Ardexa NERC Compliance

Technical Briefing

A technical briefing offered by Ardexa on NERC Compliance

Released 21th May 2019

Authors

George Cora – CEO and Director of Ardexa Pty. Ltd.

David Mohr – CTO and Director of Ardexa Pty. Ltd.

About Ardexa Security Principles

Based on our IoT Design Principles, Ardexa has developed edge software that functions on small-form, single board computers. These computers act as gateways for sensors, actuators and applications. The gateway, in conjunction with the Ardexa cloud, allows many key security functions that are crucial to the security of the plant and machines being monitored and/or controlled. This guide provides a summary of exactly how Ardexa meets the North American Electric Reliability Corporation (NERC) cyber security standards.

The key features of the cloud and edge (agent) software are as follows:

- ***Ardexa Security Feature 1***: The Ardexa IoT edge agent initiates all connections to the cloud. It does not accept any incoming connections. This means no open ports at the edge.
- ***Ardexa Security Feature 2***: The Ardexa IoT edge agent uses digital certificates which are used to authenticate and authorize access to the cloud. These certificates are not shared across devices, and so can be revoked or 'quarantined', if the need arises.
- ***Ardexa Security Feature 3***: The Ardexa IoT agent includes metadata in each stream sent by the device. It is also able to collect data from many sources simultaneously and apply metadata to fields in the stream.
- ***Ardexa Security Feature 4***: The Ardexa IoT cloud provides authentication and authorization within "work-groups". Work-group resources access is controlled and logged by the Ardexa cloud.
- ***Ardexa Security Feature 5***: The Ardexa IoT edge agent sends data to the cloud in real time. In event of connection loss, events will be hard-cached, ready for when the connection is re-established.
- ***Ardexa Security Feature 6***: The Ardexa IoT edge agent is able to be fully remote controlled from the cloud, in real time. In addition, files can be transferred in both directions, along with photos and video file formats.
- ***Ardexa Security Feature 7***: All communications are encrypted using digital certificates.
- ***Ardexa Security Feature 8***: The Ardexa Linux image allows automatic connection to the cloud. It also allows configuration of communications parameters from the cloud, in a secure manner controlled and encrypted by digital certificates.

NERC Compliance Approach

NERC standards are used to regulate activity in the North American electricity grid. In their words, "NERC Reliability Standards are developed using an industry-driven, ANSI-accredited process that ensures the process is open to all persons who are directly and materially affected by the reliability of the North American bulk power system; transparent to the public; demonstrates the consensus for each standard; fairly balances the interests of all stakeholders; provides for reasonable notice and opportunity for comment; and enables the development of standards in a timely manner. NERC's ANSI-accredited standards development process is defined in the Standard Processes Manual and guided by reliability and market interface principles."

The purpose of this document is to detail how Ardexa's cloud and edge software features, policy, procedures, testing processes, development processes and deployment contributes to meeting the NERC standards. Only those standards which are active and relevant to the deployment of the Ardexa IoT system are covered in the following sections. The standards below have been derived from the NERC website. The standards are in a constant state of change, and so only "Active" standards are covered. This document does not cover NERC standards which are subject to "Subject to Future Enforcement" or "Filed and Pending Regulatory Approval". These will be covered in updated versions of this document. Also, the level of protection can vary depending on the impact rating of the asset provided by the Responsible Entities. This is detailed in the individual policies discussed below.

Commentary on Relevant NERC Standards

BES Cyber System Categorization

Standard CIP-002-5.1a Reference: https://www.nerc.com/files/CIP-002-5.1a.pdf

This standard is "...To identify and categorize Bulk Electric System (BES) Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES...."

Ardexa Compliance: The Ardexa system, when used to monitor or control a station is classified within this NERC standard as a BES (Bulk Electric System) Cyber System, within the "Monitoring & Control named service". The cloud and edge software and hardware could all be considered a part of the BES. Ardexa will assist the "Responsible Entities" to determine the impact rating, by providing a detailed list of the components and functions of the cloud and edge processing systems. The impact rating will depend on many things outside of Ardexa's control, such as the size of the station, and the redundancy features in place within the power generation network, whether redundant communications are in place and irrespective whether the cloud is "on-premises" or whether it is hosted by an NIST approved service. This rating will be noted in the Ardexa procedures and will be reviewed on a 12-month basis.

Security Management Controls

Standard CIP-003-6 Reference: https://www.nerc.com/files/CIP-003-6.pdf

This standard is "...To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)..."

Ardexa Compliance: This standard defines the framework of security management controls, which subsequently controls the requirement to publish and maintain cyber security policy and procedures relevant to various aspects of this standard. The CIP-003-6 states a general applicability of a minimum of 300MW as the basis for these procedures. However, the Ardexa security management procedures covers a station of any size, and that is; of any impact rating. The Ardexa security management policies cover the management of the security plans detailed in the next sections, covering specific topics in cyber security. These security plans are reviewed every 12 months.

Personnel & Training

Standard CIP-004-6 Reference: https://www.nerc.com/files/CIP-004-6.pdf

This standard is "...To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems...."

Ardexa Compliance: Given the nature of Ardexa as a cloud service, its personnel will usually be granted high level of access to support and develop services. Ardexa staff need privileged access to data and edge devices. Ardexa personnel and training procedures cover how access is granted and revoked to staff, how awareness is promulgated, and steps required for those staff who may need police background checks.

Electronic Security Perimeter(s)

Standard CIP-005-5 Reference: https://www.nerc.com/files/CIP-005-5.pdf

This standard is "…To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES...."

Ardexa Compliance: Ardexa provides 2 distinct Electronic Security Perimeters (ESPs); the cloud and the edge device. At the edge, all incoming ports to the Ardexa device are closed by default. The Agent authenticates to the cloud using a digital certificate which lasts for no more than 2 years. This certificate can be renewed online and can also be revoked at any time. At the cloud, only those ports necessary for communication are open, and cloud services are regularly maintained, updated and patched. As part of the CIP-005-5 compliance, Ardexa policies include these and many more policy initiatives.

Physical Security of BES Cyber Systems

Standard CIP-006-6 Reference: https://www.nerc.com/files/CIP-006-5.pdf

This standard is "…To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES...."

Ardexa Compliance: Ardexa edge devices are co-located with the operator's on-site plant equipment. Physical security of these devices rests with the operator. Google Cloud machines and containers (but not Google software services) are used for the Ardexa cloud. Ardexa can also host the cloud "on-premises" for those clients whose security policies mandate a hosted cloud. Protection for Google Cloud has been certified in accordance with the NIST standards, as attested to in this letter: https://services.google.com/fh/files/misc/2017_google_services_800-53_letter.pdf.

No client data is stored at Ardexa premises.

System Security Management

Standard CIP-007-6 Reference: https://www.nerc.com/files/CIP-007-6.pdf

This standard is "…To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)…."

Ardexa Compliance: Ardexa security management policies cover the use of passwords and digital certificate management, including complexity and revocation. In this policy, Ardexa also details how the cloud and edge software is updated, how often and/or under which circumstances.

Incident Reporting and Response Planning

Standard CIP-008-5 Reference: https://www.nerc.com/files/CIP-008-5.pdf

This standard is "…To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirement...."

Ardexa Compliance: Ardexa has developed incident plans required by CIP-008-5. The plans detail management and responsibilities of handling an incident, and the handling of potential evidence and other forensic material. Ardexa maintains cloud security logs for key events for at least 5 years, and these form a key part of the security incident handling. This Ardexa plan is consistent with the NIST "Computer Security Incident Handling Guide" (Special Publication 800-61).

Recovery Plans for BES Cyber Systems

Standard CIP-009-6 Reference: https://www.nerc.com/files/CIP-009-6.pdf

This standard is "…To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES…."

Ardexa Compliance: Ardexa has developed contingency plans for restoration of services, in event of an incident. The plans detail management and responsibilities of handling of a recovery incident. This Ardexa plan is consistent with the NIST "Contingency Planning Guide for Federal Information Systems" (Special Publication 800-34).

Configuration Change Management and Vulnerability Assessments

Standard CIP-0010-2 Reference: https://www.nerc.com/files/CIP-010-2.pdf

This standard is "…To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES)…."

Ardexa Compliance: Ardexa uses cloud containers and hardened Linux as the preferred Ardexa edge operating system. Each edge device uses Ardexa plugins that communicate with one or more machines at the edge, to monitor and/or control equipment. This is recorded for each plant. Active vulnerability assessment and software patching, including testing, is carried out on an "test-and-acceptance" system.

Information Protection

Standard CIP-011-2 Reference: https://www.nerc.com/files/CIP-011-2.pdf

This standard is "…To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)...."

Ardexa Compliance: Ardexa details how information will be secured at rest, in transit, and whenever it has been resident on any removable media.

ARDEXA
Secure by design

For more information

Email: **support@ardexa.com**

Website: **https://ardexa.com/**