# Simulation Assisted Automation Testing in Loviisa Nuclear Automation Renewal Projects

Miikka Jokelainen[1)], Emmanuel Foudrinier[2)]

1) Fortum Power and Heat Oy, Keilalahdentie 2-4, P.O. Box 100, 00048 Fortum, Finland (miikka.jokelainen@fortum.com)
2) Rolls-Royce Civil Nuclear SAS, 23 Chemin du vieux chêne, 38240, Meylan, France (EMMANUEL.FOUDRINIER.CN@Rolls-Royce.com)

**Simulation-assisted automation testing is an efficient tool for validating the automation systems for nuclear power plants. This paper presents how Fortum and I&C supplier Rolls-Royce have utilized Apros simulator in Loviisa nuclear power plant automation renewal projects. The experiences have shown that simulation assisted testing allows the discovery of design errors in an early stage and is more realistic, efficient and less time consuming than traditional test methods.**

***Keywords—Dynamic simulation; Integrated systems; Pre-engineering; Factory acceptance tests; Apros***

## I. Introduction

Simulation assisted automation testing has been extensively used during the Loviisa Nuclear Power Plant (NPP) safety automation renewal projects. Loviisa is VVER-440 type Nuclear Power Plant with two units, which started to produce electricity on 1977 and 1980. To ensure safe and reliable operation of the plants the critical parts of the automation have been renewed.

The first project called LARA was implemented in the years 2008 and 2009. The second project called ELSA was implemented during the annual maintenance periods in the years 2016, 2017 and 2018. The third project called LASU was implemented in 2021. Due to tight project schedule and broad scale of the renewals, utilization of efficient testing methods was a necessity. Due to these constraints and existing expertise at Loviisa NPP owner Fortum and I&C supplier Rolls-Royce decided to utilize Apros simulator extensively in the ELSA and LASU projects.

## II. Simulation model

The simulation model has been implemented in Apros simulation software and it consists of a 3D reactor model, over 60 primary and auxiliary process systems, a containment model, automation systems, and electrical systems as described by Meriläinen et al. (2021) [1]. The same model is used for operator training at the Loviisa plant. The simulation model is connected to several external automation systems and human-machine interfaces. The safety automation systems included are Areva's TXS and Rolls-Royce's Spinline. Both are represented by emulated automation software based on the same engineering data as the actual safety systems at the plant. They are connected to Apros as external model libraries to ensure tight synchronization with simulation model computation. Other automation systems consist of Siemens' T2000 system, which is connected to the simulation model via network, and a monitoring system (MS) to monitor the Spinline safety automation systems. The HMI of the simulator consist of the process computer system (PCS) as the main operating interface for the operator, a qualified display system (QDS) as a user interface to the TXS system and virtual panels.

The simulation control is achieved by Testing Station software which is used to give simulation commands to all simulator components, manage test runs and to collect the test data. The test cases are implemented as sequences which can be automatically run from the Testing Station.

## III. ELSA automation renewal project

The second automation renewal project at Loviisa was implemented during the annual maintenance periods in the years 2016, 2017 and 2018 with automation supplier Rolls- Royce. As part of the ELSA project the simulator was used intensively during the design and validation phases of renewed systems.

The renewed systems included the reactor trip with automatic and manual backup, neutron flux measurement, reactor power control, reactor power limitation, accident management, preventive actuation and indication systems.

### *A. Automation emulation*

In the ELSA project several system technologies were used. The safety classified systems have been produced with Rolls-Royce proprietary Spinline safety classified technology for digital systems or in hardwired technology. Some non-safety systems have used commercial programmable logic controllers (PLC). The objective of the simulation was to be able to model all systems regardless of their technology and to use the final software embedded in digital equipment.

Technologies have been emulated in a four level model. Figure 1 below illustrates the different layers. The first two levels (at the bottom) only applied to digital equipment.

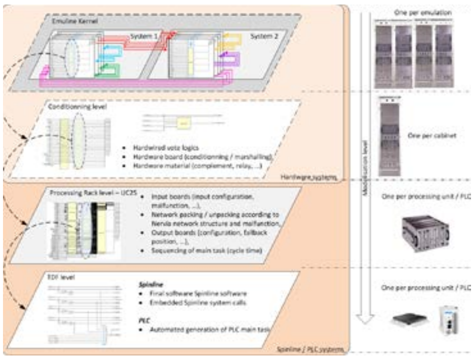
Emuline Kernel
System 1
System 2
One per emulation
Conditionning level
Hardwired vote logics
Hardware board (conditionning / marshalling)
Hardware material (complement, relay, ...)
One per cabinet
Hardware systems
Modelization level
Processing Rack level – UC25
Input boards (input configuration, malfunction, ...),
Network packing / unpacking according to Nervia network structure and malfunction,
Output boards (configuration, fallback position, ...),
Sequencing of main task (cycle time)
One per processing unit / PLC
EDF level
Spinline
Final software Spinline software
Embedded Spinline system calls
PLC
Automated generation of PLC main task
One per processing unit / PLC
Spinline / PLC systems

Fig. 1. Emulation layers

The first level corresponds to the software embedded in the equipment. For Spinline technology, the final software is used without modification. For commercial PLC, the simulated software and the final software (in the language of the supplier) are generated automatically from an interpretable description of the functional logic.

The second level models the processing carried out by the acquisition boards and operating systems. It is at this level that network packing/unpacking acquisition and generation of signals by the boards and the scheduling of the unit software are carried out. Models of boards and networks implement their functionality with their known failure modes. This allows testing degraded modes of systems in case of a failure of one of its component.

The third level emulates hardwired devices of equipment contained in cabinets. This can be the conditioning rack, hardwired votes, process of test and inhibition modes, etc. It is at this level that purely hardwired systems are modeled.

Finally on the top level, all the cabinets are interconnected. Network packets and hardwired exchanges are modeled.

### B. *Test case selection*

A systematic procedure for selecting test cases for simulation assisted automation testing is required to provide a traceable set of tests linked to the functional architecture of the plant and cover the functionalities of the tested automation system.

As described by Tikkala et al. (2017) [2] the selection and creation of test cases consisted of two procedures: selection of events for testing and test case creation. The selection procedure aims at choosing test cases for automation tests in a traceable manner. That is, a justification for each test case can be tracked. The test cases were then created by first verifying the model scope and creating a simulation sequence to launch the automation function. If the test results are acceptable, the test case was approved for testing the automation system. Otherwise, corrections either to the test sequence or the process model were made.

### C. *Basic design phase*

During the basic design phase the testing started right after first versions of software logics were sketched. Existing plant model and modelled existing automation logics made it possible to dynamically test the new automation software logics in early phase with the valid plant process model with the existing and remaining automation systems.

The automation was modeled in detail to attain reference test data for the dynamic tests with emulated and real automation systems in later phases. The plant behavior in the tests was evaluated by the operators of the Loviisa NPP.

### D. *Detailed design phase*

In detail design phase emulations of the new automation systems were integrated to the simulation model. The same test cases that were used during basic design were repeated with the emulations and evaluated by the operators. The use of emulations made it possible to test the new automation systems and train the power plant operators at the Loviisa NPP training simulator with the new Man Machine Interface (MMI) and MS.

From reference scenarios giving the response of existing systems to operational and incident scenarios, it was possible to validate the design of the renewed systems. Figure 2 below shows the variations in nuclear power obtained depending on the configuration of the power control system during the trip of a primary circulation pump. The controller is an algorithm made up of two PIDs in cascade. The controller parameterization is complex and without simulation the erroneous parametrization would have been taken into use resulting in operational losses. In Fig. 2 we can see that with the original control system (in blue) the neutron power drops rapidly to gradually rise towards the set point. We can also see that the first settings of the renovated systems did not allow the expected behavior to be reproduced: set point not reached (green), power limitation too slow during the 3 minutes following the pump trip trip (red and black)

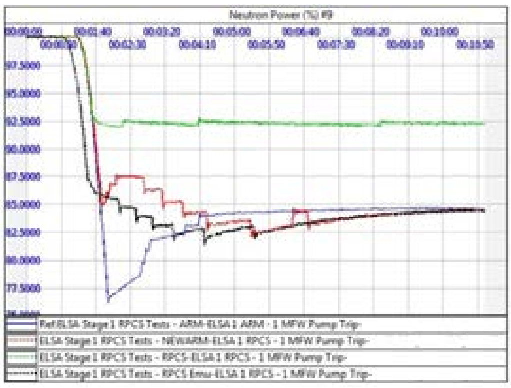

Fig. 2. First power controller simulation results

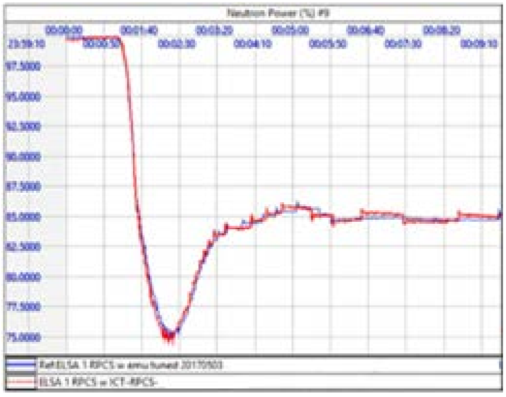

Fig. 3. Final power controller simulation results

In Fig. 3 we can see that the response obtained with the final design of the control system is very close to the functionality of the original system.

About fifty scenarios were used to ensure that the design of the renewed systems guarantee all the required safety requirements. Both accident scenarios (loss-of-coolant accident (LOCA), main steam line break (MSLB), etc.), but also transient operating modes (reactor shutdown and restart, power modulation, etc.) were carried out.

### *E. Factory acceptance tests phase*

With around 30 000 monitored signals and over 2 000 field and control room connections, conventional manually performed signal-by-signal testing was not feasible given the short time schedule. The project had to ensure that new systems were able to function properly with other existing systems. Simulations were used to validate the real equipment and a flexible inter-connected test (ICT) field was created allowing all or part of the equipment to be connected to the Apros model.

Figure 4 below shows a schematic view of the ICT. As described previously, the Apros simulator model includes the primary and secondary circuits and the containment. These models communicate with each other and are controlled by the Testing Station to launch operating or accident scenarios. Simulations of the renewed systems are integrated into the reactor calculation. Each simulated cabinet within a system is represented by a white square. To connect real equipment to the simulator, the simulated equipment in the model was replaced with a network interface shown here in yellow, which automatically connects to the test facilities.

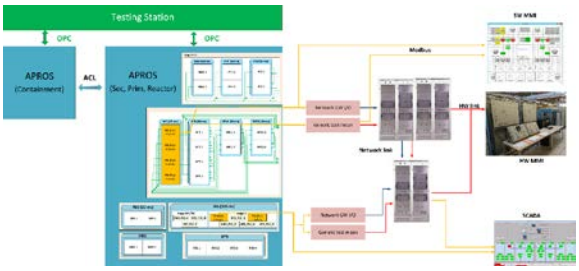

Fig. 4. Test field configuration

During a simulation cycle:

- The simulator sends sensor values to the equipment,
- The interface module transfers these values to test means,
- The test means convert the physical value into an electrical value intended for the equipment under test,
- The equipment under test acquires its inputs and calculates its outputs,
- The test means reads the electrical value at the output of the equipment and converts it into a physical value,
- The interface module reads back the physical value on the test means and injects it into the simulation of the plant.

As the simulator has a simulation time of 100 ms, exchanges with the equipment under test must be carried out within this time interval.

The ICT phase could thus be divided into several phases coinciding with the arrival of the cabinets. Initially, each system, made up of two to four cabinets, was completely individually tested in order to be able to isolate the impact of a single system on the project and thus facilitate the diagnosis in the event of a fault being detected. The tests carried out made it possible to test:

- The nominal operation regarding the reference scenarios,
- Degraded modes and their possible impacts on downstream systems (simulated),
- Periodic tests and their possible impact on downstream systems (simulated).

The validation of the nominal operation of the systems could be done by simple comparison of the responses obtained with those of the simulations. Figure 5 below shows neutron period measurement from a test case that was used to validate one of the safety functions. Following the shutdown of the reactor, the power drops (the period is therefore negative). After 8 minutes 30 we can see a small pulse corresponding to the change of range of the neutron flux measurement (intermediate to source). After 17 minutes of shutdown, the reactor was restarted. We can clearly see the three successive rises of the control rods and the stabilization of the power. To end this scenario, the last rise of the cluster is deliberately very fast to validate the reactor trip while the neutron flux measurement is in source mode. We can observe a very good match between the simulated responses (in blue) with the responses obtained with real systems (in red). Some deviations are obtained due to the inaccuracies of the test means in certain power ranges (very low currents).

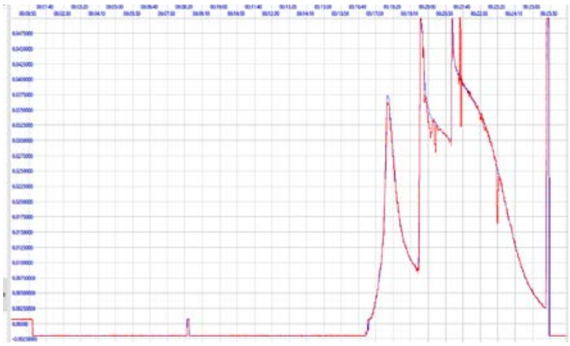

Fig. 5. Neutron period tests results with the real system compared to automation emulation

Secondly, the individually tested systems were integrated one by one. This allows for the gradual transition from a fully simulated test field to a fully hardwired test field while easily decorrelating the impact of each system on overall operation. Adding or removing a system to the test field takes less than half an hour. In this step, the control room panels were also simulated to make it possible to issue orders to the systems either automatically with the simulator or manually.

When all the systems were integrated, certain accident and operational scenarios were carried out. The chosen scenarios made it possible to validate all the safety functions. Performance and response time tests were also carried out. The performance could be measured from the triggering in Apros of an event until the actuation of the outputs of the control systems. Finally, scenarios of operation in degraded mode of the power plant were successfully implemented.

The use of simulation reduced the number of tests even by a factor of 10. Instead of creating between 60-100 tests per each system by the traditional way of testing, 10 comprehensive tests were performed. The use of simulation allowed to save a quarter of the expected time in inter-connected tests despite the volume of information to be tested (2 000 signals and 30 000 supervision data). It also guaranteed the conformity between the responses obtained in simulation and those obtained with real systems. This facilitates the use of the simulator for operator qualification and the use of a reduced inter-connected test field when upgrading systems.

After the FAT Fortum made additional simulator based tests based on the expertise of NPP operators and simulation experts. Especially normal operation profile behavior was taken into account and transients were defined for the power controller.

An additional test session was planned with the Finnish regulatory authority STUK to test some beyond-design-bases cases. The first test case was a drift of neutron flux measurements with control rods partly lowered and power controller in different operational modes. The second test case was a loss of one transmitter room during a complete blackout of half of the cabinets. The third test case was a main steam line break with a common cause failure (CCF) in the existing Engineered Safety Features Actuation System (ESFAS) leading to the impossibility of a trip on request by the reactor trip system. All results were satisfactory, even if the scenarios had not been considered during the design phases. This was further evidence that the architecture was robust and that the right level of diversity was integrated in it.

### F. *Commissioning phase*

The commissioning procedures for the new automations systems were prepared well before the outage. This gave the possibility to test and validate the applicable procedures in advance at the Loviisa NPP training simulator with plant operators. Corrections to the procedures were made and the ELSA automation systems were successfully commissioned during the annual maintenance periods in the years 2016, 2017 and 2018 [3].

## IV. LASU AUTOMATION RENEWAL PROJECT

The LASU project consisted of partial renewal of the ESFAS functions by upgrading I&C equipment installed by Rolls-Royce during the ELSA project. The role of the ESFAS is to detect abnormal situations and initiate the operation of necessary engineered safety features in order to prevent core damage and ensure containment integrity. The ESFAS is safety classified SC2 according to Finnish regulatory guideline YVL and is mandatory for the Loviisa NPP to operate.

The LASU project utilized the simulators in the pre-engineering phase by providing information about the behavior of the existing automation systems in different normal operation and accidental scenarios. The first versions of the new software logics were partially based on the simulation results and were modelled and tested further with the simulator. During detail design phase emulations of the new automation software were created and connected to the simulation model. Similar to the ELSA project test cases were selected to test the new automation system and compared to the original automation system. Apros simulator was also utilized in Human Factors Engineering (HFE) verification. The new and updated HMI was connected to the simulator and the functionality was analyzed by the plant operators with the prepared test cases and additional ad-hoc tests.

The LASU project automation systems were successfully commissioned during the annual maintenance periods in 2021.

## V. CONCLUSIONS

Simulation-assisted testing provides several benefits over traditional techniques. The automation systems are virtually commissioned at the simulator in advance compared to the plant installations. Therefore errors in automation can be noticed earlier as well as the cross-dependencies between different systems can be analyzed. This increases the speed of automation system delivery.

Progressive integration during the ICT allows a small number of real cabinets to be tested while rest of the cabinets are simulated. ICTs can start even if some cabinets are not available or under construction. The simulations are fast and flexible as the transients cover several automation functions with one test. By utilizing a simulator, the automation systems receive a realistic process response and the errors and faults can be seen from the actual process displays. This way the testing becomes very intuitive and comprehensible for the plant personnel. The tests can be run during night or weekend and the results can be examined later using Apros to ensure that there is no deterioration or non-desired effects.

The experiences from the tests have shown that the dynamic transients allow for operational profile testing which is more realistic, efficient and less time consuming than individual signal tests. In addition the use of simulations is flexible and allows very complex test cases for example common cause failure with a loss of a transmitter room. Simulation assisted automation testing supports licensing and increases authority confidence in the automation renewal projects.

## REFERENCES

[1] A. Meriläinen, O. Viljakainen, K. Honkoila, A. Lahtela, Apros-based Loviisa NPP Full Scope Training Simulator and Engineering Model, 28th International Conference on Nuclear Engineering, ICONE 28, Virtual Conference, Online, August 4-6, 2021.

[2] V-M. Tikkala, A. Rantakaulio, Test Case Selection Procedure for Simulation-Assisted Automation Testing, NPIC&HMIT 2017, San Francisco, CA, pp. 1635-1643, June 11-15, 2017.

[3] M. Lehtonen, Y. Challamel, I&C upgrade ends in success at Loviisa, Nuclear Engineering International, Vol. 64, No. 775, pp. 35-37, February 2019.