VIRTUALIZATION-ASSISTED TESTING OF NETWORK SECURITY SYSTEMS FOR NPPS

T. HOLCZER
CrySyS Lab, BME
Budapest, Hungary
Email: holczer@crysys.hu

G. BERMAN
CNEA
Buenos Aires, Argentina

S. M. DARRICADES
CNEA
Buenos Aires, Argentina

P. GYÖRGY
CrySyS Lab, BME
Budapest, Hungary

G. LÁDI
CrySyS Lab, BME
Budapest, Hungary

Abstract

Nuclear power plants use different digital assets to control the processes. These assets are normally connected by computer networks, and are targets of potential cyber-attacks. To avoid or mitigate the effect of such an attack, different security controls are used in accordance with the guidelines. Before deploying a new cyber security control, it must be tested thoroughly. The paper proposes virtual testbeds made of virtual computers and networks for these tests and shows how three widely used open source firewalls perform in such a test.

1. INTRODUCTION

The operation of a Nuclear Power Plant is based on controlling some physical processes and keeping the process values between some desired limits. This can be achieved by analogue controllers; however, digital controllers are also commonly used [1]. These sensitive digital assets (SDAs) are commonly connected to a network, where the management and the operation of the devices can be done remotely. The devices are normally distributed between systems and zones and are categorized into security levels [2][3]. The boundaries of the security levels are separated by security controls such as firewalls, but inside the levels and zones many other security controls must be used to achieve the desired level of security.

Before deploying any new system to a production environment it must be tested. This is even more important if it realizes a security control [4]. Tests should not be done in the production environment for obvious reasons; therefore, a simulator or a replica must be used. In this paper, we argue that virtual environments are very suitable for this task.

The remainder of this paper is organized as follows: In the next section we give a brief overview of virtualization techniques. In Section 3, we shortly introduce how we built our virtual testbed for security testing. In Section 4, we define the different security measures a Nuclear Power Plant can use, while in Section 5, we describe some actual testing of firewalls using the previously described virtual environment. At last we conclude the paper and give some overview of potential future work.

2. VIRTUALIZATION TECHNIQUES

Virtualization is the process of operating computers, networks, storage, and other components of the infrastructure on abstract (virtual) hardware as opposed to using physical hardware directly. Virtual hardware are backed by physical hardware (although not necessarily in a 1:1 ratio), with the virtual-to-physical mappings managed and enforced by a central component, the hypervisor.

Based on the hypervisor's location (see FIG 1), a virtualization solution may be Type 1 (also called native or bare metal) or Type 2 (also called hosted). In the case of type 1 virtualization, the hypervisor runs directly on the hardware and has exclusive control over the allocation of CPU, memory, peripherals, and other system resources. This solution allows a more fine-grained resource scheduling, and is only minimally subject to outside interference from other software components. VMware's ESXi and Microsoft's Hyper-V are Type 1 hypervisors. In case of Type 2 virtualization, the hypervisor runs on top of an existing (host) operating system as a regular piece of software, with no or little preferential treatment compared to other applications running on the same machine. Furthermore, it has no direct control over system resources, and is greatly affected by the environment. Examples of Type 2 virtualization solutions are VMware Workstation and Oracle VirtualBox.

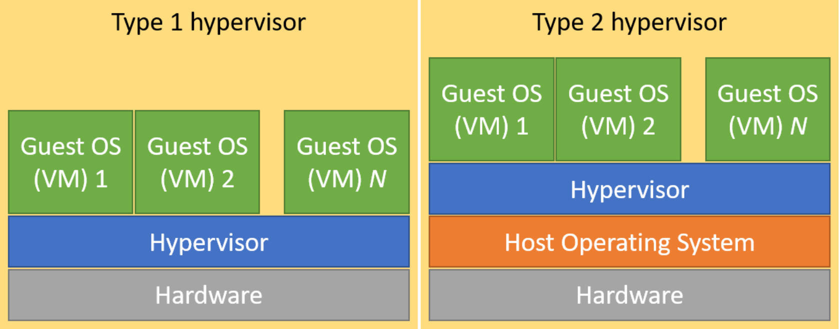

FIG 1. - Types of hypervisors

Type 1 hypervisors may work in three different modes: full virtualization, paravirtualization, and hardware-assisted virtualization. In full virtualization, the guest operating system runs without modifications, it is not aware of being virtualized and without direct access to the hardware. As a result, it will try to run privileged instructions (e.g. to access hardware), which will fail and put the CPU in an error (trap) state. The hypervisor will then be given control to handle the error, which has to make sure that the failed command achieves the intended effect from the virtual machine's point of view (emulation). This is called trap-and-emulate. Some instructions do not cause a trap, but fail silently. This is undesired, therefore, these instructions have to be replaced at runtime by others that cause traps when issued. This process is called binary translation. While full virtualization requires no guest or hardware support, it may have significant performance overhead due to the trap-and-emulate and binary translation procedures. In the case of paravirtualization, a specially modified guest operating system is used that is aware of being virtualized, and will issue hypercalls (calls to the hypervisor) instead of using privileged instructions. This eliminates most of the performance overhead, but requires a vendor-supported modified operating system which may not always exist. Fortunately, modern CPUs support hardware-assisted virtualization technologies such as Intel VT-x or AMD-V. Thanks to these, virtual machines can run unmodified and without the trap-and-emulate procedure. With hardware-assisted virtualization, the hypervisor can turn on virtual machine mode on the CPU when executing code from the guest OS, and the CPU will make sure that the instructions have the intended effect.

2.1. Advantages and disadvantages of virtualization

Employing virtual computers (machines) has the advantage that fewer (but more powerful) physical machines are required, reducing spatial requirements and physical hardware management related tasks. A physical machine may run several virtual machines, each of which could be running a different operating system at the same time, each one with different resource allocations such as CPU core count, memory size, and disk space. Most virtualization solutions support automatic or manual snapshotting. A snapshot saves the exact state of the virtual machine at the time of creation, making it possible to revert to an initial or known good state after a test or the failure of the virtualized operating system. Virtualization may also improve security by allowing system architects to isolate and lock down security-critical applications into virtual machines of their own, however, the use of hypervisors also expands the attack surface [5].

Although virtualization has many advantages, it has a few disadvantages as well. First, depending on which virtualization technique is used, there may be a noticeable performance hit. Second, one must learn how to use and manage the virtualization environment. Finally, it may be more problematic from a security point of view, considering that an attacker gaining access to the virtualization environment will then have access to all of the virtual machines, including any sensitive information stored on them. However, this is less important when virtualization is used to build test environments.

2.2. Limitations of virtualization

While virtualization is highly useful for realizing complex (test) scenarios, it has its limitations. Hypervisors can only run operating systems that are designed for the platform they are running on. This means that the usual hypervisor will only support x86 or x86-64 images, which is a problem because industrial devices such as Programmable Logic Controllers (PLCs) and other special hardware typically use different, often proprietary instruction sets. In these cases, emulators may still help. Emulators translate instructions between otherwise incompatible architectures one by one, making it possible to run binaries built for differing architectures. However, the process of emulation has a high performance penalty, and emulators are not always available for the specific architectures. As a result, at present, not all equipment can be virtualized, some physical devices are still required for testing lifelike setups.

2.3. Network virtualization

In recent virtualization solutions, not only computers can be virtualized, but also networking-related functionality. Network Interface Controllers (NICs) in the host machine may be turned into virtual switches, and can connect several virtual machines to a real physical network. Using virtual switches, it is also possible to connect a group of virtual machines in a way that no other virtual or physical machines outside of the group will be allowed to communicate with the members of the group, and traditional Virtual LANs are also typically supported. In addition, certain networking and security vendors such as Cisco or Palo Alto offer virtual appliances that may be installed just like a virtual machine which offer networking- or security-related features such as routing, proxying, Virtual Private Networking (VPN), firewalling, intrusion detection/prevention, user activity monitoring, or automated vulnerability scanning.

2.4. User emulation

Several security features rely on having (a baseline of) normal user activity – anomaly detection systems trigger when a user logs in outside of his usual login hours, a host monitoring system sends alerts when a new service is installed, and spam filters learn what is spam and what is not by inspecting what is often marked as spam by the users. For this reason, in our test environment it is imperative to have user activity.

Since our goal is automation, we aim to generate normal user activity using pre-defined user role behaviour models. In each model, a user logs in to a virtual system, and then performs a (non-deterministic) sequence of actions by typing commands into a shell or by clicking graphical user interface elements in a desktop environment. For this purpose, remote access services such as Secure Shell (SSH) or Remote Desktop (RDP) could be used; however, some machines do not support remote access or do not (must not) have it enabled. Furthermore, the use of these services skews user and network activity patterns since these generate extra network traffic that would not be present if real users were sitting in front of real computers. This is where virtualization solutions prove to be useful again: they make it possible to connect to and control a virtual machine via VNC, RDP, or a proprietary protocol in a way that no traffic is generated inside the tested network, and that to the virtual machine, it seems that it is interacting with a local user.

After introducing the basic concepts of virtualization, we show how it can be used for our purposes in the next section.

3. VIRTUAL NUCLEAR POWER PLANT

Building a virtual nuclear power plant (NPP) is a great effort. This effort is described in details in our other publication at the conference [6]. Here we only summarize some key points of the virtualized NPP. The interested reader is suggested to read the full paper referenced above.

Our virtual testbed was built with an Infrastructure as Code tool called Ansible, which can deploy tens of virtual machines and virtual networks based on some configuration files. An example of the deployed network can be seen on FIG 2. The whole network is virtualized on hypervisors, and the security controls described in the next section are analysed in this setup.

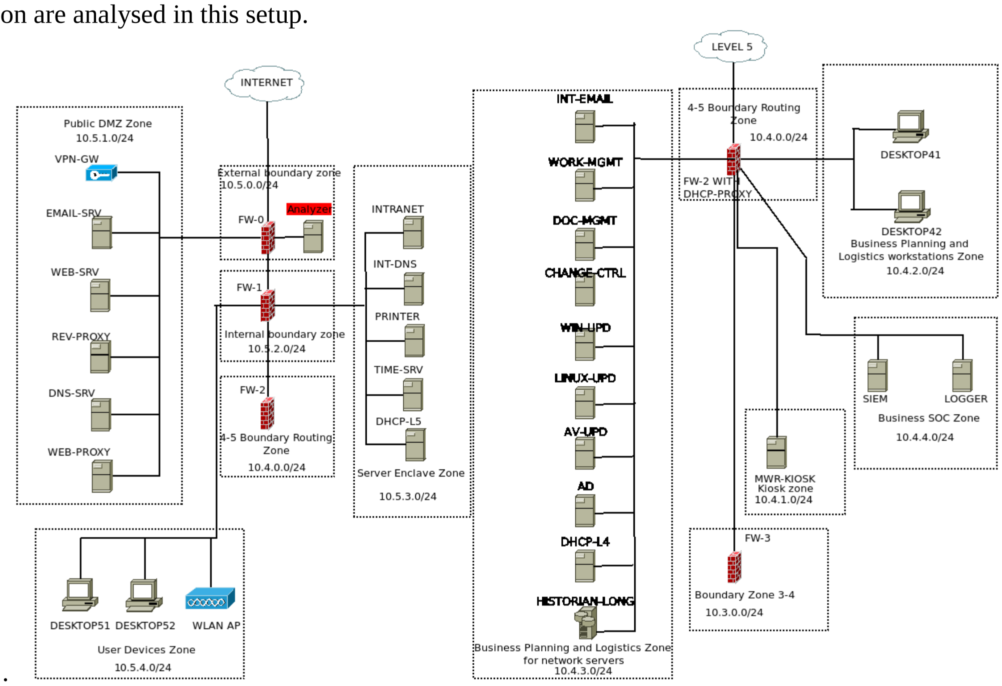

FIG 2. - Virtual infrastructure

4. SECURITY CONTROLS IN A NPP

4.1. Zones and segregation

The need to segregate a large network of devices that must be interconnected comes from several points: benefits in network administration, grouping devices that require similar controls so such controls can be implemented and monitored more easily, traffic separation allowing better control of network flow, isolation of a network, if any equipment were exploited, the attack would initially be confined to an area.

The zones will meet several of these points and can provide one or more necessary resources in our network. For example, data distribution, user equipment hosting, or packet filtering.

These Zones and Segregation of networks, must provide defence in-depth, via a design that contemplates the application of serial security controls thus weakening the initial attack since it must overcome different barriers instead of a single one. This also provides more time for incident response.

4.2. Firewall

Firewall systems provide the logical barrier to limit the entry or the exit of network traffic. Based on a traffic flow policy, rules on the firewall will be configured to filter such traffic. Furthermore, the firewall allows the redirection of specific traffic and address translation. They work primarily on layers 3 and 4 of the OSI model.

4.3. Proxy

Web proxy systems receive requests to access web resources. Thereafter the system makes such requests on behalf of the client and upon receiving the response from the destination redirects it to the client. Web proxies also allow filtering of higher layer traffic. Based on a policy, rules on the proxy are applied to limit the web resources that can be reached by the client. The rules may be based on the destination URL, time of the request, origin of the request and more. They can analyse the resource before delivering the response to the client. They work primarily in layers 3,4 and 7 of the OSI model.

4.4. Intrusion Detection System (IDS)

Intrusion Detection Systems are mostly divided into network based IDS and host based IDS. A network based IDS analyses the flow of network traffic and compare it with signatures that correspond to traffic related to known attacks or suspicious behaviour such as a port scan or malformed traffic. This allows for an early alert in case of suspicious traffic. The traffic flow to be analysed can be obtained almost anywhere in the network. Host based IDS can evaluate file integrity, log records, running process, hardware modifications, and more. Network based IDS works primarily on layers 2,3,4 and 7 of the OSI model.

4.5. Intrusion Prevention System (IPS)

Intrusion Prevention Systems are natural extensions of the IDS, since they allow to respond to an intrusion detected by the IDS to stop the attack. In this case, the IPS should be able to dynamically define new rules to be implemented by firewalls, proxies, and switches of the network. Such actions must be carefully considered since a false positive could cause a valid network flow to be stopped.

4.6. Security Information and Event Management (SIEM)

Network devices and services (desktops, servers, firewalls, switches, printers, etc.) generate countless records making it difficult to manually discern something that could be a security event. The Security Information and Event Management analyse these records and correlate them between the different devices, to give a general and centralized overview of security events in the network and to provide early warning of potential attacks to the systems. It also compares the records with pre-established rules and a database on indicators of possible attacks.

4.7. Free and Open-Source Software (FOSS)

Free and Open-Source Software has multiple advantages over proprietary software, for example it generates multiple solutions that are actively maintained allowing different solutions that can fulfil the same function -perhaps with different approaches- to be implemented at different levels, generating a more complex system to manage but at the same time more complex to successfully attack (defence in depth). As these solutions are being designed independently from each other they are less likely to share the same vulnerabilities.

Using and participating collaboratively in the development and update of free software tools from the most demanding side of the industry is a good way to actively contribute to the community.

Another benefit of working with open standards is that it allows to work with different systems no matter if they are FOSS or proprietary solutions.

The use of two or more software products from different vendors and technologies protecting against cyberattacks can improve the effectiveness of our in-depth defence.

5. SECURITY CONTROLS IMPLEMENTATIONS

A set of controls from the list provided by IEC636096 were selected to carry out the tasks that are necessary to apply the Security Policies on the devices in the network of our virtual facility. In this paper we evaluate three FOSS firewall solutions.

In TABLE 1 - List of controls and firewalls - are the results of the findings in attempting the implementation of such controls using three firewall solutions. The responses YES/NO means that the control can/cannot be implemented using that firewall.

The three firewall solutions selected are:

- IPtables / Netfilter[1]: IPtables is the user space application to manage the firewall rules and Netfilter is a module within the Linux Kernel, which will execute these rules. It does not provide any default GUI, management is performed by command line.It is the primarily firewall solution of many Linux distributions and it has great flexibility in the implementation of traffic control rules. It requires a certain level of knowledge of the underlying O.S.
- pfSense[2]: It is a firewall solution based on FreeBSD, with configuration based on WEB GUI which made it widely used in network infrastructures since it does not require knowledge of the FreeBSD O.S. nor Packet Filter -the FreeBSD firewall software- to configure it.
- Endian Firewall Community(EFW)[3]: It is a firewall solution based on RedHat, it also provides a WEB GUI that allows the administration of the solution which requires no knowledge of the underlying O.S. It uses IPtables / Netfilter with a group of network zones with predefined functionalities.

TABLE 1. LIST OF CONTROLS AND FIREWALLS

Control to implement	IPTABLES	PFSENSE	ENDIAN
Mobile devices and teleworking **Objective: Ensure the security of teleworking and use of mobile devices.**			
No remote maintenance and service Control. Remote maintenance and control should not be implemented.	YES	YES	YES
Access control **Business requirements of access control** **Objective: Limit access to information and I&C systems(assets).**			
Unused ports of network interface cards or communication equipment should be either physically locked or disabled.	YES[4]	YES	NO
Due to contractual obligations it may be necessary to forward selected process data from an I&C network towards a plant local network, e.g. a plant information network for nuclear physics engineering experts. This should be implemented without including the risk of any retroaction.	YES[5]	YES[5]	YES[5]
According to national law, it may be necessary to forward real-time or historical data to a regulatory body. This should be implemented so that the information can be received only by explicitly specified and agreed upon recipients. Any possibility of a retroaction should be excluded. In case the data towards the regulatory body is transferred via internet, the network interface towards the I&C should be via a data diode.	YES[5]	YES[5]	YES[5]
Due to technical reasons it may be necessary to forward selected information in real-time or near real-time to external specialized companies, e.g. OEMs, for equipment sanity or ageing assessments, e.g. for a turbine. Same limitation as towards regulatory body.	YES[5]	YES[5]	YES[5]
Development and engineering environment: restrictive configuration with regard to extendibility. Automatic inclusion of equipment into VLANs should be disabled.	NO	NO	NO
During operation only static network configuration should be used. Policies and technical guidance for the replacement and configuration of network interface cards or communication devices should not allow new or modified communication architectures.	NO	NO	NO

[1] IPtables / NetFilter, https://www.netfilter.org/.

[2] pfSense, https://www.pfsense.org/

[3] Endian Firewall Community, https://www.endian.com/community/

[4] The interfaces can be disabled using O.S. features

[5] A Data diode is recomended

Monitoring / network scanning	NO	NO	NO
Monitoring and logging of network use, e.g. for changing set-points of an I&C device, should be done by the supporting equipment.	YES[6]	YES[6]	YES[6]
Equipment **Objective: Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.**			
Printers should be connected to the I&C system via a firewall that only passes through the protocols and ports that are necessary for printing.	YES	YES	YES
The I&C system should be able to detect the removal of an already connected device and the subsequent connection of a new or the same device to the component standard interface (e. g., USB, etc.). Components are e. g. computers, automation controllers or network components. In addition, it should be possible to configure the I&C system in such a way that an alarm will be generated in order to initiate an analysis.	NO	NO	NO
Teleworking or other remote access to I&C equipment should not be allowed.	YES	YES	YES
Operations security **Operational procedures and responsibilities** **Objective: Ensure correct and secure operations of I&C systems within the nuclear facility.**			
Any change including additions or modification to I&C system that affect security should be controlled and coordinated according to change management policy or procedure. A baseline configuration of I&C system should be established, maintained, and documented, including at a minimum a current list of all components (e.g. hardware, and software), configuration of peripherals and software, version releases of current software, and switch settings of machine/hardware components. There should be crosscutting processes and procedures to assess and manage the potential for adverse safety and cybersecurity interactions that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures. There should be crosscutting processes and procedures to identify and leverage potential mutual reinforcements between safety and cybersecurity that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures. A change driven by safety considerations should be cross-reviewed by cybersecurity staff and reciprocally.	NO	NO	NO
Protection from malware **Objective: Ensure that information and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.**			
Implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);	NO	NO	NO
Implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);	YES[7]	YES[7,8]	YES[7,8]
Reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management;	YES	YES	YES
Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:	NO	NO	NO
Scan any files received over networks or via any form of storage medium, for malware before use;	NO	YES	YES
Scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization	NO	NO	NO
Scan web pages for malware	NO	NO	NO
Isolating environments where catastrophic impacts may result.	YES	YES	YES
Operations security **Logging and monitoring** **Objective: Record events and generate evidence.**			
Event logs recording user activities, exceptions, faults and cybersecurity events should be produced, kept and regularly reviewed. Once this cybersecurity-related events are detected and logged on the local system or network element, they should be collected and centralized in a dedicated system.	YES[9]	YES	YES

[6] While helping IDS with traffic logging

[7] Using IP address based blacklisting

[8] Using integrated web proxy

[9] Additional package must be installed and configured such as auditd https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-system_auditing/.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including: a) alterations to the message types that are recorded; b) log files being edited or deleted; c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.	YES[10]	NO	NO
Privileged user account holders may be able to manipulate the logs on I&C systems under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.	NO	NO	NO
The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source.	YES[11]	YES	YES
The time configuration of isolated I&C networks should be synchronized with the time configuration of other monitored networks. This synchronization can be performed manually or automatically, using specific filtering rules to keep segregation between the networks. Tools may be used also to keep accuracy in time management.	YES	YES	YES
Centralization of collected cybersecurity events Control Once collected the logs should be centralized in a dedicated monitoring system to avoid tampering in case of system compromise. The logs generated separately on each element should be centralized in a dedicated system to ensure to avoid tainted or deleted events in case of compromise, but also to allow multiple events from different sources to be correlated and analyzed.	NO	NO	NO
I&C-originated logs can be very specific and different from logs from IT systems. Once logs are centralized, in order to enhance the threats detection capabilities, I&C and security teams should focus not only on the identification of single isolated security events but also should build their own correlation scenarios, based on several indicators of compromise. The identification of correlation scenarios is generally based on return of experience, feedbacks from the security community, information provided by intelligence agencies or any other source of valuable information.	NO	NO	NO
Operations security **Control of operational software** **Objective: Ensure the integrity of operational systems.**			
The updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization.	YES[12]	YES	NO
Operational systems should only hold approved executable code and not development code or compilers	NO	NO	NO
An audit log should be maintained of all updates to operational program and libraries.	YES[13]	YES	YES
The controls like a software executables signing to confirm that its code has not been altered or corrupted since it was signed, should be implemented.	YES[14]	NO	NO
Operations security **Technical vulnerability management** **Objective: Prevent exploitation of technical vulnerabilities.**			
Technical vulnerabilities information sources and channels Vulnerabilities identification should rely on several sources and channels to increase efficiency in their identification. Therefore, it should not rely only on vulnerabilities publication (from suppliers, CERTs, etc.) but also from other sources such as audits, technical analysis, configuration management, security best practices compliance etc.	NO	NO	NO
Allowed removable media list should be specified for sensible systems in order to avoid undesired connections to potentially infected or harmful devices.	NO	NO	NO
The organization should define and enforce strict policies on which software is allowed to be executed on each system, to reduce the risk of malware or unwanted application execution.	NO	NO	NO
Communications security **Network security management** **Objective: Ensure the protection of information in networks and its supporting I&C systems.**			

[10] Additional package must be installed and configured such as syslog-ng https://github.com/syslog-ng/syslog-ng/.

[11] Additional package must be installed and configured such as chrony https://chrony.tuxfamily.org/

[12] ACL and sudo rules can be applied in O.S. to control file modification and services execution

[13] O.S. package management maintains a history of installed and updated packages

[14] O.S. package repository uses PKI for signing packages

All data (e. g. system software, engineering data, documentation, etc.) that will be brought into the I&C system using public networks needs to be analyzed to ensure integrity.	NO	NO	NO
The I&C system should be able to detect and log the removal of an existing device from and the subsequent connection of a new or the same device to the I&C network. In addition, it should be possible to configure the I&C system in such way that an alarm will be generated and annunciated in order to initiate an analysis.	NO	NO	NO
All security related incidents should be logged. The following incidents are examples: removal of devices, unsuccessful login attempts, malware detection, modification of executables, communication telegrams that contain inconsistent data.	YES[9]	YES	YES
For severe security events (severity could be based on threat and risk assessment) an alarm should be raised to the main control room.	NO	NO	NO
A central Security Event and Incident Monitoring (SIEM) function should be installed for the individual I&C system. The SIEM function should collect all security incidents from all I&C components (PCs, server, network devices, …).	NO	NO	NO
The SIEM function should have the capability to alarm configurable types of security incidents to the operator in the control room.	NO	NO	NO
The SIEM function should provide tools for analyzing the security incident event log.	NO	NO	NO
Security events should also be logged at local server. This is not to lose security events if the central SIEM functions is temporarily unavailable.	YES	YES	YES
Access to the authentication data should be locally available (without the need to connect to a server in the intranet or internet).	YES	YES	YES
All unused network ports and all other unused component standard interfaces (e. g. serial interfaces, interfaces for removable media …) of network devices (network switches, firewalls …) and I&C devices (e. g. computers, controllers) should be disabled by device configuration. Although devices could be physically connected, this measure ensures that devices, which are connected to unused network ports or component standard interfaces without authorization, cannot tamper with the I&C system.	YES[4]	YES[15]	NO
All communication services that are not used by the I&C should be either removed from the operating system, or if not possible be disabled.	YES[16]	NO	NO
In order to prevent an attacker from connecting to an unused network interface, all unused physical network interfaces should be disabled either in the operating system, or the BIOS, or in the firmware.	YES[16]	YES	YES
Standard communication protocols: Only secure standard protocols should be used (ssh, https)	YES	YES	YES
In order to detect abnormal and malicious communication all network traffic of an individual I&C system should be monitored by an intrusion detection system. However it needs to be implemented in such a way that the safety related properties of the I&C system stay within the required level.	NO	NO	NO
If an abnormal condition is detected this should be logged and an alarm should be displayed to the operator in the main control room. Remark: It is recognized that an intrusion detection system can produce false positives.	NO	NO	NO
If a network connection between the I&C system and non I&C networks (e. g. the office area within the NPP) is needed (e. g. for transmission of online or archived process data from the I&C system to the NPP office environment for analysis purposes) the border between the I&C network and the non I&C network should be sufficiently protected according to the result of the threat and risk analysis. For the most sensitive situations, one possible solution is a one way data communication conduit. The one way communication allows sending communication telegrams from the I&C system to the non I&C system, but ensures that absolutely no communication telegrams (not even handshake telegrams) can be sent from the non I&C system to the I&C system. Note: Such a diode mechanism is not always possible to implement.	YES	YES	YES
Direct connection of I&C systems to the internet should be prohibited, since these I&C systems are essential for keeping the NPP in a safe state in case of incidents and accidents. This control is also valid for remote I&C system service. Remote I&C service should not be allowed at all for S1 and S2 graded systems.	YES	YES	YES

[15] Feature to disable network interface not other type of ports

[16] Services can be disabled using O.S. features

Since wireless communication can be easily disturbed by interfering transmitters or, (if the firmware of the wireless device is poorly developed) could be hacked from outside of physical protection barriers, the use of wireless communication should be avoided.	NO	NO	NO
Regular checking for unknown wireless communication entry points. In order to ensure that no wireless communication entry points have been added to the I&C system in an unauthorized way, regular checking for unauthorized wireless communications is necessary.	NO	NO	NO
Blocking of not allowed inbound communication on server Block all inbound types of communication that are not supported by the I&C server.	YES	YES	YES
Wrong communication telegrams should be logged and alarmed Malformed or unexpected communication telegrams should be logged and alarmed.	YES	YES	YES
NUC - Cybersecurity and Architecture			
Objective: Provide a set of high level cybersecurity measures and controls for the I&C and ES architecture.			
The robustness of security measures and equipment used to perform segregation between two security zones should be related to the organization’s security degrees definition (for instance data diode vs firewall vs router, etc.).	YES[17]	YES[17]	YES[17]
The “need-to-know principle” must be followed also within a Security Zone. For example, an operating system administrator or network administrator should have access only to the systems or networks he has to care for, and not (by default) to all systems of a Security Zone.	YES	YES	YES[18]
Administration systems, especially dedicated to I&C and ES management, are critical within the architecture due to their high privileges regarding the managed systems (i.e. accounts management, private keys, remote server access...).Therefore they should be isolated in a dedicated administration Security Zone, which should not allow incoming network connections to reduce attack surface from the other Security Zones in case of compromise or infection.	YES	YES	YES
Data extraction and collection, Ensure that extracted and collected data for lookup purposes do not adversely impact I&C and ES systems. Confidentiality of such data should be ensured by Security Controls such as identification, authentication, access control and network filtering.	YES[19]	YES[19]	YES[19]
Integrity of data should be ensured by security measures such as digital signature for high security requirements or checksums for lower security requirements.	NO	NO	NO

6. CONCLUSION

In this paper we presented how virtualization can be used for pre-deployment testing of security controls. We introduced the basics of virtualization, and on a virtual testbed we evaluated three specific open source firewall solutions (IPtables, pfSense and Endian Firewall). In the future we want to cover other controls in our analysis such as intrusion detection systems or security incident and event management systems.

ACKNOWLEDGEMENTS

We would like to acknowledge the help of every participant of the CRP-J02008 in creating this paper, and IAEA for supporting this project.

REFERENCES

[1] RUST, J.H. Nuclear power plant engineering. Vol. 16. Buchanan, Georgia: Haralson Publishing Company, 1979.

[2] IAEA, Computer Security at Nuclear Facilities, NSS17, 2011

[3] IAEA, Computer Security Techniques for Nuclear Facilities, NSS47, Draft, 2017

[4] PARNAS, D. L., ASMIS G. J. K., and MAEDY J. "Assessment of safety-critical software in nuclear power plants." *Nuclear safety* 32.2 (1991): 189-198.

[5] PÉK, G., BUTTYÁN, L., BENCSÁTH, B., A survey of security issues in hardware virtualization, ACM Comput. Survey., 45 3 (2013) 1–34. doi:10.1145/2480741.2480757

[6] ALTSCHAFFEL R et al, Nuclear Power Plant in a Box, ICONS2020, IAEA, 2020

[17] Not recommended for security level 1

[18] Up to 4 zones

[19] Only network filtering can be achieved