An Extension of the Rasmussen Socio-technical System for Continuous Safety Assurance

Barbara Gallina
Mälardalen University,
P.O. Box 883, SE-72123 Västerås, Sweden
Email: barbara.gallina@mdu.se

Peter Munk and Markus Schweizer
Robert Bosch GmbH,
71272, Renningen, Germany
Email: Name.Surname@de.bosch.com

***Abstract*—To win the competition, diversification via software-implemented functionality, has become a trend in various domains. In the automotive domain, for instance, road vehicles are being transformed from steels and wheels to software and services, where software is expected to shape the vehicles virtuously, over their entire lifetime, by increasing customer's satisfaction via an increasing number of comfort features. However, if safety assurance is not in focus while managing variability, these features, may viciously turn into risk-bearing features potentially leading to fatalities. In the literature, the problem of safety assurance and its configuration has been addressed. The usage of the Base Variability Resolution language, for instance, was explored to systematise and configure not only product-related features but also process and assurance-related features, necessary for the justification purposes. The problem of safety assurance has also been addressed, yet without variability aspects, from a socio-technical perspective, e.g., by Rasmussen with his socio-technical system. In this position paper, we propose an extension of the Rasmussen's socio-technical system. Our extension is twofold: on one hand it embraces product lines instead of single systems, on the other hand it develops the technical and argumentation aspects in addition to the socio-aspects. We also mention how our extension can be specialised in the automotive context.**

***Keywords*—Safety assurance, Variability management, Rasmussen's socio-technical system.**

I. Introduction

To win the competition, diversification via software-implemented functionality, has become a trend in various domains. In the automotive domain, road vehicles are being transformed from steels and wheels to software and services, where software is expected to shape the vehicles virtuously, over their entire lifetime, by increasing customer's satisfaction via an increasing number of comfort features. However, if safety assurance is not in focus while managing variability, these features, may viciously turn into risk-bearing features potentially leading to fatalities. In the automotive domain, an exemplary case is the case of the power-operated window lifters, where functional safety and safety of the intended functionality need to be properly managed and configured to avoid severe consequences such as suffocation. In the literature, the problem of safety assurance and its configuration has been addressed. Within the AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) project [1]–[3], for instance, the usage of the Base Variability Resolution language [4] was explored to systematise and configure not only product-related features but, as proposed by Gallina [5] also process and assurance-related features, necessary for the justification purposes. This multi-dimension configuration was designed([6]) and partly implemented in the AMASS platform [7].The problem of safety assurance has also been addressed, yet without variability aspects, from a socio-technical perspective, e.g., by Rasmussen with his socio-technical system [8], [9]. Rasmussen highlighted the socio-technical layered nature of system safety assurance, encompassing socio (political, legal, standardisation, managerial) and technical (engineering) entities. Rasmussen also highlighted the need for vertical integration among the layers, where not only decisions made at the higher levels shall be propagated down through the hierarchal levels but also that information shall flow upwards from bottom to top. This upwards flow is necessary for improvement. In this abstract, based on work we conducted in the 4DASafeOps [10] project, we build on top of Rasmussen's socio-technical system and the AMASS project's approach. Specifically, we propose an extension (from single system to product lines, including not only the act of engineering but also the technical and argumentation artefacts) and specialisation (from domain-independent to the automotive-specific) of Rasmussen's socio-technical system. The novelty of our work consists in the introduction of a multi-dimensional product-line perspective aligned with the Rasmussen's socio-technical system and integrated with a set of proactive safety management strategies. The main key-potential of our proposal is: since a comfort feature might become a risk-bearing feature (if wrong configuration is in place), with our proposal, we prevent a wrong product configuration by considering safety-relevant inter-feature dependencies, especially when the boundary between a comfort and a risk-bearing feature is subtle, which potentially could lead to fatalities. Hence, a proactive safety assurance variability management may represent a way forward for guaranteeing a clear distinction. The rest of the paper is organised as follows. In Section II, we provide background information. In Section III we present our proposal for extending the Rasmussen's socio-technical system for continuous safety assurance. In Section IV, we discuss related work. Finally, in Section V, we present some concluding remarks and future work.

II. Background

In this section, we present essential background.

A. Variability Management via Base Variability Resolution

To manage variability, different methodological approaches have been proposed. In the context of safety-critical systems

engineering, an approach based on Base Variability Resolution (BVR) was proposed. In this position paper, we base our extension on BVR due to our familiarity with it. Thus, we recall basic information. The Base Variability Resolution (BVR) metamodel [4] is a a domain-specific language (DSL) devoted to the variability domain. BVR allows users to model (VSpec model) and resolve (Resolution model) the variability at the abstract level. The resolution models specify the desired/allowed configurations. Once a configuration is modelled, the binding between the abstract representation and the concrete representation can be realised (Realization model). More precisely, VSpec permits users to capture in a feature diagram-like fashion what varies and what remains the same. Specifically, a VSpec is a tree representation, where the tree root represents a feature that is progressively decomposed using mandatory, optional, alternative (OR), or mutually exclusive alternative (XOR) features, where a feature [11] is a system property that is relevant to some stakeholder and is used to capture commonalities or discriminate among systems in a family/set of systems. BVR also includes a constraints language to enable the formulation of constraints (inclusion/exclusion) aimed at constraining the selection of cross-tree features. BVR incorporates best practices of product line modelling.

B. Rasmussen's view on risk management

In this section, we recall Rasmussen's view on safety management. According to Rasmussen [8], first of all a socio-technical and layered system view shall be adopted. Rasmussen suggests six layers for representing the socio-space that plays a role in controlling the risk at the technical layer, which is at the bottom of the socio-space. The suggested six layers are:

1) Government - where judgement takes place based on public opinion as well as financial and geo-political considerations;
2) Regulators/Associations- where industry standards are developed based on laws and regulations;
3) Company - where company policies and procedures based on industry standards govern work processes. In the automotive domain, this is the place where company specific interpretations and tailoring of automotive standards and regulations take place in order to make standards and regulation operational;
4) Management - where company policies and procedures are implemented;
5) Staff - representing the activities and characteristics of workers performing the processes; and
6) Work - representing the equipment and environment by which work happens

According to Rasmussen [9], to function safely, the system shall guarantee vertical integration. This means that not only decisions made at the higher levels shall be propagated down through the hierarchal levels but also that information shall flow upwards from bottom to top (proactive strategy). Feedback-loops shall be in place. The interaction and dependencies across levels are critical to ensure that intended safeguards protect system states. Threats to safety result from a loss of control caused by inadequate vertical integration across levels, not just from deficiencies at any one level. The intention of Rasmussen is to propose an analytical framework to encompass a wide range of dimensions that have to be brought together to make sense of socio-technical behaviour. Rasmussen also points out that in various domains (including transportation) a very fast pace of change of technology is found and that this pace is much faster with respect to the change of the control structures at the various socio-levels. Rasmussen's observations were formulated in the late nineties of the previous century. His observations are still valid. Nowadays, in the twenties of the 21st Century, the fast pace of change has become much more faster. Regarding proactive assurance, Rasmussen points out that instead of a strategy based on attempts to remove causes of human failures, an attempt shall be made to design a strategy based on: 1) An identification of the boundaries of safe performance, 2) Efforts to make these boundaries visible to decision makers, and 3) Efforts to counteract pressures that drive decision-makers toward the boundaries.

III. An Extension of the Rasmussen Socio-technical System for Continuous Safety Assurance

In the previous section, we have recalled basic information on variability management and on the Rasmussen's view on safety risk management. In this section, we use such information to propose an extension of the Rasmussen's socio-technical system. Figure 1 shows the result of this extension, i.e., the product line-oriented extension of the Rasmussen's socio-technical system, covering not only socio-related layers but also technical and assurance case-related layers. At each layer, we have (configurable) product lines, i.e., sets of products, characterised by commonality and variability, where the product may represent a work-product, i.e., a law, a standard, a process, a technical product, an assurance case. This is why we state that we obtain a product line-oriented extension of the Rasmussen socio-technical system.

- L2a: A law property that is relevant to some stakeholder and is used to capture commonalities or discriminate among laws in a family;
- L2b: A standard property that is relevant to some stakeholder and is used to capture commonalities or discriminate among standards in a family;
- L2c: A guideline property that is relevant to some stakeholder and is used to capture commonalities or discriminate among guideline in a family. This in case guidelines exist. For simplicity, this layer is not depicted in Figure 1;
- L3a: A process property that is relevant to some stakeholder and is used to capture commonalities or discriminate among processes in a family – OEM level;
- L3b: A process property that is relevant to some stakeholder and is used to capture commonalities or discriminate among processes in a family – Tier level;
- L4: A process property that is relevant to some stakeholder and is used to capture commonalities or discriminate among processes in a family – Management level;
- L5: A process property that is relevant to some stakeholder and is used to capture commonalities or

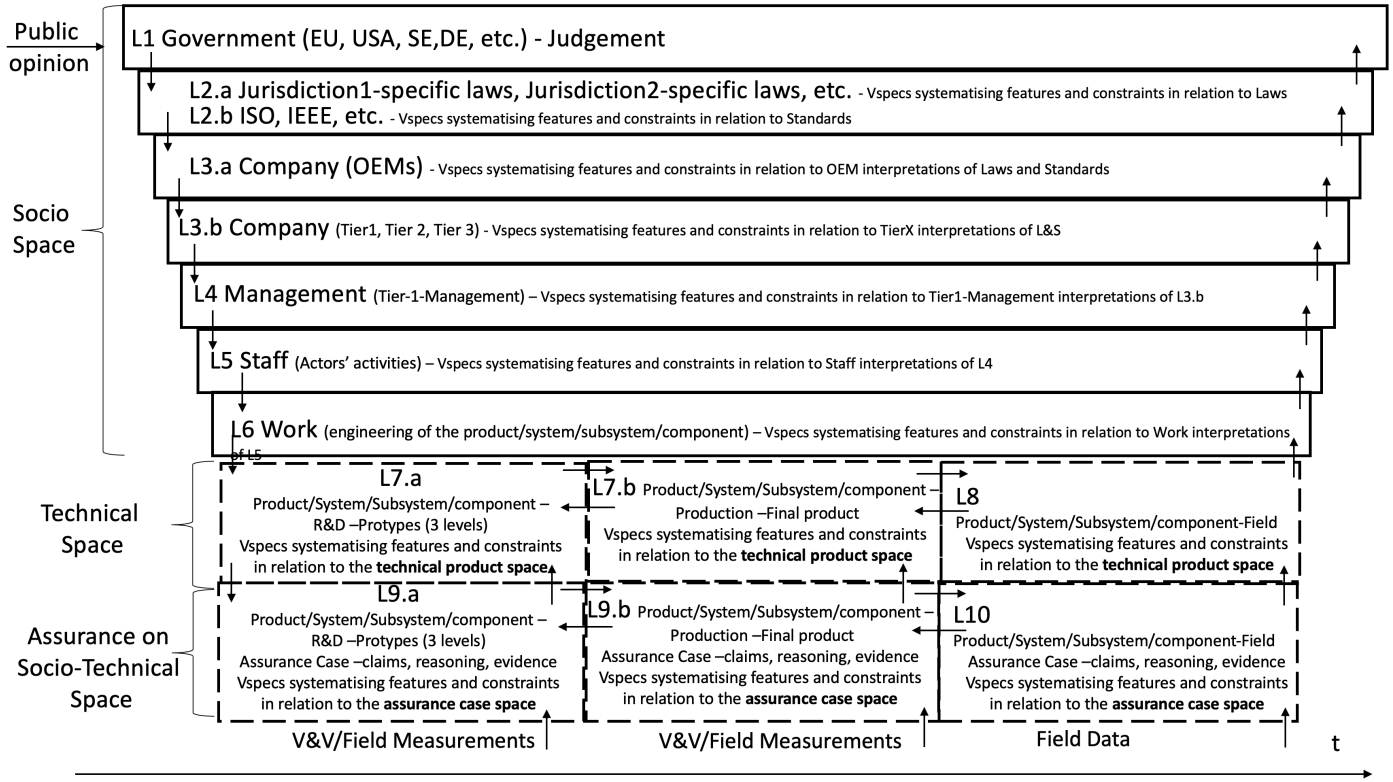

Fig. 1. Our proposal for a product-line oriented extension of the Rasmussen's socio-technical system

discriminate among processes in a family – Staff (Drivers/occupants/ as well as process staff interpretation);

- L6: A process property that is relevant to some stakeholder and is used to capture commonalities or discriminate among processes in a family – Work (interpretation at project level);
- L7a: A system property that is relevant to some stakeholder and is used to capture commonalities or discriminate among systems in a family (during prototyping);
- L7b: A system property that is relevant to some stakeholder and is used to capture commonalities or discriminate among systems in a family (in product finalisation);
- L8: A system property that is relevant to some stakeholder and is used to capture commonalities or discriminate among systems in a family (in the field);
- L9a: An assurance case property that is relevant to some stakeholder and is used to capture commonalities or discriminate among assurance cases in a family (during prototyping);
- L9b: An assurance case property that is relevant to some stakeholder and is used to capture commonalities or discriminate among assurance cases in a family (in product finalisation). This level captures the assurance case properties of the system before its release on the market. From a technical (system behaviour) perspective, it is highly coupled with L7b;
- L10: An assurance case property that is relevant to some stakeholder and is used to capture commonalities or discriminate among assurance cases in a family (in the field). This level captures the assurance case properties during the operational life of the system. Hence, it is highly coupled with L8;

It shall be pointed out that a selection at L2a (a selection of a law property) might have implications (formulated as inclusion/exclusion constraints) on all the other levels, i.e., implications on standards (the law property is interpreted as a collection of clauses in standards), implications on processes, implication on management, implication on the technical and assurance case-related aspects. It shall also be pointed out that a discovery at operational time (based on field data) shall proactively call for a change, hence towards guaranteeing continuous assurance. The call for a change might impact the technical space only or might instead call for a more impactful change at the higher level hierarchy of our extended socio-technical system. By systematising inter-feature dependencies of the control flow, we intend to contribute to the identification of the boundaries of safe performance and to their visualisation aimed at making those boundaries visible to decision makers with the purpose of counteracting pressures that drive decision-makers toward the boundaries. We also wish to highlight that in Figure 1, we have decided to use BVR/VSpecs. However, the choice of the variability specification language is not binding.

In the automotive domain, our proposal for a product-line oriented extension of the Rasmussen's socio-technical system could be interpreted as follows: UNECE and US regulations focusing on specific items might overlap. Standards

provide a technical refinement of the regulations and might overlap. For instance ISO 26262 [12] for functional safety and ISO 21448 [13] for safety of the intended functionality overlap (see for instance Hazards analysis and risk assessment). At OEM (Original Equipment Manufacturer) and at tier-level, standards are interpreted for defining internal processes, which in turn are further refined at specific management units and can be further refined depending on the staff and specific work conditions (different sets of process configurations at execution time). The refined processes as well as the regulations and standards have an impact direct or indirect impact on the configurations of the technical space (vehicle/item/component). The refined processes as well as the refined/constrained technical space (vehicle/item/component) have an impact (constraints) on the assurance case-related space. Considering a power-operated window lifter, UNECE R21 states: "Switches of power-operated windows shall be located or operated in such a way to minimise the risk of accidental closing." FMVSS 118, specifically paragraph S6 states: "Any actuation device for closing a power-operated window must operate by pulling away from the surface in the vehicle on which the device is mounted." Hence, both UNECE R21 [14] and FMVSS 118 [15] contain requirements for minimising accidental closing. This law property has implication on standard property i.e., the law property may imply the adoption of ISO 21448, which requires to conduct SOTIF-hazards analysis and risk assessment (HARA). SOTIF-HARA may in turn imply the selection of a guideline property, which, if not properly selected, might imply a wrong risk assessment (underestimation) leading to the potential development of a risk-bearing feature (switches are not operated in a way that minimises risk). Before the introduction of switch-specific legal requirements, press-down (one touch) switches used to be mounted on passenger cars and fatalities occurred due to the accidental (closing) actuation of switches by children, who died due to suffocation.

IV. Related Work

To the best of our knowledge, our work represents a novelty in its vision of considering the different layers that play a role in safety-critical systems engineering/configuration. The key novelty is in its product-line oriented extension. Other researchers have pointed out the relevance of the Rasmussen's socio-technical system and its holistic view.

V. Conclusion and Future Work

In this paper, we have presented our proposal for a product-line oriented extension of the Rasmussen's socio-technical system considering not only socio-related layers but also technical and assurance case-related layers. We believe that our proposal has the potential to contribute in systematising intra as well as cross-layer constraints and by so doing contributing to constraining the technical space to avoid risk-bearing features potentially leading to fatalities.

In the future, we intend to conduct a series of case studies to show the usefulness of our proposal for constraining downward (in case of maturity of the regulations) the configuration space. Based on historical data, we also intend to show how our proposal may proactively contribute to raising the need for reconsidering the cross-layer dependencies by e.g., introducing new regulations or by modifying existing ones thanks to the learning outcome provided during the operational life of the product (field data). Part of this case study-based research is already ongoing focusing a the product line of window lifters and focusing on showing that a specific configuration at the jurisdiction/legislation layer or standard layer constrains the technical space (the window lifter) by guaranteeing the safety of the intended functionality, avoiding for instance suffocation. An ontology-based approach is also under investigation [16].

References

[1] "AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)," 2019. [Online]. Available: https://www.amass-ecsel.eu

[2] A. Ruiz, B. Gallina, J. L. de la Vara, S. Mazzini, and H. Espinoza, "Architecture-driven, multi-concern and seamless assurance and certification of cyber-physical systems," in *Computer Safety, Reliability, and Security*. Cham: Springer International Publishing, 2016, pp. 311–321.

[3] J. L. de la Vara, E. Parra, A. Ruiz, and B. Gallina, "AMASS: A Large-Scale European Project to Improve the Assurance and Certification of Cyber-Physical Systems," in *Product-Focused Software Process Improvement*, ser. PROFES, vol. 11915. Springer International Publishing, nov 2019, pp. 626–632.

[4] Ø. Haugen and O. Øgård, "BVR - better variability results," in *Proceedings of the 8th International Conference on System Analysis and Modeling: Models and Reusability (SAM '14), Valencia, Spain, September 29-30.*, vol. 8769. Cham: Springer International Publishing, 2014, pp. 1–15.

[5] B. Gallina, "Towards enabling reuse in the context of safety-critical product lines," in *5th IEEE/ACM International Workshop on Product Line Approaches in Software Engineering, PLEASE 2015, Florence, Italy, May 19, 2015*, 2015, pp. 15–18.

[6] M. A. Javed, B. Gallina, and A. Carlsson, "Towards variant management and change impact analysis in safety-oriented process-product lines," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC '19. Association for Computing Machinery, 2019, p. 2372–2375.

[7] J. L. de la Vara, E. P. Corredor, A. R. Lopez, and B. Gallina, "The AMASS Tool Platform: An Innovative Solution for Assurance and Certification of Cyber-Physical Systems," in *Joint Proceedings of REFSQ-2020 Workshops, Doctoral Symposium, Live Studies Track, and Poster Track co-located with the 26th International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ) Pisa, Italy*. CEUR Workshop Proceedings, Vol-2584, 2020.

[8] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," *Safety Science*, vol. 27, no. 2, pp. 183–213, 1997.

[9] J. Rasmussen and I. Svedung, *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, 2000.

[10] 4DSafeOps Team, "4DSafeOps, Standards-Assurance Case-Process-Product-Aware SafeOps #49, Software Center." [Online]. Available: https://www.software-center.se

[11] K. Czarnecki and U. W. Eisenecker, *Generative Programming: Methods, Tools, and Applications*. USA: ACM Press/Addison-Wesley Publishing Co., 2000.

[12] International Organization for Standardization (ISO), *ISO 26262:2018 - Road vehicles – Functional safety*, Std., 2018.

[13] *International Organization for Standardization (ISO)*, "ISO 21448: Road vehicles — Safety of the intended functionality (SOTIF)," 2022.

[14] UNECE, "*REGULATION 21 - Uniform Provisions Concerning the Approval of vehicles with regard to their interior fittings*," 2003.

[15] Federal Register, "Vol. 69, No. 178/Wednesday, September 15, 2004/Rules and Regulations," 2004.

[16] B. Gallina, H. Dibowski, and M. Schweizer, "An ontology-based representation for shaping product evolution in regulated industries," in *21st International Conference on Software and Systems Reuse (ICSR-2024), Limassol, Cyprus, June 19-20, 2024*. Springer International Publishing, 2024.