# RAS Working Group meeting 07.10.2021

**Participants:** A. Apollonio, A. Asko, P. Bell, E. Blanco Vinuela, J. Bodingbauer, H. Boukabache, M. Brucoli, T. Cartier-Michaud, K. Ceesay-Seitz, M. Chioteli, G. Daniluk, S. Danzeca, L. Delprat, Y. Donon, L. Felsberger, B. Fernandez Adiego, E. Fortescue-Beck, P. Gkountoumis, P. Jursco, S. Kaufmann, A. La Rosa, T. Ladzinski, I. Lopez, N. Magnin, S. Ramberger, M. Sosin, B. Todd, J.-C. Tournier, N. Trikoupis, F. Waldhauser

The slides are available on Indico:

https://indico.cern.ch/event/1081108/

## *Introduction to RASWG activities - Speakers: Andrea Apollonio (CERN), Benjamin Todd (CERN)*

A. Apollonio introduced the new RASWG by presenting a brief history of previous related working groups and forums, explaining the new RASWG mandate and composition, as well as potential synergies with other forums. He concluded by a list of open questions for the RASWG community.

**Questions and Discussion after the Presentation:**

S. Kaufman commented that his section (BE-CEM-EPR) is mainly concerned with the manufacturing of PCBs and asked whether these topics will be treated in the new RASWG. A. Apollonio confirmed that this will be included in the new RASWG, although it was less addressed in the past. P. Jursco added that outsourcing and manufacturing is partially within his domain and the work done with inforEAM.

Regarding the second bullet point of the second paragraph on slide 13, B. Fernandez Adiego asked whether the risk evaluation scale includes a definition of tolerable risks on a global CERN scale, which could be carried out within the RASWG. A. Apollonio answered that the slide was referring specifically to the developed risk assessment for the consolidation project, but that in general the RASWG should be the place to discuss the approach for risk assessment also for CERN machines and experimental facilities.

H. Boukabache stated that he sees a clear link between automated fault recording, machine learning (ML) and predictive maintenance. A. Apollonio agreed that these are very important topics going forward, but explained that at the moment fault tracking is done in a manual way. Automated fault tracking is in place for SPS (Big Sister) and is being studied for LINAC4. It is very useful for short faults, which would otherwise require a lot of manual logging effort.

P. Bell asked to have access to the electronics design checklist. B. Todd explained that currently two versions exist and it is an ongoing effort to merge them into a single one. One checklist was shared by G. Daniluk (https://ohwr.org/project/ed/wikis/schematics-checklist ) and one by B. Todd (https://edms.cern.ch/document/2002392 ).

E. Blanco Vinuela asked A. Apollonio to elaborate on the third paragraph on the system testing strategy and whether it is exclusively aimed at electronics. A. apollonio replied that the aim is more general, as some systems – non necessarily electronics – are tested and are subject to so-called reliability runs (e.g. the LHC beam dumping system). For electronics specifically, BE-CEM is interested in developing a the testing service for electronic systems in the future, so this topic is of great relevance. The idea would be that the RASWG can work on standardized recommendations for the tests to be carried out depending on the criticality of the system, not exclusively aimed at electronics. E. Blanco Vinuela added that it will also be interesting from a software and controls perspective and that it will be important to stay in touch with the other forums on these topics, which Andrea agreed to.

B. Todd concluded that there is an interesting difference between safety and machine protection approaches and that he expects a cross fertilization from bringing these two viewpoints together. Furthermore, he added that he expects synergies with the ML forum as, for example, EPC has reached diminishing returns from applying 'traditional' reliability improvement efforts.

## *Discussion on Formal Methods and Verification in the RASWG - Speakers: Borja Fernandez Adiego (CERN), Enrique Blanco Vinuela (CERN), Hamza Boukabache (CERN)*

Before the talk, E. Blanco Vinuela explained the context of the presentation. They have been using formal methods for testing and verification on critical equipment for six to seven years with a focus on PLCs. They have reached maturity in applying these methods to systems and would like to both capitalize on this experience and share it with other groups interested. He discussed in which forum this would be best possible, and the quality assurance forum within ATS was suggested. However, they were only interested in standardized established procedures, so this might apply in a second stage. Hence, they are evaluating the interest to join the RASWG and reach out to colleagues in the community. The following talks by B. Fernandez Adiego and H. Boukabache shall give an impression what they are doing and should lead to a discussion whether their work really fits within the RASWG.

B. Fernandez Adiego gave a high level introduction to formal verification methods and their 'toolbox' PLCverif, which should hide the complexity of formal verification for the user. He pointed out that random failures need stochastic methods and systematic failures need deterministic methods. Formal verification is part of the deterministic methods and the intersection of formal and verification methods. The advantage of

formal verification methods over (stochastic) simulation methods is that they can handle much more system states.

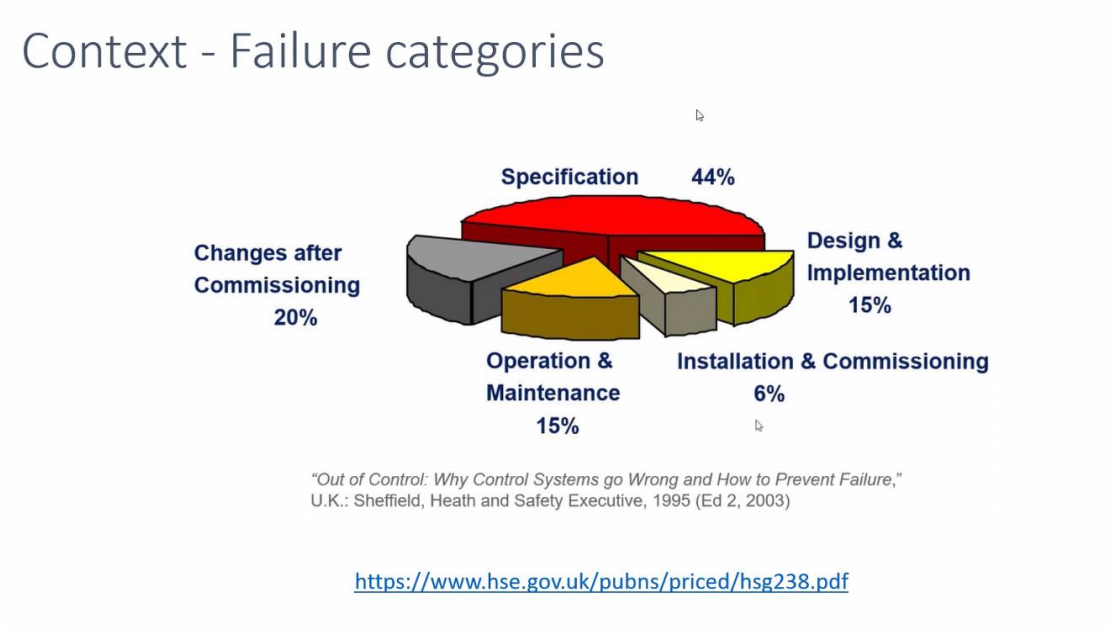
H. Boukabache presented their formal verification approaches that were used for the CROME devices. He explained that the workflow of formal verification is simple but that clear system specifications are difficult to develop and obtain. He added that formal verification allows to define system target states and whether these states can be reached. He pointed out that formal methods need to be complemented by a range of other methods, such as stochastic methods.

**Questions after the presentations:**

B. Todd commented that the application of these methods is dependent on the quality of system specifications, which is not always easy to pursue at CERN.

E. Blanco Vinuela commented that system design without specification is a key to disaster. Without specification one risks iterating in rounds without progress and recommends defining specifications for a big majority of systems. B. Todd confirmed that for many projects there are continuously features to be added.

B. Fernandez Adiego added that a study has found that 44% of faults originate in system specification (see image below).




H. Boukabache replied that they started following much more structured approaches. Even with these, some issues were later figure with to formal methods.

H. Boukabache concluded that a way to support the development of correct specifications from the beginning should maybe be defined even beyond safety critical systems.

B. Todd asked whether it makes sense to carry out formal analysis on parts of a system.

K. Ceesay-Seitz replied that she did it and that already the review of requirements and specifications revealed many insights.

B. Fernandez Adiego commented that a good specification doesn't always need to be formal. However, thinking about adding formal methods for parts of the system should certainly help avoiding problems.

A. Apollonio replied that a link to a generic criticality definition can help choosing where to apply formal methods within a system.

E. Blanco Vinuela and S. Kaufmann pointed out that when projects are outsourced, specification and quality control are essential and equally important to system design.

E. Blanco Vinuela stated that people across CERN expressed the need for guidelines to follow based on the criticality of a system.

N. Magnin confirmed that in ABT there is interest and need for formal verification methods.

E. Blanco Vinuela concluded that to identify the matching between formal methods and the RASWG he will ask B. Fernadez Adiego and H. Boukabache to elaborate on the inputs received during the meeting and then discuss again with the RASWG representatives.