# Cyber-secure Communication Architecture for Active Power Distribution Networks

Teklemariam Tsegay Tesfay, Jean-Pierre Hubaux, Jean-Yves Le Boudec, and Philippe Oechslin
School of Computer and Communication Sciences, EPFL
Lausanne, Switzerland
{tech.tesfay, jean-pierre.hubaux, jean-yves.leboudec, philippe.oechslin}@epfl.ch

## ABSTRACT

Active power distribution networks require sophisticated monitoring and control strategies for efficient energy management and automatic adaptive reconfiguration of the power infrastructure. Such requirements are realised by deploying a large number of various electronic automation and communication field devices, such as Phasor Measurement Units (PMUs) or Intelligent Electronic Devices (IEDs), and a reliable two-way communication infrastructure that facilitates transfer of sensor data and control signals. In this paper, we perform a detailed threat analysis in a typical active distribution network's automation system. We also propose mechanisms by which we can design a secure and reliable communication network for an active distribution network that is resilient to insider and outsider malicious attacks, natural disasters, and other unintended failure. The proposed security solution also guarantees that an attacker is not able to install a rogue field device by exploiting an emergency situation during *islanding*.

## General Terms

Smart grid, security

## Keywords

Smart grid security, Active distribution network, Islanding, PKI, Authentication, Unauthorised access

## 1. INTRODUCTION

Conventional power distribution networks are passive and are characterised by unidirectional power flows with a minimum level of centralised monitoring and control strategies. However, the large-scale penetration of embedded distributed energy resources and the introduction of energy storage at the distribution premises is paving way for the emergence of active distribution networks (ADNs). An active distribution network is a distribution network with local energy generation, storage capabilities and bidirectional power flow; it requires more sophisticated active monitoring and control strategies. An active distribution network is divided into a subset of loosely-coupled autonomous regional controllers that can perform monitoring and control actions for their geographical subnetwork [23]. Under normal circumstances, each subnetwork is connected to the main power grid and each autonomous controller is able to cooperate with peer controllers when necessary. Inter-domain communication among autonomous controllers is necessary for detecting unexpected power system failures and other anomalous conditions in adjacent regions or in the main grid.

In most extreme cases, when a controller detects a widespread disturbance or power failure, the active distribution subnetwork within the controller's domain can automatically isolate itself from the grid and continue to operate as an island. The power demand within the island is then supplied by the local energy generation and storage until the island back-synchronises with the grid when the faults are resolved [4]. During this *islanding* process, power flow control and voltage and frequency regulations are carried out by the autonomous island controller (IC) in coordination with sensing and actuating devices deployed within the island.

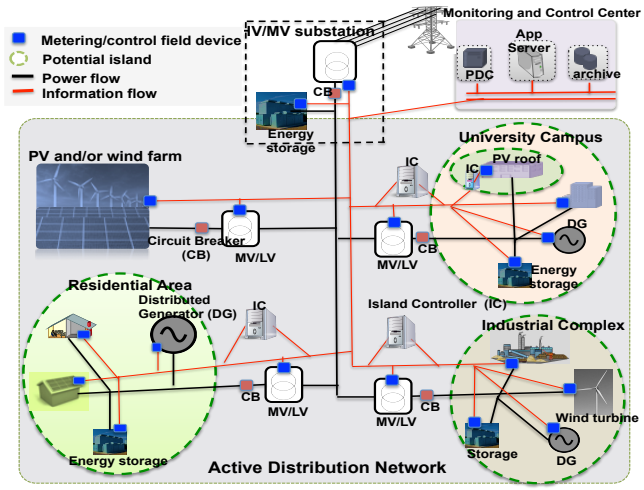


**Figure 1: An active distribution network where the sensing and control cyber infrastructure is superimposed on the physical power system infrastructure (adopted from [8]). Different possible islanding configurations are shown such that an island can be a superset of islands depending on where the fault occurs.**

Figure 1 illustrates the cyber-physical nature of a typical


*SAC 2014* March 24-28, 2014, Gyeongju, Republic of Korea.

http://dx.doi.org/10.1145/2554850.2555082.

active distribution network where the sensing and control cyber infrastructure is superimposed on the physical power system infrastructure to facilitate the sophisticated automation operations (monitoring, control and protection) of the distribution network. A sophisticated automation system at the distribution level requires deployment of a large number of electronic data-acquisition and actuating field devices, which are nonexistent today [7]. Moreover, a high-speed and reliable two-way communication infrastructure is required to facilitate a real-time transfer of sensor data and control signals.

The increasing reliance of distribution network operations on pervasive electronic automation devices and on communication networks poses an unprecedented challenge in protecting the system against cyber incidents. Cyber incidents can be intentional or unintentional. Unintentional cyber incidents can occur due to natural disasters, system failures or human errors, whereas intentional cyber incidents occur due to deliberate attacks from outsiders or insiders.

An attacker has a wide range of options to compromise a distribution automation. For example, many of the electronic automation (sensing and actuating) devices are field-deployed in remote locations where there is little protection against intruders. Moreover, the communication infrastructure for an active distribution network spans a large geographic area. Hence some of the communication cables are likely to pass through physically insecure locations, thus providing an attacker physical access to the network. Furthermore, grid operators are increasingly adopting IP-based communication standards and commercial off-the-shelf hardware and software in their networks for interoperability and for cost reduction reasons. Such standards and products are well studied by attackers and are known to be vulnerable to network attacks such as IP spoofing and denial of service (DoS) attacks.

Given such a range of vulnerability points, a malicious attacker can launch sophisticated attacks to cause maximum damage on the distribution network. An attacker can, for example, launch a coordinated cyber-physical attack by first physically destroying a critical component of the grid (e.g., one of the distributed generators) and simultaneously (or with very little time difference) attack the communication infrastructure that transfers information about the status of the critical component. This way, the operator will not know about the state of the damaged component and thus will not take any corrective actions. With no corrective actions taken, such an attack can have a cascading effect, causing a blackout. Although not due to a malicious attack, the North-East American blackout of 2003 was caused mainly because of lack of system-state awareness by an operator.

Although both insiders and outsiders can attack a distribution automation system, insider attacks are more dangerous than outsider attacks mainly because an insider has better access privileges and has better information about internal-procedures and potential weak spots in the automation system. In general, protecting a system against insider attacks is very difficult. However, implementing automated security tools and techniques to detect and identify suspicious activities from insiders can minimise the level of damage.

The main contribution of this paper is to thoroughly assess insider and outsider security threats against a power distribution automation system and propose a check-list of security solutions and best practices to counter such threats. The proposed solution guarantees secure operations even when a sub-domain of the distribution network operates in an islanded mode by preventing outsider attackers and malicious insiders from installing a rogue field device by exploiting the emergency situation.

The rest of the paper is structured as follows. In the following section we identify possible cyber-security threats in a typical active distribution network. In Section 4 we discuss security solutions and best practices that should be implemented to counter the identified security threats. In Section 5 we detail a secure device installation mechanism that guarantees only authorised field engineers can install field devices from accredited device manufacturers. We also devise an extension to the scheme that can be used to securely install field devices during an emergency situation when communication with a user authentication facility is not available from the installation location.

## 2. RELATED WORK

Smart Grid security has recently received a lot of attention both from the research community and standardisation bodies. The NISTIR 7628 [15], "Guidelines for Cyber Security in the Smart Grid" standard provides a comprehensive set of guidelines for designing cyber-security mechanisms or systems for the smart grid. The standard proposes methods for assessing risks in the smart grid, and then identifies and applies appropriate security requirements to mitigate these risks. NIST has also released a draft on Cyber Security Framework for critical infrastructure [13], which is now available for review. This draft follows a risk-based approach to secure critical infrastructures, as opposed to the process-based approach proposed by Langner in [16]. The latter approach stresses that maximising *security capability* is a prerequisite for security assurance of a critical infrastructure. The IEC 62351 standard series [14], developed by WG15 of IEC TC57, defines security mechanisms to protect communication protocols for substation systems, in particular, IEC 60870 and IEC 61850. The primary focus of this standardisation is to provide end-to-end security. The Critical Infrastructure Protection (CIP) set of standards [1] developed by the North American Electric Reliability Corporation (NERC) aims at introducing compliance requirements to enforce baseline cyber-security efforts throughout the bulk power system (transmission).

A large number of publications have also addressed smart grid security as a research problem. [2, 12, 18, 19] define smart grid as a cyber-physical system (CPS) and identify unique security challenges and issues encountered in such systems that are not prevalent in traditional IT security. They also discuss security solutions to address these unique challenges. [21] proposes a layered security framework for protecting power grid automation systems against cyber attacks. The security framework satisfies the desired performance in terms of modularity, scalability, extendibility, and manageability and protects the smart grid against attacks from either Internet or internal network via integrating security agents, security switches and security managements. Metke et al. in [11] propose a security solution for smart grid utilising PKI along with trusted computing. The paper suggests automation tools be used to ease management of the different PKI components such as registration authorities (RA), certificate authorities (CA). A comprehensive survey

of smart grid security requirements and possible vulnerabilities and potential cyber attacks is provided in [20] and [22]. They also discuss existing security solutions to counter cyber attacks on the smart grid.

In spite of the rich set of publications and standardisation on smart grid security, no work has, to our best of knowledge, addressed security challenges associated with an ADN's islanded operation in the presence of a malicious insider. In addition to proposing state of the art security solutions to the well known security issues in an ADN automation system, we also propose a scheme that prevents outsider attackers and malicious insiders from installing a rogue field device by exploiting the emergency situation during islanding.

# 3. THREAT ANALYSIS

An appropriate security architecture for an active distribution network can be determined only after a thorough threat analysis of the network architecture, information flow and security of each of the infrastructure's components. Cyber attacks can happen anywhere in a distribution automation system including at field devices (sensing and actuating devices), communication infrastructure (routers, switches etc) and at the control and monitoring centre.

Although different techniques can be used to launch cyber attacks on any of these components, the ultimate goal of an attacker is either to initiate erroneous control actions or to prevent or delay required control actions, thereby disrupting the proper operations of the physical power system. Erroneous control actions can happen either due to compromised sensor data fed to the control centre or due to a malicious injection or modification of the control signal. Likewise, an inability to send timely control signals can happen either due to absence of timely sensor data or due to control signals being maliciously dropped or delayed in the network. In the following, we discuss different possible attack vectors that can be exploited by an attacker to realise the stated goals.

## 3.1 Unauthorized Access

Although most field devices are usually located in a relatively secure location, physical access by an adversary cannot be completely ruled out. Even if devices are physically inaccessible, an adversary can still manage to gain access to a device through the network unless there is a secure perimeter that prevents unauthorised access to the communication infrastructure.

An adversary who gains local or remote access to a field device can reconfigure it such that it behaves in an undesirable way. An adversary can, for example, configure a metering device, such as a PMU, to stream incorrect phasor data so that the controller will have incorrect situational awareness about the system. Moreover, an adversary can misconfigure an actuating device to perform inaccurate actions in response to commands from a controller.

## 3.2 Man-in-the-Middle Attacks

An adversary who intrudes in the communication channel of a distribution network can launch a man-in-the-middle attack by selectively dropping or modifying sensor data (control signals) sent from a field device (controller), thus compromising the availability and/or integrity of message exchanges. A replay attack is another form of the man-in-the-middle attack: an attacker sniffing the communication channel can copy measurement data or control commands and forward them later on. Replay attacks can have catastrophic consequences especially when applied to control signals.

Note that man-in-the-middle attacks on measurement data are effective mainly if the attack is persistent. This is because the system is a dynamic system, i.e., measurement data are continuously refreshed by a new set of measurements. Thus the effect of a single man-in-the-middle attack is negligible, especially for synchrophasor measurements that are refreshed several times per second. On the contrary, a single attack on control signals can be catastrophic.

## 3.3 Rogue Device Installation

A metering field device, such as PMU, comprises sensors that sample analogue signals from the power system and a computing component that converts the sampled analogue signals to digital data. An attacker who has physical access to a metering device can tamper with the sensor and replace it with a rogue sensor that provides incorrect signals to the computing part of the field device. Similar attacks also apply to actuators. An attacker can replace an actuator with a rogue one that incorrectly acknowledges it has performed a certain control action, whereas in reality it has not.

Implementing cryptographic solutions that ensure device authentication before any meaningful communication starts can prevent an attacker from installing a field device. However, attacks that involve physical tampering of only the analogue component of field devices are difficult to prevent. The best that can be done to prevent such attacks is to harden the physical protection of the devices. Bad-data detection techniques at the control centre can be employed to filter out bad measurements from rogue sensors. However, it has been shown that existing bad-data detection (BDD) techniques do not always detect all bad measurements. Liu et al. [10] have shown that an intelligent adversary with knowledge of the power system model can corrupt a carefully selected set of sensor data to introduce arbitrary errors in the estimates of certain state variables without triggering an alarm from the BDD. A wrong state estimator output can, for example, falsely indicate a significant voltage drop (hike) in a bus, triggering the utility to inject more (less) reactive power to the bus, which may in turn have a catastrophic effect on the stable operation of the grid [9].

## 3.4 Denial of Service (DoS) Attacks

An attacker who manages to gain access to the communication infrastructure, either remotely or locally, can launch a denial-of-service (DoS) attack by flooding a critical link with bogus traffic or by saturating the computing resources of a critical network device such as a router or metering field device. Such an attack causes real-time measurement data from field devices to be delayed or at worst dropped. As a result, a DNO will not have a complete view of the distribution network's status, leading to incorrect decision making. Likewise, the attack can also delay or drop critical control signals from a controller.

## 3.5 Malicious Software Patching

Smart grid devices, such as PMUs, run software and firmware that need to be updated in order to patch bugs, to fix security vulnerabilities or to add new features for better

usability or performance. Unless necessary authentication and integrity checks are performed during update, an attacker can use deceptive methods to install a malicious code (a malware) that masquerades as a legitimate software update. What is worse, a malicious insider (field engineer) can deliberately install compromised software update to field devices.

A malicious code (malware) can be used by an attacker to perform any kind of malicious activities. For example, it can be implemented as a "logic bomb" such that it runs in parallel to the legitimate code and sets off a malicious function when a specified condition is met. Stuxnet [5] is one such example of a sophisticated logic bomb believed to be designed to attack Iran's nuclear facilities by specifically targeting Programmable Logic Controllers (PLCs) made by Siemens.

# 4. SECURITY SOLUTIONS

The cyber threats discussed in the previous section are by no means exhaustive, but they serve to illustrate risks to help us develop a secure distribution network. The first step towards securing a distribution network is to separate the automation network from the enterprise network of a DNO and to maintain a secure perimeter around the automation network. A security perimeter is achieved by using a security gateway (a perimeter firewall) that provides a protective barrier from incoming (outgoing) traffic to (from) the automation network. Moreover, internal firewalls should also be used to provide more specific protection to certain parts of the automation network. All firewalls should be deployed with tightly configured rule bases such that the default policy is to "deny everything", and then open up only what is needed (maintain a white list). Figure 2 depicts a logical positioning of firewalls in a typical distribution automation network.

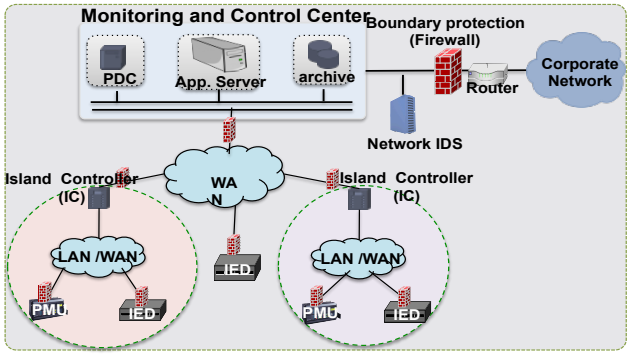


**Figure 2: Logical positioning of firewalls in a distribution automation network.**

Maintaining a secure perimeter and deploying firewalls is not sufficient to secure a distribution automation network for two reasons. First, security perimeters can fail, either due to misconfiguration or due to inherent weaknesses in the defense mechanism of the firewall. Second, a distribution network spans a large geographic area. Hence, it is impractical to define the perimeter as an attacker has a large attack space to physically connect to the distribution network and launch the attack from within the network.

Therefore, it is desirable to design a security framework that prevents attacks that emanate both from within the distribution network and from external networks. To address the security threats discussed in the previous section, we propose a set of security solutions and best practices discussed below.

## 4.1 Centralized User Authentication

Access to all devices and services should be limited only to authorised personnel. Each person authorised to access a device or a service has to have a separate user account and a secure password. All user accounts are centrally managed in a central authentication, authorisation, and accounting (AAA) server. All standard security policies such as role based access control, putting a limit on the number of unsuccessful access attempts, specifying password strength rules, etc should be enforced.

Creating and managing user accounts in a central server reduces the burden of creating and managing several accounts in each device for every authorised employee. A user's account can also be blocked from a single location when necessary. An employee's account can be blocked when he is no longer responsible for the tasks he was initially assigned to, when he leaves his job or when he is suspected as malicious based on a postmortem analysis of activity logs.

## 4.2 End-to-End Secure Delivery of Messages

Guaranteeing end-to-end security for message exchanges is essential for preventing man-in-the-middle attacks and for detecting messages from rogue devices. End-to-end security encompasses guaranteeing the confidentiality, integrity, source authenticity and freshness of measurements, control signals and other important message exchanges at all layers. Although confidentiality is not a critical requirement for measurement and control messages, a distribution network operator (DNO) may want to protect its sensor data's confidentiality in case such data contains information sensitive to the market that could be exploited by competitors.

Time-stamping, which is already part of existing SCADA communication protocols, is used to guarantee message freshness. For protocols that do not support time-stamping, sequence numbers can be used as an alternative. A systematic use of IPsec, TLS or other standard protocols can guarantee message source authenticity, integrity and confidentiality.

## 4.3 Scalable Key Management

Secure end-to-end communication depends on the existence of a secret key shared between communicating parties. Manual provisioning of such keys and updating them when necessary in a smart grid network, where there is a large number of communicating devices, can be unsafe and cumbersome. Therefore, it is crucial to design a secure and scalable key management scheme to generate, distribute and update the shared cryptographic keys. NISTIR 7628 [15], the foundation document for the architecture of the US Smart Grid, mentions key management as one of the most important research areas in smart grid security.

There is a general consensus in the smart grid research community that Public Key Infrastructure (PKI) is a viable solution as a key management scheme [3, 11]. For distribution automation systems, a DNO should support its own PKI architecture and be responsible for its devices' certificate management. Each communicating device in the distribution network is issued a digital certificate during installation by the DNO's certificate authority (CA). The exact

procedure of how a DNO's certificate authority issues a certificate to a device is described in Section 5.

Once devices are issued digital certificates, they authenticate each other's identities using standard protocols such as Transport Layer Security (TLS). Following the authentication phase, the communicating parties use a key agreement protocol such as Diffie-Hellman to derive a session key that is used to secure messages exchanged during the TLS session.

A device requires the public key of the DNO's certificate authority (trust anchor) to verify the other party's certificate. Therefore, devices have to store the root CA's public key in a secure location where an adversary cannot delete or modify it. Protecting such sensitive information using file system permissions can be bypassed. An alternative and more efficient solution to protecting sensitive information such as cryptographic keys is to use tamper-proof, special-purpose hardware tokens such as the Trusted Platform Module (TPM).

## 4.4 Secure Software Patching

Attacks that exploit software patches in order to inject malicious code (malware) can be thwarted by requiring a device to validate the authenticity and integrity of any software prior to installation. A DNO has to have its own *approval body* that approves and signs software patches from device manufacturers or third party developers. Whenever a device in the DNO's network installs a software patch, it has to first verify that the patch is signed by a DNO's approval body.

## 4.5 Tamper-resistant Credential Protection

Most field devices are deployed in remote geographic locations exposed to unauthorised physical access. Therefore, it is important to provide protection against unauthorised modification and disclosure of sensitive information, such as digital certificates and cryptographic keys, in these devices. An efficient solution to provide the required level of protection for keying materials within field devices is to use a FIPS140-validated tamper-resistant, special-purpose cryptographic module, such as Trusted Platform Module (TPM). A TPM is a secure crypto-processor that offers functionalities for secure generation and storage of cryptographic keys [6]. In addition to serving as tamper-proof storage to sensitive data like cryptographic keys and digital certificates, [11] discusses additional security benefits of using TPM for smart grid devices. Some of the benefits include secure software upgrade, high assurance booting, dynamic attestation of running software and device attestation.

## 4.6 Event Logging and Intrusion Detection

Even after the above security solutions are put in place, there can still be security incidents. Incidents could happen because an attacker installs a malware by exploiting zero-day vulnerabilities, which are inevitable in software. Incidents could also happen because of a field engineer's negligence to follow a DNO's security policy that prohibit the usage of removable media, such as USB, without a proper check for malware prior to use. Besides, disgruntled insiders can abuse their privileges to perform malicious operations.

To minimise the risks that result from such incidents, a DNO should implement automated intrusion-detection techniques to monitor events that occur in the network and to analyse them for signs of suspicious activities that violate the DNO's security policies and acceptable practices.

One type of intrusion detection is log-based intrusion detection system (LIDS) [17]. LIDS uses log data from network devices to detect suspicious activities in a device. This intrusion detection requires each device in the network to implement a secure logging mechanism that maintains a record of system events and user activities in the device. Log data must record noteworthy events such as user activity, program execution status, device configuration change, etc. Each log entry for an event must also contain detailed information about the event including identity of the user, time of the event, type of the event, etc.

LIDS should be implemented both at a device level and at a network level. For the network-level detection, devices send duplicates of their log entries to a centralised logging server. A postmortem analysis of the log files (at individual devices and at a central logging server) is used to reconstruct events and detect intrusions. The intrusion detection system can, for example, identify insiders engaged in suspicious activities and flag them as malicious.

Another type of intrusion detection is called network-based intrusion detection system (NIDS) [17]. NIDS monitors traffic directed towards critical components of the network to detect suspicious traffic patterns such as denial of service (DoS) attacks. The best location for a NIDS is to deploy it in the same location where a firewall is deployed. In general, distribution automation network traffic is more or less predictable and follows regular traffic patterns, compared to network traffic in enterprise systems. Therefore, a network-based intrusion detection for such systems can be very effective in detecting intrusions.

Note that intrusion detection should be combined with automated intrusion prevention systems (IPS) that send an alarm when intrusions are detected and are capable of taking automated prevention measures, such as resetting the connection and blocking traffic from offending IP address where such actions do not have catastrophic consequences on the grid's operations. Moreover, the operator must have proper incident response and disaster recovery procedures in place to be able to rapidly recover from any emergency (including a cyber attack) and to mitigate damage caused by such incidents.

# 5. SECURE BOOTSTRAPPING OF A FIELD DEVICE

This section focuses on secure initialisation and certification of a newly installed field device before it starts any meaningful communication. This initial stage of securely bootstrapping a field device is a precursor for the effective implementation of the end-to-end security and secure software patching solutions described in Section 4.

A secure device-installation scheme should guarantee that the device comes from one of the trusted manufacturers and that the installation is carried out by an authorised field engineer. In other words, the scheme should prevent a malicious outsider or an insider (field engineer), who is suspected as malicious after postmortem log data analysis, from installing a rogue field device. The installation scheme described below assumes that each field device comes with a certificate pre-provisioned by an accredited manufacturer's certificate authority. Furthermore, we assume that the DNO's controllers, certificate authority and Device Registry (described below) know the public keys of all accred-

ited manufacturers whose devices are installed in the DNO's network.

Our installation scheme puts full trust on an authorised field engineer to initialise a field device by securely loading the public key of the DNO's certificate authority and configuring some parameters such as disabling unnecessary ports and changing insecure default settings. An alternative to this would be for a DNO to have a safe central location where all field devices are received and securely initialised with the DNO's certificates and a field engineer is merely responsible for plugging the device into the network and setting some parameters. In this paper, the first option is chosen because we assume that a DNO might not always have pre-initialised devices that are readily available for use during emergency conditions. Thus we want to make it possible for a field engineer to be able to take uninitialised field devices (for example, borrow them from a neighbouring DNO or buy them from the closest vendor available) and securely install these devices to the network whenever required.

## 5.1 Device Installation During Normal Operations

In this subsection we describe the set of procedures required to securely install a field device in a distribution network when communication is possible from the installation location to the DNO's network management centre. The network management centre comprises among other components the AAA server, the DNO's certificate authority and the Device Registry, as depicted in Figure 3.

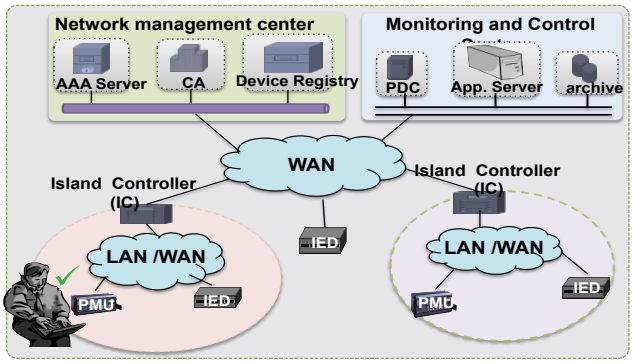


**Figure 3: An active distribution network's communication infrastructure and a network management module that facilitates secure communication.**

A successful secure installation of a field device entails execution of the following three steps before the device participates in any communicating session.

- A field engineer is authenticated by the central AAA server and obtains an authorisation token for installing the device into the network.
- An authorised field engineer registers the device as a member of the distribution network in a central database called Device Registry. This database contains a list of all devices in the network and a metadata of each device.
- The device is issued a certificate by the DNO's certificate authority. A certificate is issued only after the CA verifies that the device has a valid certificate from an accredited manufacturer and that the device is registered at the Device Registry by an authorised field engineer.

User authorisation for installing a device can be accomplished by utilising any token/ticket based standard authentication protocols such as Security Assertion Markup Language (SAML) or Kerberos. In this case we will use SAML to describe how the installation proceeds.

To install a device, an engineer performs the required initial configurations on the device and plugs it into the network. He then authenticates himself to the AAA server and is issued a SAML assertion (SAML security token) by the server. A SAML security token is an XML file that specifies whom it is issued to, what privileges the token holder has (registering a device as a member of the network). The token also contains information about its lifetime (validity period) and a digital signature signed by the token issuer (AAA server) in order to guarantee its integrity.

Once an engineer receives the security token, he initiates the device registration process. The registration proceeds only if the Device Registry verifies that the device comes from a trusted manufacturer and the engineer has the privilege of registering it. The Device Registry verifies the authenticity of the device by using the certificate issued by its manufacturer. The certificate is also used to initiate a secure session with the server. The engineer then sends the device's metadata along with the SAML security token to the Device Registry over the secure channel.

After a successful verification of the token's validity, the Device Registry assigns a unique ID to the device and creates a new entry for the device's metadata in its database. Note that a successful verification of the token guarantees the Device Registry that the engineer is trusted by the AAA server. The Device Registry then confirms a successful completion of the registration by sending back the unique ID to the device.

Upon receiving the unique device ID, the device again authenticates itself to the DNO's certificate authority (CA) and initiates a secure session by using the certificate issued by its manufacturer. A certificate request is then sent to the CA over the secure channel. The CA checks if there is an entry in the Device Registry database corresponding to the device ID that is received as part of the certificate request. If such an entry exists, the CA is convinced that the authenticated device requesting for a certificate is registered by a trusted field engineer. Therefore, the CA signs a new certificate and sends it back to the requesting device.

Now that the device has a certificate issued by the DNO's CA, it can authenticate itself to any communicating partner in the distribution network and initiate secure communication with them using standard protocols such as TLS or IPsec.

## 5.2 Device Installation During Emergency Conditions

When an island controller (IC) detects a widespread disturbance or power failure in the grid, the active distribution subnetwork within the controller's domain can automatically isolate itself from the grid and continue to operate as an island for an extended duration of time. It is possible that portions of the grid's communication infrastructure beyond the island's perimeter could be rendered unreachable as a result of the disturbance that caused the islanding. A sub-

network of a distribution communication infrastructure can also be isolated (islanded) due to a communication breakdown, irrespective of a power system failure. During such emergency situations, a DNO might want to replace some failed field devices within the islanded region. However, if the DNO's network management centre is unreachable from the island, the device installation procedure described above cannot be applied.

Therefore, it is important to design a secure device installation scheme to prevent an attacker from exploiting the emergency situation in order to install a rogue device in the island. In the following we discuss an out-of-band challenge-response-based user-authentication scheme to securely install a device within an island. The scheme utilises the island controller (IC) to serve as a proxy for the security operations required during device installation. For this we assume each island controller knows the public key of the AAA server and the public key of the CA's of all accredited manufacturers whose devices are installed in the network. Furthermore, we assume that each IC is sufficiently secure to be delegated as a subordinate certificate authority for issuing temporary certificates to devices installed within the island during the emergency situation.

With these assumptions, the installation of a device in an islanded network proceeds as follows. The engineer first configures the device and plugs it into the network. Then the device uses the manufacturer issued certificate to authenticate itself and to setup a secure session with the island controller (IC). The device's metadata is then sent to the IC over the secure channel. Before locally registering the device's metadata, the IC replies with a random challenge (nonce) to prove that an authorised engineer is registering the device.

Assuming there exists an out-of-band means of communication (for example, a mobile network) from the island to the network management centre, the engineer authenticates himself to the AAA server using his mobile phone and requests the server for an authorisation token by forwarding the random challenge. Depending on which privileges the engineer has, he receives a signature of the random challenge signed by the AAA server. This signature is sent to the controller as a proof that the engineer is trusted by the AAA server to register a device. The controller then verifies the signature and accepts the device as part of the network by registering its metadata until communication with the network management centre is restored.

If, for some reason, the engineer in the island has lost his password or is unable to login to the AAA server, he can still install the device with the help of any other engineer who is in a location where he can communicate both to the network management centre and to the island. The only purpose of the engineer in the island is to forward the random challenge to the second engineer and receive the signature from him to use it in order to finish the registration of the device (Figure 4). This way, the engineer in the island serves as a delegate to the authenticated engineer for registering the device. Note that the delegation is accomplished without revealing the authenticated user's password to the delegated engineer.

After the device is successfully registered, the island controller issues it with a new certificate. The device uses this certificate to authenticate and to securely communicate with other devices in the island. Other devices can verify the authenticity of the certificate by building a chain of trust starting from the device's certificate up to the root CA (trust anchor) of the DNO. Note that the signing key of the island controller is certified by the root CA and the public key of the root CA is preloaded to every device during installation.

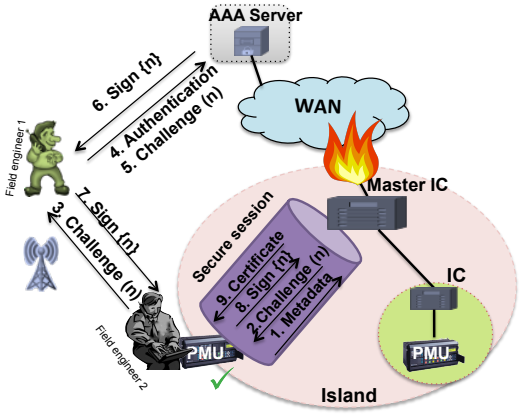


**Figure 4: Islanding - where a portion of an active distribution network is cut off from the rest of the main grid. A DNO securely installs new devices in the island in the presence of malicious outsiders or suspected insiders who would like to utilize the emergency situation to install rogue devices.**

The above description considers a single island controller per island. However, an island can be a superset of multiple islands with each member island having its own island controller. In such a situation, the different island controllers need to run a decision protocol among them to select a "master" controller which will be responsible for the tasks described above.

## 5.3 Back Synchronization of an Island

When the fault that caused islanding is cleared, the islanded facility synchronises back to the main grid [4]. The devices that are installed during an islanded operation are not recognised by the central Device Registry and do not yet have a certificate issued by the root certificate authority. The devices can still continue to communicate using the certificate issued to them by the island controller. However, building a chain of trust to verify such certificates can be complicated during another islanding incident. For example, assume a "master" controller issued a certificate to a device during a previous islanding. Furthermore, assume the device is now in another island that does not contain the previous "master" controller. If the device wants to securely communicate with another partner within the current island, the communicating partner will not be able to build the chain of trust for the device's certificate. To ease this complexity, we propose that each device be re-certified by the root CA, once the connection with the network management centre is restored. The re-certification can be automated as follows. First the IC forwards the temporarily stored metadata of these devices to the Device Registry over a secure channel. The Device Registry creates a new entry for each of these devices in its database. Following this, each such device auto-requests the CA for a certificate. The CA, upon successful verification of the existence of an entry for requesting the device in the Device Registry's database, issues a new certificate to it.

## 5.4 Securing Legacy Devices

The distribution automation network will contain not only new advanced field devices but also legacy devices, which do not have enough computational power or memory space to perform security functionalities. Communication with such legacy devices should be secured by installing a modern security device, also known as bump-in-the-wire (BITW) device, adjacent to them [21]. The BITW device is issued a digital certificate from the CA on behalf of the legacy device. All security operations on data sent from and received by the legacy device are performed in the BITW device. Note that data transfer between the legacy device and the BITW is not protected.

# 6. CONCLUSION

A smart grid's communication infrastructure is key to enabling a utility to collect and analyse data about current operating conditions of the grid and issue control signals as required. However, the critical nature of power grid makes its communication infrastructure a suitable target for cyber attacks. Therefore, implementing a comprehensive cyber security solution is necessary. In this paper we analysed different cyber security threats in a typical active distribution network and proposed security solutions and best practices to counter such threats. Our solution entails secure bootstrapping of field devices such that only an authorised personnel is able to install such devices and no malicious insider or outsider is able to install rogue field devices.

# 7. ACKNOWLEDGMENTS

This research has received funding from the NanoTera Swiss National Science Foundation project $S^3$-Grids. The authors alone are responsible for the content of this paper.

# 8. REFERENCES

[1] North American Electric Reliability Corporation. Critical Infrastructure Protection (CIP) Reliability Standards, 2009.

[2] F. Aloula, A.-A. A. R., R. Al-Dalkya, M. Al-Mardinia, and W. El-Hajjb. Smart grid security: Threats, vulnerabilities and solutions. *Intelnational Journal of Smart Grid and Clean Energy*, 1(1), 2012.

[3] T. Baumeister. Adapting pki for the smart grid. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 249 –254, Oct. 2011.

[4] A. Borghetti, C. Nucci, M. Paolone, G. Ciappi, and A. Solari. Synchronized phasors monitoring during the islanding maneuver of an active distribution network. *IEEE Transactions on Smart Grid*, 2(1):82 –91, March 2011.

[5] T. Chen and S. Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.

[6] D. Grawrock. *Dynamics of a Trusted Platform: A Building Block Approach*. Intel Press, 2009.

[7] J. Hull, H. Khurana, T. Markham, and K. Staggs. Staying in control: Cybersecurity and the modern electric grid. *Power and Energy Magazine, IEEE*, 10(1):41–48, 2012.

[8] H. Laaksonen and K. Kauhaniemi. Synchronized re-connection of island operated lv microgrid back to utility grid. In *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, pages 1–8, 2010.

[9] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici. Intruders in the grid. *IEEE Power and Energy Magazine*, 10(1):58–66, 2012.

[10] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14(1):13:1 –13:33, June 2011.

[11] A. Metke and R. Ekl. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1(1):99 –107, june 2010.

[12] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[13] NIST. Discussion Draft of the Preliminary Cybersecurity Framework. `http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf`, Aug. 2013.

[14] IEC TC57. IEC 62351 - Power systems management and associated information exchange - Data and communications security, 2013.

[15] NISTIR 7628. Guidelines for Smart Grid Cyber Security. `http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf`, Sept 2010.

[16] Ralph Langner. The RIPE Framework: A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security. `http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf`, Sept. 2013.

[17] Sunil Gupta. Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment. SANS Institute Reading Room, Jul. 2012.

[18] S. Sridhar, A. Hahn, and M. Govindarasu. Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012.

[19] E. Wang, Y. Ye, X. Xu, S. Yiu, L. C. K. Hui, and K. Chow. Security issues and challenges for cyber physical system. In *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Cyber, Physical and Social Computing (CPSCom)*, pages 733–738, 2010.

[20] W. Wang and Z. Lu. Survey cyber security in the smart grid: Survey and challenges. *Comput. Netw.*, 57(5):1344 – 1371, Apr 2013.

[21] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid*, 2(4):782–795, 2011.

[22] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys Tutorials*, 14(4):998 –1010, 2012.

[23] Q. Yang, J. Barria, and T. Green. Communication infrastructures for distributed control of power distribution networks. *IEEE Transactions on Industrial Informatics*, 7(2):316–327, 2011.