A PROTOTYPE OF A NEW VIRTUALIZED SECURE EMBEDDED PRODUCT FOR OPERATIONAL AND SAFETY RELATED I&C FUNCTIONS

ASMAA TELLABI
Framatome GmbH
Erlangen, Germany
Email: asmaa.tellabi@framatome.com

KARL WAEDT
Framatome GmbH
Erlangen, Germany

XINXIN LOU
Framatome GmbH
Erlangen, Germany

ABDELBAST SABRI
Frederich-Alexander University
Erlangen, Germany

Abstract

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 the 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 in 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. With regard to functional safety and nuclear safety a graded approach is necessary for both, safety and security. In the paper the focus will be on improved security while the impact on safety according to IEC 62589 is considered as boundary conditions.

1. INTRODUCTION

In the past, Nuclear Power Plants (NPPs) did not combine Operational Technology (OT) with Information Technology (IT), and stringent rules related to communication flows between these systems were put in place. Systems related to safety are implemented based on strict rules, and they commonly run on a dedicated Operating System (OS) and its software applications [1]. The incorporation of digital devices and multiple automation platforms in modern nuclear plants, as well as NPPs is the progressively growing usage of digital technologies. This gradual process related to digitalization can be brought either by a sequence of refurbishment projects of I&C and Electrical Power Systems (EPS) or by novel designs with new-built power plants [2]. The nuclear industry is a critical domain where safe operation is vital. The aim of a NPP is to generate electricity which is a risky process. Nuclear safety is defined by IAEA as the achievement of accurate operating conditions, prevention of accidents or mitigation of accident consequences, as well as the protection of employees, the public and the environment from dangerous radiation exposures. Contrariwise, nuclear security is seen as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious deeds relating to nuclear material, other radioactive materials or their associated facilities [3]. Safety mechanisms are supposed to prevent accidents, while security controls are integrated in order to stop intentional malicious acts that might endanger the NPP or cause the theft of nuclear materials [3]. Consequently, like any critical infrastructure confronting a rising risk of cyber-attacks, cybersecurity for NPPs has turn into a matter of rising concern.

Virtualization technologies origins come from the IT world; currently it has gained a growing popularity and attention within the automation industry. The aim of virtualization is to break the limitation of hardware and melt down the abstraction between application software, OS, and hardware. Virtualization permits the execution of various OSs and applications on the same computing entity while still being isolated from one another [4].Virtualization has multiple benefits including the facility of software management and reduced costs [5]. This technology also has a positive effect on the human machine interaction (HMI) in control system, in case it is combined with client technology, it offers an easier and cost efficient approach to control process automation systems even in critical environments [4].

The remainder of this paper is organized as follow. Section 2 gives background information on virtualization use cases in I&C systems. Section 3 presents the proposed system´s architecture. In Section 4 , a hardening policy that will be used to provide more security on the platform is described. We conclude the paper in Section 5.

2. VIRTUALIZATION USE CASES IN I&C SYSTEMS

Virtualization is defined as a group of simulated software and/or hardware above which additional software runs known as a virtual machine (VM). A hypervisor or the virtual machine monitor (VMM), is a software management layer able of running numerous different execution environments in one computing entity [6]. Various virtualization technologies are present in the market; even though this might be a good indication of the developing market, a perfect virtualization solution does not exist yet [7]. As stated by Stratus Technologies [5], they believe that by the end of 2020, 75% of companies operating in the space industry will have implemented virtual server platforms for managing and running SCADA, HMI, Historian and MES (Manufacturing Execution Systems). Based on how many system´s components will be virtualized, multiple terms can be used [4][7][8]:

- Server Virtualization: different servers including their OSs (e.g., Windows 2012 R2) are integrated on one or a few host servers. This type of virtualization might be implemented in order to separately run a backup server or a test server containing new configurations that should be tested and validated;
- Desktop Virtualization or Virtual Desktop Infrastructure (VDI): considered as one of the newest trends in the market, multiple complete desktop OSs, e.g., Windows 7, including their applications are integrated into one host server. It might be deployed in order to integrate numerous workstations with numerous applications into one centralized host server;
- Application Virtualization: A group of applications is encapsulated in sandboxes and implemented on one server. For example, operators are able of accessing these applications from their local computers even though the applications are installed and running on the server. This configuration is used often in cases where users must access to a large amount of applications that are implemented and managed by one server.

In process automation for example, the three virtualization implementations can be used. On the other hand, most of the virtualization solutions used today are based on server virtualization and VDI configurations [8].

Virtualization technologies gained a lot of attention in the research field for several years, in the industry as well as in the nuclear domain for non-safety applications. Nowadays, the hardware used has higher capabilities and perform better which gives it the ability to host multiple servers or operating workstations into a single computing entity. Using virtualization, the quantity of physical computers is decreased [4]; this has a positive effect on power consumption as well as costs reduction that are related to maintenance because there are only few units to maintain. In case an I&C System is virtualized, the dependence on a particular hardware is removed and this will make upgrades easier. Since virtualization deployments have expanded radically in the business and financial sector amongst others, multiple companies are currently offering solutions that fit process industrial use cases requirements. Virtualization technologies can be integrated into different systems in order to join numerous server nodes into one computing entity. As stated before, the amount of physical computers needed inside a virtualization set up is considerably decreased. It has some benefits related to the needed space for computers, costs related to the hardware used for computers and cabinets, as well as operating and management costs, e.g., energy costs. Some of the benefits related to the use of virtual workplaces can be [4][8]:

- Decreased room space necessities;
- Lower power consumption and cooling needs;
- Lowe room noise;
- Easier upgrades and replacements of defect hardware or client applications;
- Easier installation of virtual machines with different General Purpose OS (GPOS);
- Increased security.

3. SYSTEM´S CONCEPT

Cyber security is a vital part in the protection process of industrial infrastructure, e.g. nuclear I&C safety systems [1]. Therefore, managing all digital devices together with cyber security inside the global security program is crucial. Cyber security should be incorporated in systems´ design so that confidentiality, integrity, and availability (CIA) can be guaranteed [1].In case different functionalities are incorporated in the same hardware entity; it is very possible that some of those components will be highly critical to the survival of the platform compared to others. Mixed criticality systems (MCS) are founded on the principle of permitting applications with different levels of criticality to easily coexist within the same computing entity [2][9]. Criticality defines the level of assurance against failure, which is required for an element in the system. Approaches to attain this level of isolation are kernel separation and virtualization. In [4][6][9], an I&C architecture based on virtualization was presented, it used Xtratum [10] which is a bare metal hypervisor used for safety critical systems.

3.1. Xen

Xen [11] is an open source bare metal hypervisor, it can create numerous VMs inside a single physical host. Inside each VM a GPOS can be installed e.g., Linux or Windows. Xen has four different schedulers that support in planning the execution time of each VM on the host. As presented in [12], Xen contains four schedulers; the default scheduler is Credit scheduler, the Credit 2 scheduler, which is founded on Credit, Real time Deferrable Server (RTDS) which is a real-time scheduler in addition to the ARINC 653 based scheduler.

Xen was created in 2003 by Harham et al. [11], it is the most commonly deployed open-source hypervisor. The hypervisor is situated between VMs and the hardware, offering a virtualized memory, a virtualized network and virtual CPU (VCPU) resources to the guest OS and the control domain.

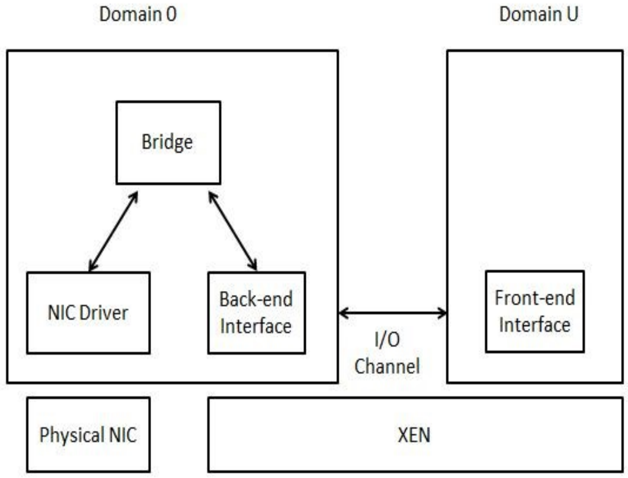

FIG. 1. Communication flow in Xen [1] .

Fig. 1. presents the communication flow in Xen. In Xen architecture, the manager domain or control domain which is known as Domain 0 is in charge of creating, suspending, resuming, and destroying the available guest domains which are known as unprivileged domains (DomU). Domain 0 implement a Linux distribution but guest domains can run on any Xen supported OS. Each domain contains a group of VCPUs and they are scheduled following a certain chosen scheduler. For inter-domain communications, the control domain or Dom0 has a netback driver that synchronizes requests with the netfront driver in each guest domain.

3.2. Components

In [6][9] a secure platform based on virtualization was presented where Partitions´ services are someway identical to TELEPERM® XS (TXS) which is Framatome's I&C system platform for safety I&C created particularly for NPPs. It includes everything needed from critical hardware to software modules. It also contains software tools required for engineering, testing and commissioning, operation as well as troubleshooting fulfilling with the most firm software development requirements present in IEC 60880:2006. The idea behind the creation of this platform is to create a single point entry from the outside world (Internet) to the inside world (Domains) and to make the Domain 0 responsible of controlling the communication flow between Domain 1 and Domain 2.

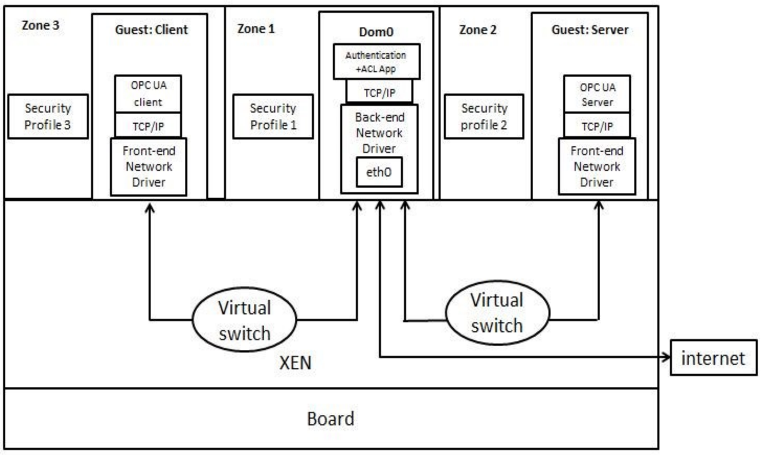

FIG.2. Platform´s architecture.

Fig. 2. shows the system view of the platform including its components. As seen from Fig. 2., the platform is divided into three zones. Zone 1 which is the control domain, it contains Domain 0 or Dom0 and is the first domain the platform is booted from. Zone 2 which is called the non-secure domain, it contains and OPC UA client. Zone 3 is called the secure domain and will include an OPC UA Server. Each domain will contain a health monitoring check application in order to test the availability of processes in each domain. This platform is based on specific communications requirements:

- Zone 3 and Zone 2 cannot communicate with internet
- Zone 1 is the only zone connected to internet
- Communications between Zone 2 and Zone 3 must be controlled by Zone 1
- Connections between the OPC UA Client (Zone 1) and Zone 2 must go through the authentication and Access Control applications in Zone 1

Zone 1 contains an Authentication and Access Control list in order to monitor the communication exchange between the OPC UA Client and OPC UA Server. For each domain, the firewall is configured in order to control the communications between domains and also with the outside world. In the Xen level, domains are connected using virtual switches; access control rules are also implemented on them to restrict communications. Each domain will have a specific security profile, which will contain the different applications and the resources they can access and also actions they can execute. This will be done using AppArmor. An IDS will be configured too in each domain and other security tools as defined in the next section.

A primary prototype of this architecture was implemented on an Intel board, the hypervisor and communication with the inside and outside world were implemented. Domain 0 runs on Ubuntu 18.04 as well as Domain 1 and Domain 2. A samba server was installed in Domain 2. In [12], schedulers were tested in order to see their performances on inter-domain communications and file transfers using SSH. Iptables were implemented in each domain and ACL on virtual switches.

4. SECURITY HARDENING POLICY

Systems hardening is defined as a set of tools, techniques, and best practices used in order to decrease vulnerabilities in the deployed technology applications, systems, infrastructure, firmware, and other system´s modules. The aim of systems hardening procedures is to decrease security risks through the removal of possible attack vectors as well as reducing the system's attack surface [13]. By removing unnecessary programs and following hardening procedures, attackers will have fewer chances to gain access to the system.

Even though the concepts behind system hardening are global, tools and methods differs based on the type of hardening. System hardening is required all the way through the lifecycle of technology, from initial setup, during configuration, maintenance, as well as support, to the decommissioning phase. System hardening processes are set as a requirement of mandates like PCI DSS and HIPAA [14]. Systems hardening was used in order to provide more security features and configure applications that are already available at the OS level. In this implementation the following hardening procedure will be used:

- Setting up the BIOS password;
- Enforcing a strong password policy by using strong passwords, disabling empty passwords and restricting the use of previous passwords;
- Minimal installation of the OS by installing only the needed services. Usually in Ubuntu already installed services are permitted and started by default, which means that the newly installed processes are, already executed based on the default configuration [15];
- Configuring the Pluggable Authentication Module (PAM), it offers authentication services to Linux based systems and a finer graded configuration approach;
- Enabling the Firewall using iptables [16]. They are a command-line firewall function which work with policy chains in order to permit or reject the traffic. For example, in case a connection attempts to start on the system, iptables search for a specific rule inside its list that will match it to this new connection. In case no matching rule is found then the connection will not be established. In this platform, iptables rules were created to stop Domain 1 and Domain 2 from connecting to the outside world, to protect against SYN Flood Attacks, UDP Flood attacks, TCP-flagless packets Attacks or Null Packets attacks, and IP spoofing;
- Configuring security profiles for each machine. Since Ubuntu is used then AppArmor [17] will be used to create security profiles. AppArmor is a Mandatory Access Control (MAC) system, it considered as a framework that limits resources and action of running processes based on profiles that are loaded into the kernel during the boot;
- Securing the shared Memory which can be used as an attack vector by malicious users against a specific service;
- Securing the console security by disabling the ´Ctrl+Alt+Delete´ combination. In case attackers have a physical access to the system, this combination will allow them to reboot the systems without logging on;
- Installing and configuring the Advanced Intrusion Detection Environment (AIDE) Software [18]. It is an open source host-based intrusion detection system that offers software integrity checking capable of detecting specific intrusions, e.g. monitoring filesystems for unapproved modifications;
- Installing and configuring a Port Scan Attack Detector (PSAD) [19], which is composed of a set of lightweight system daemons that are executed on Linux based systems. It analyzes iptables log messages in order to detect port scans and any suspicious traffic inside the system;
- Installing and configuring a Selt-test Application, Ubuntu already implements a Self-Monitoring, Analysis and Reporting Technology (SMART) application [20]. Its aim is to detect and report multiple signals of technical issues in the drive that can lead to hardware failures. In case it shows possible drive failures, the software running on the host system has to alert the system administrator thus preventive measures are taken in order to stop data loss, as well as the replacement procedure of the failing drive is easier and data integrity is preserved.

5. CONCLUSION

This paper introduced a new architecture dedicated to industrial systems including I&C systems, it is based on virtualization technologies and other security components. The virtualization layer introduces different threats, risks and challenges, as well as attack vectors to environment. Consequently, novel solutions bases on virtualization must offer preventive countermeasures as well as increase the trustworthiness of these environments. That is to say, the provided security tools have to follow virtualization requirement and not to only be adjusted to present systems. Despite the fact that multiple methods and applications dedicated to virtualization exist, their aim is to melt down the limitations of the physical hardware through the establishment of secure partitions within the hardware so it can run as if different virtual environments were running at the same time. The primary aim of virtualization is to break the existing connection between application software, OS, and hardware while still adhering to safety and security requirements. In the future, OPC UA Client and Server will be implemented using the OPC6251 Libray, self-test application will be implemented to test Linux systems using shell scripts.

REFERENCES

[1] TELLABI, A., BEN ZID, I., BAJRAMOVIC, E., WAEDT, K., “Safety, Cybersecurity and Interoperability aspects in Modern Nuclear Power Plants”, PESARO (Athens, Greece, 2018), IARIA.

[2] RRUSHI, J., CAMPBEL, R., “Detecting cyber-attacks on nuclear power plants,” The International Federation for Information Processing (ICCIP 2008), Springer, Boston, vol. 290, 2008, ISBN: 978-0-387-88522-3.

[3] INSAG-24, International Nuclear Safety Group, “The interface between safety and security at nuclear power plants,” IAEA, Vienna (2010).

[4] TELLABI, A., RULAND, C., BEN ZID, I., WAEDT, K., “Virtualization on Secure Platforms for Industrial Applications Current use cases and future perspectives,” (ICRMS, China, 2018), IEEE.

[5] STRATUS, Virtualization in industrial plants (2017), https://www.stratus.com/assets/Virtualization-in-Industrial-Plants.pdf.

[6] TELLABI, A., PETERS, L., RULAND, C., WAEDT, K., “Security Aspects of Hardware Virtualization Technologies for Industrial Automation and Control Systems,” GI (Berlin, 2018).

[7] KAREN, S.; MURUGIAH, S.; Paul, H., “Guide to Security for Full Virtualization Technologies,” NIST Special Publ., vol. 800(2011).

[8] PEPPERL+FUCHS, “HMI & Virtualization in Process Automation,” (2018).

[9] TELLABI, A., PAREKH, M., RULAND, C., EZZIYANI, M., “A case study of virtualization used in Mixed Criticality Systems,” (AI2SD, Morocco, 2019), Springer.

[10] FENTISS, XtratuM Hypervisor (2017), www.fentiss.com/xtratum.

[11] XEN, Xen Project Scheduler (2018), https://wiki.xenproject.org/wiki/Xen_Project_Schedulers.

[12] TELLABI, A., RULAND, C., “Empirical study of real-time hypervisors for industrial systems”, CSCI, IEEE, Las Vegas, USA (2019).

[13] BEYONDTRUST, Systems Hardening (2018), https://www.beyondtrust.com/resources/glossary/systems-hardening.

[14] SECURITYINTELLIGENCE, How to Build a System Hardening Program From the Ground Up (2019), https://securityintelligence.com/how-to-build-a-system-hardening-program-from-the-ground-up/.

[15] SERVERHARDENING, Server Hardening (2018), http://www.serverhardening.com/.

[16] UBUNTU, Dedicated to the security of Ubuntu (2019),https://ubuntu.com/security.

[17] UBUNTU WIKI, AppArmor (2019), https://wiki.ubuntu.com/AppArmor.

[18] UBUNTU MANUALS, AIDE (2019), http://manpages.ubuntu.com/manpages/bionic/man1/aide.1.html.

[19] DIGITALOCEAN, How To Use psad to Detect Network Intrusion Attempts on an Ubuntu VPS (2014), https://www.digitalocean.com/community/tutorials/how-to-use-psad-to-detect-network-intrusion-attempts-on-an-ubuntu-vps.

[20] UBUNTU WIKI, Smartmontools (2015), https://help.ubuntu.com/community/Smartmontools.