SANDIA REPORT
SAND2023-09887
Printed October 2023

Sandia National Laboratories

Remote Operations and Monitoring: Attack Surfaces

Christopher C. Lamb, Shadya Maldonado

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

Remote operations and management of nuclear power systems is becoming an attractive design option for system designers to reduce both the costs and the technical footprint of reactor installations. In fact, due to the lower margins associated with small modular reactor systems coupled with the new deployment models these systems support remote operational management may in some cases become a design requirement. To support these operational models, system designers must understand cybersecurity vulnerabilities associated with these systems and the kinds of controls that can be used to mitigate those threats. In this paper, we propose to develop an attack surface model on nuclear systems controlled via remote access, identify technical concerns that current remote access technologies may not adequately address, and outline approaches to resolve both identified threats and attacks and gaps that current remote access techniques may have when used to manage nuclear systems.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND TERMS

Acronym/Term	Definition
5G	Fifth Generation (wireless protocol)
AS	Autonomous System
BGP	Border Gateway Protocol
C&C	Command and Control
CA	Certificate Authority
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSec	Domain Name System Security Extensions
GRE	Generic Routing Encapsulation
HTTP(S)	Hypertext Transfer Protocol (Secure)
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
ISO	International Standards Organization
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LTE	Long-term Evolution (wireless protocol)
MPLS	Multiprotocol Label Switching
PCN	Private Cellular Network
PKI	Public Key Infrastructure
PLC	Power Line Communication
PPTP	Point-to-Point Tunneling Protocol
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OT	Operational Technology
REST	Representational State Transfer
SAE	Society of Automotive Engineers
SD-WAN	Software Defined Wide Area Network
SMR	Small Modular Reactor
SSH	Secure Shell
TLS	Transport Layer Security
VPN	Virtual Private Network

Acronym/Term	Definition
WIFI	IEEE 802.11 Wireless Network Protocols
WLAN	Wireless Local Area Network

This page left blank

1. INTRODUCTION

Telemetry systems have been the target of several cyber-attacks in recent years, particularly in industries that rely on critical infrastructure, such as power plants, oil and gas pipelines, and water treatment facilities. In the automobile industry, remote telemetry systems are crucial for electronic vehicles to enable vendors to monitor the health of a given automobile. Likewise, a remote operational and management system in a nuclear power plant would typically include a wide range of hardware and software components to monitor and manage various plant parameters, as well as other critical parameters that impact the safe and efficient operation of the power plant.

We will first discuss related work and highlight the gaps with respect to attack surface analysis current applicable literature. We will then present a conceptual model of remote monitoring and operational management systems, including expected system configurations and protocols typically used in the presented contexts. We will then present a conceptual attack surface for remote access systems, and then move into specific technical attacks and potential countermeasures. We will then close with future work and conclusions.

This page left blank

2. RELATED WORK

Modern smart grids rely heavily on the communication infrastructure to function properly. Using communication technology ensures a reduction in energy consumption, effective operation of the smart grid, and coordination between all components of smart grids, from generation to end users. However, a paper by Baime et al. provides an overview of existing communication technologies, including ZigBee, WLAN, cellular communication, WiMAX, and Power Line Communication (PLC), their deployment in smart grids and the drawbacks [1]. In the automobile industry, telemetry systems are critical for monitoring and managing various electrical parameters, such as battery voltage, current, and temperature. According to a study by Maple et al., current research has created several reference architectures, but none specifically for attack surface analysis [2]. Similar systems could be used in advanced nuclear reactors to keep an eye on electrical parameters and digital systems, which is important for safe and effective operation. However, the use of vulnerable or weak communication protocols in critical infrastructure systems can increase the risk of cyberattacks, as demonstrated by Wen et al. [3]. Plapper et al. describe the importance of attack surface assessment for automotive cybersecurity in a way compliant with ISO/SAE 21434. In this work, they introduce a reference architecture with an associated attack surface, and they attempt to rate attacks against that surface from a feasibility perspective. They claim that the attack feasibility rating meets the requirements of associated standards that require threat and risk assessment. While this may be the case, outlined attacks can shift from expert to layman quickly with the emergence of new flaws and tools to exploit those flaws [4]. In 2014, Miller et al. examined the remote attack surface of cars. They were able to go into great technical detail about remote attacks on these systems and the ranges involved [5]. In 2011, Leverett used Shodan[1] to find industrial devices exposed to the internet and then evaluated the attack surface of those devices [6].

Overall, there was a large amount of work dealing with the attack surface of remote access to automobiles. There is no unified presentation standard for attack surfaces however, especially for the attack surfaces of critical systems where the control and monitoring traffic travels through systems that the consumers of that information do not own nor control.

[1] Shodan is a search engine that allows users to search for and gather information on industrial devices attacked to the internet. It provides a variety of accounts to allow for both free and commercial access at https://www.shodan.io.

This page left blank

3. CONCEPTUAL MODEL

In evaluating the attack surface for remote monitoring and operations of remote nuclear energy facilities, we will conduct a threat analysis over the end-to-end communications of both monitoring data from a given system and commands to be delivered to a given system. Identifying the possible threats and attack scenarios that the device may face can help prioritize and target security measures.

Figure 1 shows a hypothetical model of remote operations and monitoring for a given remote reactor system. This system includes remote access to centralized operational infrastructure, which may not always be present. The operational infrastructure is out of scope for our analysis however, though secure communication gateways can certainly be attacked from within the datacenter. To further bound the scope of this report, the attack surface analysis addresses **reconnaissance** and **initial access** only [7]. Adversary attacks related to compromise execution, resource development, and other tactics are out of scope for this analysis. Certain technical areas in an expected system design are also out of scope; In **Figure 1**, translucent areas including remote individual access are out of scope for this attack surface analysis. While important to recognize as potential attack vectors, they are not specifically related to remote reactor system access even if they are related to remote access in general.

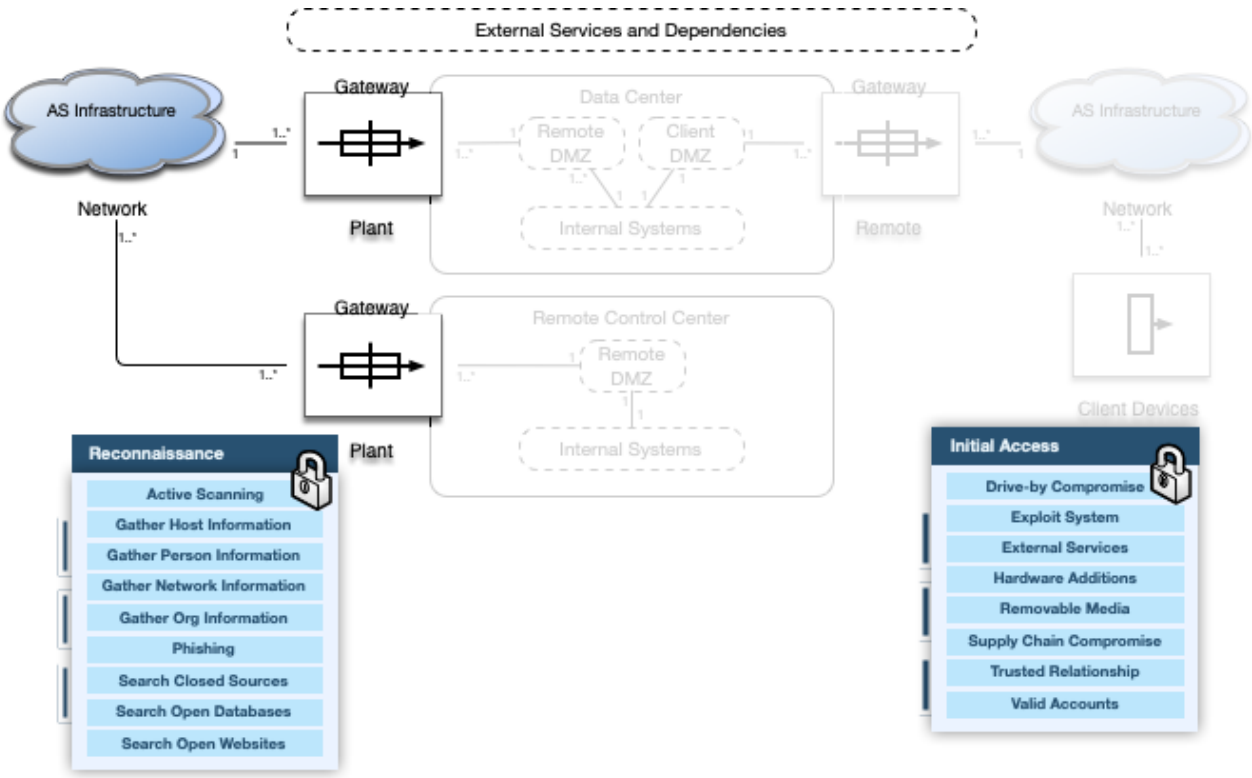

Figure 1: Conceptual model of remote monitoring and operations, including specific attack classes and categories of interest.

Within the conceptual model, Gateways are any kind of system providing remote access. Gateways are any kind of system providing remote access – they could be VPN access points, secure SSH servers, or secured web-based systems.

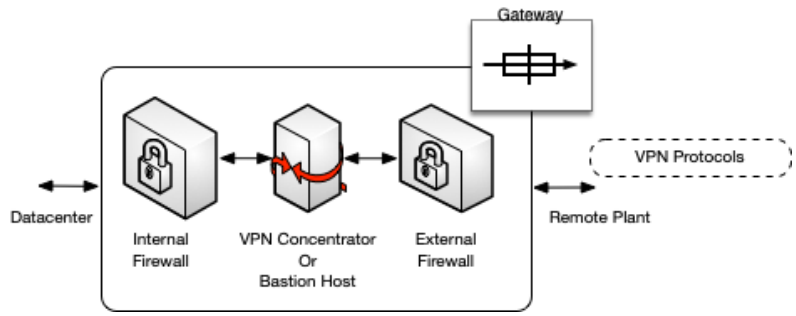

Figure 2: Gateway system technical elements. The Internal Firewall may protect other systems in the DMZ that contains the concentrator or bastion host.

Figure 2 shows a more detailed architecture of a gateway. External services in this context include anything that could impact data traversing paths between the centralized control system and a remote reactor system.

Specific examples include protocols like domain name services (DNS), network time protocol (NTP), or public key infrastructure (PKI). A secure communication gateway, for example, can be attacked from within a data center if appropriate security measures are not in place. An internal firewall can help to protect other systems in the DMZ that contains the VPN gateway or bastion host, but it may not be sufficient to prevent attacks on the gateway itself.

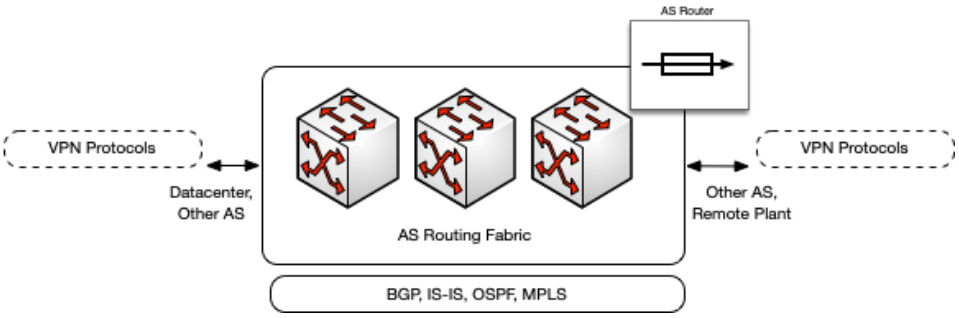

Figure 3: Representation of router infrastructure at an AS. Supporting protocols include BGP, IS-IS, OSPF, and potentially MPLS. VPN protocols pass through this routing fabric.

The elements illustrated in **Figure 3** can be connected directly to the remote plant, the data center that hosts the control room, or other Autonomous Systems (AS). BGP (Border Gateway Protocol), IS-IS (Intermediate System-to-Intermediate System), and OSPF (Open Shortest Path First) are all routing protocols used in computer networks to exchange routing information between routers and enable the efficient routing of data between different parts of the network. These protocols can also be used in conjunction with other network technologies, such as VPNs or MPLS, to provide secure and reliable routing of data between different parts of the network.

Remote operations and monitoring communication can traverse either private networks or the internet. Private cellular networks (PCNs) using LTE or 5G networks are certainly an option, as shown in **Figure 4**, where these networks are usually managed by a third party. Power line communications (PLC) can enable communication in some cases as well, though smaller small modular reactor systems may not be tied into a larger power grid but will still need to be monitored and managed.

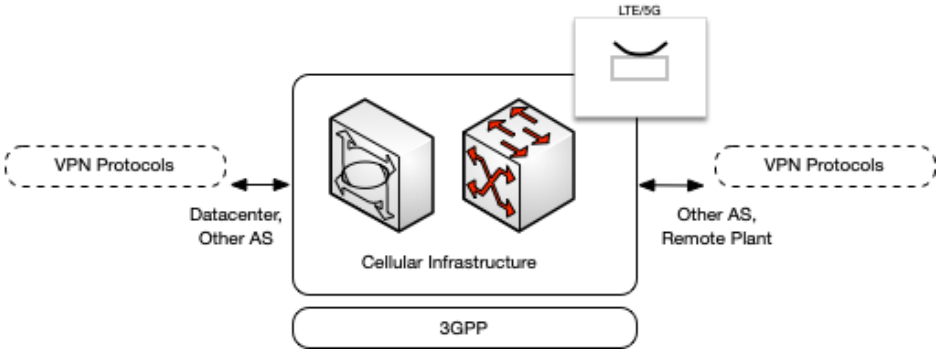

Figure 4: This represents LTE/5G specific infrastructure hosted at a cellular provider.

This infrastructure could be connected to ASs on both sides, or the data center, or the remote plant. Typical use would have cellular access for the last figurative mile to a remote plant. Due to the distances involved, data will very likely traverse the internet at some point. We will need to include PCN and internet routing protocols as a result [8]. PLC may be used in some cases, but as it cannot be used in many Small Modular Reactor (SMR) remote use cases, we will consider this out of scope for this analysis.

From an attack surface analysis perspective, this gives us three distinct elements we can combine into a system for end-to-end communication with a remote reactor system. These elements are connected by communication traffic protected by various secure communication protocols.

Overall, it is important to consider a combination of different security measures to protect OT systems. Encryption should be used in conjunction with other methods such as physical security, network segmentation, and access control to provide a comprehensive approach to securing these systems.

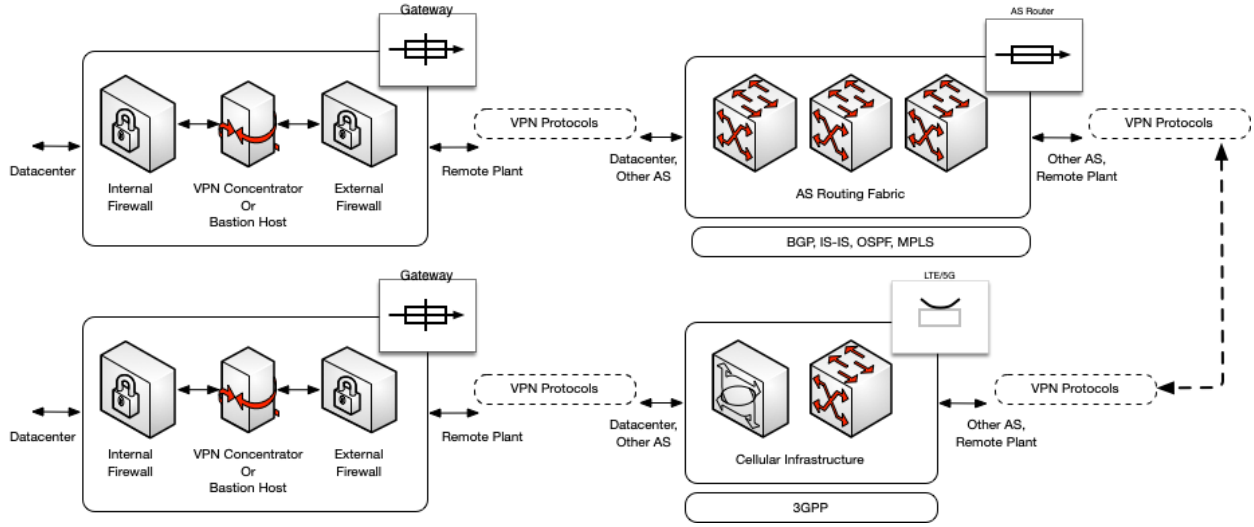

Figure 5: An example of integrated, end-to-end communication between two SMR vendor-controlled gateways.

Figure 5 shows how the individual elements can be combined. This shows an end-to-end remote monitoring and operations infrastructure. Just as the components can be combined, the defined attack surfaces can be combined as well, typically cumulatively.

This page left blank

4. CONCEPTUAL ATTACK SURFACE

In this section, we describe possible attacks using the MITRE ATT&CK framework which could be used to access or cause effect on a remote monitoring system [7]. The attacks described in MITRE ATT&CK are conceptual, and as such a good fit for the conceptual model in **Figure 1**.

Reconnaissance attacks that are usually executed to gather information for upcoming initial access attacks. Reconnaissance includes **Active scanning** which consists of IP block scanning, vulnerability scanning, or wordlist scanning. **Gather Host Information** addresses gathering hardware, software, firmware, or configuration information. **Gather Network Information** involves collecting information on external services used (i.e., DNS or PKI), IP address ranges, trust dependencies, and other network properties**. Gather Employee Information** entails, first, finding who employees are and then attempting to collect information on their hobbies, technical interests, family, and special dates. Adversaries will also attempt to find previously compromised username/password combinations to leading to password stuffing attacks. Collecting information on the people working in and their places in an organization fall under **Gather Org Information**.

Phishing is well understood and is frequently effective in extracting information or convincing employees to navigate to exploit kits or install malicious software. In some cases, attackers will **Search Closed Sources** by purchasing information from private companies on employees or credentials or similar information on the black market. **Search Open Databases** and **Search Open Websites** involve searching through open databases like DNS and WHOIS for information and searching social media and open code repositories. For our analysis, we include **Search Victim-Owned Websites** in the Search Open Websites class of attacks. While these are all part of the overall attack surface, the only attack in this category that is technically oriented is Active Scanning. To alleviate the non-technical information collection attacks, organizations need to practice strict operational security, and staff must understand the need to be circumspect with respect to information they share. Engineers with public source code repositories can release information with respect to the technologies used in an implementation, for example. Likewise, organizations need to understand the risks of exposing technical information on these kind of implementations in conferences, or by releasing names of partners that may allow attackers to understand companies that may have access to internal systems or may be responsible in some way for remote access.

Initial access attacks include **Drive-by Compromise**, in which a system is compromised by an exploit kit hosted on a malicious website a web browser is redirected to. Drive-by compromises are frequently triggered via phishing attacks as well, or they can be triggered by changing DNS records associated with frequently visited sites to redirect browsers from an organization to hosted exploit kits. The exploit kits can then forward browsers to the real site post-exploitation. Attackers will attempt to **Exploit Systems** if those systems are public facing, or the attacker can get access to the system via a compromised, internal, trusted system. **External Services** include remote access services of any kind, public facing programming interfaces, or control panels. **Removeable Media** is always a threat and has been used to compromise systems with notable instances recorded over a decade [3].

Another attack could be carried out through **Hardware Additions** to cause effect on a remote monitoring system. This involves surreptitiously placing hardware in or around systems to effect system function or to exfiltrate data from a system. Examples of these kinds of attacks include placing pass-through hardware on ethernet cabling that can also provide access to that data for exfiltration via a hidden WIFI network hosted from the device.

Initial access attacks can also be carried out through the Supply chain. This type of attack can occur at any point, from the manufacturer of the device to the delivery of the device to the end user. **Supply Chain Compromise** is a large issue in long range communication systems that rely on third-party managed infrastructure. Individual systems may suffer from supply chain attacks, but the infrastructure remote monitoring and management depend on are valid targets as well, and SMR managers have no control over the security posture of those systems. **Trusted Relationships** with third-party partners can be exploited as well for system access as well, if those partners are given access to systems of any kind [4]. Finally, **Valid Accounts** used for legitimate purposes can be exploited for systems access if they are not appropriately protected by strong, secret credentials or multi-factor techniques.

5. MODEL ANALYSIS

We have a variety of design options and infrastructure configurations. Common solutions that exist today include site-to-site VPNs, dedicated private Multi-protocol Label Switching (MPLS), or Software Defined WANs (SD-WANs). SD-WANs essentially aggregate a variety of underlying connections into a single software defined networking overlay, and as such still require underlying VPN or MPLS implementations. These implementations will typically use the wider internet, LTE/5G, or PLC for some combination of base data routing and last-mile communication. Remote access VPN technology could be used as well depending on engineering and budgetary constraints.

With remote access in place, TLS/SSH or TLS/HTTPS connections can be used to both monitor and manage remote sites. For example, REST connections could provide data via websockets or polling via TLS/HTTPS, and then either via TLS/SSH (for command line access) or TLS/HTTPS (for secure HTTP access to a web-centric management application). Common protocols for site-to-site or remote access VPNs include IKEv2/IPSec, TLS, PPTP, L2TP, and GRE (typically used with either PPTP or IPSec). OpenVPN is a common option, built using TLS and OpenSSL. Of these, both PPTP and L2TP are recognized as insecure and considered obsolete [9].

Gateways. As shown in **Figure 2** the secure communication endpoint (e.g., a bastion host or a commercial VPN gateway) is hosted within a network DMZ typically protected by both an internally- and externally facing firewalls. The endpoint itself will typically be on a LAN segment within the DMZ with other services or systems that need external access.

Table 1: A secure gateway attack surface. These are specifically externally facing attack surface characteristics. Internal attacker goals, like compromising saved information, are not part of the external attack surface and are excluded. Internal host manipulation for persistence or execution of an attack against a goal are likewise excluded.

Attack	Class	Action	Mitigation
NMAP scanning	Active Scanning	Attempted scans of a given system through internal or external firewalls.	(1) **Hardened system**; (2) **Honeypot** installation; (3) **Sensors** to detect and trace scanning; (4) appropriate **logging** for adversarial pursuit; (5) internal **firewalling software** to detect scanning
Manual port connections looking for banner information or other characteristics to identify a host	Gather Host information	Connections to the gateway host from internal or external sources	(1) **Hardened system**; (2) **Honeypot** installation; (3) **Sensors** to detect and trace scanning; (4) appropriate **logging** for adversarial pursuit;

			(5) internal **firewall** software
Phishing	Phishing for information; Phishing	Sending messages to personal or business accounts to attempt to convince the user to download unwanted software	(1) **Hardened system** (e.g., no browser software available to exploit via phishing messages); (2) **logging** system activity for forensic examination; (3) Strict **firewall rules** that only allow traffic out of the DMZ related to remote connections; (4) **monitor** for new outgoing communications that may be indicative of C&C traffic; (5) **Endpoint protection** to detect exploitation
Attacks via exploit kits	Drive-by Compromise	Redirecting a browser to a site hosting an exploit kit that can then exploit vulnerabilities in the browser for system access	(1) **Hardened system** (e.g., no browser software available to exploit via phishing messages); (2) **logging** system activity for forensic examination; (3) Strict **firewall rules** that only allow traffic out of the DMZ related to remote connections (4) **monitor** for new outgoing communications that may be indicative of C&C traffic; (5) **Endpoint protection** to detect exploitation; (6) Enable firewalls to detect attempted connections to **suspicious domains**
Exploiting installed applications for	Exploit Public Facing Application	Exploiting a known vulnerability to gain	(1) **Hardened system** (e.g., no unneeded

privilege escalation or system access		access or increase privilege	applications or software); (2) **Endpoint protection**; (3) **logging** system activity; (4) **monitoring** for unexpected communication (5) Implementing robust **patch management** processes
Installing hardware implants on a system or the DMZ LAN to either assume control of the system (typically on boot), capture traffic, or to run software	Hardware Additions	Hardware implants can be installed on the DMZ network and can then exfiltrate collected data over cellular or hosted WIFI connections	(1) Strict physical security; (2) Scanning regularly for unauthorized RF traffic; (3) **logging** system activity for forensic examination; (4) Strict **firewall rules** that only allow traffic out of the DMZ related to remote connections (5) **monitor** for new outgoing communications that may be indicative of C&C traffic; (6) **Endpoint protection** to detect exploitation; (7) Enable firewalls to detect attempted connections to **suspicious domains**
Compromising installed software via corrupting the source of that software	Supply Chain Compromise	Software repositories of both commercial and open-source software can be used to insert malicious changes into software	(1) **Limiting software acquisition** to third parties with clear security controls in place to prevent this kind of exploitation; (2) Establish **contractual agreements** for source code protection and notification of

			compromise if possible; (3) **logging** system activity for forensic examination; (4) Strict **firewall rules** that only allow traffic out of the DMZ related to remote connections (5) **monitor** for new outgoing communications that may be indicative of C&C traffic; (6) **Endpoint protection** to detect exploitation; (7) Enable firewalls to detect attempted connections to **suspicious domains**; (8) **Inspections** on software components
Installing compromised hardware into installed systems	Supply Chain Compromise	Hardware in systems can be compromised as well as software	(1) **Limiting hardware acquisition** to third parties with clear security controls in place to prevent this kind of exploitation; (2) Establish **contractual agreements** for source code protection and notification of compromise; (3) **logging** system activity for forensic examination; (4) Strict **firewall rules** that only allow traffic out of the DMZ related to remote connections (5) **monitor** for new outgoing communications that may be indicative of

			C&C traffic; (6) **Endpoint protection** to detect exploitation; (7) Enable firewalls to detect attempted connections to **suspicious domains** (8) **Inspections** on software components
Third party management of systems allows remote access or information injection into the gateway system	Trusted Relationship	Allowing a third-party access to critical systems can extend the overall attack surface and make the gateway systems more vulnerable.	The vulnerability of using a third party is heavily dependent on that party. Some venders (like major cloud computing providers) have excellent overall security practices. Others may not. (1) **Contractual agreements** for security practices can be established with third parties; (2) **Logging** of network connections and systems and monitoring for changes in activity; (3) **Endpoint protection**; (4) **Suspicious domain** monitoring
Trust relationships between the gateway system and other enterprise systems or services (e.g., PKI) that may allow those enterprise systems to shut down remote access	Trusted Relationship	If a system like a CA in a PKI has a weaker security posture than the remote services gateway itself, attackers may compromise the CA and alter Certificate Revocation Lists (CRLs). Depending on certificate validation procedures in place, this can result in a denial-of-service.	All dependent systems must have **equivalent security** and be secured at the same level as the most secure dependent system.

Exploiting DNS or other common services to act as a C&C channel or to redirect traffic to attacker-controlled domains	Trusted Relationship[2]	If an attacker can compromise DNS records, that attacker can potentially redirect traffic to domains they control.	(1) **Firewall configurations** that do not allow traffic from the gateway to systems other than remote sites and required local services; (2) Use of **secure protocols** like DNSSec [10] whenever possible to verify data and connections; (3) **Logging** and **monitoring** of packet traffic for anomalous behavior like larger than expected packet sizes
Cracking weak system credentials	Valid Accounts	Accounts can either not have default passwords changed or may be using weak or otherwise compromised credentials	(1) **Checking accounts** for weak credentials; (2) **multi-factor authentication**; (3) **logging** system activity for forensic examination; (4) Strict **firewall rules** that only allow traffic out of the DMZ related to remote connections (5) **monitor** for new outgoing communications that may be indicative of C&C traffic; (6) **Endpoint protection** to detect exploitation; (7) Enable firewalls to detect attempted connections to **suspicious domains** (8) **Inspections** on software components

[2] This is not specifically the meaning of *Trusted Relationship* within ATT&CK; rather, this is a *Trusted System Relationship* that is being exploited.

Injecting data or compromising the integrity of information[3]	Trusted Relationship[2]	Information within the perimeters can be compromised via a variety of attacks without information integrity and system identification guarantees	Strong standards-compliant identification and information protection (e.g., x509v2 certificates and TLS 1.3 with strong cipher suites and no fallback to weak cipher suites. Zero-trust techniques with no access to data without ongoing authentication and authorization

Table 1 contains a group of possible attacks against VPN Gateway systems. The attacks cover reconnaissance and initial access attacks, classify the attacks via the MITRE ATT&CK taxonomy, describe the action of the attack, and then list various mitigations.

Overall, many of the mitigations the same, though some are unique. First, operations need to **log and monitor** both network traffic and system performance and actions. This should be part of a larger threat hunting effort and should take advantage of **SIEM systems** and storage. This monitoring information should be saved for a long period of time to enable staff to see when systems may have been initially compromised. Staff should be trained for ongoing **threat hunting** and **adversarial pursuit tasking**, as well as **network and host forensics** (though contracted third parties may be a more effective way to gain this expertise). Typically, this data should be maintained for roughly a year, and analysis should be automated as much as possible to shorten time-to-detection [11]. **Honeypot** or **honeynet** systems can be used to detect and distract attackers as well. Equipment should be ready and available to replace operational equipment to enhance overall operational and cyber resiliency.

Systems should use **multi-factor authentication**, **endpoint protection**, and be **hardened** such that only required systems and applications are installed. Internally and externally facing **firewalls should be restrictively configured** to only allow network traffic and connections to known, trusted hosts. This may require secondary DMZ dedicated to remote system access. **System dependencies** (e.g., DNS, PKI) and transitive trust relationships between systems need to be understood rigorously managed, and systems should use **secure verifiable protocols** like DNSSec as much as possible.

Organizations need to create responsive **patch management** processes. Patches need to be applied to systems quickly and safely. This requires extensive secondary testing systems and highly rigorous data quality control and measurement processes. They also need to **inspect installed software and hardware** to verify integrity as much as possible. This typically requires some kind of administrative

[3] Attacking data in motion can be considered at attack on a goal state by an attacker and could have been excluded. We included it here as it is an attack on the external surface of the overall system – in this case, data moving between systems rather than data stored within a system.

root-of-trust implemented via an understanding of the quality control processes of the supplier and then verifying installed software via digital signatures or published hashes.

Finally, third parties should be held **contractually liable** for negligence, with significant penalties for non-compliance.

AS and LTE/5G Systems. External systems through which remote access traffic travels are targets as well. These systems are managed by third parties that reactor operators likely know nothing about. Large ISPs regularly route large amounts of network traffic without examining that traffic and without the originator or receiver of that traffic even knowing that those ISP handle it – these kinds of peering agreements are essentially the contractual backbone of the modern internet. The attack surface of these systems is very similar to that of gateway systems, with the addition of the use of routing protocols that allow these systems to know how to correctly route internet traffic. These protocols (e.g., BGP, IS-IS, and OSPF) have a history of vulnerability to false data injection attacks [12] [13] [14].

Cellular systems have many of the same issues as AS systems, in that they typically handle large amounts of internet traffic. The attack surface of cellular systems is larger than that of AS systems because of the radio-frequency aspects of cellular systems. The mitigating controls are equally limited in this domain however as developers have very little control over how these kinds of services are secured.

In nuclear monitoring and operation systems confidentiality attacks are not as much of an issue as integrity and availability attacks. Developers have no control over the controls in place to protect these systems and can only use compensatory controls and meticulous protection of encrypted communication tunnels between remote control rooms and reactor systems. Compensatory controls include autonomous reactor control systems that can shut a system down if needed, secondary and tertiary monitoring and command channels to remote systems using a robust heterogeneous ISP strategy to eliminate as much common routing as possible, and contingency planning to enable personnel to travel to remote sites if needed. Secure protocols used to provide connectivity to remote sites must be meticulously managed and configured with strong cipher suites that cannot be downgraded.

Data-in-motion. Remote nuclear system managers do have control over the protocols used to exchange monitoring and operational data with remote sites. As PPTP and L2TP are insecure and obsolete [9], most remote access will be over modern, secure implementations like IKEv2/IPSec, OpenVPN, or TLS/HTTPS/SSH. Still, IPSec attacks are common and frequent [15] [16]. Likewise, TLS systems have a history of vulnerability. Network communication does not map well into MITRE's ATT&CK framework, which is primarily host focused. Nevertheless, the attack surface with respect to VPN protocols centers around key compromise, algorithm degradation, insider attacks, and endpoint compromise. The kinds of vulnerabilities that appear in these protocols are outside of the scope of the remote monitoring and operating organization to solve. Correct protocol configuration following appropriate standards coupled with the robust cybersecurity controls used to protect the gateway systems will provide protection against attacks on data-in-motion.

Note that there have been attacks against encrypted traffic where that traffic has been rerouted to other organizations and stored for later deciphering [17]. This is not a significant threat against OT systems where availability and integrity are more important than confidentiality.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we first assembled a conceptual model of a secure remote operations and monitoring system for a remote reactor. With this in mind, we then described the classes of attacks against the attack surface of that conceptual model based on MITRE's ATT&CK taxonomy, as the model itself was abstract as are the attack classifications from ATT&CK. With this in place, we then extracted expected technical elements from the conceptual model with exemplar technologies needed to implement the systems and combined the technical elements into an end-to-end solution. With this as a reference, we then described the attack surface a remote reactor control system could control, the attack surfaces of related elements outside of the control of that remote control system and mitigating and compensatory controls that need to be in place to reduce risk.

Now that we have defined a conceptual architecture for remote operations and management infrastructure for a remote reactor system, we will more closely examine the technology stack needed to build this kind of a system and the attributes of that kind of system once built. We expect to assemble a secure proof-of-concept for remote reactor monitoring and management using open technologies to examine the operational characteristics of this kind of a system more closely. This will include system attributes measured via penetration testing and other security analysis as well as performance and will use emulated reactor systems built via tools like Asherah to provide the highest fidelity results possible without using an actual remote reactor system.

REFERENCES

[1] D. Baimel, S. Tapuchi and N. Baimel, "Smart grid communication technologies- overview, research challenges and opportunities," in *International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, 2016.

[2] C. Maple, M. Bradbury, A. T. Le and K. Ghirardello, "A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis," *Applied Sciences,* vol. 9, no. 23, 2019.

[3] "Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as a New over-the-Air Attack Surface in Automotive IoT," in *29th USENIX Conference on Security*, 2020.

[4] C. Plappert, D. Zelle, H. Gadacz, R. Rieke, D. Scheuermann and C. Krauß, "Attack surface assessment for cybersecurity engineering in the automotive domain," in *29th Euromicro international conference on parallel, distributed and network-based processing (PDP)*, 2021.

[5] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," in *Black Hat*, 2014.

[6] E. Leverett, "Quantitatively assessing and visualising industrial system attack surfaces," University of Cambridge, Darwin College , 2011.

[7] MITRE, "MITRE ATT&CK," [Online]. Available: https://attack.mitre.org/. [Accessed 22 February 2023].

[8] D. Baimel, S. Tapuchi and N. Baimel, "Smart Grid Communication Technologies- Overview, Research Challenges and Opportunities," in *International Symposium on Power Electronics, Electrical Drives, Automation and Motion*, 2016.

[9] NordVPN, "Why we have discontinued L2TP and PPTP protocols?," NordVPn, 1 December 2018. [Online]. Available: https://support.nordvpn.com/General-info/1221989272/Why-we-have-discontinued-L2TP-and-PPTP-protocols.htm. [Accessed 22 February 2023].

[10] The Internet Society, "RFC 2535 - Domain Name System Security Extensions," The Internet Society, 1999.

[11] IBM, "Cost of a Data Breach Report 2022," IBM, 2022.

[12] P. O'Neill, "Telegram traffic from around the world took a detour through Iran," Cyberscoop, 30 July 2018. [Online]. Available: https://cyberscoop.com/telegram-iran-bgp-hijacking/. [Accessed 16 February 2023].

[13] L. Tung, "AWS traffic hijack: Users sent to phishing site in two-hour cryptocurrency heist," ZDNet, 25 April 2018. [Online]. Available: https://www.zdnet.com/article/aws-traffic-hijack-users-sent-to-phishing-site-in-two-hour-cryptocurrency-heist/. [Accessed 18 February 2023].

[14] D. Goodin, "Russian-controlled telecom hijacks financial services' Internet traffic," ArsTechnica, 27 April 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/. [Accessed 18 February 2023].

[15] D. Felsch, M. Grothe, J. Schwenk, A. Czubak and M. Szymanek, "The Dangers of Key Reuse: Practical Attacks on IPsec IKE," in *Usenix Security Symposium*, 2018.

[16] S. Gatlan, "US govt: Hacker used stolen AD credentials to ransom hospitals," Bleeping Computer, 18 April 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/us-govt-hacker-used-stolen-ad-credentials-to-ransom-hospitals/. [Accessed 21 February 2023].

[17] D. Moore, "Offensive Cyber Operations: Understanding Intangible Warfare," Oxford Academic, 2022.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Ben Cipiti	8845	bbcipit@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya LeBlanc	katya.leblanc@inl.gov	Idaho National Laboratory

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.