RAS Working Group meeting 09.12.2021

Participants: A. Apollonio, A. Asko, P. Ariel Alvarez, T. Barbe, P. Bell, D. M. Belo Freire De Carvalho, R. Berberat, M. Bes, W. Bialas, S. Blanchard, E. Blanco Vinuela, A. Boccardi, J. Bodingbauer, H. Boukabache, M. Brucoli, A. Byszuk, E. Calvo Giraldo, T. Cartier-Michaud, K. Ceesay-Seitz, J. Cortes, G. Daniluk, I. Degl'Innocenti, M. D. M. Gomez-Jordana Manas, L. Delprat, M. Dolent, J. Emery, L. Felsberger, B. Fernandez Adiego, C. Fluder, E. Fortescue-Beck, G. Foucard, F. Ghawash, T. Gingold, P. Gkountoumis, J. L. Gomez Costa, E. Gousiou, R. K. Grimmer, F. W. Hoguin, J. J. John, P. Jurcso, M. Kalinowski, A. La Rosa, D. Lampridis, I. D. Lopez-Miguel, M. Lupi, M. Marin Rodrigues, C. Martinez, R. Mompo, D. Monteiro, K. J. Motala, P. Peronnard, D. Perrin, T. Podzorny, A. Pulli, S. Ramberger, B. Schofield, R. Secondo, J. Serrano, A. Siemko, J. Steckert, L. Strobino, B. Todd, J.-C. Tournier, A. Tovar, N. Trikoupis, J. Uythoven, S. Uznanski, W. Viganò, A. Zmuda

The slides are available on Indico:

https://indico.cern.ch/event/1103063/

The meeting has been organised as a joint meeting between the Electronics Community Forum, the Industrial Controls Community Forum, and the RASWG of the ATS sector. Two presentations were given on the topic of formal methods and verification:

Introduction to formal methods and an Industrial Controls use case - Speaker: B. Fernandez Adiego

B. Fernandez Adiego presented an introduction to Formal Methods and Verification (FMV) which at CERN started to be applied in the HSE-RP and BE-ICS groups. FMV are techniques and measures to identify and mitigate systematic failures in a design ranging from the formal specification of a system to the formal verification of the design. In the framework of the RASWG one objective is to build a CERN formal methods community, see last slide of the presentation for the egroup and more information. On slides 15 to 19 B. Fernandez Adiego introduced a formal verification tool developed by BE-ICS which can be used for PLC programs: *PLCverif*. This model checking tool is able to verify whether the created formal model of the specific property meets the formal requirement. Additional documentation for *PLCverif*, as well as *PLCspecif*, a tool for formal specification of PLC programs, can be found under:

https://readthedocs.web.cern.ch/display/ICKB/PLCverif

https://readthedocs.web.cern.ch/display/ICKB/PLC+formal+specification

A digital electronics design use case and general conclusions – Speakers: K. Ceesay-Seitz, H. Boukabache

H. Boukabache and K. Ceesay-Seitz presented an HSE-RP use case of a design applying FMV in parallel to simulation/emulation, and prototyping with according tests. H. Boukabache pointed out, that all these methods need to be used in a complementary way. For the CERN RadiatiOn Monitoring Electronics (CROME) with its safety-critical FPGA and mixed signal ASIC H. Boukabache, K. Ceesay-Seitz, and their team applied an entire verification methodology which includes FMV to verify the design by individual blocks. This enabled to find and remove 33 faults.

Questions and discussion after both presentations:

W. Viganò asked how the users themselves can be modelled by such an approach. For example an operator who is enabled to modify certain things of the system. B. Fernandez Adiego replied that for PLCs operators send configurations or commands which are to be executed. This can be modelled as a non-deterministic variable that the operator is enabled to take any such action. There would be for example 2 variables which may come from the operator. It can be modelled that these variables are non-deterministic. K. Ceesay-Seitz added, that in their case all potential input combinations are considered. Therefore, whatever the user may do is covered and verified that the device behaves as it should.

W. Viganò asked what would be the case if the system is in a stressed condition which would exceptionally give certain people an authorization to intervene. K. Ceesay-Seitz replied that this would rather be a security concern about who is allowed to operate the system. B. Fernandez Adiego added, that also safety constraints can be included in the model. The model would identify a violation of the set property.

A. Pulli asked if the model checker has been used to check for random failures. B. Fernandez Adiego replied, that there are other techniques which may fit better for such a purpose. Nevertheless, for example probabilistic model checking can be used in such a case. H. Boukabache agreed and added that random failures can better be checked with a process approach, which means performing a quality process, reviews and other such methods. Both such approaches should be combined. A. Apollonio added, that there are systematic ways to find potential failures, e.g. an FMECA. In addition, a probabilistic simulation can be added which can take more states into account, complementing the approach.

J. Uythoven asked about the SPS system verification study, whether it is finished and if there is any documentation available, regarding a currently ongoing collaboration with GSI for their access system. B. Fernandez Adiego pointed to a paper and documentation linked on the presentation slides. He does believe that this can be used for the GSI access system. In their case, the result was that the model checking helped them to define a better specification. Model checking helped to find specification

deficiencies and to push themselves to write better specifications. J. Uythoven agreed that writing specification is a crucial point.

A. Apollonio asked about the size of the overhead when applying such methods. H. Boukabache replied that he does not think that there is a big overhead. There is however a certain learning curve to be followed. One can find bugs with very few knowledge, but probably not as many as if one is an expert. He points out that it is not very complicated to apply the methods and that the time investment is worth it in his opinion. K. Ceesay-Seitz added, that especially when using automated tools, their set up is rather easy. Getting first results is basically learning the language. The full proof of a system however requires more time investment. B. Fernandez Adiego added that if tools are available that take directly the HDL design, it is not necessary to create the models, since this is automatically done by the tool. For their PLC project it has been a big investment, because the models had to be created by themselves. H. Boukabache agrees, that in their case tools were available. He adds, that experience matters a lot and that for every use case one has to have a strategy.

T. Podzorny asked if it is planned to summarise some highlights as a follow up for the community. B. Fernandez Adiego suggested to send around a mailing list to follow up after the meeting. → See added last slide of his presentation

S. Uznanski asked if there is anything that can be set up so other teams can use the tools in an easy way. Such as a tool which takes the design, creates the model and generates the result. K. Ceesay-Seitz replied that commercial tools are generally easier to set up, but that licensing is an issue. S. Uznanski wondered if there are synergies and if we could look into open source solutions as a follow up. B. Fernandez Adiego mentioned that there are also open source tools for FPGAs.

A. Pulli pointed out that formal verification is only as good as the defined requirements. Often times the requirements are only in someone's head. H. Boukabache said that in their case they had precise requirements from the beginning of the project. But it is true that without requirements one does not get very far. K. Ceesay-Seitz added, that the designer should define the requirements and that these should be reviewed by a requirements engineer. One can also use natural language properties and ask a system responsible how the system behaves to ensure that both parties have the same understanding. B. Fernandez Adiego added, that from his experience specification is the main source of problems. One could eventually start to define properties that the system has to respect. To get to the full and complete specification is a big challenge. One has to first find the right abstraction level. H. Boukabache pointed out that this discussion would be something to be carried out under the RASWG. It would be a topic of requirement engineering and system engineering. A. Byszuk added that one could also work with building blocks to divide the system, to which B. Fernandez Adiego replied that this is what they did.