The 14th International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-14) Log Number: 505
Hilton Toronto Hotel, Toronto, Ontario, Canada, September 25-29, 2011.

SECURITY IN A NUCLEAR POWER PLANT SIMULATOR

M. Giersch[1], N. Muellner[1] and F. D'Auria[1]
[1] University of Pisa, San Piero A Grado Nuclear Research Group, Pisa, Italy
m.giersch@ing.unipi.it, nikolaus.muellner@univie.ac.at, f.dauria@ing.unipi.it

Abstract

INPACEA-TIE (integrated nuclear plant accident, component and environment analyzer – technological information elaboration) provides the possibility to simulate and visualize all stages of NPP accidents with precision and detail. The tool presents an integrated approach for safety and security concepts in three ways:

1. NPP security - security features which are implemented at the NPP are simulated
2. Simulator security - access control and user privileges can be adjusted at the simulator itself
3. Testing and improving of security measures – a method to detected security deficiency with INPACEA-TIE

Introduction

In contrast to full scope simulators the tool INPACEA-TIE (integrated nuclear plant accident, component and environment analyzer – technological information elaboration) provides a platform to simulate and visualize all stages of NPP accidents with precision and detail. The modular approach, which allows incorporating the most advanced computer codes, ensures that every aspect of an accident is treated by the adequate calculation code (Relap5, Trace, Melcor, Nestle, CFX, CIAU e.g.). A prototype, simulating Central Nuclear Atucha 2 (CNA2) of the tools is currently under development at Gruppo di Ricerca Nucleare San Piero a Grado GRNSPG of University of Pisa.

Standards, regulations and guides provide a frame for security concepts in NPP – which does usually not apply for NPP simulators. Therefore most NPP simulators do not consider security aspects in a systematic manner. INPACEA – TIE presents an integrated approach for safety and security concepts at following level: Main NPP security features are simulated; access control and user privileges can be adjusted at the simulator itself; INPACEA supports the testing and improving of security measures. INPACEA therefore is able to support identification of security deficiencies and to improve concepts in security by design (SbD), logic (I&C security) and operational procedures.
The paper overviews how security aspects can be considered systematically at level of nuclear plant accident analyser (NPP-Simulator INPACEA-TIE) in a modular approach to reach simulator application compliance with potentially also different security concepts.

1. Focus of Full Scope Simulator and Nuclear Plant Accident Analyser

NPP full scope simulators are used for training of plant operators and license of operating staff. The systems represent a detailed copy of the plant control room and provide simulation environment for connected I&C and physical systems. NPP Accident Analysers (like INPACEA) can also be used for operator training, but in addition to support deep understanding of plant behaviour during selected transient sequences. Plant Analysers are representing the most important instruments and functions

of the plant but not necessarily in full detail. The scope of analysers is concentrated on plant design, design approval, validation of simulating codes, nodalisation as well as fundamental concepts of interaction of plant design and operation – under this extend also relevant for operators. INPACEA plant accident analyser provides support at three different levels: 1. Operator training, 2. code validation and design qualification, 3. support mode with links and access to relevant second and third level documents and literature for extended knowledge management and documentation related to interaction of processes, procedures and licensing bases. Security aspects and integrated safety and security approach are relevant on all three levels and are considered by INPACEA.

The operator mode runs transients, which were simulated with the chosen code package and frozen nodalisation (containing in case logic, thermal-hydraulics, neutron-kinetics, computational fluid dynamics and radiological consequences simulation tools etc.). This mode provides a quasi-full scope simulator environment to train operators for interactions on special situations and to demonstrate event characteristics in full detail. Nevertheless the results are pre-calculated, the simulation has to be done before due to the requested high calculation time.

The analytical mode is interfering at the level of reactor and system design. Simulation code changes can be implemented or the nodalisation can be changed in a strictly documented way to simulate system adaptations of plant I&C (e.g. by changing of setpoints or limits) or structures.

The third INPACEA mode provides access to an extended database of supporting documents related to the plant design, operating procedures, the nodalisation and code environment and interaction and licensing documents.

2. NPP Accident Analysers and Security Issues

2.1 Security Relevance

NPP simulators are currently used for several applications mainly from nuclear operators and plant designers to train and license operating people, in case of accident analysers also to support design development or design conception [1], [2], [3].

Also beyond nuclear sector and in other critical industries, like aerospace, naval or defence sector, simulators are used to improve quality of products, training of involved staff and to accelerate development and competiveness with reliable costs. These industries are aware of the strengths and effectiveness of simulation tools in identifying critical aspects of design and operation. Both, safety and security related aspects can be simulated but specifics have to be considered. Following IAEA definition [4] of the two analogical expressions safety and security, the first one could be described as freedom of technical risks, security as absence or successful protection against human intended risk. The security approach therefore concentrates on: Protection of product development and intellectual property rights on the one hand side and on countermeasures against infiltration and misuse and sabotage by unauthorised persons or groups [5], [6], [7], [8].

Digital Instrumentation and Control (I&C), Information and Communication Technology (ICT) and Supervisory Control and Data Acquisition (SCADA) systems are nowadays significant part of nuclear facilities and energy infrastructure and used also in safety critical areas. These systems are frequently part of the safety systems and therefore also possible affected by unintended human (operation) errors or target of human intended attacks and sabotage, creating a security issue. Digital I&C system safety features are matter of extended discussion of plant designers, operators and safety authorities [9], [10]. Because they are per definition computer based, also related risks have to be

considered. The Stuxnet attack of nuclear facilities of Natanz and NPP Busher demonstrated that I&C security issue is not just an academic issue and is able to open serious safety challenges.

Digital I&C systems and simulators or plant analysers are frequently using the same or similar tools for data processing and logic per definition. Security threats could affect both.

The 9/11 event was based on training performed at an ordinary plane simulator. Because of the high degree of system complexity, the high number of safety critical systems, the relative low number of plants and connected low statistical analyses, NPP accident analysers and simulators are able to contribute significantly to systematic safety checks in design and operation. It is therefore necessary to protect the results but also the simulator itself [9], [10].

2.2 Regulatory Frame

Since several years regulators consider the benefits from full scope simulators to train and license operating staff as well as to analyse and improve plant design or to provide support for conceptual studies [11]. Security aspects in nuclear facilities, beyond physical protection and implementation of non-proliferation regime was not in focus for long time and rosed up with international attention on security debate and more distributed use of digital I&C and SCADA systems [11], [12]. Several safety authorities are concentrated on updating the existing regulations on nuclear I&C systems to consider the new spectra of options [10], applications and threats with new requirements [9]. Some of the changes in regulations are also relevant in use and set up of simulators. There are also significant and coordinated activities at the level of international organisations for exchange of experiences and to define best practice guidelines for I&C, ICT and simulator security and integrated approach of safety and security analyses [13], [14]. Applicable guidelines are considered for INPACEA at different implementation level as described in the following section.

2.3 Security features on plant level

The UNIPI INPACEA considers main security features of plant design and operation modes. Four plant security levels are identified; they are not used for ranking but distinguish between the security targets: 1. Physical protection and consistency of retention functions, 2. Security of Systems and Components, 3. Instrumentation and Control System Security, 4. Operational safety and security management.

All of these areas are also covering safety relevant or safety critical systems or topics, because a security risk could only change into real danger by transforming into a technical risk and damage with transfer from security arena into the safety arena. INPACEA considers the specific security measure or action from the plant according to the area (1-4 as described). The issues are documented in a security catalogue linked to the affected area (e.g. I&C systems).

The security analysis is starting as case by case mode from anticipated transients or events and considers the status of security table entry at certain critical steps. Each safety system is attributed with a security value ranked by vulnerability to security attacks within a scale from 1 (very difficult to attack) to 10 (highly vulnerable on multiple threats). The safety system security attributes create an additional category. The table of attributes provides additional information about security status of plant at certain simulated safety level.

2.4 Simulator Security

Simulator security can be subdivided into: A) physical protection of simulator against intended or unauthorised access and B) software security.

2.4.1 The physical protection is ensured by:

Physical access control measures: INPACEA system is setup in physical secure environment, which is protected by fire safe doors and multilayer video control of access unit. Redundant presence sensing systems are permanently active and trigger unauthorised access alarm in case of closed-mode activation.

2.4.2 Software security is guaranteed by:

Island operation mode: INPACEA system is physically disconnected from internet. Software changes, data transfers and updates can be performed only by authorised INPACEA staff with personal authorisation of physical access and password protected login. All file transfers are logged for statistical and analytical reasons. The log-files are documented.

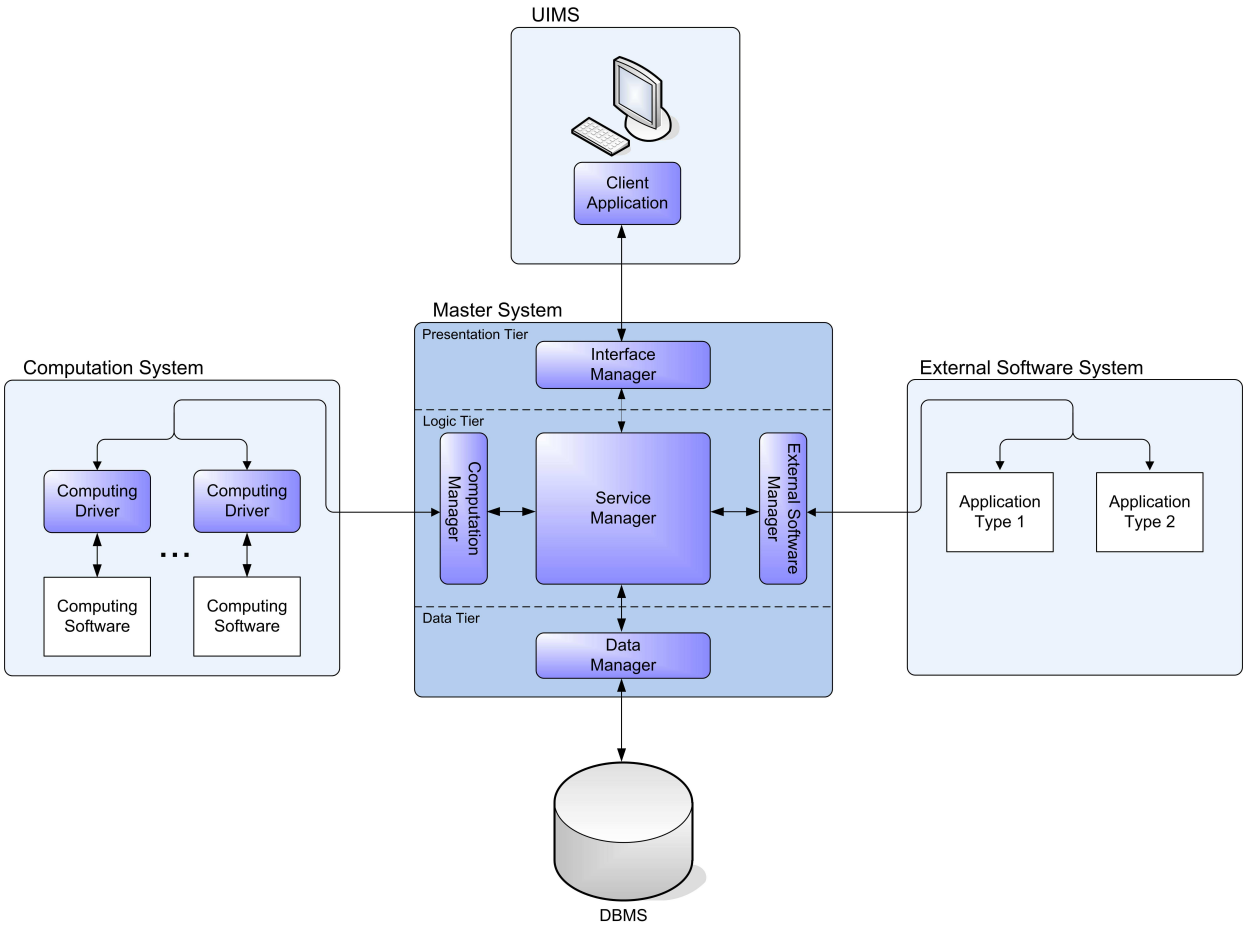

Figure 1 INPACEA architecture.

The INPACEA environment is the only system with full interaction and function of separated and modular tools, databases and programmes at this time. Single code segment development environment is protected by QA approved ISO 9001:2008 data and process management conditions.

The chain of qualification includes also subcontractors.

As shown in Fig. 1 the INPACEA system architecture consists of five modules. The Master System (centre) represents the general service manager (SM) and connects the databases, computational systems and external software to the user interface (upper module). The SM is the central part of INPACEA and is therefore physically and electronically protected. Standard users and analysts do not have access to administration of SM. They are able to use the services and request data and computational power but are not allowed and able to change the rules for the services provided. The same level of security is implemented for the DBMS data base (lower part). Computational systems (left shown modules) are also handled secure but here changes from analysts are possible under predefined criteria.

The whole architecture like shown is not connected to internet. The external software systems (demonstrated at the right side) are treated like the computational systems. Code license and intellectual property rights from third parties have to be considered in addition.

2.5 Testing and Improving of Security Measures

Starting from security attribute table of safety systems, the level of integrated plant safety and security can be investigated and improved. If (safety) relevant systems are affected by (additional) security event(s), the transient history will change. For systematic analyses the security attribute (level of vulnerability) of a safety system has to be considered. The analyses are performed with the security class starting with the most vulnerable system(s). In case that a safety system is considered as relevant at selected security level, a total damage or unfavourable effect of the system has to be anticipated. The damage is implemented in simulation code(s) like additional boundary condition starting from time of initialisation of changed transient history in relation to the lower security level, where the system is still effective and not affected by the security attack.
This approach is also applicable in case of different security attributes (e.g. for distinguishing between external and internal threat vulnerabilities, more detailed attack characterisation etc.).

Within a systematic approach several relevant security events have to be considered at different time and extend and provide initial and/or boundary conditions comparable to that of safety sensitivity analysis. Security events have to be considered on:

- Level of design (corresponding to plant nodalisation at INPACEA),
- plant I&C (image of the plant logic at INPACEA) and
- Operator actions (if considered during the transient or event).

Within the security event arena active countermeasures by operators have additional relevance in relation to separated safety analyses for single security events. Depending on system interactions a security driven event tree has to be simulated. Security impact could affect simulation output by:

- Physical behavior of plant, logical response of systems,
- Availability of safety systems,
- Common mode aspects etc.

The results are documented in output files and data for post processing.

The concept of nuclear plant analyser provides the possibility to consider and investigate design changes (at the level of structures, systems and plant logic) and definition of operational interactions, as far as covered by system response. It is therefore possible to investigate effects of changes also related to security issues with three implications: Effectiveness of Security by Design (SdB), interaction with safety design and (both, safety and security) procedures, as far as they are simulated.

INPACEA is able to support the qualification of suggested security measures by demonstrating the effect on plant behaviour. The process of transformation of security issue(s) into plant response is quite essential. Applicable and reasonable criteria for security events have to be used to generate an adequate security matrix for the event family (using design bases threat and security target requirement concept). The pre-selection of events directly implies the focus and the security related transient impact. Systematic approach how to deal with single, double and multiple security events - also on different levels – has to be defined before starting simulations. Integrated safety and security event conditions are implemented like technical event conditions before starting the simulation within INPACEA software code modules e.g. at the level of heat structures, plant nodalisation and geometry, neutron kinetics, fuel conditions, availability of operational and safety systems or plant setpoints, limits and logic. Security improvements of the plant are resulting in changing security vulnerability attributes and improvement of safety system availability at a certain security level. Improvement measures can be simulated like described. Key aspects are the availability of a system by higher protection, decrease of component threat, diversification or additional systems etc.

Table 1 Security aspects of Integrated Nuclear Plant Accident Analyzer

Plant Analyzer characteristic	Security aspect
Tool for analysts	Support to “Security by Design”
Behavior of plant not fully known, focus on analytic support for decision making	Improvements and qualification of integrated safety and security concepts, also at procedural and operational level
Development of normal, abnormal, emergency procedures	Security aspects of normal, abnormal and emergency operational procedures
New scenarios-problems to test or extend capabilities of NPP	Definition support for new scenarios, design bases threat, security related requirements and acceptance criteria
Target group considerable in size	Overlapping safety and security community representatives
Quality components, but limited hardware requirements	Physical protection, access control and login procedure like for full scale simulator required. Life cycle control required
Everyday access for any analyst	Access under predefined user security rules

3. Conclusions

Integrated approach in analyses and implementation of safety and security aspects is important also at the level of NPP Simulators and NPP Accident Analysers. Most essential technical and operational plant security features have to be simulated for better understanding of interaction of safety systems with security threat scenarios. For realistic simulation of security events, input and interaction tables have to be developed carefully at the level of threat analyses, plant design and security of operation. To avoid unintended information spreading about design conceptions and security related countermeasures for scenarios, simulator related security has to be enforced: Access control and user privileges can be adjusted at the INPACEA simulator.

In combination with sensitivity runs INPACEA provides an optimal platform for systematic analyses and better understanding of security related plant effects and integrated safety concept and supports improvements of design and procedures or both on measurable level by concept of security attributes.

4. References

[1] USNRC, “Regulatory Guide 1.149 – Nuclear Power Plant Simulation Facilities for Use in Opreator Training and License Examination”, Rev. 3, Oct. 2001 (Draft was issued as DG-1080) http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg/01-149/.

[2] Rostov NPP, “Rostov NPP has successfully undergone the integrated security status check”, July 2010, Public Information Centre of Rostov NPP/ROSATOM.

[3] Francisco Bustío, Pedro Corcuera and Eduardo Mora, “Training simulator for Garoña Nuclear Power Plant”, EUROCAST '95, Lecture Notes in Computer Science, 1996, Volume 1030/1996, 523-529, DOI: 10.1007/BFb0034786, Toronto, Ontario, Canada, 2002 June 2-5.

[4] IAEA, “Concepts and Terms – IAEA Safety Standards”, 06.11.2010, Vienna.

[5] IAEA, Dep. Of Nuclear Safety and Security, Office of Nuclear Security “SYLLABUS”, Computer Security for Nuclear Facilities, Regional Workshop, 2011, Vienna.

[6] IAEA, “Computer Security at Nuclear Facilities”, IAEA Nuclear security Series, Technical Guidance, 2010, Vienna.

[7] IAEA, “International Computer Security Advisory Service (ICASA) Guidelines”, IAEA Nuclear security Series, March 2009, Vienna.

[8] IAEA, “Protection and Confidentiality of nuclear Security Information”, 2011, Vienna.

[9] Tim Mossman, “Security of Digital Safety Systems”, Oct. 2010, ANS, Las Vegas, U.S. Nuclear Regulatory Commission.

[10] USNRC, “Regulatory Guide 1.152 - Criteria for Use of Computers in Safety Systems of Nuclear Power Plants ”, Rev1, 2 and 3, U.S. Nuclear Regulatory Commission.

[11] K. Korsaha, R. Wetheringtona, R. Wooda L.F. Millerb , K. Zhaob, A. Paulb C. E. Antonescu, Oak Ridge National Laboratory, University of Tennessee, USNRC Project

Manager, “Emerging Technologies in Instrumentation and Controls: An Update”, Date Published: January 2006, Prepared for Division of Engineering Technology Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission Washington, DC 20555-0001 NRC Job Code Y6962.

[12] Franz Altkind, Manfred Märzendorfer, “Modernisation of NPP, Consideration of CCF aspects”, June 2007, Swiss Federal Nuclear Inspectorate (HSK), NPP Leibstadt Switzerland (KKL).

[13] Hauptabteilung für die Sicherheit der Kernanlagen (HSK), “HSK-R-46/d: Anforderungen für die Anwendung von sicherheitsrelevanter rechnerbasierter Leittechnik in Kernkraftwerken”, April 2005, http://www.hsk.ch.

[14] Atos Origin, “The Full Scope Simulator for the N4-Type Nuclear Power Plant”, July 2008, Atos Origin – Communication & Marketing France - 200807 - Image EDF MEDIATHEQUE / DR.