Reconciling the ISO 26262-compliant and the agile documentation management in the Swedish context

Barbara Gallina, Mattias Nyberg

Reconciling the ISO 26262-compliant and the agile documentation management in the Swedish context

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

Mattias Nyberg
Scania AB,
Södertälje, Sweden
Email: mattias.nyberg@scania.com

***Abstract*—Documentation management represents a relevant and mandatory activity according to ISO 26262 [1]. The same activity tends to be considered as a waste according to the agile manifesto [2]. Thus, agile and ISO 26262-compliant documentation management styles seem to form an odd couple. When this couple is located in the Swedish cultural context, reconciliation and negotiation within it represent a true challenge. In this paper, based on the state of practice in industrial settings, we report about our findings and propose our envisioned solution to face this challenge and get a balance. Finally, conclusion and perspectives for future work are also drawn.**

***Keywords*—Safety-critical systems, ISO 26262, Swedish culture, documentation management, safety cases.**

I. Introduction

Safety standards (e.g. ISO 26262 [1]) define safety life-cycles to be adopted during the development of safety-critical systems. Typically, these life-cycles describe or prescribe: how to break down the work in order to develop the desired systems (i.e., breaking down the work into atomic units of work, e.g., steps or into composite units of work, e.g., phases, activities, etc.); the roles that should be involved, the work products that should be taken in input or should be produced in output, the methods to be adopted to perform the work.

Besides, safety life-cycles targeting the development, the standards also proposes/imposes guidelines for managing the hundreds of hundreds of documents. Managing the documentation represents a relevant activity especially in safety-critical systems engineering. The documentation process is usually tightly coupled with the development life-cycle. Life-cycle's work products represent immediate as well as direct evidence to be used during the safety assessment process to support the claims about system's safety [3]. More specifically, the left-hand side work products of the V-model (e.g., requirement specification) represent immediate evidence; while the right-hand side work products of the V-model (e.g., verification results) represent direct evidence. Improper documentation/evidence management may indirectly result in certification risk [3]. In the context of ISO 26262, for instance, the goal of the documentation process is to make documentation available: 1) during each phase of the entire safety lifecycle for the effective completion of the phases and verification activities; 2) for the management of functional safety, and 3) as an input to the functional safety assessment.

It should be noted that ISO 26262, which was released in 2011, can still be considered a new entry in the automotive domain. At the time being ISO 26262 addresses functional safety of electrical/electronic (E/E) and programmable electronic safety-related systems within road vehicles with a maximum gross weight of 3.5 tons. Heavy trucks are not yet contemplated by the standard. A new version of the standard is expected to be issued by 2018. Manufacturers of heavy trucks, however, are keeping a constant eye on the ongoing revision of the standard and they are strategically planning its timely adoption by 2018 [4], [5]. Gap analysis as well as alignment investigations are typically performed to identify necessary adaptations/changes to be introduced in order to reach a state of practice that can be considered compliant with the state of the art, represented by the standard. In some contexts, the adoption of ISO 26262 may result much more challenging than in others due to cultural background as well as agility-oriented mentality. In this paper, we focus our attention on one of such challenging context: the Swedish (due to its cultural specificity) and agility-oriented context. After having analyzed such context, we provide our solution proposal aimed at easing a smoothly introduction of ISO 26262 within such context.

The rest of the paper is organized as follows. In Section II, we provide essential background information. In Section III, we identify a true challenge related to documentation management. In Section IV we present our proposal aimed at reconciling the Swedish odd couple. Finally, in Section V, we present some concluding remarks and future work.

II. Background

In this section, we present the background information related to the problem space. In particular, in Section II-A, we recall ISO 26262 requirements in general and more specifically we focus on requirements related to documentation management. In Section II-B, we recall agile principles. In Section II-C, we present the current findings concerning the Swedish culture. Finally, in Section II-D, we introduce the Swedish and agile-oriented context at Scania.

A. ISO 26262-compliant documentation management

In this section, to make the paper self-contained, we recall essential information related to ISO 26262-compliant development life-cycle and documentation management. The intention is to let the reader realize the complexity of documentation management in the context of automotive safety-critical systems engineering due to the huge amount of work-products that are expected to be provided. The intention is also to let

the reader realize the necessity of roles and responsibility in the context of automotive safety-critical systems engineering.

ISO 26262 [1] is a functional safety standard that targets the automotive domain. This standard introduces safety integrity levels, called ASILs, which are specific for the automotive domain and requires the adoption of specific processes for developing the system, managing the documentation, qualifying tools, etc.. Thus, to develop an item in compliance with the standard, the development process shall be adopted and all the work-products shall be provided, including a safety case, which is supposed to progressively compile the work products that are generated during the processes. Similarly, the requirements concerning documentation management should be fulfilled. According to part 10.2 of ISO 26262, the documentation can take various forms and structures and tools can be used to generate documents automatically. In part 10 of the standard it stated that "the documentation process shall be planned in order to make documentation available. The documents should be: a) precise and concise, b) structured in a clear manner, c) easy to understand by the intended users, and d) maintainable". In part 10.4.4, it is stated that the structure of the entire documentation should consider in-house procedures and working practices. It shall be organized to facilitate the search for relevant information. The standard, however, is not fully rigid. Flexibility is allowed if properly introduced, i.e., via the application of tailoring rules [1]. Moreover, since the standard is a human creation and thus only perfectible but not perfect, it is likely that additional shortcomings, beyond those that have already been spotted, are present. Moreover a general consensus on its interpretation is not available yet [6], [7]. In part 6.4.2.1, it is also stated that a "project manager shall be appointed at the initiation of the item development". Once appointed, he/she shall ensure that the safety manager is appointed, who shall be responsible for the planning and coordination of the functional safety activities in the development phases of the safety process.

B. Agile documentation management

The agile manifesto is constituted of twelve principles [2]. These principles can be summarized by the following four slogans: 1) individuals and interactions over processes and tools; 2) working software over comprehensive documentation; 3) customer collaboration over contract negotiation; 4) responding to change over following a plan. From the above self-explanatory principles, we can infer that the agile way of working is radically informal and flexible.

C. Swedish (business/management) culture

The Swedish culture is characterized by some fundamental principles, which can be identified by a handful of interrelated keywords: consensus-based informal decision making, flat hierarchy, trust, team-focused leadership, fika. In what follows, we explain these keywords since we believe that to the uninitiated they might be unintelligible or misleading. Our explanation builds on top of research studies [8], [9], which were aimed at identifying and describing such principles. **Consensus-based informal decision making** - Each team-member is expected to express his/her opinion on what product to make and how to make it. Each team-member is typically considered as a critical resource for market know how. Top-down imposition of decisions are typically considered dysfunctional for working well-being. **Flat hierarchy** - A semi-democracy characterize the working places. Distributed control replaces centralized and vertical control. **Trust** - Juniors are expected to feel responsible and act. Seniors are expected to abstain themselves and coach and delegate. Trust replaces command and control. **Team-focused leadership** - Formal leaders are expected to empower the team. Their role is not to be dominant. They should inspire and set examples. They should never override others' responsibility. **Lagom** - this Swedish term can be translated in English as moderation. "Lagom"may imply that the employees take care of each other' s well-being and resist managerial pressures by conforming to this cultural norm [10].

These main keywords are then made cohesive via another one: **fika**. Fika is a Swedish term that denotes a recreation time-slot that Swedish employees introduce twice a day. A fika is supposed to be spent collectively in order to strengthen the team. During a fika, employees share time and space, practice the art of behaving lagomly, build trust among each other via conviviality, and, as a consequence, enable the creation of flat hierarchy, where team-focused leadership becomes natural. This amalgam of keyword permeates the Swedish society and functions in homogeneous contexts, where people share the cultural background. As investigated in the previously cited studies, when Swedes have to co-work with non-Swedes, some adaptations and negotiations are needed.

D. Safety culture and state of practice at Scania

Scania is a major Swedish automotive industry manufacturer of commercial vehicles - specifically heavy trucks and buses. Scania develops, manufactures and sells trucks with a gross vehicle weight of more than 16 tonnes intended for long-distance haulage, regional, and local distribution of goods, as well as construction haulage. Scania's bus range is concentrated on bus chassis, intended for use in tourist coaches, as well as urban and intercity traffic. Both trucks and buses are classified in typed series and characterized by various variations. From a management point of view, Scania fully incorporates the Swedish management style introduced in Section II-C. On one page of Scania's website [11], for instance, we can read: "Respect for the individual means recognizing and utilising each employees knowledge, experience and ambition in order to continuously improve and develop working methods. Inspiration and new ideas are born out of day-to-day operations. This helps ensure higher quality, efficiency and job satisfaction." At Scania, imposed processes, assigned jobs, and status rather than merit are not welcome. Roles are weakly defined and destructive interference is carefully avoided. Concerning quality, Scania states "Elimination of all forms of waste is the way Scania can ensure that all deliveries meet the expectations of demanding customers. Deviations from targets and standards are used as a valuable source of continuous improvement in Scanias processes." [11]. This statement is clearly in line with the agile manifesto.

III. A TRUE CHALLENGE

The background has set the stage and introduced the main characters and their context. From the background,

we have learnt that documentation management is perceived in an almost opposite way from the agile-community and the safety-standard community. In the context of automotive safety-critical software engineering, these two communities necessarily come together. However, given their opposite way of working, these two communities represent an odd couple. When this couple lives in Sweden, reconciliation of and negotiation within these two communities represent a true challenge. As we can retrieve from the background, the Swedish culture and the agile manifesto exhibit some similarities. For instance, the agile slogan "Individuals and interactions over processes and tools" is related to the Swedish trust and flat hierarchy. Introduction of specific roles, conflicts with the coaching and team-based leadership style.

IV. Soft and hard pieces of solution

In this section, we present our solution which comprises soft and hard pieces. Both pieces borrow from OSLC (Open Services for Lifecycle Collaboration). Thus, to let the reader follow the discussion, first of all, in Section IV-A,we recall basic information on OSLC. Then, in Section IV-B, we present the soft piece of our solution, while the hard piece is presented in Section IV-C. These pieces of solution are being developed in the framework of two ongoing projects: Espresso and Gen&ReuseSafetyCases. Espresso [12] is aimed at building a Scania-specific model-based solution aimed at making documentation management more efficient and more aligned to ISO 26262. To reach its goal, Espresso will benefit from the cooperation with Gen&ReuseSafetyCases [13]. Gen&ReuseSafetyCases is aimed at proposing Scania-specific solutions for enabling model-based self assessment via safety case generation in compliance with ISO 26262.

A. OSLC

OSLC is a standard that targets tools used during a product's life cycle and enables their integration and interoperability. OSLC 3.0 [14] is the current version of OSLC. Tools for requirements engineering, design, implementation, etc. are expected to interoperate in a traceable manner i.e. traceability between the respective work products can be easily retrieved and shown. To enable interoperability, different specifications, called *domains*, need to be provided. Requirements Management domain (RM) represents a sample of these domains. OSLC builds on top of Linked Data [15], Resource Description Framework (RDF) [16], and HTTP protocol. Each work product is described as an HTTP resource, identified via a Uniform Resource Identifier (URI). Work products are manipulated via HTTP methods (i.e., GET, POST, etc.). To interoperate via a work product, a tool that acts as a provider has to associate an URI to the work product and post it; a tool acting as consumer can get the work product via the URI.

B. Soft piece of solution

The soft piece of solution focuses on cultural and management aspects and consists of a negotiation and reconciliation strategy compatible with the Swedish environment. Since agility-oriented (documentation) management can hardly coexist with the ISO 26262-compliant (documentation) management, trade-offs are needed. Our soft piece of solution is aimed at triggering the employee's sense of responsibility and consequent participation in establishing trade-offs to be implemented in the hard solution.

As we have recalled in Section II-A, ISO 26262 is under revision and a consensus concerning its interpretation is still to be achieved. We believe that these undefined circumstances are favorable and may constitute a fertile soil to align employees towards a common strategy: achieving a Scania interpretation of ISO 26262, jointly with safety assessors, in order to comply with the standard in an agile manner, i.e. complementary extension of the current state of practice. The idea is to build an ISO 26262-compliant, semantic, and distributed-but-interconnected Scania management. Figure 1, adapted from the original OSLC figure [17], gives an intuition of the ISO 26262-compliant Open-minded Teams for Lifecycle Collaboration. In line with the Swedish management style, teams will keep their autonomy. However, interoperability will be enabled in order to identify and address cross-team needs. According to Note 1 in part 6.4.3.1, the safety manager can delegate tasks to persons that possess the required skills, competences and qualifications. Already in place team leaders will be trained with respect to ISO 26262. Teams, working at different abstraction levels will take the responsibility to choose appropriate ways to comply with the standard according to their current way of working. Their responsibility entails the selection of process elements with the adequate ASIL-related stringency (i.e., activities and associated methods and tools (if any) as well as work products). To maximize agility and stick to the current Scania management, lagomly the just enough number of work products will be provided. ISO 26262-compliant tailoring will be applied under the supervision of safety assessors in order to identify allowed minima. Tool-supported techniques will be privileged with respect to manual techniques in order to increase automation and enable semi-automatic generation.

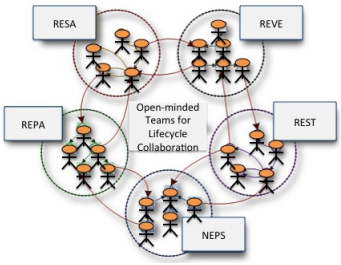

Fig. 1. Open-minded Teams for Lifecycle Collaboration.

C. Hard piece of solution

Once cultural and managerial aspects are reconciled via establishment of trade-offs, the hard piece of solution may focus on the infrastructure for documentation management. More specifically, the solution consists of a Scania-specific model-based development aimed at integrating current and future in-house/off-the-shelf/outsourced ISO 26262-compliant tools within an interoperable tool-chain satisfying Scania purposes and requirements, including scalability. To make the tool-chain interoperable, we intend to adopt OSLC and create a family of interoperable tools that support all phases of the product lifecycle, via the exploitation of the OSLC-related family of core web service specifications plus Scania-specific OSLC-compliant domains. We opt for OSLC since, as stated by

Biro [18], "it has the potential to have a determining impact on the future of software process compliance" and we believe that this potential is for any process compliance, including documentation management related to the item development. We also believe that in terms of the so called 'Hype-cycle", OSLC will reach the plateau of productivity phase. The intermediate-term goal is to explore real feasibility concerning large-scale tool integration. The long-term goal intention is to make this tool-chain available to enable cooperation throughout the supplier-manufacturer chain.

Within ESPRESSO, the current Scania documentation (mainly in .docx and .excel-based format) should be converted into machine-representable or even better machine-understandable Linked Data [15] (more precisely, RDF-based data formats [16]) to be consumed/provided within the OSLC-based documentation/development management tool-chain. At the time being, only a portion of the tool-chain is implemented. A tool called Requirements Specifier (RS), for instance, permits requirements engineers to specify requirements at each level of the ISO 26262-compliant hierarchy. Thus, Safety Goals (SGs), Functional Safety Requirements (FSRs), Technical Safety Requirements (TSRs), Hardware and software requirements (HSRs and SSRs) are supported. RS implements the notion of contract structure proposed by J. Westman et al [19]. RS is expected to provide URI-tagged resources based on ISO 26262-compliant and Scania-specific RM domain. Assumed that safety goals are formulated to avoid unreasonable risk, this traceable and hierarchical requirements structure can be used for arguing about absence of such risk [4]. Within Gen&ReuseSafetyCases, to generate such arguments, we build upon model-based safety certification ideas developed by I. Sljivo et al [20] and by B. Gallina [21] and we develop a tool for safety case creation. In principle the safety case creator should generate the safety case representation by consuming interrelated work products, which constitute immediate, direct, indirect evidence as well as (a)tomic goals. To argue about process compliance, ISO 26262-compliant process information can be inferred via the interconnected work products. Thus a process is not imposed from the top but is obtained bottom-up semi-automatically. By doing so, we can avoid the introduction of additional hierarchical human roles and thus flat hierarchy is preserved. The unique safety manager will be replaced by a safety case generator, which will consume and compile the work performed by the different teams according to thoroughly specified generative rules. The tool-chain is expected to guarantee the availability/searchability/maintainability of the documents as well as enhanced precision and structure as required by ISO 26262, part 10. Finally, semi-automation is expected to save time and thus reduce waste, in line with the agile practices within Scania.

V. Conclusion and Future Work

In this paper, we have presented a true challenge: ISO 26262-compliant documentation management in agility-oriented Swedish context. After having introduced a broader perspective on the challenge, we have reported our finding within Scania. Then, we have proposed our OSLC-based soft and hard solution to contribute in facing such challenge and our research agenda towards the concretization of our solution.

Acknowledgments: This work has been partially financially supported by the Swedish Foundation for Strategic Research via the SSF Gen&ReuseSafetyCases project [13] project and the Vinnova Espresso [12] project. We also thank C. Mattila.

References

[1] ISO26262, "Road vehicles Functional safety. International Standard, November," 2011.

[2] Agile Manifesto, "http://agilemanifesto.org."

[3] S. Nair, J. de la Vara, A. Melzi, G. Tagliaferri, L. de-la Beaujardiere, and F. Belmonte, "Safety evidence traceability: Problem analysis and model," in *Requirements Engineering: Foundation for Software Quality*, ser. Lecture Notes in Computer Science, C. Salinesi and I. van de Weerd, Eds. Springer International Publishing, 2014, vol. 8396, pp. 309–324.

[4] R. Dardar, B. Gallina, A. Johnsen, K. Lundqvist, and M. Nyberg, "Industrial experiences of building a safety case in compliance with iso 26262," in *IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 2012, pp. 349–354.

[5] B. Gallina, A. Gallucci, K. Lundqvist, and M. Nyberg, "VROOM & cC: a Method to Build Safety Cases for ISO 26262-compliant Product Lines," in *SAFECOMP 2013 - Workshop SASSUR (Next Generation of System Assurance Approaches for Safety-Critical Systems)*, M. ROY, Ed., Toulouse, France, Sep. 2013, p. NA.

[6] 5th International Conference on ISO 26262, "http://www.iso26262-conference.com."

[7] M. Ellims and H. Monkhouse, "Agonising over asils: Controllability and the in-wheel motor," in *7th IET International System Safety Conference, Edinburgh, UK*, 2012.

[8] M. Salminem-Karlsson, "Swedish and indian teams: Consensus culture meets hierarchy culture in offshoring," in *Proceedings of the 7th European Conference on Information Systems Management and Evaluation*, ser. ECIME. Academic Conferences Publishing, 2013, pp. 147–154.

[9] P. Isaksson, "Chinese views on swedish management- consensus, conflict-handling and the role of the team," VINNOVA Swedish Governmental Agency for Innovation System, Tech. Rep. vR 2009:33, 2009.

[10] S. M. B. Wieland, "Struggling to manage work as a part of everyday life: Complicating control, rethinking resistance, and contextualizing work/life studies," *Communication Monographs*, vol. 78, no. 2, pp. 162–184, 2011.

[11] Scania-strategy, "http://www.scania.com/scania-group/strategic-platform/."

[12] VINNOVA, 2011-04446-ESPRESSO, "http://www.vinnova.se/sv/resultat/projekt/effekta/espresso/."

[13] Gen&ReuseSafetyCases-SSF, "http://www.es.mdh.se/projects/393-genreusesafetycases."

[14] Open Services for Lifecycle Collaboration, "http://open-services.net/wiki/core/specification-3.0/."

[15] Linked Data, "http://www.w3.org/designissues/linkeddata.html."

[16] RDF Primer, "http://www.w3.org/tr/rdf-primer/."

[17] OSLC Community - open-services.net, "Oslc diagram."

[18] M. Biro, "Open services for software process compliance engineering," in *SOFSEM 2014: Theory and Practice of Computer Science*, ser. Lecture Notes in Computer Science, V. Geffert, B. Preneel, B. Rovan, J. tuller, and A. Tjoa, Eds. Springer International Publishing, 2014, vol. 8327, pp. 1–6.

[19] J. Westman and M. Nyberg, "Extending contract theory with safety integrity levels," in *High Assurance Systems Engineering (HASE), 2015 IEEE 16th International Symposium on*, Jan 2015, pp. 85–92.

[20] I. Sljivo, B. Gallina, J. Carlson, and H. Hansson, "Generation of safety case argument-fragments from safety contracts," in *The 33rd International Conference on Computer Safety, Reliability and Security*, ser. LNCS, vol. 8666. Springer-Verlag, 2014, pp. 170–185.

[21] B. Gallina, "A model-driven safety certification method for process compliance," in *2nd International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), joint event of ISSRE 2014*, November 2014, pp. 204–209.