Addressing Electric Aviation Infrastructure Cybersecurity Implementation

Anthony Markel and Anuj Sanghvi

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-82856
December 2022

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

Addressing Electric Aviation Infrastructure Cybersecurity Implementation

Anthony Markel and Anuj Sanghvi

National Renewable Energy Laboratory

Suggested Citation

Markel, Anthony, and Anuj Sanghvi. 2022. *Addressing Electric Aviation Infrastructure Cybersecurity Implementation*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-82856. https://www.nrel.gov/docs/fy23osti/82856.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-82856
December 2022

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by Federal Aviation Administration, Airport Technology Research & Development Branch (ANG-E26), under contract No. 692M15-21-N-00003. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photo from iStock 1223449835.

NREL prints on paper that contains recycled content.

Acknowledgments

The authors would like to acknowledge the sponsorship of the Federal Aviation Administration, Airport Safety R&D Section (ANG-E26), that has enabled the collection of content and assessments incorporated within this technical publication. We appreciate the leadership of Jonathan Torres in providing focus to this work. Lastly, the review comments from Wesley Major, Russ Gorman, and Darian Byrd were key to providing a quality outcome relevant to the FAA mission.

List of Acronyms

ACI	Aviation Cyber Initiative
DER-CF	Distributed Energy Resources Cybersecurity Framework
DMZ	Demilitarized zone
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
ES-C2M2	Energy Systems Cybersecurity Capability Maturity Model
EV	electric vehicle
EVSE	electric vehicle supply equipment
FAA	Federal Aviation Administration
FedRAMP	Federal Risk and Authorization Management Program
ISAC	Information sharing and analysis centers
IT	Information Technology
LAN	local area network
NAVFAC	U.S. Navy Naval Facilities Engineering Command
NIST	National Institute of Standards and Technology
OCPP	Open Charge Point Protocol
OIG	Office of Inspector General
OSI	Open Systems Interconnection
TLS	Transport Layer Security
VPN	Virtual private network

Executive Summary

This technical report evaluates key considerations of cybersecurity systems in preparation for the electrification of both legacy and new aviation services. The objectives are to consider the landscape of components and interconnections, review sensitivities and the criticality of operational data, consider applicability of existing best practices, and identify gaps associated with the cybersecurity of electric charging systems for the aviation sector. It is noted that cybersecurity analysis is a key component of the overall hazard analysis for aviation electrical infrastructure necessary for safely providing energy to aircraft.

The infrastructure needs for charging energy storage systems onboard aircraft will include interactions with a broad and diverse set of stakeholders. It is important to develop a common understanding of cybersecurity policies and practices for this stakeholder landscape that will limit the overall attack surface and improve response capabilities. This paper discusses references and existing knowledge within the development space of ground vehicles that are relevant for application to the aviation sector. Additionally, facility requirements that are currently specific to the aviation sector are considered for applicability to future charging systems.

Given the early stages of electric aviation deployment, developers can plan and integrate cybersecurity strategies into the complete electric aviation system during the initial stages of design and procurement. By employing a common framework for cybersecurity early in the development process and throughout the overall aviation charging system, the operational infrastructure could be more defensible and resilient to cyberattack impacts. Key cybersecurity strategies and resources for potential application to forthcoming electric aviation systems will be presented.

Table of Contents

System Components and Stakeholders

The electric vehicle (EV) infrastructure ecosystem that is currently under development in support of a future electrified aviation fleet has significant complexity but also has parallels to the existing ground transportation electrification infrastructure. It is useful to consider a system diagram with key stakeholders, components, and interactions, as depicted in Figure 1, to begin considering cybersecurity risks. The National Institute of Standards and Technology (NIST) defines cybersecurity as “the prevention and limitation of unauthorized access, use, disclosure, disruption, modification, or destruction of information technology (IT), operational technology, and information assets to ensure their confidentiality, integrity, and availability” (NIST SP800-37). With this guidance the assessment can be more focused on digital connections and data than an all-hazards analysis that would address broader physical and weather-related impacts. Note that the specific scenario, stakeholders, and components depicted in Figure 1 help to frame our assessment; however, these could vary depending on the unique aspects of the host facilities and use cases for electric aviation vehicles at that facility, so the diagram presented should only be considered a sample scenario. The operational dependency on data being transmitted between nodes makes communication channels, protocols, and the information itself a potential target for attackers to cause disruptive cybersecurity incidents.

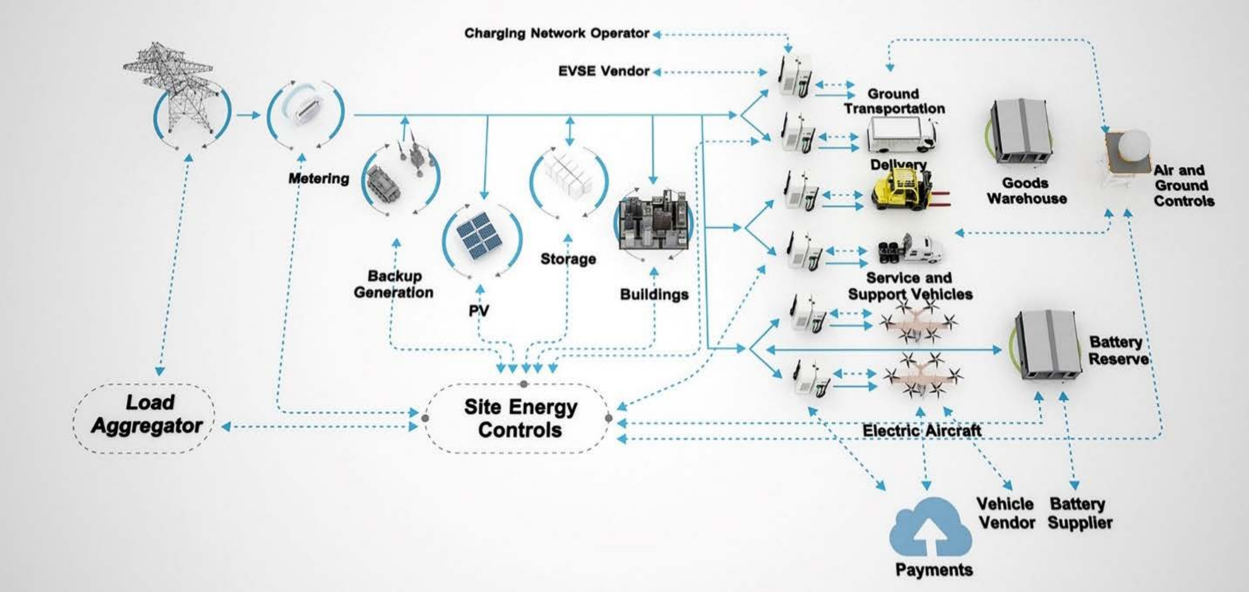

Figure 1. Electric aviation ecosystem and stakeholders. The solid lines represent energy flow, and the dashed lines represent information flow.

Figure by NREL

The diagram shows a series of EV charging stations (to the left of the electric aircraft label) serving a breadth of users and vehicles, which may include aircraft, ground transport, and service and delivery vehicles. Power transfer interfaces are depicted with solid lines, and the network and data interfaces are shown with dashed lines and include arrows to depict the direction of flow. Depending on the placement within an aviation facility, charging stations could be dedicated to a specific vehicle type or user or could be more open for multipurpose scenarios. There can also be various owner, lease, operator, or contractor scenarios to consider for the chargers and facilities to which they are connected. The vehicles currently depicted in Figure 1 include electric aircraft and ground support/service vehicles, both likely to be on the air side of a typical airport facility, whereas delivery, ground transportation, and personal vehicles would likely interface on the land side of a typical airport facility. In each case, the vehicle and/or user is expected to communicate and interact with a charging station, either physically via a touch pad or digitally via a mobile app, for individual charging sessions. From a security perspective, physical access may be managed with fencing and barriers, while digital access is likely managed through authentication and registered user accounts.

The left side of the diagram shows the power delivery networks that will serve facility loads, such as physical buildings, and could integrate local energy resources, including energy storage, photovoltaics, and backup generation. All of these power delivery and generation resources, along with the charging stations, could communicate via internal networks with site energy controls to optimally satisfy the energy demands of an aviation facility. By coordinating loads and generation assets, a facility can manage grid energy demands and cost of operations. The bulk grid and load aggregation services are shown beyond the local facility metering. A load aggregator would generally have insight into the site behavior and flexibility such that it could negotiate on behalf of the site to provide grid services. This generates value potential for an aviation facility to participate in future grid transactive market scenarios, but it also creates an additional digital network information path and potential cyberattack surface to which risk management strategies should be applied.

The right side of the diagram shows additional stakeholders that could have interactions specific to aviation electrification. A battery reserve facility could house and provide replacement batteries to electric aviation vehicle power systems that use an exchange model. When the batteries are not being used by the aircraft, they could act as controllable load or a generation source to aid with overall facility energy management, and thus they've been shown to include both power and communications interfaces. The depiction of the air and ground control systems indicates that information could be exchanged about vehicle location and ownership, energy storage status, and potentially load forecast or charging reservation data sets associated with aircraft and site-hosted charging infrastructure. The complexity of many stakeholders and devices interacting and making local decisions will present a significant cyber monitoring challenge.

The top and bottom of the diagram show vendor management and support functions related to specific components. Both the electric vehicle supply equipment (EVSE) manufacturer and the vehicle manufacturer would likely communicate via remote cellular connections with their respective components for status and health reporting on a regular basis. These connections would also enable firmware maintenance and system configuration through restricted authorized user accounts. Various networking configurations connect devices to each other and also connect the devices to an external network that leverages Ethernet, Wi-Fi, and/or cellular media. The charging station network operator generally connects to groups of chargers that could be from various manufacturers, and it has the responsibility to manage accessibility and availability for approved charging events with vehicles and users. Finally, a transactions and payment vendor system would also be needed to manage financial transaction aspects. The diagram shows the transactional components directly interfacing with the vehicle and charger, but the components could alternatively pass through a third-party transaction brokering entity.

This depiction of the EV ecosystem within the aviation context is a single representation, and many variations could be implemented. The key takeaway should be that the ecosystem is comprised of many computing device end points that operate on software systems that will leverage both internal and external data connections, including interactions with various stakeholders—therefore, cybersecurity strategies that provide defense-in-depth mitigation approaches at all phases of planning, procurement, and operations are needed to ensure that threat actors have a significant challenge in causing physical harm or jeopardizing sensitive data quality and trust. Defense-in-depth approach is a holistic method to add multiple layers of security mechanisms at each stage of system and operation life cycle with the intent to make it increasingly more difficult to affect the most critical components of a system.

Depending on the roles and responsibilities of managing and maintaining continued operations, certain cybersecurity best practices enable increased security and resilience. The first sections of this report define the unique requirements of the aviation sector. The latter sections explain prior work analyzing cybersecurity consequences and mitigations for potential applicability for the aviation charging sector.

This discussion highlights the complexity of information flows and the decisions that individual components make that leverage trusted information across an expansive network. There is potential for significant impacts from cyberattacks, so this report presents a fundamental background on relevant tools and strategies that reduce the overall cyberattack surface and their potential implementation to aviation electrification systems.

Electric Vehicle Infrastructure Cybersecurity

Present-day EV charging infrastructure was conceived and planned during the early 2000s through various industry working groups to achieve interoperability, scalability, and a satisfying user experience. Only recently has the cybersecurity of the EV charging infrastructure come forward as a critical need.

Federal fleets have been leading the transition to electrification. Hodge et al. (2019) introduced cybersecurity risk reduction strategies related to vehicles and their charging and telematics systems with the perspective of how federal fleets should be aware of these potential issues. The paper presents a collection of mitigation actions to minimize cyber risks, both physical and remote, to forthcoming EV charging infrastructure. The paper also introduces procurement options that should lead to equipment that includes at least a minimum level of security functions.

To understand the risks associated with charging infrastructure, it is important to consider the communications backbone between the charging stations and the central system controllers. This traffic typically flows over cellular connections either via private networks or the public internet. Open Charge Point Protocol (OCPP) is often used to enable interoperability between stations and operators, although security features vary depending on the version used and configurations. OCPP is an open standard protocol that is widely adopted by EVSE manufacturers to enable back-end communication with charging stations for coordinating EV charging information along with managing energy consumption dependencies. Insecure implementation may leave open the potential for denial-of-service[1] and man-in-the middle[2] attacks, among others, that can impair the operational state. Mitigation approaches discussed in Hodge et. al. (2019) include encryption using certificate and key management by leveraging the best available Transport Layer Security (TLS); using digital signatures for all message exchanges; and additional considerations for data at rest and data in transit for personally identifiable information, vehicle-specific information, billing information, etc. The two attacks mentioned above are just samples from a long list of possible methods. The MITRE ATT&CK (https://attack.mitre.org/matrices/ics/) provides a detailed listing of attacker techniques and tactics related to various target outcomes for cyber threat actors.

Scenarios and tests conducted in Sanghvi et al. (2021) and Sanghvi (2021) were driven by the expectation of on-site distributed energy generation that would be coordinated with charging and introduce potential security implications from energy management system dependencies along with local energy assets intended to support overall site operations. These tests also focused on preventing denial-of-service attacks and manipulation through man-in-the-middle attacks via defense-in-depth mitigation approaches that can strengthen the overall posture and increase the defensive layers against compromise. These tests and mitigation actions address only a subset of consequences that have been identified by a national laboratory working group. Further study of the various entry points and attacker tactics specific to aviation electrification systems would be a possible path for future research.

[1] Denial of service is a type of cyberattack where the access to a network, resource, or service is disabled or blocked, often by means of overloading a device with requests.

[2] Man-in-the-middle is a type of cyberattack in which the attacker is able to route communications intended to go between two specific devices to an intermediate device that is able to then read and/or change the contents of the message prior to delivery to its intended destination.

Within the working group project scope, an effort was conducted to identify and rank a broad range of high-consequence events that could result from cyber threats and vulnerabilities within EV infrastructure (Carlson 2021). The prior study ranks the EV/EVSE threats and impacts and further researches several high-impact scenarios. These included the potential to coordinate emergency stop functions across a fleet of high-power chargers to cause grid-level power disturbances. Additionally, for high-power charging systems (generally greater than 50 kW), cooling systems within the charger and cable are necessary to achieve performance and safety benefits. Disabling the cooling system could result in degraded service and/or overheating of cables and connectors, risking user safety and device functionality. The same effort also performed cyberattack scenarios, including a man-in-the-middle attack between the energy storage and management systems, a malicious command injection to the site meter, and message hijacking between the server and client. The high-consequence events identified as a part of the project were categorized as grid impacts, safety, hardware damage, denial of service, and data theft all deriving from risks associated with EVSE. These risks and mitigation recommendations include the use of TLS, certificate authorities, and security design functions, which are described in more detail in the later sections of this report. These efforts identified that the operators and sites are dependent on control and sensor data, rate limitations, and functional aspects of other systems, each of which may be equally susceptible to cyberattack and data manipulation.

In another U.S. Department of Energy-funded effort, Johnson et al. (2020) provides overview guidance for cybersecurity best practices related to charging stations, networks, and operations. The insights collected and shared are based on evaluations of existing systems and an understanding of expectations for the future scale and function of deployments. The best practices are grouped into those targeted at business networks and operations, EVSE device security, EVSE networking, and EVSE operations. The paper notes that overall, the NIST Cybersecurity Framework should guide system assessments. For EVSE devices, the best practices highlight the importance of understanding the supply chain, managing both the physical and network access to infrastructure, and using data encryption. At the system level, the use of firewalls and network segmentation offers the ability to limit attacker mobility and the potential for scaling impacts. Although not yet offered, the use of intrusion detection and prevention systems will likely be needed at scale to improve the visibility and to maximize the value of threat activity alerts from monitoring systems. Understanding that the procurement and operations of EVSE for aviation might not be directly controlled by the Federal Aviation Administration (FAA), it will be important to clearly define requirements and operator responsibilities in contracting language.

Prior work on conducting cyber risk assessments of EV charging system has significant relevance to electric aviation and the charging infrastructure needed to support it. Lessons learned and the resulting best practices from the assessments and tests should be leveraged within the electric aviation design phases and thus enable intrinsic security mechanisms to be embedded within rather than be included as add-on solutions.

Cybersecurity Guidance

Resources are available that can be used as guides toward addressing cybersecurity requirements for charging infrastructure integration for future electric aviation scenarios. The following content provides summaries of key resources along with their relevance to electric aviation technologies. These are a subset and should be considered relative to the specific case of facility deployment and operation of the charging infrastructure. Aviation facility implementation and ownership models are likely to vary from one site to another, and therefore the responsibilities for the charging infrastructure might vary too. Certain cybersecurity guidance documents are specifically targeted to federal owners and operators, whereas others might be more broadly targeted to both government and public/private entities. Next, this section discusses the specific cyber guidelines to be considered based on the ownership models of the host site and the charging infrastructure.

The application of cybersecurity guidance and/or requirements will likely be affected by the various owner, operator, and sponsor scenarios that lead to the development and operation of the electrified aviation sites. Some sites might be owned by the FAA, whereas in other locations, the FAA might lease space and services from a public or privately owned facility. There might also be publicly available facilities where, through targeted resources, the FAA has funded the deployment of infrastructure to aid with sector growth. Finally, some electric aviation facilities could be fully privately funded and operated. Those that have an FAA ownership arrangement or FAA direct funding will likely need to adopt federal rules and guidelines for the cybersecurity of equipment and operations. In scenarios where the FAA is simply using or leasing resources and capabilities provided by others, it's possible that federal requirements may not be required, while recommendations from industry-wide standards organizations, including NIST, would likely need to be considered. Given that aircraft will move between geographically diverse sites with varying rules and requirements on cybersecurity, a gap exists on how to maintain security and consistent data handling methods along with a trusted user experience across the entire ecosystem. Reviewing the various owner/operator implementation models might need to be considered, and relevant cybersecurity guidance will need to be adopted and documented.

Federal Aviation Administration Cybersecurity Guidance

Although no specific EV and charging infrastructure cybersecurity guidance was directly noted from the FAA, cybersecurity in aviation facilities and operations has certainly been a growing priority of the Biden-Harris Administration. In congressional testimony, FAA Chief Information Security Officer Larry Grossman summarized that the FAA cybersecurity strategy includes five high-level goals (Grossman 2021):

1. Refine and maintain a cybersecurity governance structure to enhance cross-domain synergy.
2. Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery.
3. Enhance data-driven risk management decision capabilities.
4. Build and maintain workforce capabilities for cybersecurity.
5. Build and maintain relationships with, and provide guidance to, external partners in government and industry to sustain and improve cybersecurity in the aviation ecosystem.

Additionally, the Aviation Cybersecurity Initiative (ACI) was initiated and is an interagency task force between the FAA, the U.S. Department of Homeland Security, and the U.S. Department of Defense with a mission to address the cyber risk and resilience of the national aviation ecosystem. Given the early nature of aviation electrification and its associated charging infrastructure, aviation electrification and the related cyber needs are not present in the initiative. The efforts of the ACI working groups address information-sharing needs, workforce development, testing, and analysis for system resilience and creating metrics for understanding the cyber risks. As part of the ACI, an annual Aviation Cybersecurity Summit provides a venue for collaboration and coordination among government organizations (U.S. DOT OIG 2020; ACI 2021). Incorporating topics on aviation electrification and the associated cybersecurity risks to consider during planning and operations would further address the immediate needs to support such a technology transition.

Planning and Procuring Equipment for Government Fleets

The EV charging infrastructure to support aviation electrification might be multipurpose because it could serve both private and government electrified vehicles. In considering the procurement of such infrastructure, an important resource is from the U.S. Naval Facilities Command (NAVFAC), in collaboration with the U.S. Department of Transportation (DOT) Volpe Center. That report studied the EVSE cybersecurity needs for procuring and installing EV charging infrastructure within government and commercial facilities (U.S. DOT Volpe Center 2019).

The report focuses on existing vulnerabilities potentially of concern in the manufactured EVSEs that were associated with credential management, code injection, and SQL database injection and proposes threat modeling for data and information disclosure. It notes that for federal government implementations, the applicability of "NIST SP 800-37: Guide for Applying the Risk Management Framework" and "NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations" should be considered. If the charging systems within federal facilities leverage cloud-based systems, then the environment would be required to follow the Federal Risk and Authorization Management Program (FedRAMP) to ensure that any federally owned data are properly secured and stored with limited access. FedRAMP is a government-wide program that provides a standardized approach to cybersecurity assessment, authorization, and continuous monitoring for cloud products and services, such as EVSE back-end network (U.S. DOT Volpe Center 2019). The U.S. DOT Volpe Center (2019) also denotes physical security considerations for the EVSE environment that include the use of anti-tamper hardware, event and incident monitoring, video surveillance hardware, and tamper alerts for the EVSE components.

Cybersecurity Design and Operations—Secure Controls and Measures

Electrification of U.S. air transportation involves complex systems and interconnections for data and power transfers. Network communications support critical operations, and thus an increased emphasis is needed to protect them from cyberattacks. Due to mission-critical support functions, prioritizing and securing the charging behaviors of electric aircrafts via security controls and measures must be considered further.

Defining the mission and the support function, though not technically within the scope, shapes the design and planning of electrification and its requirements. Electric aircraft, much like ground-based EVs, are supported by a charging infrastructure comprising high-power charging stations, battery reserves, vendor-connected cloud functions, overall building load management systems, etc. Figure 1 depicts the interconnectedness of these systems. The cybersecurity implications and attack vectors exist for each component, along with grid edge devices, which pose risks to the federally owned ecosystem, including networks, information, personnel, and other dependent entities. Distributed energy resources that primarily act as support or provide backup supply and enhance sustainability also introduce potential vulnerabilities to the infrastructure and its mission. Resources like the Distributed Energy Resources Cybersecurity Framework (DER-CF)[3] should be leveraged to undergo foundational risk assessments and identify gaps and mitigation action items.

A memorandum for federal agencies that operate within the critical infrastructure realm was released from the White House in early 2021 targeting future transitional guidance from the Office of Management and Budget on the implementation of zero trust systems (OMB 2022). In response, NIST developed SP 800-207 on zero trust architecture. According to the NIST guidance, a zero trust architecture assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location, and requires additional information for authentication and authorization to establish each session demanding resources. Zero trust methods are applicable to remote connections, cloud-based servers, and other resources located both inside and outside an organization-owned boundary. We are not aware of an application of zero trust within the EV charging ecosystem, but its use may provide benefits. Additional resources and guidance could be considered for conducting proof-of-concept designs that would lay a foundation for future more secure zero trust infrastructure both for aviation and ground electrification.

Cybersecurity Authorizations for Electric Vehicle Supply Equipment

The FAA will likely need to perform and/or accept from others the cybersecurity testing and verifications for specific federally funded aviation charging equipment and systems that would then enable an authorization to operate. An authorization to operate is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations, assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.[4] For standardization and compliance through the Federal Information Security Management Act, NIST SP 800-37 promotes the adoption of security controls from NIST SP 800-53R5 and the industrial control system overlays from NIST SP 800-82. These form the basis of cybersecurity best practices and need to be tailored/enhanced for site-specific needs. Airport improvement and cybersecurity enhancement programs might include provisions to implement the security controls as laid out in the requirements but might also need additional tailoring and/or modifications for the future needs of electric aviation. Completing the risk assessment process using the NIST guidelines early in the planning stages could enable robustness in the documentation of anticipated risks that need mitigation approaches to be planned, response strategies to be developed, or acceptance of the identified risks.

As it relates to typical charging infrastructure that might exist in a future aviation environment, the components that function together for the purpose of charging consist of the EVSE owner/operator, the site controller, the charge network operator, and the grid operator, as depicted in Figure 1. A

[3] More information on DER-CF tools at www.dercf.nrel.gov.

[4] https://csrc.nist.gov/glossary/term/authorization_to_operate

potential requirement exists for the vendor's cloud infrastructure to be FedRAMP certified in cases when it would support charging systems with monitoring, control, and software update functions.

Non-cloud components that interface with other federal networks might need to be approved through the NIST Risk Management Framework, which primarily undertakes NIST SP 800-53 security controls. Overlays for securing industrial control systems can also be leveraged through NIST SP 800-82, which has supplemental guidance for legacy and operational technology devices and assets. These control system devices differ from information systems from a basic priority of system availability over data confidentiality and can be addressed through adherence with additional NIST publications.

Recommendations

Recommendations based on prior work and the discussion presented include, but are not limited to, the following:

- **Procurement and conformance testing:** Includes available cybersecurity requirements through current standards and guidelines—for example, the NIST SP 800 series and the General Services Administration/NAVFAC EVSE guidance—to acquire accepted systems and to enable a mechanism to run tests that identify potential cybersecurity gaps early. Tabletop and/or physical tests are ideal for calculating risks and threats that often accompany the system being integrated and enable constructing an informed risk response strategy. More detail is outlined earlier in this report in the section titled *Planning and Procuring Equipment for Government Fleets.*
- **Cybersecurity within design:** Facilities depend on vendors and manufacturers for providing devices and applications that enable operations. This dependence can include a clear identification of roles and responsibilities regarding the management of risks. Contracts developed with vendors/manufacturers will benefit from incorporating cybersecurity language along with requirements such as participation in periodic vulnerability assessments and maintenance of facility-specific security postures. More detail is outlined in the section titled *System Stakeholders and Components.*
- **Network segregation, zoning, and segmentation:** The concept of network segmentation allows not only the capability to organize network traffic but also to implement security mechanisms such as access control and prevent network transversal. Within the context of EV infrastructure, dividing the architecture and the communicating devices into zones significantly narrows the attack surface. For example, in a controlled-segmented network architecture, a compromised site energy management server will not be able to manipulate an EVSE controller's operation because of the restrictions on device traffic and content flow between segments. More detail is outlined in the section titled *Electric Vehicle Infrastructure Cybersecurity.*
- **TLS:** TLS is an authentication mechanism to ensure that a client and server can each be validated to increase trust in the sources of data to be exchanged. TLS is a process for encrypting communications by sharing information only the trusted entities are aware of. This is done by certificates and is issued by certificate authorities. Devices in EV ecosystems—such as back-end servers, charging station clients, and third-party cloud services—can benefit from having a restricted and protected communications channel leveraging certificate authorities. This also enables end device whitelisting, ensures that only trusted devices on the network are communicating, and enforces that the communications are encrypted. More detail is outlined in the section titled *Electric Vehicle Infrastructure Cybersecurity.*
- **Virtual private networks (VPNs) and zero trust:** VPN provides a means of having private communications over public channels. Services provided by various devices use web servers that connect over public internet. Such communications must be encrypted to enable data confidentiality and limit risk of leakage and/or manipulation. In addition to the use of VPNs, conducting demonstration of zero trust implementations within an EV charging ecosystem for aviation would align with administration priorities for federal government-operated facilities and networks.

- **Application-aware firewalling:** Functions that support operations in the EV ecosystem depend on specialized communications protocols and gateway devices—such as next-generation firewalls and intrusion detection/prevention devices—that understand these custom and proprietary applications assist in the ability to detect abnormal traffic.
- **Traffic monitoring and baselining:** This refers to network taps and other devices that enable traffic mirroring without adding any delay, allowing operators to actively monitor network traffic. This helps with understanding normal communications and behavior and allows for tracking user and device activities as well. Baselining the "normal" behavior of devices can enable the active documentation of potential alerts of "abnormal" network activities and the characterization of consequences.
- **Incident Response and Recovery:** The development and review of cyber incident response and recovery plans can reduce the impact of an ongoing incident while also reducing the time required for recovery. NIST SP 800-184 and Cybersecurity and Infrastructure Security Agency (CISA) 2021 provide approaches to creating playbooks (an action plan with roles and responsibilities) that address the key steps to recovery. Response and recovery planning should include identifying triggers for enacting the response plan, resources necessary to contain and recover, internal and external communications strategies, and frequency of practice and updates to planning documents. Additionally, information sharing and analysis centers (ISAC)—including the Auto-ISAC, the Aviation-ISAC, and the Multi State-ISAC—provide frequent updates on current threat activities that can help organizations be proactive in updating plans and observations.
- **Performing periodic risk assessments:** A critical aspect of risk response is conducting risk assessments that assist in identifying assets that might be vulnerable. Using industry-adopted mechanisms can be beneficial in quantifying risks, while certain tailoring should be implemented to classify electric aviation-specific functions that are mission critical.

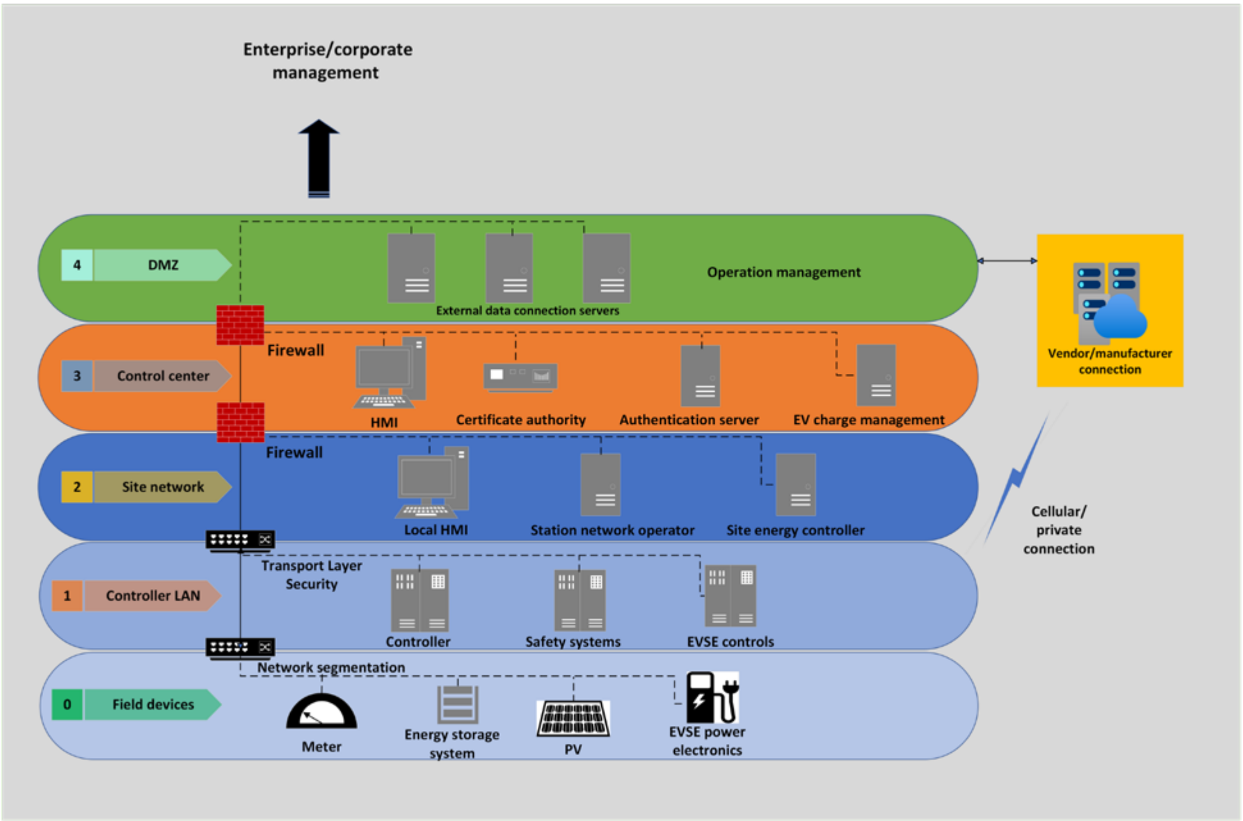

Figure 2. Layered security architecture for EV charging systems

Figure by NREL

Implementing a secure architecture calls for a defense-in-depth strategy and the adoption of key recommendations. The Purdue model provides a strategy for planning the criticality and function of components and specifically defining the needs for monitoring and defense strategies for each network layer. Figure 2 shows a layered security architecture related to charging system components. In this diagram, the Open Systems Interconnection (OSI) layers are interpreted within the EV charging ecosystem as Layer 0: Field devices; Layer 1: Control local area network (LAN); Layer 2: Site network; Layer 3: Control center; and Layer 4: Demilitarized zone (DMZ). Outside the DMZ, a connection to enterprise networks (including business and IT resource devices) is shown. A single mitigation or a solution cannot adequately protect the complexities of a charging infrastructure. A layered approach with overlapping security controls is desired to be able to optimally decrease the impact of a cybersecurity incident. This approach includes the use of several mechanisms, such as network segmentation, segregation or separation based on services and assets, access control lists, and the creation of demilitarized zones, along with effective security policies. This strategy also enables the understanding of possible attack vectors at each layer and helps with realizing potential gaps.

These overlapping security mechanisms between layers comprise a defense-in-depth approach. Layer 4 and beyond have interconnectedness with management and business function systems and operations. There are requirements from the enterprise networks to access operational data for monitoring, control, and/or making business decisions. These requirements vary with organizations and need to be carefully considered. The principle of least privilege, access control for restricting “view only” data, and the unidirectional flow of data to the management layers are key mechanisms to be implemented.

Special emphasis might be given to external connections, either to third-party applications or to vendor/manufacturer cloud connections for various purposes. These connections from the context of the facility should be treated as untrusted, and measures such as virtual private networks, zero trust, and/or Secure Shell protocols should be considered for wired or wireless connections to external systems.

Conclusions

The future of electric aviation support infrastructure is in the early stages of planning, design, and development, while significant uncertainty remains regarding the breadth and specifics of the use cases and requirements. As a result, there is sufficient opportunity to build cybersecurity into the overall system design lifecycle with informed planning. Cybersecurity actions could address facility design and procurement, stakeholder roles and responsibilities, and operational strategies that reduce the overall impact of potential cyber threats.

Facilities benefit from initiating cybersecurity awareness assessments that leverage existing frameworks, such as the U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), NIST SP 800-82, and the critical infrastructure protection documents from the U.S. Department of Homeland Security. The Distributed Energy Resources Cybersecurity Framework (DER-CF) provides a starting point to conduct assessments and generate basic cybersecurity practices to be identified and implemented for organizations' business processes, technical management, and physical security. Cybersecurity frameworks provide a foundation from which modules for specialized deployments and operations tuned for electric aviation can be created, accounting for the needs and requirements of the potential architecture and stakeholders (Figure 1) and the associated unique cybersecurity challenges.

Identifying key personnel both internally and externally who will be responsible for gathering and embedding cybersecurity requirements for the organization into facilities' design plans and procurement activities for the aviation charging system is expected to provide benefits. The aim of this report is to build awareness into different stages of developing and configuring charging infrastructure for electrical aviation and the existing knowledge and resources to be consulted. These stages include structuring procurement requirements, articulating system performance, conducting cybersecurity assessments, performing risk management activities, and maintaining secure operations through the adoption of best practices. This report also outlines prior work and existing guidance that can be leveraged for reference. Experience with performing experiment design, evaluation, and cybersecurity-specific analysis will contribute to the successful evaluation of aviation sector-specific approaches to cybersecurity features integration across the system life cycle.

Conducting maturity-based assessments for a technically complex system (such as EV charging for aviation) and the system's integration with facility networks and grid systems should highlight priorities. Additionally, organizations can benefit from conducting cybersecurity-focused acceptance testing of running software, firmware, and hardware prior to integration into the production environment. Such tests may help validate cybersecurity capabilities of design and inform future process improvements.

This initial cybersecurity assessment for EV charging infrastructure systems to be deployed at aviation facilities has laid a foundation for the path forward. It will be important to understand the key cybersecurity actions that apply in the design, procurement, operations, and monitoring phases. The definition of clear responsibilities specific to the deployment situation (public, private, FAA, or other federal) will help smooth the secure and trusted growth of infrastructure. This report briefly discussed a few core resources that can guide the requirements and risk mitigation actions.

Further efforts should quickly address remaining gaps and concerns to enable the electric aviation sector infrastructure transformation.

References

Aviation Cyber Initiative (ACI): Interagency Task Force. Fact Sheet. 2021. https://www.faa.gov/air_traffic/technology/cas/aci/media/documents/aci.pdf. Accessed January 18, 2022.

Bartock, Michael, Jeffrey Cichonski, Murugiah Souppaya, Matthew Smith, Greg Witte, and Karen Scarfone. 2016. *NIST Special Publication 800-184. Guide for Cybersecurity Event Recovery*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184.

Carlson, Richard "Barney." 2021. "Consequence-Driven Cybersecurity for High-Power EV Charging Infrastructure." Presented at the DOE Vehicle Technologies Program Annual Merit Review, Washington, D.C., USA, June 24, 2021.

Cybersecurity and Infrastructure Security Agency (CISA). 2021. *Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems.* Washington, D.C. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

Executive Office of the President, Office of Management and Budget (OMB). 2022. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.* Washington, D.C., January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

Grossman, Larry. 2021. *Before the United States House of Representatives Committee on Transportation and Infrastructure: The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure*. Congressional Testimony. Thursday, December 2, 2021.

Hodge, Cabell, Konrad Hauck, Shivam Gupta, and Jesse Bennett. 2019. *Vehicle Cybersecurity Threats and Mitigation Approaches*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-74247. https://www.nrel.gov/docs/fy19osti/74247.pdf.

Johnson, Jay, Benjamin Anderson, Brian Wright, Josh Daley, Josh, and Roland Varriale. 2020. *Recommended Cybersecurity Practices for EV Charging Systems.* An infographic for EVSE cybersecurity recommendations and best practices. Albuquerque, NM: Sandia National Laboratories. SAND2020-11401 D. https://doi.org/10.13140/RG.2.2.11141.37602.

Sanghvi, Anuj, Tony Markel, Steve Granda, Adarsh Hasandka, and Myungsoo Jun. 2021. *Identification and Testing of Electric Vehicle Fast Charger Cybersecurity Mitigations*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-80799. https://www.nrel.gov/docs/fy22osti/80799.pdf.

Sanghvi, Markel. 2021. *Cybersecurity for Electric Vehicle Fast-Charging Infrastructure*. Presented at the IEEE Transportation Electrification Conference and Exposition (ITEC), June 21–25, 2021. https://www.nrel.gov/docs/fy21osti/75236.pdf.

U.S. Department of Transportation (DOT) Volpe Center. 2019. *Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report*. Prepared for the U.S. Navy Naval Facilities Engineering Command (NAVFAC). Cambridge, MA. DOT-VNTSC-NAVY-20-01. https://rosap.ntl.bts.gov/view/dot/43606/dot_43606_DS1.pdf.

U.S. Department of Transportation (DOT), Office of Inspector General (OIG). 2020. *FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities*. Washington, D.C. Report No. AV2020043. https://www.oig.dot.gov/sites/default/files/FAA%20Aviation%20Cyber%20Initiative%20Final%20Report%5E09-02-20.pdf.

Bibliography

Georgia, Lykou, Argiro Anagnostopoulou, and Dimitris Gritzalis. 2018. *Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience.* Presented at the 2018 IEEE Global Internet of Things Summit (GIoTS), June 1–6, 2018. https://doi.org/10.1109/GIOTS.2018.8534523.

Mültin, Marc. 2022. "The Four Key Ingredients for a Thriving E-Mobility Ecosystem." *Switch*, January 18, 2022. https://www.switch-ev.com/blog/the-four-key-ingredients-for-a-thriving-e-mobility-ecosystem.

National Institute of Standards and Technology (NIST) Joint Task Force. 2020. NIST Special Publication 800-53 R5. *Security and Privacy Controls for Information Systems and Organizations.* Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Motor Freight Traffic Association. 2018. *Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cyber Security Baseline Reference Document—May 30, 2018. Version 1.2.1*. Alexandria, VA.

Ross, Ronald S. 2018. *NIST Special Publication 800-37 R2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

Schwab, Amy, Anna Thomas, Jesse Bennett, Emma Robertson, and Scott Cary. 2021. *Electrification of Aircraft: Challenges, Barriers, and Potential Impacts*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-6A20-80220. https://www.nrel.gov/docs/fy22osti/80220.pdf.

Stouffer, Keith, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. 2015. NIST Special Publication 800-82 R2. *Guide to Industrial Control Systems (ICS) Security.* Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.