Safety Implications Concerning Usage of Tools in Complex System

Rafael Augusto, Nuno Silva

▶ **To cite this version:**

Rafael Augusto, Nuno Silva. Safety Implications Concerning Usage of Tools in Complex System. Fast abstracts at International Conference on Computer Safety, Reliability, and Security (SAFECOMP), Sep 2016, Trondheim, Norway. hal-01370199

HAL Id: hal-01370199
https://laas.hal.science/hal-01370199

Submitted on 22 Sep 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Safety Implications Concerning Usage of Tools in Complex System

Rafael Augusto, Nuno Silva
ASD-T Safety Engineering
Critical Software
3045-504 Coimbra, Portugal
hraugusto@criticalsoftware.com, nsilva@criticalsoftware.com

***Abstract*— Integration of tools and configuration data is nowadays present in all railway systems and plays a central role in functionality, flexibility and the safety of railway systems. This paper aims to present the challenges and the importance of tools, the configuration data integrity and the toolchain definition in the design of railway systems safety. We focus on the relevant implications on the safety analysis and safety assurance of such systems. Two examples of the usage of tools and strategy to assure safety are presented here.**

Keywords—toolchains, configuration data, safety, SIL

I. INTRODUCTION

The demands of more complex, larger, more flexible and safer railway systems are currently a challenge for the industry. There is a growing need to serve more passengers, especially in the suburban areas, and to provide a more flexible movement of freight trains as more business models rely on them for fast and reliable delivery. General technological breakthroughs in hardware and software engineering have opened up a new world of possibilities, both in operations (higher train frequency, ERTMS and Automatic Train Operation (ATO)) as in new on-board services for passengers. All these aspects contributed for the need to develop increasingly larger and more complex systems that rely on the use of toolchains and configuration data and both these subjects are covered nowadays by the CENELEC standards (e.g. EN50128 [1]).

The use of tools influences the safety assessment programme and the overall product safety analysis strategy. The integration of a tool that deals with configuration into a system with a specific Safety Integrity Level (SIL) raises the question around the relationship between the tool and the overall safety of the system. On the other hand, when relying on configuration data, one must ensure the required safety integrity of the data before integrating it into the system and the safety impacts of the configuration data on the overall system safety.

II. SAFETY IMPLICATIONS OF CONFIGURATION DATA AND TOOLCHAINS

Section 6.7 of the European CENELEC standard EN50128 [1] approaches tools, defining it as following (clause 6.7.1):

The objective is to provide evidence that potential failures of tools do not adversely affect the integrated toolset output in a safety related manner that is undetected by technical and/or organisational measures outside the tool. To this end, software tools are categorised into three classes…

According to EN50128 clauses 3.1.42 to 3.1.44, the classes that define tools are:

- **T1** - Generates no outputs which can directly or indirectly contribute to the executable code (including data) of the software. (ex: Text editor or requirement/design tool (no code generation capabilities); configuration control)
- **T2** - Supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software (ex: Test harness generator; test coverage measurement: static analysis)
- **T3** - Generates outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system (ex: Source code or data/algorithms compiler; tool to change set-points during system operation; compiler that incorporates an executable run-time package)

This means that the nature of the tools will determine the applicable safety assessment and methods as well as the EN50128 [1] sub-clauses applicable to the tool development and assessment. This assumption distinguishes the tools from the Safety Integrity classification attributed to a system. According to clause 6.7.1, a tool can be safely integrated in a system "*…if an argumentation on the integrity of tools output is given and the integrity level of the software is not decreased…*".

According to this clause, is not mandatory that a given tool is bound to the SIL of the system it supports. Rather, a safety argument which proves that the tool does not decrease or impacts negatively the integrity level of the systems must be provided assuring safety integrity at the level of the interface (data produced or input signal) with the system. In fact, the tool itself can be designed and implemented with no relation to a determined SIL (or even limitations/requirements imposed by standards), as long as the data or signals generated by the tool do not compromise the defined safety integrity level of the system it is integrated in.

III. Tools and Toolchains Safety

Fig. 1 shows an example of a system implemented to meet a SIL4 target that integrates two tools in its overall design, one to generate configuration data and another to support system operation.

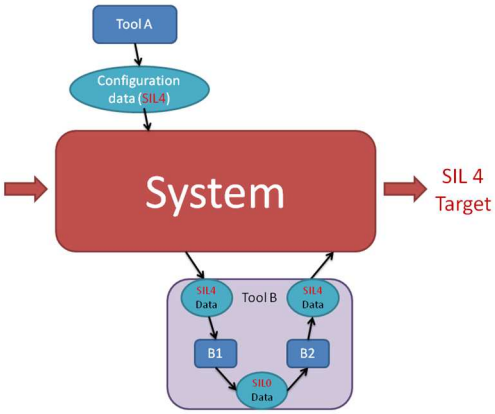

Fig. 1. SIL4 system with tools integrated

Tool A enables the definition of configuration data for a specific deployment of the system. Configuration data aims to represent the physical infrastructure of a network. This is used to allow a system to be deployed or updated in different circumstances and environments (for example when specifying a generic product) without changing the inner design or implementation. Different models of data can be used: Physical, Operational or Planning [4]. Some examples of configuration data used in railway systems include zones of control for Control & Display, routes for Interlocking and balise telegrams for Automatic Train Protection (ATP).

As Tool A is a class T3 tool, one direct way to assure that related EN50128 [1] clause 6.7.4.4 is accomplished is to guarantee that the output produced by the configuration tool is compliant with SIL4. The data can be directly integrated in the system without risking compromising the final target safety integrity. In order to comply with the required target SIL, the data produced by the tool shall be compliant with SIL4. In the example presented this is achieved by designing and implementing the tool itself to be compliant to SIL4.

Tool B processes a signal from the system and returns the processed output back to the system. This interaction can happen in real-time or during installation or maintenance. An example of this is a tool that provides timetable recalculation to address delays on operation, automatically or by human operator intervention.

In terms of showing compliance of the interface with the overall system, Tool B exemplifies a more delicate case where the tool itself is not designed as SIL4 compliant, neither in its architecture and design nor in the data it produces. In this case the solution was to transform Tool B into a toolchain composed by tools B1 (SIL0 with the tool core functionality) and B2 (detached from the core functionality, with the single purpose of producing a SIL4 interface with the system). When it comes to safety integrity in the integration on a system, both tools and toolchains can be approached with the same view: the focus should be to guarantee the safety integrity level of the output produced and not of the tool itself.

It is very important to note at this point that, for either examples Tool A or Tool B, the assurance that the output is compliant to SIL4 does not mean that the tool itself is also covered by this compliance. In the case of toolchain B, the tool B1 with SIL4 classification is positioned to process the output data which facilitates the argumentation that the data produced is SIL4 compliant and may lead to improperly classify the entire toolchain with the same SIL. In all cases, sufficient evidence must be provided to assure that the integration of the toolchain in the system does not compromise the final safety integrity.

IV. Conclusion

This paper presented the implications on the safety analysis of a system that integrates tools, toolchains and configuration data in its overall design. The considerations of the standard EN50128 [1] regarding the specific use of tools were referenced alongside the definition of what a tool is and how it is classified. It was shown that tools can be integrated in a system with a required target SIL as long as the output interfacing with the overall respects the same SIL. This can be achieved by the effective definition of a toolchain that guarantees that, regardless of the design of the functional tools, the generated output to feed the system meets the expected safety integrity.

The following steps could be done in the future in search of a more standardised approach to the problem:

- Definition of an effective toolchain: for each complex system, chances are high that tools will be used. An early definition of a toolchain and its system's interface definition will facilitate the integration of tools through it. The toolchain and its interface requirements can be part of the safety assessment programme from the start and avoid later last minute search for solutions;
- Standards improvement: currently there are no considerations on railway EN standards [1] [2] [3] that refer specifically to configuration data. As with tools, configuration data is a component of railways systems with its own safety implications and should have a set of dedicated clauses.

References

[1] CENELEC CEI EN 50128 - Railway Application – Communications, signalling and processing system. Software for railway control and protection system, July 2011

[2] CENELEC CEI EN 50126 – 1/2/3 - Railway Applications, The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999

[3] CENELEC CEI EN 50129 - Railway applications - Communication, signalling and processing systems. Safety related electronic systems for signalling, 2003

[4] Felix Redmill & Tom Anderson, "Components of system safety", Proceedings of the Tenth Safety-critical Systems Symposium, Southampton, UK, 6 December 2012