LOGIIC
Virtualization Project

February 2015

Final Public Report

Document Title	*LOGIIC Virtualization Project Public Report*
Version	*Version 1.0*
Primary Author	*A. McIntyre (SRI)*
Distribution Category	*LOGIIC APPROVED FOR PUBLIC DISTRIBUTION*
Approval Status	*APPROVED FOR LOGIIC USE*
Reviewed by AF Legal	*2015-02-25*
Approved (date)	*2015-02-25*
Approver (EC or AF)	*EC*
Digital Signature for PDF	*Signed by the Managing Director Automation Federation on February 25, 2015*

REVISION HISTORY

Version	*Author*	*Date*
1.0	A. McIntyre (SRI)	1-19-2015

EXECUTIVE SUMMARY

The LOGIIC[1] Consortium was established by members of the oil and gas industry in partnership with the Cybersecurity Research and Development Center (CSRDC) of the U.S. Department of Homeland Security (DHS), Science and Technology (S&T) Directorate to review and study cyber security issues in Industrial Automation and Control Systems (IACS) which impact safety and business performance as they pertain to the oil and gas sector. LOGIIC has sponsored research initiatives that involve the interests of oil and gas sector stakeholders.

The LOGIIC Virtualization Project focused on the use of virtualization solutions in the operational environment. The principal project objective was to evaluate and test current automation vendor industry practices to generate guidelines and reference architectures that demonstrate methods for securing virtual environments that span multiple process control network layers.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to the IACS environment, and their cyber security capabilities. Hands-on assessment activities conducted in an IACS environment identified the security capabilities of virtualization solutions and the impacts associated with their use in an operational setting.

Like many technologies applied in the IACS environment, optimizing a process or maximizing benefit often requires interface with complex technologies. Virtualization requires strong technical skills to design, set up, and manage the system, and collaboration with the automation vendor to maximize benefit of the technology. In addition, lifecycle maintenance for the system is required to ensure that it remains secure.

The detailed technical findings and operational conclusions derived during this project produced a set of topics that should be evaluated when considering the viability of virtualization in a specific IACS environment. This includes the product evaluation, planning and design, and implementation phases.

As a result of the technical assessment and analysis, this report presents conclusions on the use of virtualization in an IACS environment. The objective of this report is to convey important factors that should be weighed when considering virtualization in an IACS environment and to support a dialogue between asset owners and automation vendors.

[1] LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity.

Table of Contents

Table of Figures

DISTRIBUTION

This report is approved by U.S. Department of Homeland Security and the LOGIIC Executive Committee for unlimited public distribution.

ABSTRACT

The LOGIIC program was established to review and study cyber security issues as they pertain to the oil and gas sector, and has sponsored research initiatives that involve the interests of oil and gas sector stakeholders. The exponential growth in attempted and successful cyber threats, whether malicious or unintentional, combined with operational demands for increased system reliability and availability motivate the need for a better approach.

The LOGIIC Virtualization Project focused on the use of virtualization solutions in the operational environment. The principal project objective was to evaluate and test current automation vendor industry practices to generate guidelines and reference architectures that demonstrate methods for securing virtual environments that span multiple process control network layers.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to Industrial Automation and Control Systems (IACS) environment, and their cyber security capabilities. Hands-on assessment activities conducted in an IACS environment identified the security capabilities of virtualization solutions and the impacts associated with their use in an operational setting.

This report discusses the assessment attributes, findings, and considerations for using virtualization solutions in IACS environments.

ACKNOWLEDGEMENTS

The project to evaluate virtualization technologies was developed and guided by the members of the international LOGIIC forum, who devote their time and expertise to conduct projects that will lead to improvements to cyber security in the oil and gas industry, and to the IACS community in general. The Automation Federation serves as the LOGIIC host organization and provides a necessary home and legal framework for our efforts.

LOGIIC would like to thank the DHS S&T Directorate for providing leadership, vision and commitment to enhancing cyber security.

We would also like to express our appreciation for the work of our team of subject matter experts (SMEs) who refined the evaluation strategy, performed the system evaluations, and developed the project reports. Since the inception of LOGIIC, the scientific research organization SRI International has provided coordination, project management, and subject matter expertise.

The work performed on this project by SRI International and its subcontractors was funded under contract to the DHS S&T Directorate. The content is solely the product and responsibility of the LOGIIC program and does not necessarily represent the official views of DHS.

1 INTRODUCTION

The LOGIIC program was established to review and study cybersecurity issues as they pertain to the oil and gas sector, and has sponsored research initiatives that involve the interests of oil and gas sector stakeholders. LOGIIC initiatives are applicable to many industries with control systems.

The LOGIIC Virtualization Project focused on the use of virtualization solutions in the operational environment. The principal project objective was to evaluate and test current automation vendor industry practices to generate guidelines and reference architectures that demonstrate methods for securing virtual environments that span multiple process control network layers.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability the IACS environment, and their cyber security capabilities. Hands-on assessment activities conducted in an IACS environment identified the security capabilities of virtualization solutions and the impacts associated with their use in an operational setting.

This report presents conclusions on the use of virtualization in an IACS environment. These conclusions are a result of technical assessment and analysis. The objective of this report is to convey important factors that should be weighed when considering virtualization in an IACS environment and to support a dialogue between asset owners and automation vendors.

The intended audience for this report is the IACS technical and security communities, and automation and security vendors.

2 PROJECT SUMMARY AND BACKGROUND

The LOGIIC Virtualization Project was established and defined by the LOGIIC members (Technical Team, Executive Committee, and the DHS sponsor). Automation vendors were engaged and invited to participate in an assessment.

Project 8's primary objective was to evaluate and test current automation vendor industry practices to generate guidelines and reference architectures that demonstrate methods for securing virtual environments that span multiple process control network layers.

In August 2013, LOGIIC conducted a survey of virtualization technologies available from a selected automation vendor set. At the same time, LOGIIC conducted a survey of Executive Committee members on their use of virtualization and related decision factors in implementation. Many members seek a level of confidence in key areas (security, maintainability, implementation, and optimization) prior to expanding the use of virtualization in their organizations.

Presently, LOGIIC members are utilizing, or are considering utilization of virtualization in the following ways[2]:

- Access to and movement of data between security zones
- Management of legacy systems and applications
- Historization
- Factory acceptance testing
- Training and maintenance/admin functions
- Lab and simulation environments
- Utility systems that support the BPCS
- HMI workstations and servers
- Footprint reduction
- Advanced control applications
- Calculation programs
- Domain controllers
- Optimization systems
- Database systems

To meet the project objectives, an automation vendor selection process was established; candidates were evaluated; and selections were made based on established criteria. Expanding knowledge in virtualization required LOGIIC to conduct hands-on testing activities. A selection process chose multiple automation vendor technologies for evaluation by a selected SME. Building upon previous surveys, test scenarios were selected to reflect core questions posed by the LOGIIC team members. These areas of interest validated the investigation of risks associated with using virtualization in an operational environment.

The objectives of the project's assessment focused on answering key technical questions related to the use of virtualization in an operational environment. Test scenarios were crafted to produce results that answer technical questions relating to implementation, design, specific use cases; and to provide input to primary conclusions regarding the use of virtualization in general.

[2] LOGIIC Member Survey, August 2013

The assessment sought to answer the following questions:

- What are the ramifications of using a hardware vs. software solution?
- What are the security differences between Hyper-V® and VMWare®?[3]
- Are resource utilization and SCADA optimization attainable while maintaining security?
- What are the security risks associated with maintaining and remotely accessing the virtual machines?
- Are there risks associated with very standard and open software choices?
- How much automation vendor access to the systems is required, and does this pose a risk?
- Do the increased fault tolerance and rollover capabilities of virtualization provide a more secure solution?
- Can the thin client be used as a threat vector?
- What are the ramifications of shared memory space in a virtualized environment?
- Do patch management and update processes present threat vectors?

This assessment focuses on the testing and analysis of the underlying technologies and architectures which support virtualization solutions, including both VMWare® and Hyper-V® components. As defined by LOGIIC, the following scenarios in Figure 1 were within the scope.

[3] Hyper-V is a registered trademark of Microsoft. VMware is a registered trademark of VMware.

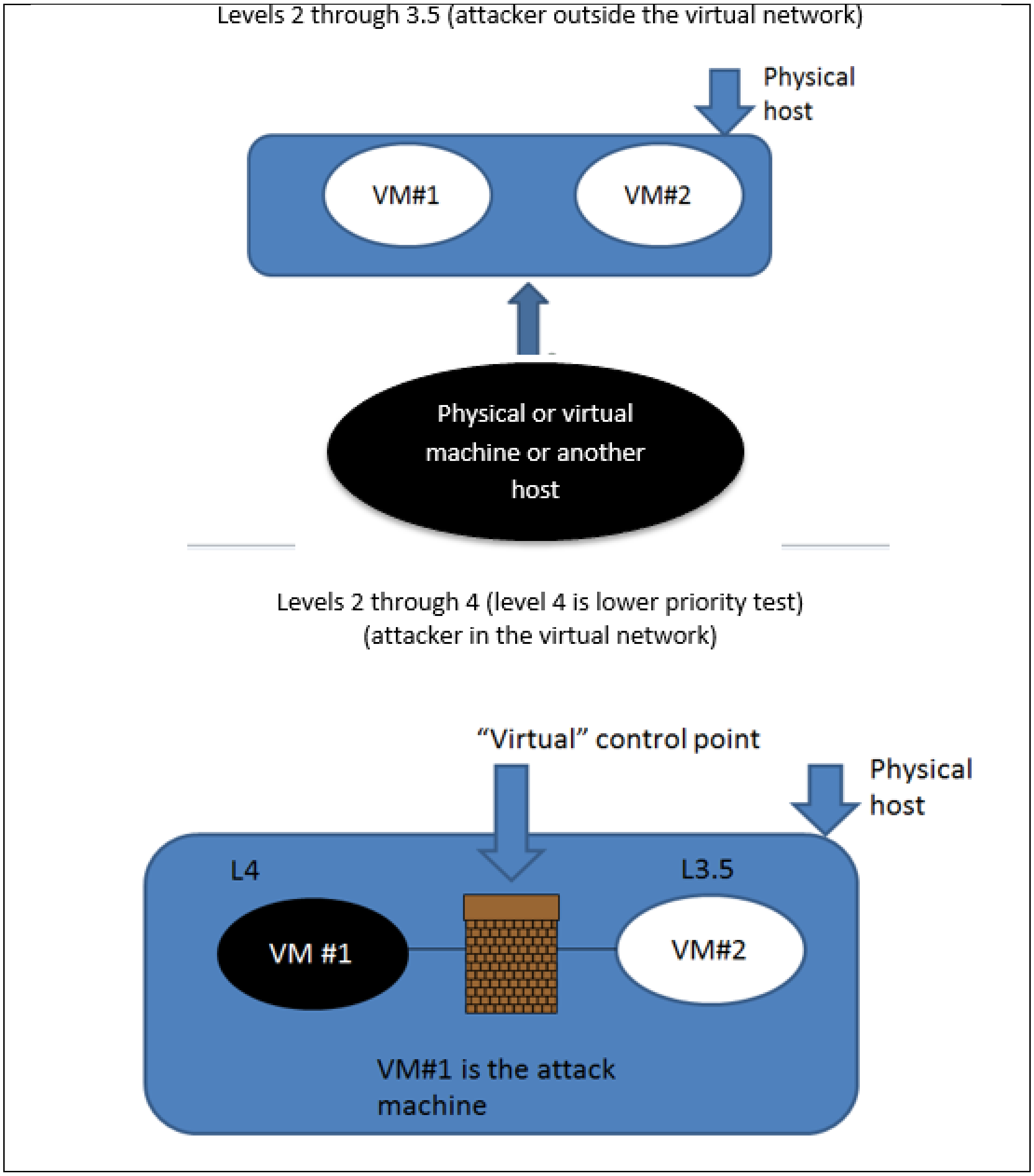

Levels 2 through 3.5 (attacker outside the virtual network)
Physical host
VM#1
VM#2
Physical or virtual machine or another host
Levels 2 through 4 (level 4 is lower priority test)
(attacker in the virtual network)
"Virtual" control point
Physical host
L4
L3.5
VM #1
VM#2
VM#1 is the attack machine

Figure 1: LOGIIC-Defined Test Scenarios

The project scope included the virtual machine/application and the system architectures used to host the servers. The LOGIIC team defined the scope to focus on the operational environment. This scope is reflected in the figure below.

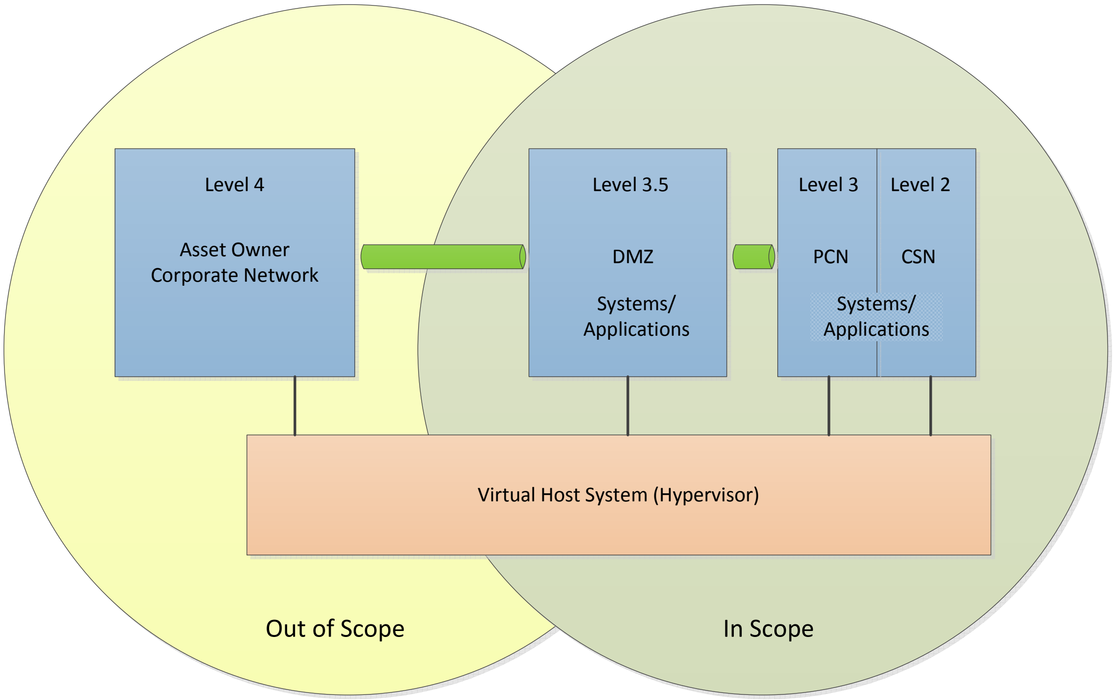


Figure 2: LOGIIC Defined Scope

3 TECHNICAL APPROACH

Technical surveys, market reviews, and engagement with automation vendors contributed to the scoping of the project and individual test scenario. Assessment and analysis followed a standard approach and used previously tested assessment methodologies. The details of the approach are outlined in this section.

Assessment Methodology

LOGIIC consistently bases all assessments on the foundational risk equation, where Risk = Threat x Vulnerability x Consequence. This ensures that all testing expresses a plausible threat that is applicable to the oil and gas industry. The assessment scope and individual test scenarios were defined by characterizing risk in terms of threat, vulnerability and consequence.

After selecting an automation vendor and a SME in testing virtual technologies, a Test Plan was developed that identified test scenarios and rules of engagement. The automation vendor provided network and design diagrams in advance, as well as a demonstration of the system and key factors in implementation. Therefore, the assessment was considered a “full knowledge” assessment, with the automation vendor providing information and device details in advance.

The following high-level steps were followed during the assessment for each device or system of devices:

1. Reconnaissance
2. Information Capture/Data Retrieval Attempts
3. Targeted Attack

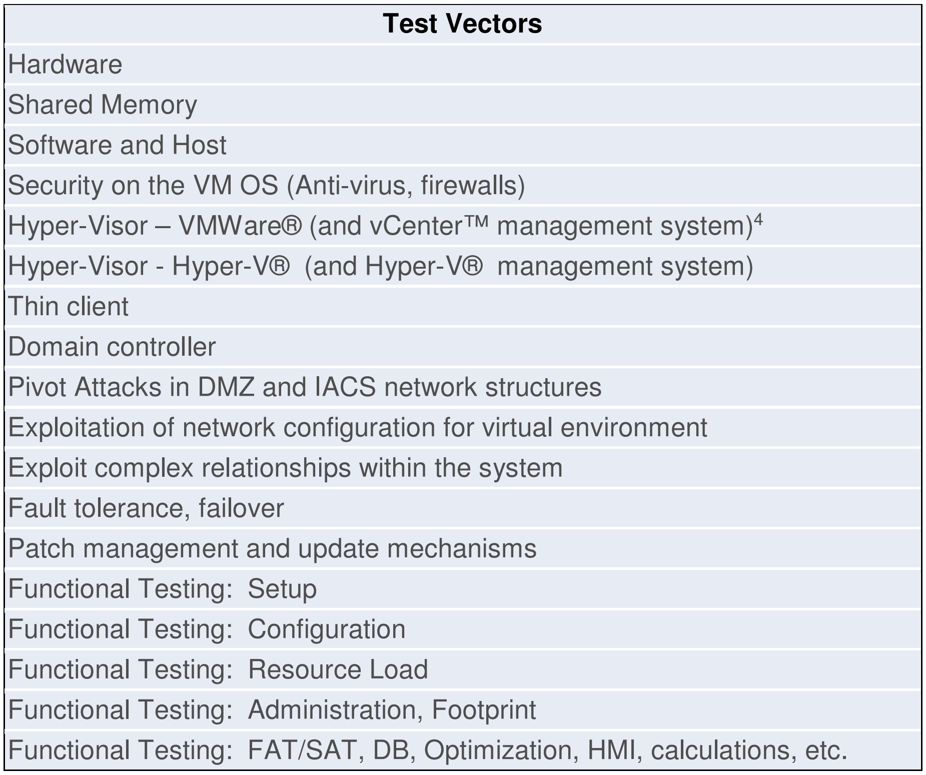
As with the standard LOGIIC assessment approach, attacks were only considered viable if they were traceable and reproducible.

While technical activities, such as reconnaissance and attack, form the basis for most of the assessment findings, observations about interactions with devices, setup, and troubleshooting can provide valuable information for the LOGIIC team. Performance of security features, resilience, and robustness were measured by technical results and by general observations during the assessment.

Assessment Approach

Two main virtualization products, VMWare® and Microsoft Hyper-V®, serve as the basis for nearly all virtualization solutions presently offered by automation vendors. Implementations of both products were tested during a single assessment period.

Test vectors were developed by the LOGIIC team, and by the SME, to answer key questions of specific interest to the LOGIIC members. These test vectors, listed below, were utilized by the SME to develop broader test scenarios and select applicable tools.



Test Vectors
Hardware
Shared Memory
Software and Host
Security on the VM OS (Anti-virus, firewalls)
Hyper-Visor – VMWare® (and vCenter™ management system)[4]
Hyper-Visor - Hyper-V® (and Hyper-V® management system)
Thin client
Domain controller
Pivot Attacks in DMZ and IACS network structures
Exploitation of network configuration for virtual environment
Exploit complex relationships within the system
Fault tolerance, failover
Patch management and update mechanisms
Functional Testing: Setup
Functional Testing: Configuration
Functional Testing: Resource Load
Functional Testing: Administration, Footprint
Functional Testing: FAT/SAT, DB, Optimization, HMI, calculations, etc.

Figure 3: Test Vectors

The SME conducted the test scenarios using their attack methods, payloads, and equipment. Two assessment teams (one aligned with Hyper-V® and another with VMWare®) performed concurrent tests where possible.

The following is a list of significant targets that occurred over the 10-day assessment period. Some tests were scheduled according to the attendance of LOGIIC members with interest in specific topics.

1. VM OS assessment
2. Thin client and remote access
3. Hardware, including network and storage
4. Hypervisor assessment
5. Fault tolerance
6. Custom exploit development and fuzzing

[4] vCenter is a trademark of VMware.

The SME employed reconnaissance and attack techniques that included the following steps:

Reconnaissance

- Survey the architecture
- Identify unnecessary services
- Survey and/or verify encryption
- Survey access control
- Search for known vulnerabilities in the architecture
- Identify assets and keys
- Perform auditing
- Identify attack and denial of service (DoS) vectors within the architecture

Testing

- Assess configuration against standard implementation practices
- Identify exploitable vulnerabilities
- Image management investigation
- Test upgrade/patch functionality
- Test stability of system
- Virtual environment network configuration evaluation
- VM OS isolation investigation
- Virtual environment application evaluation
- Pivot attacks

Figure 4 Test Techniques

Tools utilized included publicly available products alongside custom scripts developed by the SME:

- Kali Linux™ distribution for penetration testing[5]
- Wireshark®[6]
- Computer forensic tools
- Custom attack scripts
- Existing exploits
- Reverse engineering tools

[5] Kali Linux ™ is a trademark of Offensive Security.

[6] Wireshark is a registered trademark of the Wireshark Foundation.

White cell[7] activities during the assessment were performed by the LOGIIC Technical Lead. All test techniques, steps, results, and observations were noted during the assessment.

Analysis of Findings

The technical conclusions conveyed in the following sections of this report are based on a series of inputs and data sources, including:

- Background research conducted under the project
- Product documentation, technical briefings, and design details from the automation vendor
- Assessment test scenario results
- Background information on each threat vector provided by the SME
- Observations during the assessment
- Functional and usability testing

Although the assessment focused on the security aspects of using virtualization technologies in the IACS environment, and any risks associated with such an implementation, consideration was also given during the testing to ease of setup, maintenance, knowledge and resources to maintain, and usability. The SME assessment team, automation vendor, and LOGIIC technical leadership worked together to form broader conclusions.

[7] A white cell is an independent person who collects findings and records events during the assessment. White cell activities are not typically performed by a red teamer or a vendor.

4 Assessment Findings

The assessment produced numerous technical and operational findings. This section presents technical and operational findings and key discussion points.

Technical Findings and Vulnerabilities

During the assessment, the SME conducted approximately the same number of test cases against both Hyper-V® and VMware® architectures. While some test cases were direct exploit attempts, other cases focused on information collection as building blocks for other attacks. Findings from each test case were reviewed and ranked by consequence-based severity and likelihood. Technical vulnerabilities were identified in hardware, software, and implementation areas. These vulnerabilities are grouped into broader risk categories listed in the remainder of this section. Each area is relevant when considering the use of virtualization in an IACS environment, and should be included in the evaluation, selection, and design process.

Design, Implementation, and Management

As with any computing capability implemented in an IACS environment, security must be considered at all logical layers of the solution and throughout the life cycle. All standard security considerations within hardware, software, implementation, usability, and performance impacts that are typically weighed in a new project must be considered with a virtualization solution. However, due to the reduced footprint and potential complexities of the system, additional attributes must be evaluated. Security must be built into the design, including measures beyond maintenance of the VMs. For example, the following must be considered not only for guest operating systems and control system software, but also for hypervisors and virtualization management software:

- Role-based access control
- User and administrative account management
- Password management, such as removal of default passwords, and requirements for minimum complexity and expiration
- Operating system and software updates and patches
- System log monitoring and intrusion detection

Standard components of virtual solutions, such as common services, ports, and web elements, may contain vulnerabilities that are not necessarily mitigated by virtualization. Common components include Remote Desktop Protocol (RDP), the Windows NT LAN Manager (NTLM) used as the challenge/response protocol, and common credentialing systems. These may be vulnerable to man-in-the-middle (MITM) attacks, dictionary attacks, and other common exploits. Therefore, layered cyber security that considers these risks is necessary throughout the design and implementation.

Despite the separation of VMs, the security and stability impacts of shared hardware and networking must be considered. Hypervisors and virtualization management components become critical, high-value assets. Many of the findings from the LOGIIC assessment focused on the importance of the Hyper-V® Manager and the Server for vSphere®[8]. The technical findings led to the conclusion that configuration is critical among these high-value components. The Hyper-V® Manager controls all VM actions such as starting, stopping, configuration, creation, and deletion. Reduction of risks at setup and good management practices can together mitigate many vulnerabilities. For example, these practices include bans on single-user accounts, regular patching, bans on default passwords, and logging and monitoring. Likewise, vCenter™ Server accounts should also use role-based access control without default passwords. Both the vCenter™ Server and Hyper-V® Manager can be used with firewalls. These should be configured and maintained accordingly.

An asset owner's clear understanding of the automation vendor's virtualization offering is important in the design and implementation of the product. Asset owners should be fully aware of the automation vendor's design, implementation plan, risk mitigation and patch management schema. The importance of life-cycle planning and patch management is significant, and discussed in further sections in detail. In general, however, asset owners should be aware that automation vendor practices should include:

- Inherent layered security
- Documented security recommendations
- Fault tolerance, high availability, and failover options
- Good coding practices, such as code obfuscation and no hard-coded passwords
- Long term manageability and scalability
- Established processes to manage changing risks with growth

Another broad design and implementation consideration is threat and physical access. Insider threat and physical access to hardware provide numerous opportunities for exploitation.

Physical access to the hardware provides an opportunity to compromise the system, and it poses a security risk that should be evaluated and mitigated with site security controls. This may include access to USB and other open ports with options to access the BIOS, keyboard, and logon screens. Technical conclusions made by the SME indicate that physical access may indicate full ownership of the system.

Networking

Networking design and its security are critical considerations in a virtualization solution. Complexities associated with the virtualization components must be considered. For example, when using a blade system or system with multiple Network Interface Cards (NICs) or multiple networks, setup should be performed carefully, to ensure there is no network cross-traffic. Networks are subject to MITM attacks, particularly from the insider threat perspective. Likewise, the presence of standard components, such as RDP, offer the possibility for RDP credential capture, syn floods, and other DoS attacks.

Like physical systems that may or may not be entirely maintained by the automation vendor, virtual systems require perimeter security. Network design should consider the location and potential need for outbound and inbound traffic. Some solutions may require a connection to a management network or outside connection through a DMZ for setup or to perform maintenance and patching. These connections may be persistent or periodic. If connections are made beyond the immediate IACS environment, then DMZ configuration and other perimeter security must be considered. For example, if a management network connects to the Internet through a poorly configured DMZ, it could potentially become an attack vector from an outsider threat.

[8] VSphere is a registered trademark of VMware.

Good networking practices pertain to virtualization solutions as well. Firewalls, whether embedded or physical, must be carefully configured and maintained, with a focus on incoming ports. Passwords should not be transmitted in the clear. Remote user accounts should be configured carefully, with consideration to role-based access control, monitoring, log management, and intrusion detection.

Planning

Virtualization solutions are not inherently secure unless designed and configured accordingly. Virtualization may reduce some risks but introduce others. Clear objectives, planning, design, and project definition is important to maximizing the benefits of virtualization. Asset owners and automation vendors should collaborate to plan, scale, and implementation the solution. Specific aspects of the system require consideration during the initial planning stages; these aspects include the need for high availability, fault tolerance, and failover capabilities (discussed in detail in a later section). Performance, optimization, and footprint reduction are aspects that can be best realized during the initial planning stages. However, the asset owner must also forecast the skillsets and time required to manage and grow the solution over the entire lifecycle.

Scalability

One of the main reasons virtualization is used today in process control is the reduction in footprint. Correct implementation of virtualization provides a reduction in number of required hardware pieces. It is important to note that system growth and future needs must be carefully considered during the initial implementation. Limitations of the hardware and software can impact scalability. Without careful planning, the asset owner may destabilize the system through growth, or quickly reach maximum capability. In this case, the asset owner may have to purchase additional hardware and reduce the full return on investment of a reduced footprint. Example considerations:

- Hyper-V® allows an administrator to grow and increase VMs without limitation, which could overextend resources and crash the system.
- VMWare® does not allow growth beyond limits that could break the system. Instead, an alert is generated, and the action is lost.

Optimization and growth, such as adding equipment or planning for new hosts (rather than VMs), can occur without introducing new security risks. Aside from potential destabilization through resource usage, addition of new hosts does not create new threat vectors or impact overall security.

Cluster and Blade Environments

Security considerations differ between the cluster and blade environments. Blade environments mitigate certain security risks via reduced networking and distribution. For example, an iSCSI network in a traditional cluster environment may present new attack vectors. Although more attack vectors may exist in a cluster due to its distributed nature, these risks should be weighed against issues known to blade environments. For example, embedded switch risks and cross-traffic issues can exist in a blade if it is not correctly configured. Embedded switch configuration may be controlled by the hardware manufacturer, not the automation vendor. Misconfiguration of the switch could present new threat vectors.

Threat

The use of virtualization at Layer 3/3.5 or below assumes that risks come from the insider threat. Insider threats can be managed with physical security and role-based access control, policies, and procedures. Virtualization does not necessarily reduce the risk to insider threat, although it may change the threat landscape and potential vectors. In cases where connection to a management network is required to support the virtualization technology, outsider threats may pose a risk, but only if other perimeter defenses are compromised. Outsider threats would have to penetrate the DMZ and the management network to access assets on that network and below. As mentioned previously, if networks are interconnected, the asset owner must rely on proper configuration and DMZ structuring to ensure the security of the virtual systems.

Component Management and Shared Memory

It is important to consider the fact that although hardware may be reduced in size and number in a virtual environment, several key components still exist that require ongoing management. These include the core hypervisors and hardware (whether a cluster or blade), thin clients, and any networking components such as hubs and physical firewalls. The configuration should be secured, and ongoing component management and maintenance should be performed to ensure that no new threat vectors are introduced.

Shared memory in a virtualization environment held particular interest to the LOGIIC members. The SME performed research specific to this threat and crafted customized exploits to identify attack vectors that exploit shared memory. While this attack vector is theoretically possible, conclusions were developed that suggest a nation-state-level threat would likely be required for successful completion of this attack. The complexities, time, and resources required to exploit shared memory indicate that other, more accessible, vectors are more attractive to an adversary.

Patching

Perhaps the most important of the assessment’s operational findings is the need for patching and system maintenance. Many of the attacks succeed because the system was not fully patched and up-to-date at the time of testing. This indicates the importance of up-to-date patching. Unpatched systems have significantly larger attack surfaces. An important consideration is the fact that Hyper-V® and VMWare® patches may not be accredited by the automation vendor, or may not be accredited immediately. This requires the asset owner to independently download and install qualified[9] patches for VMWare® and Hyper-V®. Some asset owners may be reluctant to do this without automation vendor accreditation. Likewise, patching increases the number of resources required for maintenance of the security of the system. If patches were not updated over the course of time, a significant number of attacks could be potentially successful. Asset owners may choose to utilize the IEC 62443-2-3 as a guideline for patch management in the IACS environment

Considerations with Failover, High Availability, and Fault Tolerance

A number of automation vendors offer different hardware solutions based on the customer’s objectives. Perhaps the most important consideration when designing an architecture is the need for failover, high availability, and fault tolerance. It is important for asset owners to engage the vendor to obtain a clear

[9] Per IEC 62443-2-3, qualified patches are tested and deployed in a manner that reflects the production environment, to ensure that the reliability and operability of the IACS is not negatively affected when patches are installed.

understanding of how vendors define these capabilities in the context of their architecture designs and product offerings.

Significant time during the assessment was dedicated to the discussion of failover, high availability, and fault tolerance. An asset owner's use of the system, criticality of the applications hosted, and overall risk portfolio must be considered when planning continuity of operations. Planning for this continuity when using virtual systems must occur during the design phase. Failover, high availability, and fault tolerance have hardware dependencies and relative time scales that must be evaluated. The following is a description of each.

These terms are sometimes used interchangeably in other areas of IT or business, but there are distinct differences in the virtual environment. The descriptions below were derived from discussions between the automation vendor, LOGIIC team, and SME during the assessment to assist in forming broader technical conclusions.

Failover

The term "failover" is used when focusing on hardware. Failover occurs in a cluster environment when one host (such as a blade server) fails, or stops, and one or more other hosts takes over the responsibilities of the failed host. Note that this is not software or application failover. Host failover is available only in a cluster environment but can be used with Hyper-V® or VMWare®.

Fault Tolerance

Fault tolerance offers the capability to continue operating through disruptions or failures, and occurs automatically. Fault tolerance occurs when a host fails, or stops, and ghost VMs automatically take over responsibilities. The ghost is a bit copy of the original host. This capability is available in VMWare® but not Hyper-V®, and is only available in a cluster environment. During the shift of responsibilities to the ghost VMs, there is approximately a 30 second loss of view to the operator. There is no loss of control, however. The operator is aware that a shift of responsibilities is underway though a notification on the display.

In VMWare®, if more than one virtual CPU is in use on a host, then fault tolerance is not an option. Likewise, cross-platform fault tolerance cannot occur. Replication using dedicated networks may be a substitute for this capability. However, replication requires a manual mode switch with temporary loss of control, and is not a direct failover.

High Availability

High availability is available with Hyper-V® or VMWare®, but only in a cluster environment. High availability occurs when a host fails, or stops, and the VMs are restarted on other available hosts within the same cluster. Because this process requires the bootup of an additional system, additional time may be needed. This process takes between 30 seconds and 3 minutes to complete. High availability of modules on workstations results in temporary loss of control. High availability of modules on the main server results in temporary loss of view.

It should be noted that virtualization does not prevent common-mode or cascading failures. Virtualization of numerous servers in the IACS environment on single platforms create critical points of failure. This should be considered when designing the architecture with the vendor. Reduction in the risks of critical failure points may require failover capabilities and fault tolerance or other redundancies.

5 Conclusions

Like many technologies applied in the IACS environment, optimizing a process or maximizing benefit often requires interface with complex technologies. Virtualization, whether in the Hyper-V® or VMWare® environment, requires strong technical skills to design, set up, and manage the system, and to maximize the benefit of the technology. Use of virtualization in the IACS environment requires evaluation of risks to core systems. Identification and mitigation of the risks to core systems created by shared hardware, physical access, and complex networking should occur in the design phase. This evaluation should include identification of any critical failure points and determine the needs for failover, fault tolerance, and high availability. Early engagement with the automation vendor is important in order to specify the most applicable design prior to implementation. Although setup and implementation may be performed primarily by the automation vendor, it should be assumed that the asset owner will need strong technical resources available at their site to manage and monitor the virtual environments. These resources should include server, system, and networking skills. As concluded by the testing, implementation errors or misconfigurations could lead to vulnerabilities, but may also destabilize the system.

Vulnerabilities were discovered in both the Hyper-V® and VMWare® test architectures. Some findings were technical in nature; others were operational. In cases where technical vulnerabilities were discovered, implementation issues or lack of patches were typically the root cause. Some design vulnerabilities were primarily discovered in the hardware or platform management components, requiring collaboration between the automation vendor and the manufacturer.

In architectures that remain within the IACS network, no severe vulnerabilities were discovered that could make this virtual system easily exploitable by the outsider threat. The outsider threat relies upon poor DMZ and network security that can be used as a vector to exploit the management network. The insider threat has several attack vectors, but each requires some knowledge of the system and its configuration. In many cases, physical access to the systems may be the most attractive and easiest threat vector.

Several takeaways were discussed with the team, including the following key points:

- VMWare® and Hyper-V® architectures provided a nearly equivalent attack surface. Vulnerabilities focus more on implementation and patching, and less about the virtualization product itself.

- Technical vulnerabilities, though reduced in number, exist mainly due to patching issues, implementation issues, or limitations of the hardware/software. Standard products and services, such as RDP, provide a broader attack surface that typically requires patching.

- Operational findings are not specific to automation vendor products. These general findings should be considered during the decision to design and implement a virtual solution in an IACS environment. These findings apply to the implementation of VMWare®, Hyper-V®, blades, clusters, and scalable configurations.

Reviewing the project questions, the following brief conclusions were made:

- What are the ramifications of using a hardware vs. software solution?

  The hardware and software components of the solutions offered today vary depending on the automation vendor. Hardware and software components each present threat vectors and risks. These may be managed by the automation vendor or the asset owner, but should be determined during design.

Hardware risks that are inherent to the manufacturer's design may be more difficult to mitigate without direct engagement of the manufacturer.

- What are the security differences between Hyper-V® and VMware®?

In this project assessment, Hyper-V® and VMware® presented approximately the same number of risks, although the attack surface may be slightly different. One product did not appear significantly more secure than the other in the IACS environment. The findings that indicated the importance of patch management, careful networking, and secure configuration, apply to both products. The automation vendor software may, however, interface differently with each product; these interfaces should be clearly identified in early design discussions.

- Are resource utilization and SCADA optimization attainable while maintaining security?

The virtualization environment can be operated securely, particularly if risks are mitigated at the beginning of the life cycle. Some risks are present when core functions exist on single hardware platforms or on shared resources. Failover and fault tolerance planning, redundancy, and resilience should be addressed during the design phase. An asset owner may need to determine the level of acceptable risk based on the desire for footprint reduction and optimization. This can occur through careful planning and discussions with the automation vendor.

- What are the security risks associated with maintaining and remotely accessing the virtual machines?

Remote access risks are highly dependent on the automation vendor approach. Standard remote access risks exist, as do risks that arise if the automation vendor does not accredit all patches affecting the virtualization software. The asset owner must then determine a patch maintenance program to mitigate risks to the virtualization software.

- Are there risks associated with very standard and open software choices?

As with other technologies, standard software choices can present well-known and attractive attack surfaces. Standard products such as VMware® and Hyper-V® represent the majority of virtual solutions offered in automation vendor products. While some vendors may offer more proprietary solutions, these products were not tested during this project.

- How much vendor access to the systems is required, and does this pose a risk?

Access is highly dependent on the automation vendor model. Any connection to or from the IACS environment poses additional threat vectors. Asset owners should review automation vendor access to a virtualized solution prior to design and implementation, and evaluate the risk accordingly.

- Do the increased fault tolerance and rollover capabilities of virtualization provide a more secure solution?

Failover and fault tolerance can mitigate risks that single points of failure can create. These are more effectively implemented at the beginning of the life cycle.

- Can the thin client be used as a threat vector?

Yes, thin clients can be used as a threat vector. Thin client offerings vary depending on the automation vendor's solution. Management of the thin client is necessary to reduce risk.

- What are the ramifications of shared memory space in a virtualized environment?

Though shared memory does provide an attack vector, assessment results indicated this would require a sophisticated threat. As virtualization becomes more common in the IACS environment, emerging threats that leverage shared memory should be monitored.

- Do patch management and update processes present threat vectors?

Patching through remote access may present a threat vector, but should be addressed as a remote management risk. Conversely, the threat of not patching is significant. A patch management plan is critical. This plan should be a significant part of the design and planning discussion with the automation vendor.

The detailed technical findings and operational conclusions derived during this project produced a set of topics that should be evaluated when considering the viability of virtualization in a specific IACS environment. This includes the product evaluation phase, planning and design, and implementation phases. As determined in previous LOGIIC research projects, implementation of new technologies in a critical operational environment requires careful evaluation and planning. While technical vulnerabilities due to a missing patch or the need to change a default password can be easily mitigated, larger implementation issues may require more effort. These include:

- Planning for growth and long-term needs (scalability)
- Criticality and availability of systems
- Engagement with automation vendor on plans for and limitations in failover, fault tolerance, and high availability options
- Management of the systems, including patching and system health monitoring

This assessment concludes that that Hyper-V® and VMWare® virtualization solutions can be implemented securely if carefully designed, patched, and managed. The vulnerabilities identified in this assessment can be mitigated through patching and careful configuration. Operational findings regarding the use of different structures, such as blade servers or clusters, or the use of common products such as VMWare® and Hyper-V®, may be applied to broader considerations in the use of virtualization for IACS environments.

ACRONYMS

Term/Acronym	
CSRDC	Cybersecurity Research and Development Center
DB	Database
DHS S&T	Department of Homeland Security Science & Technology Directorate
DMZ	Demilitarized Zone
DoS	Denial of Service
FAT/SAT	Factory Acceptance Testing/ Site Acceptance Testing
HMI	Human Machine Interface
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LAN	Local Area Network
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
NTLM	NT LAN Manager (Windows NT)
OS	Operating System
RDP	Remote Desktop Protocol
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
USB	Universal Serial Bus