# Automating the conformity assessment of Cyber-Physical Systems software

Guillaume Nguyen
guillaume.nguyen@unamur.be
NADI, University of Namur
Namur, Belgium

## Abstract

Cyber-physical systems (CPS) are tools used by humans to enhance the way they perform tasks. CPSs make tasks more efficient, more precise, and safer. Those systems are omnipresent in human lives, e.g., in cars with Advanced Driver Assistance Systems (ADAS), in Unmanned Aerial Vehicles (UAV) for self-balancing or even in medical devices. CPSs can read information from the real world, process it, and affect the real world back, considering constraints such as real-time processing. Furthermore, the safety and security of the software controlling the CPS are directly linked with the safety and security of human bystanders. The European Union (EU) has a process to assess the conformity of specific products exchanged within the EU to ensure the safety of its citizens. Recently, regulations and directives such as the Cyber Resilience Act (CRA) pressed European actors to provide compliant software products. Requirements on software started with the Medical Device Regulation (MDR) in 2017. However, technical requirements are challenging to understand from legal texts, and certification processes rely solely on manufacturer documentation. On the one hand, the EU has difficulty monitoring and opening the European market to products deemed compliant. On the other hand, manufacturers have difficulty understanding what is technically required of them when introducing products. This thesis aims to reconcile both parties.

## CCS Concepts

• **Computer systems organization** → **Embedded and cyber-physical systems**; • **Software and its engineering** → **Software testing and debugging**.

## Keywords

CPS, testing, quality assurance, conformity, embedded systems, IoT, regulation

**ACM Reference Format:**
Guillaume Nguyen. 2025. Automating the conformity assessment of Cyber-Physical Systems software. In *33rd ACM International Conference on the Foundations of Software Engineering (FSE Companion '25), June 23–28, 2025, Trondheim, Norway*. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3696630.3731468

*FSE Companion '25, June 23–28, 2025, Trondheim, Norway*


## 1 Introduction

Cyber-Physical Systems (CPS), Real-time systems, Embedded (computer) Systems, and the Internet of Things (IoT) all share common concerns in terms of safety and security. The term '*Operational Technology* (OT)' is often used when talking with industrial actors. Gartner defines OT as '*hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events*' [9]. Rajkumar et al. provide us with a definition insisting on how CPS will change how people interact with the world and with one another [19].

Such systems are becoming prevalent. Technology such as Advanced Driver Assistant Systems (ADAS) [2] or connected medical devices [16] are becoming common. As the correct functioning of those devices is directly related to the safety of users, governments look into ensuring the safety of their citizens through market control. In fact, the European Union (EU) began to require the European Conformity (CE) marking on software products in 2017 with 'Regulation (EU) 2017/745' and 'Regulation (EU) 2017/746' [8] on medical devices. More recently, the Cyber Resilience Act (CRA) or 'Regulation (EU) 2024/2847' [8] includes CE requirements for the software components of industrial devices (among others).

While the EU intends to provide its citizens with safe products (and CPS), the tools and processes shared with stakeholders (citizens, member states, manufacturers, etc.) seem insufficient to ensure the expected implementation. Indeed, the current way the CE marking works depends on whether or not there is a specific EU regulation (in the broader sense). Then, depending on the presence of related harmonized European Standards (hEN) or European Standards (EN) the manufacturers need to undergo the compliance checking of their products to those standards (or any relevant standard with a proof of relevance). Afterward, the manufacturer needs to document their products. Depending on the applicable regulation, they can either grant themselves the CE marking or require the verification of their documentation by an accredited EU body or third party. The European Commission provides a guide compiling various legal texts for more clarity: 'The 'Blue Guide' on the implementation of EU product rules 2022' [7].

The three European Standardization Organizations provide the standards as laid out in 'Regulation (EU) 1025/2012 on European standardization' namely the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunication Standard Institute (ETSI) that can collaborate with (or delegate to) respectively the International Standard Organisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) for providing EN [8]. Figure 1 gives an overview of the process related to CE markings.

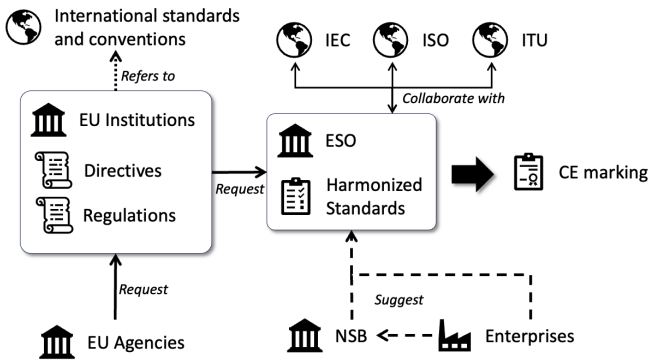


**Figure 1: The reduced and simplified EU legal texts and standards scheme [18]**

Nevertheless, the current way the CE marking works might not prevent introducing defective products on the European market. Indeed, as the conformity of the product is only assessed (or self-assessed) through documentation, an assessor might overlook the practical conformity of a product as they are not assessing the actual product. A product is only directly assessed when a complaint or a concern reaches the EU Market Surveillance: thus, when a problem (critical or not) happens. However, the actual assessment of a software product might require tremendous cross-expertise in software engineering, let alone all the other categories of products that require CE marking.

In this thesis, we aim to bridge the gap between software engineering and conformity assessment by providing a methodology and a conceptual tool for assessors or auditors when reviewing a product. We want to allow them to collect information directly about a System Under Conformity Assessment (SUCA) without solely relying on the provided documentation.

# 2 Background

## 2.1 Technical Requirements

Multiple domains of industry use CPS and real-time communication protocols. To build a tool able to collect information on a SUCA, we need to consider communicating with most of those technologies. The communication protocols and systems may come from industry standards such as IEC and IEEE, but the number of proprietary protocols and systems can not be neglected. Thus, we must ensure the following technical requirements when building a tool for conformity assessment:

**Robust Data Handling.** Security features such as authentication, encryption, and integrity checks can also vary across protocols and application domains. While some protocols offer robust security measures, such as Secure DNP3 with authentication and integrity checks [14] or 6LoWPAN with all measures available [11].

**Versatile Connectivity Options.** CPS and real-time protocols are numerous. The OSI layer (when relevant) at which each protocol operates provides insights into its communication characteristics. Protocols like Modbus RTU/TCP IP [14] and TCP ROS [23] primarily function at the application layer, while others like Profibus [14], UART, and CAN Bus [5] operate at the physical layer. The bandwidth and wire configurations vary depending on the protocol and application domain. Wireless protocols such as GPS (Galileo) [1], ZigBee [13], and LoRaWAN [15] operate within specific frequency ranges, enabling communication in remote or mobile environments.

**Resistance To The Environment Under Test.** Finally, the tool must be reliable and able to withstand various environmental conditions and extended periods of assessment. This is of utmost importance when assessing industrial applications that may involve exposure to heat, vibration, electromagnetic interference, or remote working environments.

## 2.2 Related Work

Putting the emphasis on existing research related to European regulations and conformity assessment, we find the most relevant studies related to the Regulation (EU) 2016/679 or General Data Protection Regulation (GDPR) [8]. More specifically, Aberkane et al. showed a relationship between Natural Language Programming (NLP), Requirements Engineering (RE), and GDPR [1]. Thus, using NLP for requirements engineering seems to be the preferred method, even in cases such as extracting requirements from European regulations. However, this is not the only method to extract requirements from legal texts. For example, Sleimi et al. developed a machine learning model to extract mandatory and prohibited actions [21]. Torre et al. started to develop a method using Universal Modeling Language (UML) [24] to assess the compliance of a system. Similarly, Sacre et al. worked on creating two meta-models [20]: the first is a legally compliant but theoretical model based on the SUCA's description, and the second represents the actual system. Then, they could list discrepancies between the two models. Shifting towards our specific domain, Kaneen et al. worked on a model-based approach in the context of GDPR for IoT [12]. While focusing on a subset of GDPR-related concerns and providing much manual work in the initial phases of their approach, they managed to produce a working proof of concept.

Large Language Model (LLM) [25] could replace NLP. Hassani et al. recently conducted an empirical study on using LLM to extract legal requirements from regulations [10]. They show that recent technologies are more prone to identify and generate testable legislative requirements using BERT and GPT, two types of LLM. They leveraged significantly good results with a simpler method. However, the authors only use Canadian regulatory texts, and they confirmed their approach using regulatory texts from the USA with standards concerning the creation of food-safety regulations. So, the creation of conformity tests might remain too high-level compared to EU legal requirements. Nevertheless, their research was triggered by the request of one of their industrial partners to develop a temperature sensor for food, which shows the interest and challenges of industrial actors in producing compliant products.

Looking at compliance checking for CPS, Bicaku et al. suggest a multi-layer approach [4]. Using international standards, they extract the relevant and measurable requirements or Measurable Indicator Points (MIPs) related to safety, security, and organizational concerns. Then, they set up monitoring agents with the ability to

[1] https://www.gsc-europa.eu

assess those MIPs for a specific technology. Their approach enables continuous checking of the system's conformity. However, it requires the creation of technology-specific monitoring agents, which might be extensive considering all proprietary technologies. Nevertheless, it still alleviates the testing effort as technical requirements only need to be extracted once.

Shifting towards formal verification, Deshmukh et al. propose a review of existing techniques for the generation of requirement-driven tests [6]. Relying on Model-Based Development (MBD) practice from various industrial actors, they suggest various falsification techniques (temporal specifications and trajectory splicing). Their method seems particularly efficient when MBD practices are in place. However, our approach relies on actual products for conformity testing.

## 3 Methodology

We use a *Design Science* approach with case studies carried on at industrial sites to validate our approach. This research has a strong industrial orientation with a primary focus on Belgium. To provide testers with a helpful test framework for CPS, we will reuse the preliminary results of our survey to carry out interviews involving use cases at industrial actor sites. Initially, we wanted to produce a classification framework for CPS across domains that could be used to pinpoint similarities between those systems thus, the tests that could be performed. However, we shifted our focus to the legal conformity assessment due to various limitations (few answers, few willing industrial collaborators, etc.). So, we will look into existing use cases within three domains of applications: health, transport, and energy sectors, which seem to be the most resourceful.

Then, we will work on creating a prototype for a physical device that could communicate with various CPSs depending on the technology used to assess the conformity to relevant European regulations. Of course, we should and could not attain a full conformity assessment; however, we aim to provide tangible signals for agnostic assessors and help them review the conformity of a SUCA.

## 4 Research Questions

At first, we aimed to provide a test-based classification of CPS as we assumed that sensors and actuators composing CPS across industries were similar and that the testing effort could be alleviated. Indeed, CPSs are mostly tested under specific conditions, and the most complex systems benefit from specially tailored tests. Thus, we carried out a survey targeted at technical C-Levels (or close) from industrial companies. We only gathered 8 usable answers out of the hundreds of people approached (contact lists, LinkedIn, industrial partners, participating to industrial salons, etc.). Most of the time when we could get an enthusiastic response from an engineer we would get stuck with their legal department not even suggesting the use of an NDA for the survey. Here is a list of our research questions:

**RQ1. How can we assess the conformity of a CPS?** Assess the technology required to perform a conformity audit on CPS across application domains. Start designing a testing tool.

**RQ2. What are the relevant regulations and standards for each domain of application?** Go through the available material and start mapping legal requirements with technical requirements.

**RQ3. What can be automatised when testing the conformity of a CPS?** Understand the technical requirements related to automatising the conformity testing of CPS. Look for use cases on which we can evaluate our findings and improve/build our method.

## 5 Results

We have few results at the moment. However, several elements encourage us to pursue our research in the direction mentioned earlier. Our initial vision is described in an early doctoral symposium published at the Software Product Lines Conferences (SPLC) 2023 [17]. We also put an article on Arxiv and are looking for a relevant venue: *'Towards Comprehensive Legislative Requirements for Cyber Physical Systems'*, which lays out the Background section of this paper more extensively [18].

**Initial survey.** This research has a strong industrial orientation with a primary focus on Belgium. To provide a helpful test framework for CPS, we designed a survey. The aim is to find a test-oriented classification framework for CPS in order to perform efficient testing taking into accounts the requirements and challenges of the various domains of application. For this classification we approached CPS from 3 main axis:

- CPS Testing - How are CPS tested across industries?
- CPS Engineering - How are CPS built across industries?
- CPS Context - What are the non-functional requirements of CPS across industries?

The preliminary results of the survey answered by 8 actors showed that testing was mostly done at all 4 phases of product development (design, development, prototyping and production) with the exception of one company in robotic services who was only testing during the prototyping phase. Concerning the time spent testing it varied a lot from 1 hour to as much time as needed to satisfy the test results. Interestingly, most were not solely relying on tests performed by manufacturers and performed their own tests while involving third parties for testing as well. Concerning the technologies used, they all had systems from different manufacturers although they all worked with Siemens and most of them with Raspberry Pi and Microsoft. The programming languages used were also quite different while most of them used Python and we were surprised to see the usage of JavaScript for half the respondents. In terms of communication protocols we can see the same disparities while Ethernet, MQTT, OPC UA and USB seemed to be quite the norm. Concerning non-functional requirements we expected the same kind of answers. However, most of the respondents did not seem to know which regulation/standards was applicable for them (besides the IEC 62443 on industrial control systems cybersecurity and related [2]). Which is also part of the reason why we shifted our focus towards legislative requirements and how to automate conformity in the context of CPS and Software Engineering.

**A3S3 Prototype.** We also produced a prototype for a tool called *A3S3 - Automated Android Audit of Safety and Security Signals*[3]

[2] https://webstore.iec.ch/en/publication/7030
[3] https://github.com/sabredefable/A3S3_python

that we are currently evaluating. By combining expertise in both Android programming and European Regulation requirements analysis, we aim to provide the ability to assess the conformity of a software to non-technical auditors. Of course the solution would still require the approval seal of a human auditor as we only return *Signals* from decompiled code. A3S3 works as follows: The auditor starts the tool, chooses an application, selects or creates an applicable audit file. The tool works like FlowDroid by decompiling android application and analyzing the decompiled code [3]. However, A3S3 looks for specific signals and produces a human-readable report. Finally, The auditor reads the report and states on the conformity of the application while taking into account the classical European Conformity process of course.

We are currently working with other researchers with the same concerns and we are looking to produce an holistic audit file for at least one European Regulation. The chosen audit will be based on the Medical Device Regulation as we noticed a growing interest for Android and Medical devices on Google Scholar.

## 6 Workplan

For the remaining time of this thesis, we will focus on getting real-life data on existing CPS to identify challenges related to producing and maintaining a conform system. To do so we created interview plans based on the preliminary data from our survey and we will aim at actors from at least 2 different domains of application suggested by Tekinerdogan et al. (Health, Smart Manufacturing, Transportation, Process Control, Defence, Building Automation, Robotic Services, Critical Infrastructure, Emergency Response, and Other) [22]. For both chosen domains we will produce a meta-model of a product and include the relevant legal requirements as features. Then we will validate it with industrial actors. In parallel we will work on automating the identification of a CPS and its components to ease the collection of data about the SUCA.

Concerning A3S3, we will work on providing a more accomplished version and look for industrial validation. This tool requires work on our end with Android and Legal specialist to provide a comprehensive set of signals relevant when assessing the conformity of an Android application in the context of Medical Devices. It will be a supporting tool on which we will base our design science approach. Indeed, we will be able to demonstrate our approach in making links between legal requirements, technical requirements and actual signal collection.

## Acknowledgments

This research was funded by the CyberExcellence by DigitalWallonia project (No. 2110186), funded by the Public Service of Wallonia (SPW Recherche).

## References

[1] Abdel-Jaouad Aberkane, Geert Poels, and Seppe Vanden Broucke. 2021. Exploring Automated GDPR-Compliance in Requirements Engineering: A Systematic Mapping Study. *IEEE Access* 9 (2021), 66542–66559. https://doi.org/10.1109/access.2021.3076921

[2] Fabio Arena, Giovanni Pau, and Alessandro Severino. 2020. An overview on the current status and future perspectives of smart cars. *Infrastructures* 5, 7 (June 2020), 53.

[3] Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, Damien Octeau, and Patrick McDaniel. 2014. FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. *ACM SIGPLAN Notices* 49, 6 (June 2014), 259–269. https://doi.org/10.1145/2666356.2594299

[4] Ani Bicaku, Christoph Schmittner, Patrick Rottmann, Markus Tauber, and Jerker Delsing. 2019. Security Safety and Organizational Standard Compliance in Cyber Physical Systems. *Infocommunications journal* 1 (2019), 2–9. https://doi.org/10.36244/icj.2019.1.1

[5] Mehmet Bozdal, Mohammad Samie, and Ian Jennions. 2018. A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. IEEE. https://doi.org/10.1109/iccecome.2018.8658720

[6] Jyotirmoy V. Deshmukh and Sriram Sankaranarayanan. 2019. *Formal Techniques for Verification and Testing of Cyber-Physical Systems*. Springer International Publishing, 69–105. https://doi.org/10.1007/978-3-030-13050-3_4

[7] EC. 2022. Commission notice The 'Blue Guide' on the implementation of EU product rules 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2022.247.01.0001.01.ENG [Accessed 10-10-2024].

[8] EU. 2024. EUR-Lex Access to European Union law. https://eur-lex.europa.eu/ [Accessed 29-01-2024].

[9] Gartner. [n. d.]. Definition of Operational Technology (OT) - Gartner Information Technology Glossary — gartner.com. https://www.gartner.com/en/information-technology/glossary/operational-technology-ot [Accessed 04-Jul-2023].

[10] Shabnam Hassani, Mehrdad Sabetzadeh, and Daniel Amyot. 2025. An Empirical Study on LLM-based Classification of Requirements-related Provisions in Food-safety Regulations. https://doi.org/10.48550/ARXIV.2501.14683

[11] Md. Milon Islam, Sheikh Nooruddin, Fakhri Karray, and Ghulam Muhammad. 2022. Internet of Things Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain: A Review. (2022). https://doi.org/10.48550/ARXIV.2204.05921

[12] Christos Karageorgiou Kaneen and Euripides G.M. Petrakis. 2020. Towards evaluating GDPR compliance in IoT applications. *Procedia Computer Science* 176 (2020), 2989–2998. https://doi.org/10.1016/j.procs.2020.09.204

[13] Salam Khanji, Farkhund Iqbal, and Patrick Hung. 2019. ZigBee Security Vulnerabilities: Exploration and Evaluating. In *2019 10th International Conference on Information and Communication Systems (ICICS)*. IEEE. https://doi.org/10.1109/iacs.2019.8809115

[14] Eric D Knapp and Joel Thomas Langill. 2015. Industrial Network Protocols. In *Industrial Network Security*. Elsevier, 1–7.

[15] Michael Krutwig, Bernhard Kölmel, Adrian Tantau, and Kejo Starosta. 2019. Standards for Cyber-Physical Energy Systems—Two Case Studies from Sensor Technology. *Applied Sciences* 9, 3 (Jan. 2019), 435. https://doi.org/10.3390/app9030435

[16] Mohamed R Mahfouz, Gary To, and Michael J Kuhn. 2012. Smart instruments: Wireless technology invades the operating room. In *2012 IEEE Topical Conference on Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireleSS)* (Santa Clara, CA, USA). IEEE.

[17] Guillaume Nguyen. 2023. A configurable approach to cyber-physical systems fuzzing. In *Proceedings of the 27th ACM International Systems and Software Product Line Conference - Volume B* (Tokyo Japan). ACM, New York, NY, USA, 1–5.

[18] Guillaume Nguyen, Manon Knockaert, Michael Lognoul, and Xavier Devroey. 2024. Towards comprehensive legislative requirements for Cyber Physical Systems testing in the European union. (2024). arXiv:2412.04132 [cs.SE]

[19] Ragunathan Rajkumar, Insup Lee, Lui Sha, and John Stankovic. 2010. Cyber-physical systems. In *Proceedings of the 47th Design Automation Conference* (Anaheim California). ACM, New York, NY, USA.

[20] Antoine Sacre, Jean-Noel Colin, and Benoît Hosselet. 2021. *ARRCIS: évaluation et renforcement de la conformité réglementaire d'un système d'information*. Number 52 in Collection du CRIDS. Larcier, 159–176.

[21] Amin Sleimi, Nicolas Sannier, Mehrdad Sabetzadeh, Lionel Briand, Marcello Ceci, and John Dann. 2021. An automated framework for the extraction of semantic legal metadata from legal texts. *Empirical Software Engineering* 26, 3 (March 2021). https://doi.org/10.1007/s10664-020-09933-5

[22] Bedir Tekinerdogan, Dominique Blouin, Hans Vangheluwe, Miguel Goulão, Paulo Carreira, and Vasco Amaral. 2020. *Multi-Paradigm Modelling approaches for cyber-Physical Systems*. Academic Press, San Diego, CA.

[23] Christopher S. Timperley, Gijs van der Hoorn, André Santos, Harshavardhan Deshpande, and Andrzej Wąsowski. 2024. ROBUST: 221 bugs in the Robot Operating System. *Empirical Software Engineering* 29, 3 (March 2024). https://doi.org/10.1007/s10664-024-10440-0

[24] Damiano Torre, Ghanem Soltana, Mehrdad Sabetzadeh, Lionel C. Briand, Yuri Auffinger, and Peter Goes. 2019. Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. In *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*. IEEE. https://doi.org/10.1109/models.2019.00-20

[25] Joseph Weizenbaum. 1966. ELIZA—a computer program for the study of natural language communication between man and machine. *Commun. ACM* 9, 1 (Jan. 1966), 36–45. https://doi.org/10.1145/365153.365168