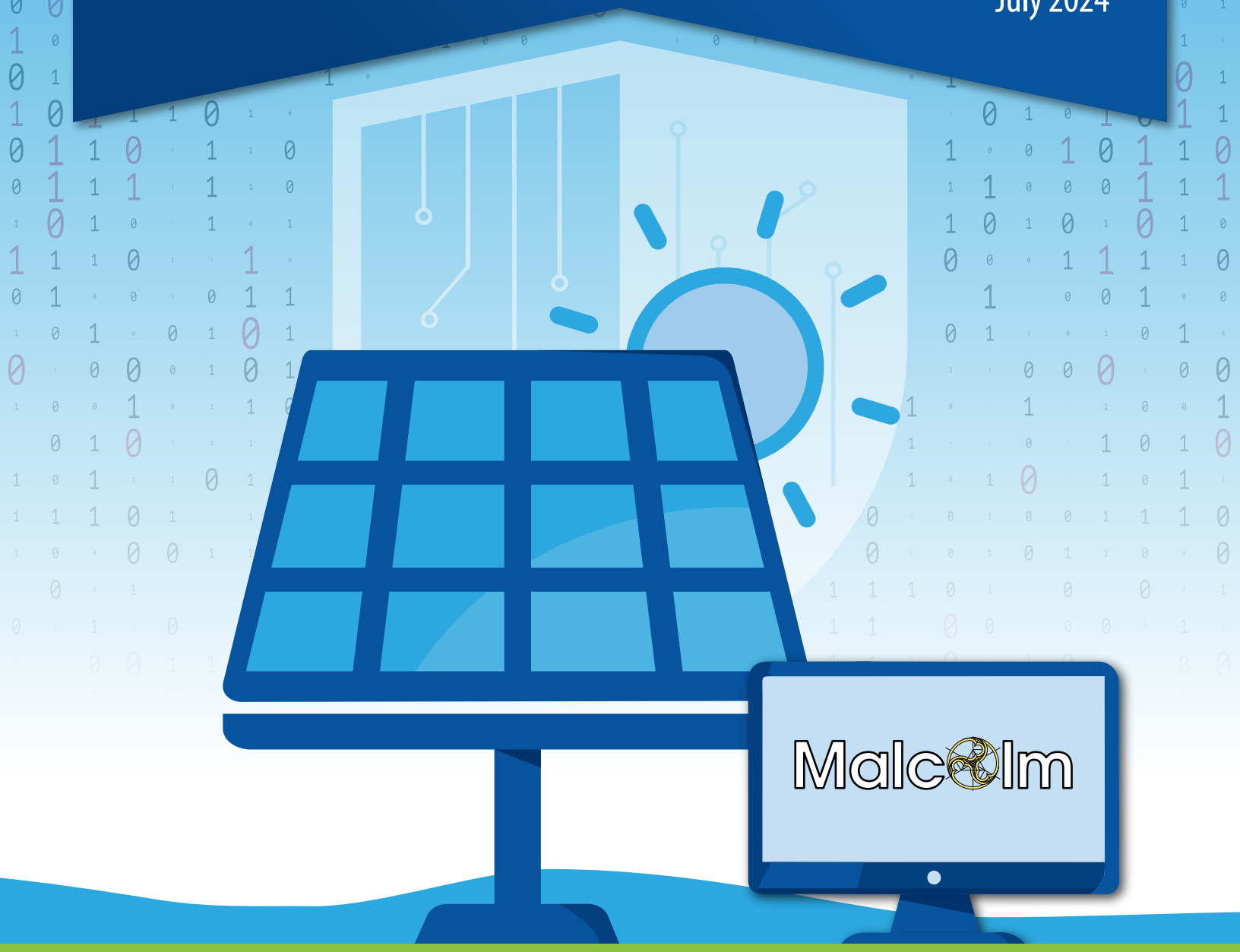
Malcolm Deployment

Guide for Solar Power Generation Systems

July 2024



Daniel Ricci | Seth Grover | Michael McCarty

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS 24-79751 Revision 1

CONTENTS

FIGURES

DANIEL RICCI
Power Systems Engineer, INL

SETH GROVER
Computer Security Researcher, INL

MICHAEL MCCARTY
Computer Security Researcher, INL

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

***Prepared for the* U.S. Department of Energy**
Office of Solar Energy Technology
Under DOE Idaho Operations Office

1. INTRODUCTION

MALCOLM IN SOLAR POWER GENERATION SYSTEMS

Malcolm, a robust network traffic analysis tool suite, is particularly effective when deployed in Solar Power Generation systems. These systems consist of various network-connected components such as solar panels, inverters, and trackers and generate significant network traffic data. Malcolm can process this data in full packet capture (PCAP) files, Zeek logs, and Arkime sessions to provide valuable insights into the system's network communications[1].

Malcolm processes the network session data generated by various components such as solar panels, inverters, and trackers. It enriches this data with additional lookups and mappings. This includes GeoIP mapping, which can be crucial for understanding the origin of inbound/outbound IP address traffic for solar power generation sites spread across multiple geographical locations[2]. It also provides hardware manufacturer lookups from organizationally unique identifiers (OUI) in MAC addresses, which can help identify the manufacturers of different components in the system. Malcolm also assigns names to network segments and hosts based on a user-defined asset inventory, providing a clear and organized view of the network. Furthermore, it performs JA4 fingerprinting, enhancing the security monitoring of the Solar Power Generation System[3]. These features make Malcolm a powerful tool for managing and securing the network of a Solar Power Generation System.

PURPOSE AND SCOPE OF THE GUIDE

This guide provides detailed instructions for deploying Malcolm in Solar Power Generation systems. It covers the deployment process, from understanding the network architecture of these systems to configuring network switches and Switched Port Analyzer (SPAN) ports or mirror ports or TAPs. The guide also includes best practices for deploying Hedgehog sensors, another critical component in these systems. Following this guide, users can enhance network visibility, improve their system's security, and effectively troubleshoot common issues.

[1] Idaho National Laboratory. "Overview." Malcolm: A powerful, easily deployable network traffic analysis tool suite, 2024. https://malcolm.fyi/docs/.
[2] Ibid.
[3] Ibid.
[4] "Hello Sunshine: The Future of Solar Power," Solar energy explained | National Grid Group, 2024, https://www.nationalgrid.com/stories/energy-explained/how-does-solar-power-work.

2. UNDERSTANDING SOLAR POWER GENERATION SYSTEMS

OVERVIEW OF A SOLAR POWER GENERATION SYSTEM

Solar power generation systems harness the sun's energy to produce electricity. These systems primarily consist of solar panels containing photovoltaic (PV) cells that capture sunlight and convert it into direct current (DC) electricity . An inverter then transforms this DC electricity into alternating current (AC), which is usable by household appliances and the grid. The process of conversion is known as the photovoltaic effect, a phenomenon first discovered in 1839[5]. Silicon, a semiconductor, is commonly used in PV cells due to its ability to absorb and convert sunlight efficiently.

NETWORK-CONNECTED EQUIPMENT IN SOLAR POWER GENERATION SYSTEMS

The integration of solar power into the electrical grid involves various network-connected equipment that ensures the seamless flow of electricity while maintaining grid reliability. Key components include inverters, which convert DC to AC electricity, and power electronic devices that manage the flow of electrical power[6]. Additionally, solar-plus-storage systems incorporate batteries to store energy for later use, addressing the intermittent nature of solar power[7]. Grid resilience is supported by real-time monitoring of solar energy production and advanced inverters that enable solar systems to operate independently during outages.

SOLAR SYSTEMS INTEGRATION BASICS

Solar systems integration is the development of technologies that allow solar energy to be added to the electricity grid. This includes managing two-way electricity flow due to the presence of distributed energy resources (DER) like rooftop solar installations[8]. The grid now comprises both large-scale power plants and smaller, dispersed sources, necessitating advanced grid management and real-time data on electricity production[9].

INVERTERS AND GRID SERVICES

Inverters play a crucial role in solar energy systems by converting DC electricity from solar panels into AC electricity for grid use. Modern inverters also monitor the system and facilitate communication with computer networks. As the grid evolves, a significant portion of electricity is expected to flow through power electronic devices like inverters by 2030[10].

UNDERSTANDING A SOLAR POWER GENERATION SYSTEM

Understanding Solar systems and its network-connected equipment is crucial for a successful Malcolm deployment. This knowledge allows for a more effective and tailored deployment of Malcolm's network traffic analysis capabilities. One can strategically place Malcolm sensors to capture the most relevant data by comprehending the unique network architecture and data flow within a Solar Power Generation System. This results in more accurate and comprehensive network visibility, improving threat detection and system security. Furthermore, understanding the equipment and their network behaviors can help configure Malcolm to reduce false positives and focus on genuinely significant events. Therefore, a deep understanding of the solar power generation system is not just beneficial but essential for optimizing Malcolm's deployment and functionality.

[5] Ibid.

[6] Department of Energy (DOE). "How Does Solar Work? | Department of Energy." Solar Energy Technologies Office, 2024. https://www.energy.gov/eere/solar/how-does-solar-work.

[7] Department of Energy (DOE). "Solar-plus-Storage 101 | Department of Energy." Solar-Plus-Storage 101, 2019. https://www.energy.gov/eere/solar/articles/solar-plus-storage-101.

[8] Department of Energy (DOE). "Solar Integration: Inverters and Grid Services Basics." Solar Energy Technologies Office, 2024. https://www.energy.gov/eere/solar/solar-integration-inverters-and-grid-services-basics.

[9] Ibid.

[10] Department of Energy (DOE). "Solar Systems Integration Basics | Department of Energy." Solar Energy Technologies Office, 2024. https://www.energy.gov/eere/solar/solar-systems-integration-basics.

3. MALCOLM DEPLOYMENT BASICS

MALCOLM DEPLOYMENT BASICS

Malcolm is a powerful network traffic analysis tool suite designed with several key goals in mind[11]. It is easy to use, accepting network traffic data in the form of full packet capture (PCAP) files and Zeek logs[12]. These artifacts can be uploaded via a simple browser-based interface or captured live and forwarded to Malcolm using lightweight forwarders[13]. In either case, the data is automatically normalized, enriched, and correlated for analysis[14].

Visibility into network communications is provided through two intuitive interfaces: OpenSearch Dashboard, a flexible data visualization plugin with dozens of prebuilt dashboards providing an at-a-glance overview of network protocols; and Arkime (formerly Moloch), a powerful tool for finding and identifying the network sessions comprising suspected security incidents[15].

Malcolm operates as a cluster of Docker containers – isolated sandboxes that each serve a dedicated function of the system[16]. This Docker-based deployment model, combined with a few simple scripts for setup and run-time management, makes Malcolm suitable to be deployed quickly across a variety of platforms and use cases[17]. Whether it be for long-term deployment on a Linux server in a security operations center (SOC) or for incident response on a MacBook for an individual engagement.

All communications with Malcolm, both from the user interface and from remote log forwarders, are secured with industry standard encryption protocols[18]. Malcolm is comprised of several widely used open-source tools, making it an attractive alternative to security solutions requiring paid licenses[19].

While Malcolm is great for general-purpose network traffic analysis, its creators see a particular need in the community for tools providing insight into protocols used in industrial control systems (ICS) environments[20]. Ongoing Malcolm development will aim to provide additional parsers for common ICS protocols[21]. Although all the open-source tools that make up Malcolm are already available and in general use, Malcolm provides a framework of interconnectivity that makes it greater than the sum of its parts[22].

In short, Malcolm provides an easily deployable network analysis tool suite for full PCAP files and Zeek logs[23]. While Internet access is required to build Malcolm, internet access is not required at runtime[24].

MALCOLM DEPLOYMENT PROCESS OVERVIEW

Malcolm is designed for streamlined deployment across various platforms and use cases[25]. It operates as a cluster of Docker containers, each serving a dedicated function of the system[26]. This Docker-based deployment model, combined with a few scripts for setup and run-time management, makes Malcolm suitable to be deployed quickly[27]. These Docker images can be pulled from GitHub by running docker "**compose --profile malcolm pull**" from within the Malcolm installation directory, or they can be built from source by following the instructions in the Quick Start section of the documentation.

All communications with Malcolm, both from the user interface and remote log forwarders, are secured with industry-standard encryption protocols . While Internet access is required to build Malcolm, internet access is not necessary at runtime[29].

The Malcolm Deployment process starts with planning and requires Information Technology (IT) and Industrial Control Systems (ICS), or Operational Technology (OT) personnel working together to enable a successful selection of the deployment location and identified of hardware requirements (See Figure 1). IT professionals will be key to supporting the building and configuring of Malcolm prior to deploying the docker containers. Once Malcolm is installed and started, the Malcolm containers can be launched. The next step in this process will be to run Malcolm to begin the passive gathering of network traffic from the ICS/OT devices and systems within the Solar Power Generation system. As network traffic is gathered, both OT and IT personnel can begin to analyze the data and begin using Malcolm for asset identification, anomaly detection, and threat monitoring.

[11] "Malcolm | A Powerful, Easily Deployable Network Traffic Analysis Tool Suite." Malcolm, 2024. https://malcolm.fyi/.

[12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29] Ibid

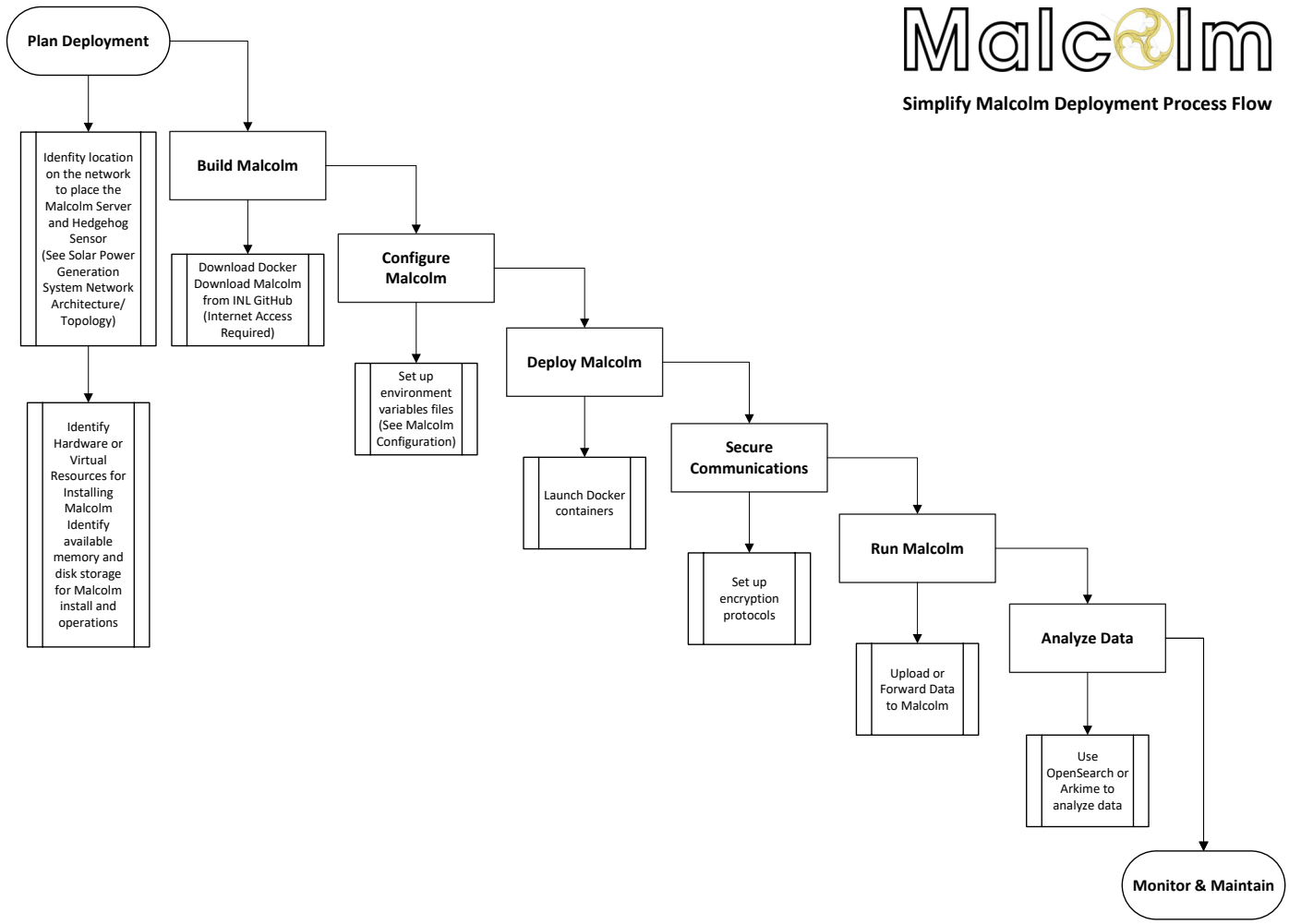


Figure 1. Malcolm deployment process

When deploying Malcolm in Solar Power Generation Systems, it's essential to consider the unique network architecture and data flow within these systems. By understanding these aspects, you can strategically place Malcolm sensors to capture the most relevant data, leading to more accurate and comprehensive network visibility. This will ultimately enhance the security monitoring and threat detection capabilities within your Solar Power Generation System.

4. NETWORK ARCHITECTURE FOR MALCOLM DEPLOYMENT

NETWORK ARCHITECTURE OF SOLAR POWER GENERATION SYSTEMS FOR MALCOLM DEPLOYMENT

Solar Power Generation Systems are complex networks that involve a variety of components and technologies (See Figures 2 & 3). When deploying Malcolm in such an environment, understanding the network architecture is crucial. Malcolm can process network traffic data generated by various components such as solar panels, inverters, and trackers, and battery energy storage providing valuable insights into the system's network communications[30].

The electrical grid is separated into transmission and distribution systems[31]. The transmission grid carries electricity from centralized generation sources like large power plants, while the distribution grid refers to low-voltage lines that eventually reach homes and businesses[32]. Modern electrical grids involve variable energy sources like solar and wind, energy storage systems, power electronic devices like inverters, and small-scale energy generation systems like rooftop installations and microgrids[33]. These smaller-scale and dispersed energy sources are generally known as distributed energy resources (DER)[34].

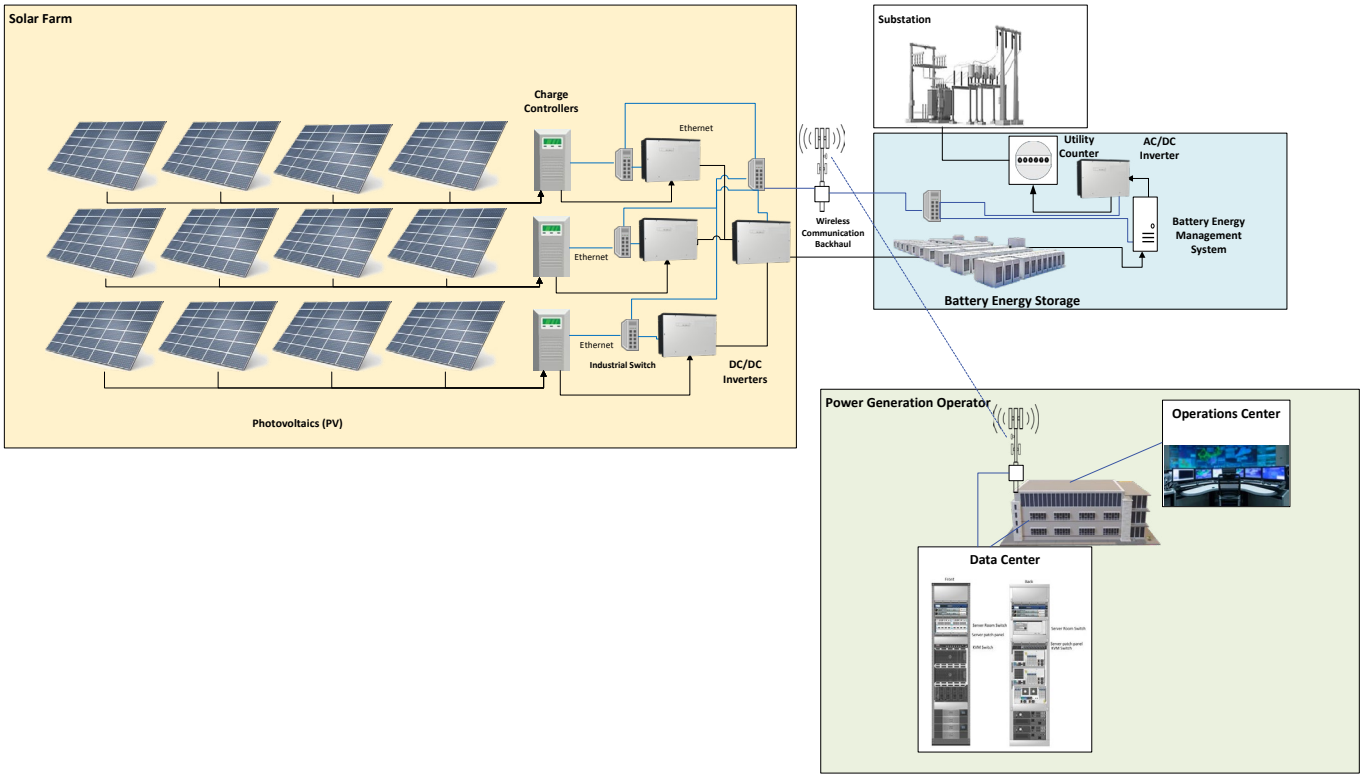


Figure 2. Network architecture diagram for a Solar Power Generation System (Wireless)

30, 31, 32, 33, 34 Ibid

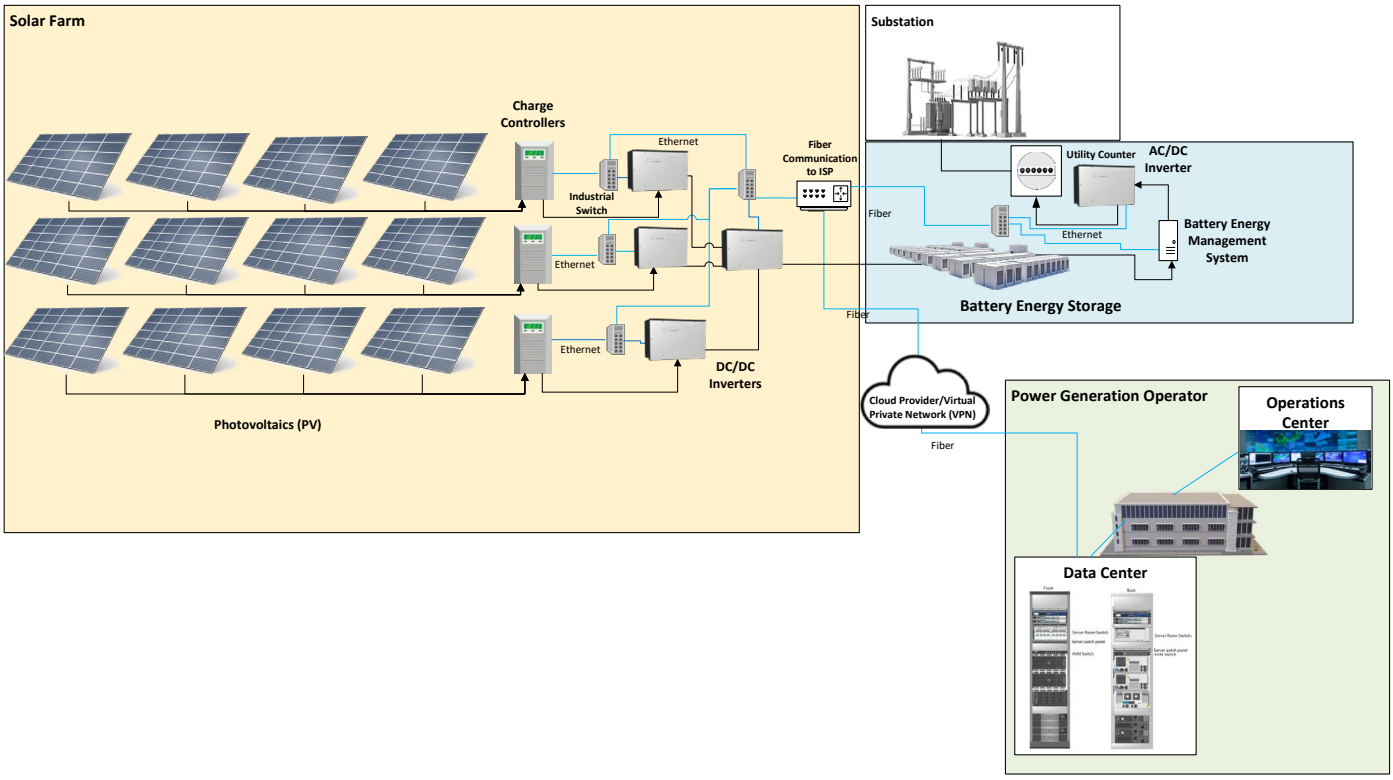


Figure 3. Network architecture diagram for a Solar Power Generation System (Fiber & Cloud)

When deploying Malcolm in a Solar Power Generation System, it's important to understand where to place network switches and how to configure SPAN ports or TAPs[35]. Network switches should be strategically placed to capture the most relevant data from the network-connected equipment in the Solar Power Generation System. A Network TAP (Test Access Point) is a hardware device that is placed on a network segment, allowing you to access and monitor network traffic[36]. For example, a network tap can connect two devices (e.g., switch and router) by being inserted "in-line" between the switch and router.

SPAN port configuration, also known as port mirroring or SPAN, is a feature in network switches that allows administrators to monitor and analyze network traffic[37]. It involves copying traffic from one or more source ports to a destination port, allowing network administrators to capture and analyze network packets[38]. This feature is essential for network troubleshooting, security monitoring, and performance optimization[39].

In the context of a Solar Power Generation System, these configurations can help in capturing and analyzing the network traffic data generated by various components such as solar panels, inverters, and trackers. This will ultimately enhance the security monitoring and threat detection capabilities within your Solar Power Generation System.

[35] "Malcolm | A Powerful, Easily Deployable Network Traffic Analysis Tool Suite." Malcolm, 2024. https://malcolm.fyi/.

[36, 37, 38, 39] Ibid

5. DEPLOYING HEDGEHOG SENSORS

DEPLOYING HEDGEHOG SENSORS IN SOLAR POWER GENERATION SYSTEMS

Deploying Hedgehog sensors in Solar Power Generation Systems involves several key considerations. First, it's essential to understand the network architecture of these systems[40], this includes knowing where to place the sensors to capture the most relevant data from the network-connected equipment connected to Industrial Control Systems (ICS) or Operational Technology (OT) devices and systems in the Solar power generation system and the battery energy storage system (BESS) (See Figure 4).

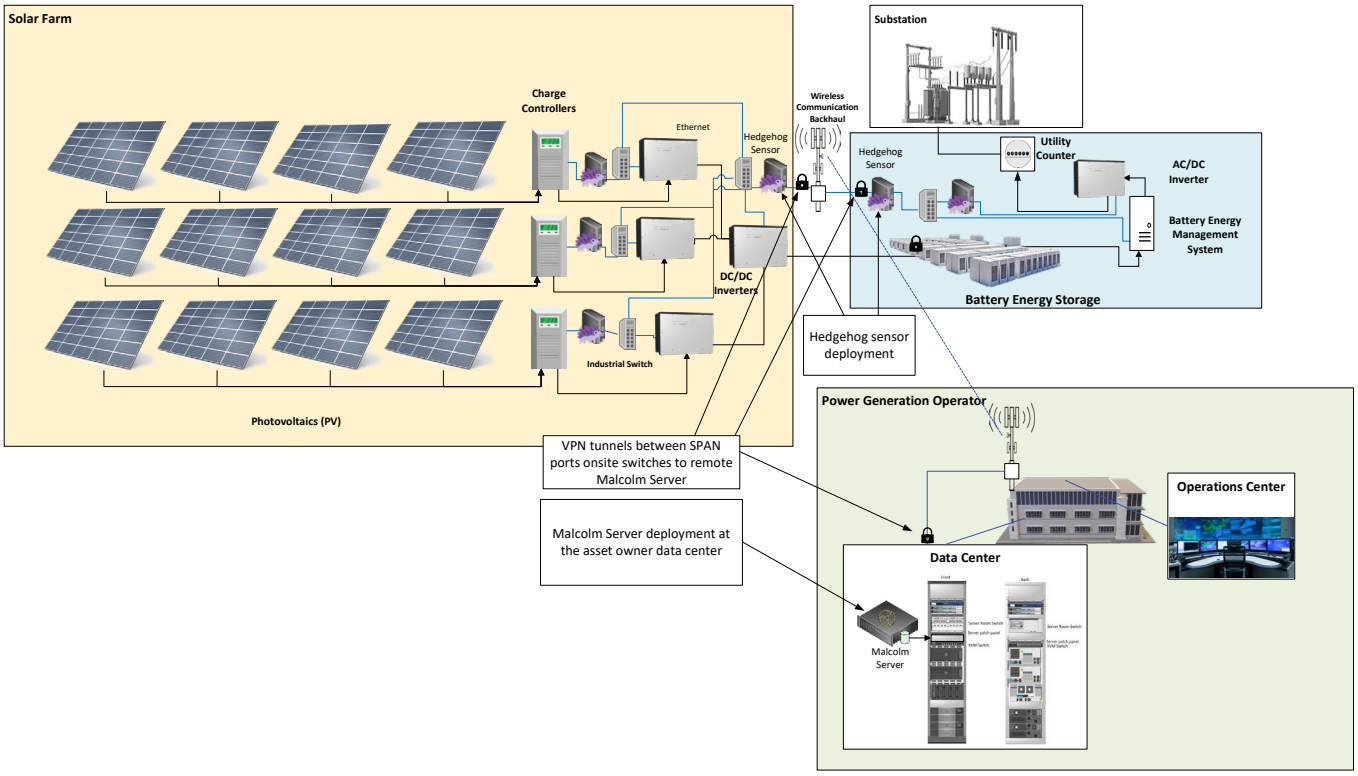


Figure 4. Network architecture diagram for a Solar Power Generation System (Wireless)

Second, the sensors should be configured to monitor optimal parameters for asset identification and threat monitoring[41]. It also includes logging activities and detecting different monitoring parameters. Familiarity with these parameters and their logging techniques is essential in developing an efficient photovoltaic energy threat monitoring system[42]. Details on deployment options and configuring Hedgehog sensors can be found on the Malcolm website for Hedgehog Linux.

Finally, deploying Hedgehog sensors should consider the environmental conditions of the Solar Power Generation System[43]. Various components of these monitoring systems are exposed to extreme weather conditions which reduce

[40] Idaho National Laboratory (INL). "Hedgehog Linux." Malcolm, 2024. https://idaholab.github.io/Malcolm/docs/hedgehog.html.

[41] Laboratory, Idaho National. "Overview." Malcolm: A powerful, easily deployable network traffic analysis tool suite, n.d. https://malcolm.fyi/docs/.

[42] Ibid

[43] Idaho National Laboratory (INL). "Hedgehog Linux." Malcolm, 2024. https://idaholab.github.io/Malcolm/docs/hedgehog.html.

their lifespan. Therefore, the sensors should be deployed in a manner that protects them from these conditions while still allowing them to effectively monitor the system[44]. An example of this would be deploying a Hedgehog sensor on an industrial computers that is DIN rail mountable or a Raspberry Pi Platform within the same enclosure as the industrial switches nearest to the controllers, inverters, trackers, and BESS.

Deploying Hedgehog sensors in Solar Power Generation Systems can significantly enhance the system's monitoring capabilities to identify assets operating in the environment and detect potential threats. By providing valuable insights into the system's operation, these sensors can help ensure optimal efficiency and reliability of the Solar Power Generation System.

6. DEPLOYMENT OF MALCOLM SERVER

DEPLOYING A MALCOLM SERVER IN THE NETWORK

Deploying a Malcolm server in a Solar Power Generation System involves a series of steps that ensure the server is optimally placed and configured to capture the most relevant data[45]. The first step is to understand the network architecture of the Solar Power Generation System where the server will be placed depending on environmental and space restrictions. This is important to understand if the server is to be placed within a data center or non-climate-controlled communication closet nearest to the network-connected equipment in the BESS near the Solar Farm.

Once the network architecture is understood, the next step is to place the Malcolm server to support maximum network traffic visibility across the Solar Farm and the BESS. The server monitors network traffic mirrored to it over a SPAN port on a network switch or router, or by using a network TAP device[46]. The placement of the Malcolm server should be strategic, aiming to capture the most relevant data from the network-connected equipment in the Solar Power Generation System and the BESS[47] (See Figure 5).

The final step in the deployment process is the configuration of the Malcolm server. This involves setting up environment variables, configuring network settings, and launching Docker containers[48]. All communications with the Malcolm server, both from the user interface and from remote log forwarders, are secured with industry standard encryption protocols[49].

BEST PRACTICES FOR MALCOLM SERVER DEPLOYMENT IN AN ICS/OT NETWORK USED IN SOLAR POWER SYSTEMS

When deploying sensors in an Industrial Control Systems (ICS) or Operational Technology (OT) network used in Solar Power Systems, there are several best practices to consider[50, 51, 52, 53]. First, it's important to consider a defense-in-depth strategy[54]. Implementing a defense-in-depth strategy is particularly relevant and beneficial for a Malcolm deployment in a Solar Power Generation System. This strategy involves multiple layers of security measures, ensuring that if one layer is breached, others are still in place to protect the system.

In the context of a Malcolm server deployment, these layers could include network segmentation, firewall configurations,

[44] Laboratory, Idaho National. "Overview." Malcolm: A powerful, easily deployable network traffic analysis tool suite, n.d. https://malcolm.fyi/docs/.

[45] "Malcolm | A Powerful, Easily Deployable Network Traffic Analysis Tool Suite." Malcolm, 2024. https://malcolm.fyi/.

[46, 47, 48, 49] Ibid.

[50] "Malcolm | A Powerful, Easily Deployable Network Traffic Analysis Tool Suite." Malcolm, 2024. https://malcolm.fyi/.

[51] National Institute of Standards and Technology (NIST). "Guide to Operational Technology (OT) Security." NIST Special Publication NIST SP 800-82r3, September 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

[52] Department of Homeland Security (DHS)'s National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). "Recommended Practice: Defense in Depth." ICS Recommended Practices, September 2016. https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[53] "Recommended Cybersecurity Practices for Industrial Control Systems." ICS Recommended Practices, May 2020. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf.

[54] Ibid. 54.

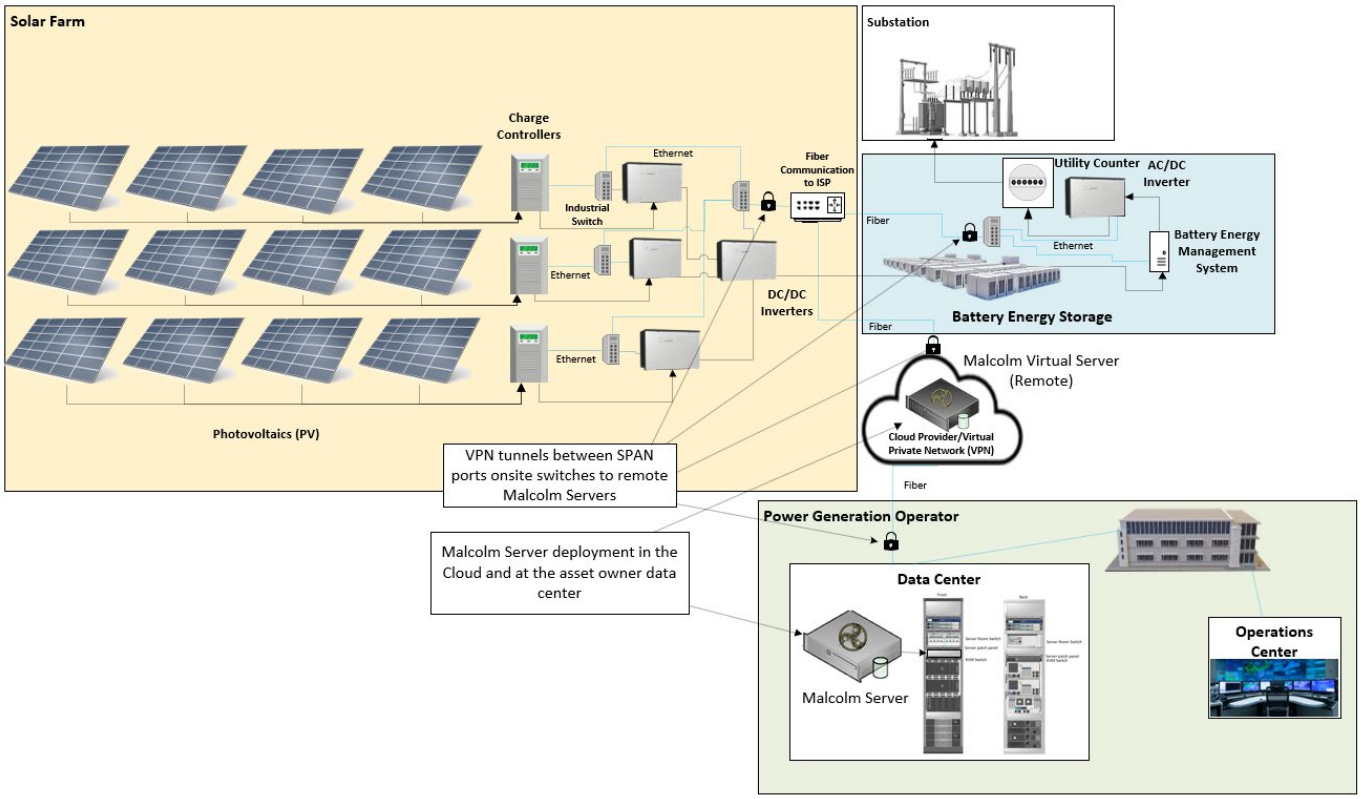


Figure 5. Deployment of Malcolm server in a Solar Power Generation System (Fiber & Cloud)

secure communication protocols, and regular system updates. For instance, network segmentation can prevent an attacker from gaining access to the entire network if they breach a single device. Firewalls can block unauthorized access, while secure communication protocols can protect data in transit. Regular system updates ensure that the system is protected against known vulnerabilities.

Moreover, the Malcolm server itself can be considered as a layer in this defense-in-depth strategy. By providing comprehensive network traffic analysis, the Malcolm server can detect potential threats and anomalies in the network, adding an additional layer of security.

Therefore, a defense-in-depth strategy not only enhances the overall security of the Solar Power Generation System but also maximizes the effectiveness of the Malcolm server deployment in monitoring and protecting the system. This multi-layered approach ensures that the system remains secure even if a single security measure fails or a single component is compromised.

Second, network segmentation should be utilized where possible. Network segmentation is a crucial aspect of a Malcolm deployment, particularly in complex environments like Solar Power Generation Systems. Network segmentation involves dividing the network into smaller, isolated segments or subnetworks, each with its own set of rules and controls.

In the context of a Malcolm server deployment, network segmentation can enhance both the performance and security of the system. From a performance perspective, network segmentation can reduce network congestion and improve network performance by limiting the amount of traffic that needs to be processed by the Malcolm server. This allows the Malcolm server to focus on analyzing the most relevant traffic, improving the efficiency of its network traffic analysis.

From a security perspective, network segmentation can limit the spread of threats within the network. If a threat actor gains access to one segment of the network, the impact of the breach can be contained within that segment, preventing the threat actor from moving laterally

across the entire network. This is particularly important in Solar Power Generation Systems, where a breach could potentially disrupt the operation of the entire system.

Furthermore, network segmentation can make the network easier to manage by breaking it down into smaller, more manageable parts. This can simplify the task of monitoring and securing the network, making it easier to identify and respond to potential issues.

Therefore, when deploying a Malcolm server in a Solar Power Generation System, it's essential to consider how the network can be segmented to improve performance and security. This involves understanding the network architecture of the system, identifying how the network can be divided into segments, and configuring Malcolm to monitor these segments effectively.

Finally, when deploying OT network sensors, use sites, and zones to segment your network[55]. Sites reflect many devices grouped by a specific geographical location, such as the office at a specific address[56]. Zones reflect a logical segment within a site to define a functional area, such as a specific production line[57].

By following these best practices, you can enhance the security of your Solar Power Generation System and ensure that your Malcolm deployment is as effective as possible.

7. POST-DEPLOYMENT

GUIDELINES FOR MONITORING AND MAINTAINING THE SYSTEM AFTER DEPLOYMENT

Once Malcolm is deployed in a Solar Power Generation System, ongoing monitoring and maintenance are crucial to ensure its effectiveness and the overall security of the system[58].

Monitoring involves regularly checking the system's performance and the alerts generated by Malcolm[59]. This can help identify any anomalies or potential threats in network traffic. Malcolm's intuitive interfaces, OpenSearch Dashboard and Arkime, can be used for this purpose[60]. They provide an at-a-glance overview of network protocols and a powerful tool for finding and identifying the network sessions comprising suspected security incidents[61].

Maintenance involves keeping Malcolm and its components up-to-date. This includes updating the Docker containers that Malcolm operates as and ensuring that the latest versions of PCAP files and Zeek logs are being used[62]. Regular system updates ensure that the system is protected against known vulnerabilities[63].

TROUBLESHOOTING COMMON ISSUES

Despite best efforts, issues may arise during the operation of Malcolm in a Solar Power Generation System. Troubleshooting these issues involves understanding the problem, investigating its cause, and implementing a solution[64].

Common issues may include network data not being properly captured or forwarded to Malcolm, and alerts not being generated when expected[65]. These issues can often be resolved by checking the configuration of Malcolm and the network switches, ensuring that SPAN ports or TAPs are correctly set up, and verifying that the network traffic data is being properly captured and processed[66].

In case of persistent or complex issues, it may be necessary to seek assistance from the INL Malcolm support team[67]. They can provide expert guidance and help resolve the issue[68].

Post-deployment monitoring and maintenance, as well as effective troubleshooting, are key to ensuring the successful operation of Malcolm in a Solar Power Generation System. By following these guidelines, you can ensure that Malcolm continues to provide valuable insights into your network traffic and enhance the security of your Solar Power Generation System.

[55, 56, 57] Ibid.

[58] "Malcolm | A Powerful, Easily Deployable Network Traffic Analysis Tool Suite." Malcolm, 2024. https://malcolm.fyi/.

[59, 60, 61, 62, 63, 64, 65, 66, 67, 68] Ibid.

8. CONCLUSION

DEPLOYING HEDGEHOG SENSORS IN SOLAR POWER GENERATION SYSTEMS

This guide has provided a comprehensive overview of deploying Malcolm, a powerful network traffic analysis tool suite, in Solar Power Generation Systems. We began with an introduction to Malcolm and its capabilities, highlighting its ability to process network traffic data and providing valuable insights into a system's operation. We then delved into the specifics of Solar Power Generation Systems, discussing the various network-connected equipment and the importance of understanding the network architecture for a successful Malcolm server and Hedgehog deployment.

We outlined the basics of Malcolm server deployment, including its key features and the deployment process. We also discussed the network architecture for Malcolm deployment, explaining where to place network switches and how to configure SPAN ports or TAPs. The guide also covered the deployment of Hedgehog sensors, another key component in these systems, providing guidelines for their deployment in Solar Power Generation Systems.

The guide then detailed the steps for deploying Malcolm sensors in the network and shared best practices for sensor deployment in an ICS/OT network used in Solar Power Systems. Finally, we discussed the importance of post-deployment monitoring and maintenance and provided tips for troubleshooting common issues.

Deploying Malcolm in a Solar Power Generation System can significantly enhance the system's monitoring capabilities, providing valuable insights into the operation of the system and helping to ensure optimal efficiency and reliability. By following the guidelines and best practices outlined in this guide, you can effectively deploy Malcolm in your Solar Power Generation System and maximize its benefits. Whether you're a security analyst looking to enhance your network visibility, or an IT professional tasked with maintaining network security, this guide aims to provide you with the knowledge and tools you need to get the most out of Malcolm. Thank you for choosing Malcolm for your network traffic analysis needs.