TGN Energy

System Security

TGN Grid

Contents

1 Introduction

A TGN Grid is a local power grid, limited to one or a select few grid access points, with a TGN FlexControl to regulate power flow. Power flow can be controlled to optimize cost reductions and profitability, energy security and power quality, or grid support. Combinations of these are also possible.

As energy is a vital precondition for life and a functional property, security is considered paramount in a TGN Grid. To this end, the system is designed to ensure the continued operation and minimized exposure cross section. This is especially important for implementations of a TGN Grid in cases of critical infrastructure.

This document aims to provide an overview of the security aspects built into a TGN Grid and its constituent systems. It also outlines security recommendations for added security in cases of critical infrastructure implementation.

2 Communication

Communication security is paramount in an energy control scheme and the TGN Grid is designed with communication security as a central axiom.

2.1 Local communication

2.1.1 Communication protocols

TGN FlexControl, the control core of the TGN Grid, is able to communicate with virtually any communications protocol. The preferred mode of communication is by means of MODBUS TCP/IP as it offers the highest degree of flexibility. Regardless of industrial communications protocol, however, these lines of communication are all non-encrypted. As they are non-remote and require physical access to compromise, they are considered secured by physical access restrictions.

2.1.2 Modes of communication

All wireless control communication between grid equipment is avoided due to the inherent security and data quality challenges. All communication is conducted though wired connections, most commonly through cat6e network cable.

2.2 Long distance site communication

A TGN Grid can span a large physical area and include whole industrial complexes. These can have several forms of energy storage and energy generators spread over a large area, and thus a secure form of communication is required on-site.

For communication between peripheral systems communicating on TCP/IP form, existing internet connections can be utilized. For other communications protocols, dedicated lines are required. For more sensitive installations, however, a dedicated network is employed, either as a dedicated ethernet network or a fibre optic network, depending on distances. This also allows for non-TCP/IP based protocols to communicate over large distances without the need for dedicated lines. Serial communication protocols like RS232 and RS485 can thus be utilized over large distances securely.

2.3 Global communication

In order for the full range of system operations to be available, a TGN Grid must have access to the internet. This is a prerequisite for ancillary service trading, arbitrage, cost optimizations and other operations that require non-local information.

Each piece of information attained from sources other than local resource, are assumed to be compromised and of a malicious nature. Therefore, each operation taken based on such information is evaluated in relation to any potential harm it can cause to the TGN Grid and its continued operation before it is acted upon in any manner.

2.3.1 Modes of communication

Hardline

Any modern hardline capable of communication bandwidths of 5 Mbit or more is sufficient to ensure proper internet communication.

LTE/4G/5G

The TGN Grid can be equipped with a dedicated wireless router which can be set as the primary means of communication in the event there is no available hardline or as a communication backup. This allows for a high degree of flexibility and system redundance to ensure continuous operation.

2.3.2 Communication across international borders

All non-local communication is assumed to occur across international borders. Therefore, all communication is encrypted and utilizes a VPN connection with end-to-end encryption in order to ensure information integrity.

3 Access limitation

3.1 Remote access limitation

The TGN Grid is connected to the internet via the TGN FlexControl in order to facilitate intelligent energy optimization and trading in ancillary markets. This necessitates a high degree of access limitation through encryptions and systematized limitations in digital access.

3.1.1 TGN FlexControl

TGN FlexControl sends and receives data via an end-to-end encrypted VPN tunnel. This allows for secure communication with the cloud service provider where all information can be verified behind high security firewalls and encryptions to ensure communication safety. Remote access to TGN FlexControl is possible only through TGN Energy and special access keys used for remote maintenance.

3.1.2 TGN Aggregate

TGN Aggregate receives updated information from the TGN FlexControl from each site. This is a one-way communication that allows the user to get an overview of the status, earnings, and trends from each site as well as the collection.

All communication is encrypted and access to TGN Aggregate requires multi-factor authentication (MFA) in order to ensure privacy and data security.

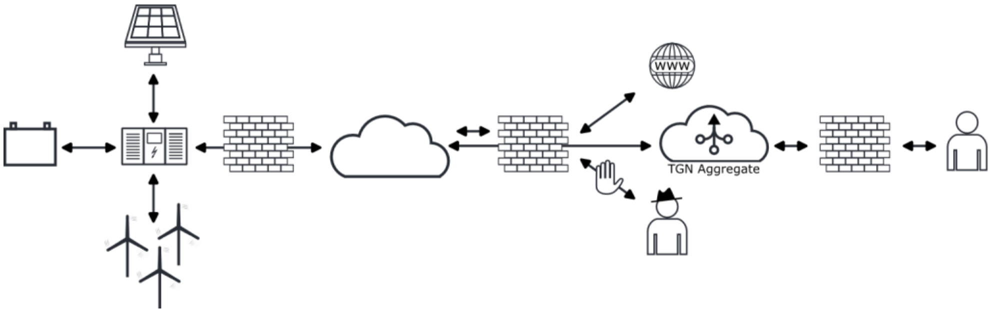


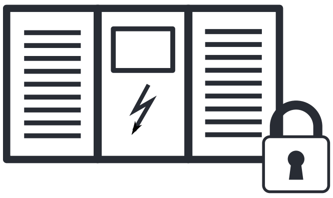
Figure 3.1: Schematic topology of remote access limitations in a TGN Grid. Malicious actor indicated by black hat.

3.2 Physical access limitation

3.2.1 TGN FlexControl

It is a truism in cyber security that physical access to a computer or data storage device will negate practically all digital defences. Therefore, it is imperative that the central computing and logging equipment contained within the TGN FlexControl is protected from physical intrusion.

The TGN FlexControl is comprised of a physical control cabinet containing the controllers, logging equipment, communications hardware and connections to peripheral equipment and sensors. This is assumed placed indoors, in a room with traditional physical access restriction. The cabinet itself provides a second level of physical access restriction, by means of a key-lock door.



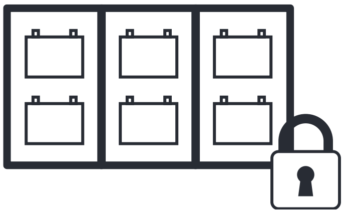
3.2.2 ESS/BESS

Any energy storage system (ESS) will have to restrict physical access in order to properly be protected from misuse, sabotage, and accidents. TGN Energy delivers battery energy storage systems (BESS) in two configurations: Free standing cabinet clusters or completely containerized solutions.

Free standing systems

Free standing systems generally have the equipment accessible to the level of battery cabinets, hydrogen gas reservoirs, inverters, etc. This necessitates that each such component is individually secured. In the case of BESS, each battery cabinet is individually locked.

In addition, TGN Energy recommends that access to such sites be restricted though fencing or other forms of entry denial.



Containerized systems

Containerized BESS systems contain batteries in locked cabinets, encapsulated transformer, and a locked TGN FlexControl cabinet. In addition, the entire container is access restricted through locked container doors, either by padlock or digital access lock.

3.2.3 Other

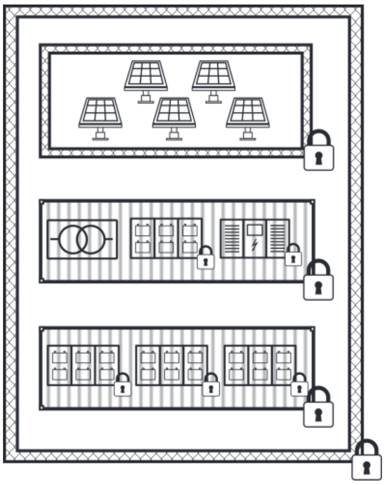
Energy production systems with site-distributed inverters and generators will require physical access restriction to be secured. Communication with TGN FlexControl at the heart of the TGN Grid is recommended take place via dedicated fibreoptic network. In cases where this is not feasible, communication via traditional local area network (LAN) is possible.

4 Critical infrastructure

Power systems are not seldom considered critical infrastructure and may be part of other types of critical infrastructure. Bridges, ports, airports, hospitals, and water pumping stations are all examples of critical infrastructure where the power system is a vital function. In such locations, more stringent security measures have to be taken to ensure their continued operation. TGN Energy has therefore composed a set of recommendations for how the power system may be further secured.

4.1 Physical access

Critical infrastructure should in all cases have strict entry restrictions, especially to sensitive areas. Even if the critical facility is a hospital or a school, some areas will have to be restricted. Power grid infrastructure should be one such area. The bear minimum should be restricted access to the room or building housing the more sensitive equipment, such as inverters and control equipment like the TGN FlexControl.



Ideally, the facility should restrict access as well as have a secondary layer of access restriction in the form of access to a room or building that houses the power grid equipment. Digital access with access logs and surveillance is recommended mixed with physical keys to prevent remote access overrides and digital entry attacks.

4.2 Communication security

4.2.1 Dedicated intranet

A smart power grid implemented in a critical infrastructure site, may contain several subsystems. Solar PV arrays, wind power, energy storage through batteries and/or other devices, electric car chargers, and so on. In order to properly protect the power systems from remote access by a malicious actor, all power system communication must be air-gaped from the general internet.

A separate network may be used for internet access, such as a traditional wi-fi, so long as there is no wi-fi capabilities in any of the power system components. Any person working on the site may then utilize the internet as usual through handheld devices and laptop computers without risking malicious access to the power systems.

4.2.2 Communication redundancy

In cases where it is vital for the user to communicate with the TGN Grid and communication failure must be minimized, TGN FlexControl can be set up such that the communication defaults to a secondary communication uplink should the primary fail. This can be done with any relatively low latency uplink such as LTE/4G/5G. In some cases, where mobile service is minimal, it can be set up via satellite uplink such as Starlink from Space X.

4.3 Control system security

4.3.1 Independent control system

A TGN Grid can be set up in a manner that allows for it operate without any access to external data but act solely on the status and characteristics of the power supplied to the premisses. This protects the system from outside malicious actors to feed the system false information in order to have it act on faulty data and potentially break the system's ability to operate. This can be done in two ways: Strict data independence or a hybrid of data independence and data integration.

Strict independence
The most sensitive of our critical infrastructure may have significantly higher interest in power quality and supply security than in economic benefits. In such cases, strict security measures should be in place to ensure the integrity and operability of the infrastructure.

In such cases, the TGN Grid can be set to operate solely on internally sourced data and the connection to the internet can be omitted.

Hybrid independence and integration
Some infrastructure may necessitate trading and financial optimization of the power consumption in order to finance the system and allow for a generally elevated power security. In such cases it is possible to employ a hybrid solution where the system defaults to a strict independence if the data input fall outside certain parameters. Such parameters will be dependent on the site in question and will likely be restricted information.

Including external data in such a system involves carefully curated data exchange protocols. By integrating external data in this way, the system can selectively integrate external data without compromising its core functions or security posture.

The hybrid solution would allow for a balance of financing and security in situations where it's necessary to balance the benefits of data integration with the imperative of maintaining system independence and security.

4.3.2 Control system redundancy

For some installations, it may be absolutely vital that the system operates at all times. Even if the TGN FlexControl is a highly reliable piece of equipment, nothing is infallible. When the requirements dictate that there be no downtime, a secondary FlexControl can be installed to act as a control redundancy. Depending on system complexity, this can be a fully equipped FlexControl or it can be a scaled down variant with only the most vital control capabilities. This saves significant cost but reduces the capabilities of the redundancy control system.

5 Software robustness

5.1 Data backup and disaster recovery

All data logging occurs on a cloud server equipped with redundant systems and backup protocols, ensuring the recreation of any lost data due to hacking attempts or system failures.

5.2 User security

5.2.1 Role based credentials

Each user is given access only to the sections of the software that the user needs to perform the required duties. This need-to-access policy prevents untrained or irrelevant users from accessing information that may be regarded as sensitive in nature.

5.2.2 Activity logging

Comprehensive activity logging enables the tracking and detection of errors and malicious operations, enhancing transparency for auditing purposes. Communication activity involving TGN FlexControl, the cloud service provider (CSP), and TGN Aggregate is meticulously logged and securely backed up by the CSP.

5.2.3 Regular auditing

The system periodically checks for active users and reports on user activity. This highlights the activity within the system as well as any authorizations that ought to be removed. This report is sent to the specified system administrator.

5.3 Authenticated reporting

TGN Aggregate offers the functionality to dispatch system reports to the leadership of system owners or central authorities. These reports can be configured as recurrent standardized deliveries, featuring digital signing for data source verification, and establishing accountability. This feature proves particularly essential for public organizations and larger corporations.

5.4 Continuous monitoring and alerting:

Continuous monitoring of system health and performance parameters allows for early detection of anomalies or deviations from normal operation. Automated alerting mechanisms promptly notify administrators of potential issues, enabling proactive troubleshooting and resolution before they escalate into critical problems.

5.4.1 Software parametrisation

In order to prevent erroneous data to corrupt the operations of the system, data parameters is employed that disallow settings or commands to devices that may be damaged by extreme value settings. This is the case for both data that is retrieved from external sources, and data from sensors and other operational technology (OT) devices.

IT parametrization

External data is retrieved from API sources and fed through the CSP via the VPN tunnel to TGN Grid. This data is filtered for reliability and all anomalous datapoints are logged and reported. Anomalous data is disregarded until checked by an administrator and verified.

OT parametrization

Every input from peripheral devices is filtered for data reliability. All anomalous datapoints are logged and reported. Anomalous data is disregarded until checked by an administrator and verified.

Implementation parametrization

Filtered data from IT and OT is married in the implementation stage. Prior to implementation, however, action signals to equipment and outbound communication is again filtered to account for possible side effects of accepted data combining to unacceptable outputs.

5.5 Automated self-healing:

TGN FlexControl features automated self-healing capabilities that can identify and remediate common issues without human intervention. Through intelligent algorithms and predictive analytics, the system can proactively address potential problems, optimizing uptime and minimizing service disruptions.

5.6 IT-OT separation

Internet technology (IT) and operational technology (OT) are two sides of automation that have to cooperate seamlessly in order for a complex system to function properly. From a security standpoint, however, the two networks have to be protected from one another. Therefore, the implementation of OT will be on a separate network from the IT network. In less critical implementations this can be attained through virtualization, whereas for high security systems it is imperative that the two systems are physically separated.

The two systems meet at the TGN FlexControl where parametrization and other security features ensure the data reliability and keep the signals entirely separate.