085-3.
- [20] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks — revealing the secrets of smart cards*. Springer, 2007. ISBN 0-387-30857-1, <http://www.dpabook.org/>.
- [21] Mario Zuniga et al. Embedded Systems Threat Matrix™, August 2025. <https://estm.mitre.org/wp-content/uploads/2025/09/MP250155-Embedded-Systems-Threat-Matrix-3.0.pdf>.
- [22] MITRE. Embedded Systems Threat Matrix™, 2025. <https://estm.mitre.org/>.
- [23] MITRE. The MITRE EMB3D™ Threat Model, April 29 2025. <https://emb3d.mitre.org/>.
- [24] National Cyber Security Center (NCSC). Risk management, 2026. <https://www.ncsc.gov.uk/collection/risk-management>.
- [25] National Security Agency. The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, December 2024. Ver. 2.1. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.
- [26] NIST Computer Security Resource Center (CSRC). NIST Risk Management Framework (RMF), 2026. <https://csrc.nist.gov/Projects/risk-management>.
- [27] NIST FIPS (Federal Information Processing Standards) publication 140-3. Security Requirements for Cryptographic Modules. 22/03 2019. <https://csrc.nist.gov/publications/detail/fips/140/3/final>.
- [28] Office of Space Commerce. Space Policy Directive-5 (SPD-5), September 4 2020. <https://space.commerce.gov/president-signs-space-cybersecurity-policy-directive/>.
- [29] Andrew Regenscheid. NIST Special Publication (SP) 800-193 – Platform Firmware Resiliency Guidelines, May 2018. (also casually known as “PFR”). DOI: <https://doi.org/10.6028/NIST.SP.800-193>.
- [30] Anass Sbail. Chiplets System-in-Package Protection Profile, July 1 2026. Version 1.0; <https://www.secure-ic.com/services/advancing-security-for-chiplet-based-systems-thought-leadership/>.
- [31] Kris Tiri, Moonmoon Akmal, and Ingrid Verbauwhede. A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards. In *European Solid-State Circuits Conference (ESSCIRC)*, pages 403–406, September 2002. Florence, Italy, <http://citeseer.ist.psu.edu/tiri02dynamic.html>.
- [32] Kris Tiri and Ingrid Verbauwhede. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In *DATE, 16-20 February 2004, Paris, France*, pages 246–251. IEEE Computer Society, 2004.
- [33] Trusted Computing Group. Hardware Requirements for a Device Identifier Composition Engine, March 22 2018. Committee Draft. Family “2.0”, Level 00, Revision 78.
- [34] USA. Executive Order (EO) 14028 - “Improving the Nation’s Cybersecurity”, May 12 2021. <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>.
- [35] Enea Zhulati. When EUCC Over-Delivers: A Pilot Study on CRA Alignment for Class I and II Products (B12c), September 29. ICCS (International Conference on Common Criteria), Cardo Roma, Roma, Italy. Online: <https://tinyurl.com/43av6ycw>.
- [36] Mario F. Zuniga and Matt Janson. Platform Independent Vectors of Techniques (PIVOT) — An Approach for System-of-System Attack Path Analysis, May 2022. <https://apps.dtic.mil/sti/pdfs/AD1180518.pdf> (transferred to MITRE).