Synchronisation of an Automotive Multi-concern Development Process

Martin Skoglund[1], Fredrik Warg[1], Hans Hansson[2], Sasikumar Punnekkat[2]

[1]RISE Research Institutes of Sweden, Borås, Sweden,
[2]MRTC, Mälardalen University, Västerås, Sweden

Published in:

Proceedings of *Computer Safety, Reliability, and Security. SAFECOMP 2021 Workshops, DECSoS, MAPSOD, DepDevOps, USDAI, and WAISE*, York, UK, September 7, 2021, pp 63-75.

The final publication is available at Springer via
https://link.springer.com/chapter/10.1007%2F978-3-030-83906-2_5

DOI: *10.1007/978-3-030-83906-2_5*

Postprint – Appears in *DECSoS 2021*

Synchronisation of an Automotive Multi-Concern Development Process

Martin Skoglund[1][0000−0001−6901−4986],
Fredrik Warg[1][0000−0003−4069−6252],
Hans Hansson[2][0000−0002−7235−6888], and
Sasikumar Punnekkat[2][0000−0001−5269−3900]

[1] RISE Research Institutes of Sweden, Borås, Sweden
[2] MRTC, Mälardalen University, Västerås, Sweden

Abstract. Standardisation has a primary role in establishing common ground and providing technical guidance on best practices. However, as the methods for Autonomous Driving Systems design, validation and assurance are still in their initial stages, and several of the standards are under development or have been recently published, an established practice for how to work with several complementary standards simultaneously is still lacking. To bridge this gap, we present a unified chart describing the processes, artefacts, and activities for three road vehicle standards addressing different concerns: ISO 26262 - functional safety, ISO 21448 - safety of the intended functionality, and ISO 21434 - cybersecurity engineering. In particular, the need to ensure alignment between the concerns is addressed with a synchronisation structure regarding content and timing.

Keywords: Functional Safety · Cybersecurity · Multi-concern · SOTIF · Automotive · ISO 26262 · ISO 21448 · ISO 21434.

1 Introduction

The complexity of embedded systems that are developed and integrated by manufacturers into modern cars is increasing. Advanced driver assistance systems (ADAS) progress by leaps and bounds, and soon the advent of vehicles with automated driving systems (ADS) is upon us. The chief design principle is no longer that of a fail-safe system, i.e., which has the option to become unavailable when a problem occurs. ADSs with level 3 and level 4 features according to SAE J3016:2018 [17], which intend to remove active supervision by a human driver, will need to replace the driver with fail-operational systems. There is also an increased reliance on connectivity and sensors to attain this new level of automation [21]. However, external communication and environmental sensors make the vehicles susceptible to security threats that may incapacitate or fool the ADS. Therefore, in engineering an ADS, both safety and security and their interplay must be addressed.

In many domains, including automotive, standards are often used to ensure quality concerns are appropriately treated. There is, however, a lack of experience in dealing with security in safety engineering and vice versa. Even though fundamental requirements for cooperation between concerns exist - e.g., ISO 26262:2018 expresses the need to take interdependence with cybersecurity into account - there is little guidance on transforming these requirements into a practical process that makes adherence to several standards with different concerns possible. Such details are also missing in the recently released technical report ISO/TR 4804, dealing with safety and cybersecurity specifically for ADSs; however, it does point to the three road vehicle standards ISO 26262 (functional safety), ISO 21448 (safety of the intended functionality), and ISO 21434 (cybersecurity engineering) for dealing with safety and security. In addition, there is a need for procedures to assess the conformity of an identified minimum set of standards for a dependable and secure system. ISO/TR 4804 will be expanded into a technical specification, ISO 5083, but the completion of this initiative is a long way off, and it is not yet known what it will contain. In the meantime, there is an urgent need for hands-on guidelines on best practices for multi-concern development, using the already available (or soon to be available) standards.

The contributions of this paper are intended to support the implementation of a multi-concern development process that could operate within the current standardisation landscape. It contains a unified chart, organised around a generic V-model, describing relevant processes, artefacts, activities, and a mechanism for synchronisation regarding content and timing between concerns at each step in the process.

2 Methodology and Scope

The paper builds upon work within the SECREDAS project [16]. The goal of the corresponding task in the project is to provide a hands-on guideline for continuous multi-concern qualification/certification, focusing on safety and security concerns. Multi-concern and continuous development are in this investigation considered as different aspects. This paper concentrates on refining the guideline regarding multi-concern development in the automotive domain for phases before the release to market. Phases after the first release are more relevant to address in relation to continuous development and successive releases.

The methodology entails surveying the applicable standards for relevant findings affecting continuous and multi-concern certification as a first step. A hypothesis regarding how to order and characterise the information is put forward in a unified development V-model, generalised to suit all standards. It was considered essential to have a starting point and iterate rather than analyse details and then generalise. The findings were inventoried and aggregated into this V-model. Analysis of the finding then resulted in assembling a chart and guideline for a multi-concern development process, encompassing safety and security concerns for the automotive domain. The complete survey of the standardisation landscape in the SECREDAS project was more vast in scope than the results

presented here, encompassing general system engineering, functional safety and information security, and other domains in addition to automotive.

3 Guideline for a Multi-concern Development Process

The process outline for multi-concern development resulting from our analysis of standards can be seen in Fig. 1. The figure is illustrating the life-cycle for nominal functions with added activities for functional safety and cybersecurity. The interplay between concerns in the coloured phases is described in this chapter. Phases dealing with software and hardware development had to be omitted due to space constraints, and the development of components is expected to have a lesser need for alignment if inconsistencies are appropriately dealt with in previous phases. Synchronisation and coordination will be necessary as the system is integrated. However, the pattern is similar to the system development phases.

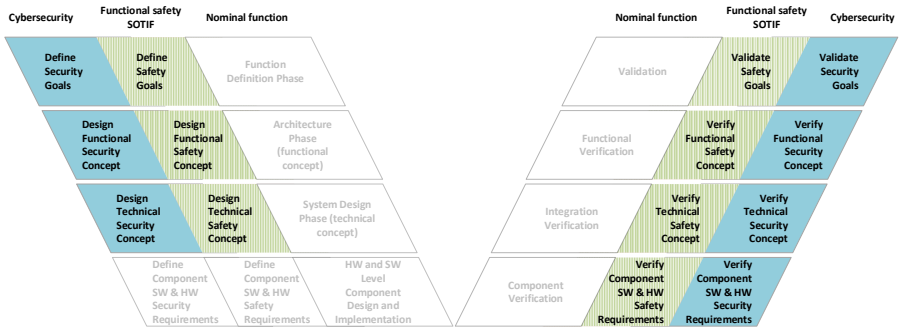

Fig. 1. Multi-concern development lifecycle, with current scope highlighted.

The used set of applicable standards can be narrowed down to a non-dispensable minimum relevant for the specific implementation and domain. In this paper, the chosen domain is automotive, with an envisioned implementation of an ADS with advanced environmental sensors susceptible to manipulation. The relevant standards for a non-dispensable minimum are, ISO 26262 [7] (addressing functional safety), PAS ISO 21488 [8] (addressing the safety of the intended functionality, SOTIF) and final draft of the ISO/SAE 21434 [10] (addressing cybersecurity). ISO/TR 4804 [9] can also be considered; however, as it gives some guidance but does not contain any normative requirements, it will not be directly considered in the multi-concern life-cycle described in this chapter.

Development of the nominal function can be regarded as the backbone of the process structure following a V-model. The V process model is an extension of the waterfall model in which each phase of development resulting in a successively refined design (shown on the left leg of the V) has a corresponding

verification phase[3] (shown in the right leg). Additional concerns are expanding the process scope with additional activities for each concern in each phase. In our figures and tables, functional safety and SOTIF are considered to intertwine into a general safety concern, while cybersecurity is maintained separately. The separation is due to scope, process, and treatment; it and is not intended to suggest an orthogonal outcome in the implementation. The suggested synchronisation is to address inconsistencies when concerns overlap. For example, cybersecurity threats and exploits that affect safety must be identified and resolved, and correspondently, safety assured integrity guarantees need to be put on the cybersecurity mitigations. The structure of all three aforementioned standards follows or can be adapted to the V-model development life-cycle. The multi-concern activities in phases on the left side of the V is referred to as co-design and discussed in Section 3.2, while on the right side, we talk about co-verification (including validation and assessment) in Section 3.3.

For the identified process phase scope (Fig. 1) there are 8 synchronisation points, 4 for the co-design part of the V model, and 4 for the co-verification part. The suggestion is that these 8 points in the combined process for the concerns are natural places for synchronisation that gives practical guidance on what and when synchronisation should occur. Thus, the proposed alignment is more refined than the normative requirements for cooperation between concerns found in the standards currently. If synchronisation is infrequent or imprecise regarding content, there is a risk of missing issues that may cause costly major redesigns if discovered late — or even worse, resulting in too high residual risks if inconsistencies are not discovered at all. Therefore, the claim is that the 8 synchronisation points are the minimum necessary for an effective alignment of the processes. To assess if the suggested synchronisation is sufficient to align concerns successfully is not possible without comprehensive evaluation and validation, to be investigated in the future. A possible evaluation scheme could compare loosely aligned processes, the suggested synchronisation approach, and a seamless process approach. A loosely aligned process would constitute the normative requirements in the standards where hazard and threat analysis and resulting risks are unified, and a seamless process approach would be a tailored total alignment of concerns with no distinction. Parameters of evaluation would be throughput and total effort in design and verification.

As mentioned in Section 2, the investigation is limited to activities from the initial design of the function up to validation thereof. This is the initial step for the future endeavour to present recommendations for a complete multi-concern *continuous* development, which also require guidelines encompassing the deployment and assessment activities during and after a release to market (e.g., maintenance, audits, incident detection and handling, over the air updates).

[3] It should be noted that it is primarily a model expressing dependencies in the refinement of design and verification phases for traceability, and does not necessarily mean the entire development project is performed in this sequence.

3.1 Elaboration on Concerns

Aspects of each concern under consideration can be allocated to the categories of means to attain dependability and security put forward by Avizienis et al. [1]. The categories are fault prevention (preventing the introduction of faults, e.g., with good engineering practices), fault tolerance (avoiding failures with a system design that can tolerate the existence of faults, e.g., redundancy), fault removal (removing faults from the system with, e.g., rigorous testing), and fault forecasting (evaluation of the system to forecast likely incidence and consequences of faults). Fig. 2 shows the sources and interrelation of faults treated by each of the three standards and whether the sources stem from the operational context, i.e., the environment in which the vehicle will operate or from system development.

The functional safety concern addresses malfunctioning behaviour that stems from random hardware faults, foreseeable non-malicious misuse, and systematic faults. As shown in Fig. 2, random hardware faults and non-malicious misuse stem from the operational context. The risks introduced by these aspects are mitigated by fault forecasting and fault removal and implemented in the system development. There might be a need for further mitigation by fault tolerance mechanisms. Unavoidable fault modes need to have verified diagnostic coverage, e.g., diagnostics, monitoring and exception-handling mechanisms. The function is analysed for risks, specified, implemented, and tested in the system development process, potentially introducing systematic faults. The rigour of the process provides the primary prevention mechanism against systematic faults, and testing rigour provides additional fault removal.

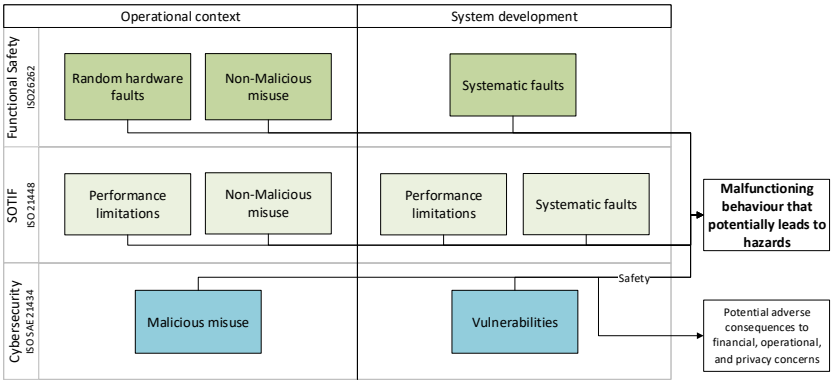

Fig. 2. Detailed multi-concern scope

An analogous logic applies to the safety of the intended functionality and cybersecurity, where risks of malfunctioning behaviour due to the operational context need to be mitigated and correctly addressed in the system development. During the system development, measures are needed against the introduction

of systematic faults and vulnerabilities. Cybersecurity, in general, addresses the broader scope of adverse consequences to financial, operational, safety, and privacy concerns brought on by malicious misuse exploiting vulnerabilities, but here the focus is on safety issues.

In a multi-concern development life-cycle, there is a need to align fault forecasting, fault prevention, and fault tolerance between the concerns in the co-design of the system. Additionally, there is an advantage in coordinating and aligning the fault removal activities in the co-verification, and validation [23]. Fig. 1 illustrates this combined life-cycle for a nominal function with added functional safety, SOTIF, and cybersecurity activities.

For each synchronisation point, one work product is identified from each concern for the reasons mentioned above. Thus, the synchronisation is incremental both in time and in content. The timing of synchronisation is dependent on the development phase, and the subject is dictated by the content of the identified work products. The selection of work products is the most seminal one for each refinement of the system. The mapping of each concern into a unified process revealed a natural set of triplets of work products to be synchronised both in time and content. A larger process scope would contain more synchronisation points. The goal of the work presented here is to enhance and formalise the alignment between concerns by introducing natural synchronisation points in a development life-cycle in the following Sections.

3.2 Co-Design

A multi-concern approach has many prerequisites on the capabilities of the development organisation—organisational competence covering both security and safety areas and the processes thereof—the ability to plan and follow up the progress of a very complex and multi-faceted life-cycle—in-depth knowledge of all the consideration when choosing sensors and actuators and implementing controllers. The considerations of the operational context need to be correctly transferred to multi-concern risk management. From there on, it is vital to maintain consistency and completeness between process outputs. It is imperative to maintain effective communication channels between the concerns and provide an established trade-off process to detect and handle inconsistencies.

con

We suggest using a systematic way of defining a set of synchronization points in a unified multi-concern development process to support alignment between concerns. A conclusion from our analysis is that the natural place for synchronisation is on the process output. In Fig. 3 the allocation to significant work products from the three standards is illustrated. The synchronisation points in the co-design are expected to support a common understanding of the operational context. In the system design, the synchronisation points align analysis methods, countermeasures, and requirements. In general, for co-design, the main advantage of treating all concerns in parallel is completeness, i.e., that all concerns and their interplay are considered throughout all phases, reducing the risk

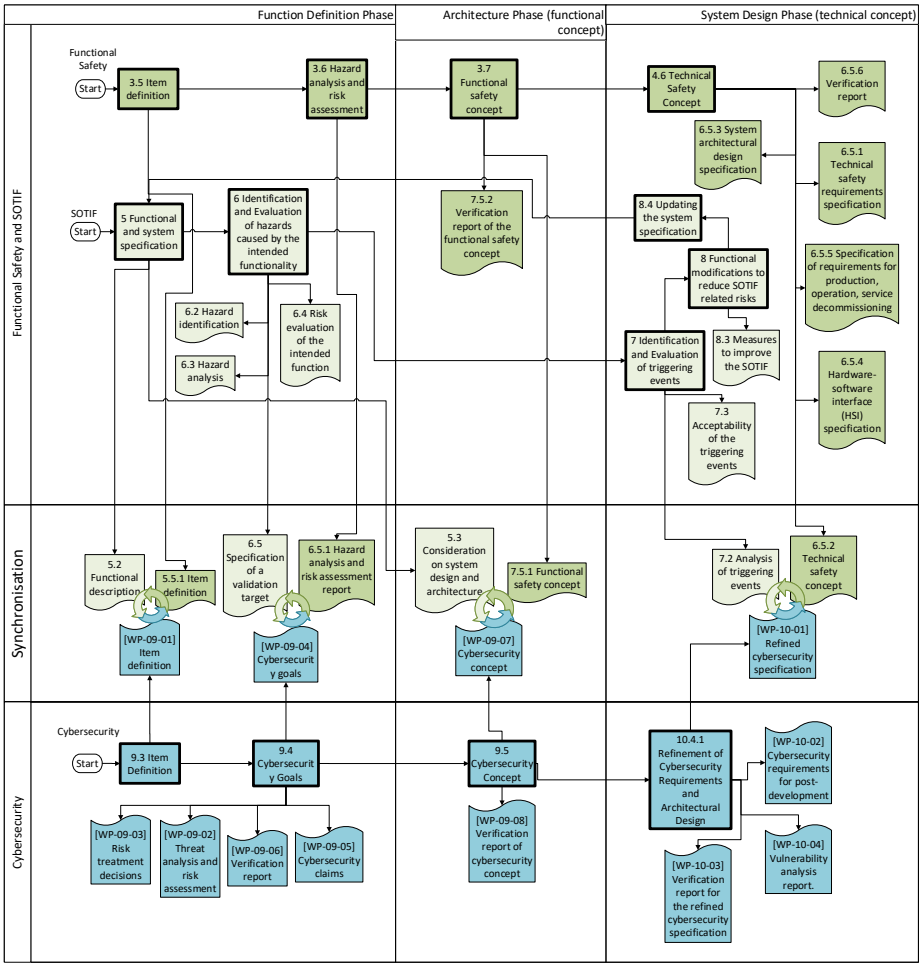

Fig. 3. Multi-concern process for co-design

Table 1. Co-design synchronisation points

ISO 26262	***ISO 21488***	***ISO 21434***
Function Definition Phase		
Item definition	Functional description	Item definition
When product development is initiated, the system is defined and described—elaboration on dependencies and interactions in the operational context, e.g., users, the environment, and other systems. Each concern has a slightly different scope (see Fig. 2), formalising the operational context, primary the overlap in fault forecasting needs to be synchronised.		
Hazard analysis and risk assessment report	Specification of a validation target	Cybersecurity goals
When analysing risks and establishing goals for the system stemming from the different concerns, it is essential to align assumptions of exposure, likelihood, consequences and interplay of faults in the work products.		
Architecture Phase		
Functional safety concept	Consideration on system design and architecture	Cybersecurity concept
While defining a functional concept that realises the intent and goals of the function, there is a need to remove inconsistencies in the degradation strategy, architectural requirements, fault tolerance measures and validation criteria.		
System Design Phase		
Technical safety concept	Analysis of triggering events	Refined cybersecurity specification
When refining the concept, the same considerations as defining the concept need to be addressed. A more comprehensive analysis is essential as technical details are available.		

of missing inconsistencies that may cause malfunctioning behaviour of the system. Common for all synchronisation points in Table 1 is that the rigour of the analysis and process provides an added fault prevention mechanism, and review stringency delivers additional fault removal of inconsistencies.

3.3 Co-Verification

The V-model's right side covers checking whether the system adheres to given properties formalised as requirements. Co-verification aims to act as fault removal activity for the particular concerns and presents an opportunity to investigate the interplay, implementing a well-thought-out integration test strategy coupled with verification and validation activities. An integration test strategy coordinates the use of test environments and test techniques for the concerns—considers how the techniques need to interact with the system—how close to production intent the system needs to be for the results to be relevant.

We suggest introducing systematic synchronisation points in the multi-concern co-verification process to maximise synergies in the use of test environment, and methods [23]. Therefore, synchronisation is allocated to the verification specification outputs. In Fig. 4 identified work products is shown. Test strategies are a subject of synchronisation, test reports not, since it assumed that any inconsistencies discovered in the testing results would be fed back into an appropriate co-design phase for analysis before planning the subsequent integration stage.

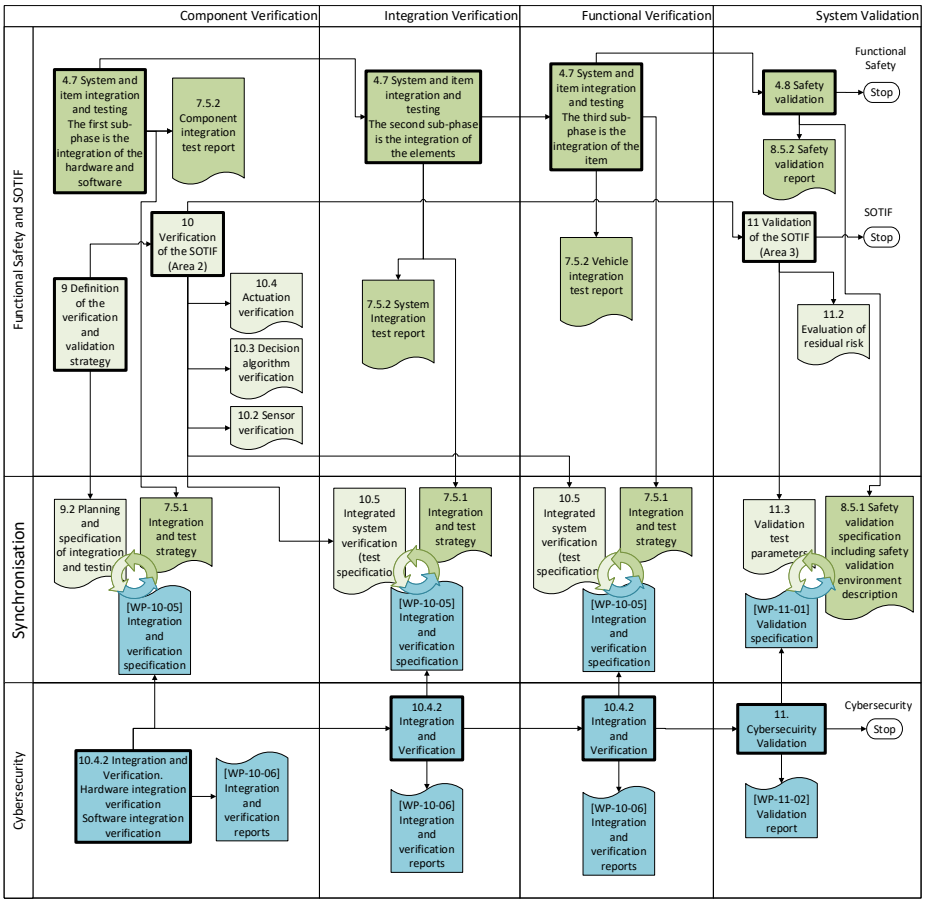

Fig. 4. Multi-concern process co-verification and validation.

Table 2. Co-verification synchronisation points

ISO 26262	***ISO 21488***	***ISO 21434***
Component Verification		
Integration and test strategy	Planning and specification of integration and testing	Integration and verification specification
Integration Verification		
Integration and test strategy	Integrated system verification (integration testing)	Integration and verification specification
Functional Verification		
Integration and test strategy	Integrated system verification (system testing)	Integration and verification specification
The integration steps are dealing with system components, integrating components into a system, and the integrated system, respectively. A general concern is the planning and coordinating of the testing efforts to remove the risks associated with random hardware faults, non-malicious misuse, performance limitations, and malicious misuse. An effort that establishes the underpinning for detecting and eliminating systematic faults and vulnerabilities while avoiding introducing new issues.		
System Validation		
Safety validation specification including safety validation environment description	Validation test parameters	Validation specification
Validation checks that the implemented system fulfils the top-level specifications, proving that all measures are appropriate and adequate in achieving the defined goals and validation criteria for all the concerns; synchronisation ensures alignment of the results.		

The bulk of testing required is not safety- or cybersecurity specific per se, but rather aimed at ensuring correct nominal function and good product quality in general and would require minimal alignment attention. Common to all synchronisation points in Table 2 is that testing rigour delivers fault removal.

Co-Assessment. The aggregated evidence from all preceding safety and security-related activities proving that the system is safe and secure will need to be independently assessed. ISO 26262:2018 expresses the need to take interdependence with cybersecurity into account, but there is no support in transforming these requirements into a practical assessment process that checks adherence to ISO 21434. The same is true for ISO 21448, where it is stated that the examination of the results of the SOTIF activities can be considered in ISO 26262-2:2018 functional safety assessment, but not further explained how. ISO 21434 has a separate section that addresses cybersecurity assessment; however, the exact connection to ISO 26262 assessments is a non-normative annex. For example, one link to ISO 26262 states that the safety risks are best defined within the ISO 26262 scope and collected. All standards, however, suggest the use of the ISO 26262 scheme of independence for assessment.

The conclusion is that assessing if the interplay between concerns has been adequately addressed is not possible if the assessments are conducted independently for each concern. However, there is little practical guidance for conducting

co-assessment and what it would entail, a topic that needs to be addressed soon. The assumption is that the suggested synchronised development process (Section 3) supports a joint incremental assessment/certification process with a similar approach, which might be enhanced by an assurance case template approach [3].

4 Related Work

Safety and security work has primarily been performed as independent activities, although there are several recent efforts towards unification or harmonising these concerns [12]. However, the endeavour to combining safety and security aspects during the development processes has been identified as non-trivial due to the high interference between these aspects and their respective treatment by Huber et al. [6]. One of the challenges identified, and one that is targeted by this paper, is the lack of experience, standards, and guidelines concerning the combination of the safety and security domains. Huber et al. also conclude that utilising a conceptual model unifying relevant documentation artefacts from requirements engineering, system modelling, risk assessment, and evidence documentation is the way forward, which aligns well with the suggested synchronised process in Section 3.

An alternative, more ad-hoc approach to synchronisation is suggested by Martinez et al., where interference analyses trigger co-engineering meetings and trade-off analyses [14]. The bottom-up triggering mechanism with a loose connection to governing processes could be a disadvantage for assessment, process control, and ease of adoption but might be preferable in agile development.

Supporting investigations into commonalities and cross-fertilization can give guidance on optimising and streamlining planning and implementing synchronisation concerns [11], [15]. There are substantial efforts in investigating the safety and security interplay [5], [4] that are useful in addressing them simultaneously. There is a need for special attention to bridge the gap between standards for automotive security engineering and hands-on, actual-system testing for verifying and validating automotive cybersecurity [13], [22], that could be integrated into the process structure suggested in this paper.

There are several frameworks put forward that addresses safety and security. In general, our approach can, on a high level, be seen as a specialisation of [18]; set in a different standardisation landscape. However, we suggest keeping the life-cycle domain-specific to retain risk calibration to automotive. To handle the complexity for co-engineering safety and security concerns, it essential for tool support, which might be remedied by the explicit systematisation and management of commonalities and variabilities [2]. However, the scalability of the approach needs further investigation.

As a starting point to identify the scope of the applicable standard for the work presented here, the standards were inventoried [20] and enhanced [19].

5 Conclusions

This paper focuses on refining synchronisation guidance targeting multi-concern in several crucial development phases within the automotive domain — providing the basis for implementing a multi-concern process that operates within the envisioned relevant standardisation landscape. The result put forward builds on a unified process chart, organised around a generic V-model, describing relevant processes, artefacts, and activities, and a mechanism for synchronisation regarding content and timing between concerns at each step in the process. In addition, each concern is further refined and allocated to the categories of means to attain dependability and security.

The synchronisation suggested to be inserted in the process output on a non-dispensable standard set, ISO 26262 [7] (addressing functional safety), PAS ISO 21488 [8] (addressing the safety of the intended functionality, SOTIF) and final draft of the ISO/SAE 21434 [10] (addressing cybersecurity). The synchronisation of concerns when developing ADS aids the elimination of inconsistencies between concerns as early as possible due to the support of a common understanding of the operational context. For co-design, the main advantage of treating all concerns in parallel is completeness, i.e., that all concerns and their interplay are considered throughout all phases. In addition, the introduction of synchronisation points in the multi-concern co-verification process maximises synergies in using the test environment and methods. The evaluation of the effectiveness of the proposed synchronisation has not been investigated. As alignment does not alter the process or the outputs directly, a future evaluation could compare the added effort of alignment to the effort saved by the enumerated benefits.

The current investigation is a work in progress and limited to the initial design of the function up to validation thereof and presented here as the initial step for the future endeavour to support a complete multi-concern life-cycle—support covering the deployment and assessment activities addressing *continuous* development where co-assessment of interdependent concerns would be of particular interest.

Acknowledgement. This work was supported by the SECREDAS project with the JU Grant Agreement number 783119, and the partners national funding authorities.

References

1. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing **1**(1), 11–33 (2004)
2. Bramberger, R., Martin, H., Gallina, B., Schmittner, C.: Co-engineering of safety and security life cycles for engineering of automotive systems. ACM SIGAda Ada Letters **39**(2), 41–48 (2020)
3. Chowdhury, T., Lesiuta, E., Rikley, K., Lin, C.W., Kang, E., Kim, B., Shiraishi, S., Lawford, M., Wassyng, A.: Safe and secure automotive over-the-air updates.

In: International Conference on Computer Safety, Reliability, and Security. pp. 172–187. Springer (2018)
4. Favaro, J.: AQUAS d1.3: Report on the evolution of co-engineering standards
5. Folkesson, P., Svenningsson, R., Söderberg, A., Wallerström, M., Montan, S.: HEAVENS d4 - interplay between safety and security
6. Huber, M., Brunner, M., Sauerwein, C., Carlan, C., Breu, R.: Roadblocks on the highway to secure cars: An exploratory survey on the current safety and security practice of the automotive industry. In: International Conference on Computer Safety, Reliability, and Security. pp. 157–171. Springer (2018)
7. ISO: ISO 26262:2018 Road vehicles – Functional safety (2018)
8. ISO: ISO/PAS 21448:2019 Road vehicles – Safety of the intended functionality (2019)
9. ISO: ISO/TR 4804:2020 Road vehicles — Safety and cybersecurity for automated driving systems (2020)
10. (ISO SAE): ISO SAE DIS 21434 (e) road vehicles – cybersecurity engineering
11. Lautieri, S., Cooper, D., Jackson, D.: SafSec: Commonalities between safety and security assurance. In: Redmill, F., Anderson, T. (eds.) Constituents of Modern System-safety Thinking, pp. 65–75. Springer London (2005)
12. Lisova, E., Šljivo, I., Čaušević, A.: Safety and security co-analyses: A systematic literature review. IEEE Systems Journal **13**(3), 2189–2200 (2019). https://doi.org/10.1109/JSYST.2018.2881017, https://ieeexplore.ieee.org/document/8556001/
13. Marksteiner, S., Marko, N., Smulders, A., Karagiannis, S., Stahl, F., Hamazaryan, H., Schlick, R., Kraxberger, S., Vasenev, A.: A process to facilitate automated automotive cybersecurity testing. arXiv preprint arXiv:2101.10048 (2021)
14. Martinez, J., Godot, J., Ruiz, A., Balbis, A., Nolasco, R.R.: Safety and security interference analysis in the design stage. In: International Conference on Computer Safety, Reliability, and Security. pp. 54–68. Springer (2020)
15. Pièrre-Cambacédès, L., Bouissou, M.: Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety **110**, 110 – 126 (2013). https://doi.org/https://doi.org/10.1016/j.ress.2012.09.011
16. Pype, P.: Secredas project – secredas will increase consumer trust in connected and automated transportation and medical industries., https://secredas-project.eu/
17. SAE: SAE J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (2018)
18. Schmittner, C., Ma, Z., Schoitsch, E.: Combined safety and security development lifecylce. In: 2015 IEEE 13th International Conference on Industrial Informatics (INDIN). pp. 1408–1415. IEEE (2015), http://ieeexplore.ieee.org/document/7281940/
19. Schoitsch, E., Schmittner, C.: Ongoing cybersecurity and safety standardization activities related to highly automated/autonomous vehicles. In: Zachäus, C., Meyer, G. (eds.) Intelligent System Solutions for Auto Mobility and Beyond, pp. 72–86. Springer International Publishing (2021)
20. Shan, L.: SECREDAS project deliverable d10.2 state-of-the-art analysis and applicability of standards (2019)
21. Skoglund, M., Thorsén, A., Arrue, A., Coget, J.B., Plestan, C.: Technical and functional requirements for v2x communication, positioning and cyber-security in the HEADSTART project. In: Proceedings of ITS World Congress 2021 (2021)
22. Skoglund, M., Warg, F., Hansson, H., Punnekkat, S.: Black-box testing for security-informed safety of automated driving systems. In: 2021 IEEE

93rd Vehicular Technology Conference (VTC2021-Spring). pp. 1–7 (2021). https://doi.org/10.1109/VTC2021-Spring51267.2021.9448691
23. Skoglund, M., Warg, F., Sangchoolie, B.: In search of synergies in a multi-concern development lifecycle: Safety and cybersecurity. In: Hoshi, M., Seki, S. (eds.) Developments in Language Theory, vol. 11088, pp. 302–313. Springer International Publishing (2018)