Contribution ID: **486** Type: **Paper**

A prototype of a new virtualized secure embedded product for Operational and Safety Related I&C Functions

Virtualization technologies were developed first by the information technology (IT) industry. Now they have started being deployed in the process industry. Virtualization is a set of technologies that can be applied to a wide variety of applications and fields. Hardware and/or software can be virtualized: Hardware virtualization can be deployed in the process automation, where process engineering departments supervise the process application software. Current technologies, specifically virtualization alongside fault tolerance and more reliable hardware and software components, are able of making plants operate smarter, faster, safer, and also facilitating the overall management system. Before, virtualization was an unknown concept for industry, nowadays some companies have chosen to deploy virtualization also for its benefits in terms of cost savings. As virtualization technologies keep growing, new implementations and improvements are rising. Some of the emerging virtualization technologies can be challenging to deploy for project managers and integrators. Currently, numerous organizations are implementing virtualization technologies on the server´s side; in order to lower their power consumption, optimize facilities´ space and surface requirements which are related to servers´ implementations. In terms of conserving Confidentiality, Integrity and Availability (CIA) requirements, virtualization technologies are able of providing high availability for critical applications. Virtualization capabilities go beyond simplifying IT processes, it permits IT organizations to react rapidly to the varying business requests. The growing complexity, variety and diversity of products and also long innovation´s phases present some of the important challenges surrounding products´ developments within factories and plants. Virtualization´s product development is a possible solution to deal with these challenges. By adopting diverse virtualization technologies (VT) products can be developed faster, cost effectively and with a higher quality. On the other hand, virtualization technologies necessitate novel skills within organizations and also operations. In some cases, multiple applications with different levels of criticality are implemented in the same platform even though each application requires a different level of security.
In this paper, an architecture of a new secure platform based on virtualization will be presented. In this prototype, security is applied both in the software layer and the hardware layer as well. This architecture can potentially be applicable for Industrial Automation and Control Systems (IACS) of Industry 4.0 but also for Safety Instrumentation & Control (I&C) and Operational I&C in Nuclear Power Plants. In this paper, we will list most common security, scalability and legacy issues surrounding traditional I&C systems and explain how the proposed architecture can solve some of the security concerns. With regard to functional safety and nuclear safety a graded approach is necessary for both, safety and security. In this paper the focus will be on improved security while the impact on safety according to IEC 62589 is considered as boundary conditions.

State

Germany

Gender

Female

Author: TELLABI, Asmaa (Framatome GmbH/University of Siegen)

Co-authors: Dr WAEDT, Karl (Framatome GmbH); LOU, XinXin (Framatome GmbH); SABRI, Abdelbast (FAU)

Presenter: TELLABI, Asmaa (Framatome GmbH/University of Siegen)

Track Classification: CC: Information and computer security considerations for nuclear security