genua.

A Fast Response Center for the Energy Transition

The availability of energy technology equipment is becoming increasingly important for the energy industry. That's why operators and service providers have been working with remote maintenance for years. However, due to the increasing complexity of networks and the increasing threat of cyberattacks, the security of such systems is increasingly coming into focus. The example of Hitachi Energy's Grid Automation Service shows how remote maintenance can be operated safely and efficiently: Between 80 and 100 support cases are processed there per month, many of them with remote access.

SECURE REMOTE MAINTENANCE

Frank Jablonski, journalist

SecurITy made in Germany

It is perhaps the first time since industrialization that an essential pillar of the economy in Germany has changed as dramatically as the energy landscape is currently doing. Several parallel drivers are accelerating the change: From the phase-out of nuclear energy, to the gas shortage at the beginning of the Russian war of aggression on Ukraine, to climate change, these events are leading to unprecedented growth in decentralized energy sources and new, decentralized distribution grids. And with them, the demands on electricity producers, grid operators and suppliers are growing.

Project Description

The Customer:

Hitachi Energy, headquartered in Switzerland, plans and realises high-voltage direct current transmission systems, substations, transformer stations and numerous other energy supply systems.

The Task:

Support for Hitachi customers worldwide who require support for alarms and malfunctions or machine monitoring, remote diagnostics or remote access scenarios.

The Solution:

genubox secures remote access to the customer's systems and allows the user complete connection control into his network.

A Technology Leader in the Energy Industry is Hitachi Energy

Headquartered in Switzerland, the company employs around 45,000 people in 90 countries and generates business volumes of around $13 billion USD.

Customers in the energy, industrial and infrastructure sectors all face the same challenge: to drive the energy transition towards a climate-neutral future in an increasingly complex world without losing track. This can only be achieved with intelligent concepts, embedded in a secure, largely automated and digitized structure.

“We are further developing our customers’ energy systems to make them more sustainable, flexible and secure, while at the same time aligning them with economic, ecological and social values,” says Michael Joos. He is head of the Collaborative Operations Center, or COC for short, in Baden in Switzerland. “Automation and flexibility are particularly important at our Grid Automation business unit. One aspect is becoming increasingly important for our customers: the availability of the systems and networks,” adds Joos.

To maximize this, Hitachi Energy’s Grid Automation Service focuses on six performance areas:

- Intelligent spare parts supply and supply
- Software and firmware support
- Tailor-made training
- Tools and know-how for preventive maintenance
- Cybersecurity solutions and
- Fast and flexible support in the event of service.

Energy supply facilities are part of the critical infrastructure. Hitachi Energy relies on genua’s genubox technology for remote maintenance access within its Grid Automation Services.

More than 40 engineering and service centers are strategically located around the globe to address these issues and keep the automation and communication systems of users from more than 140 countries running. Equipment and system training ensures that operating personnel can respond quickly and efficiently. Where this is not enough, Joos and his colleagues identify and analyze the causes of equipment failures and propose effective measures. They advise on spare parts, upgrades and retrofits, as well as cybersecurity issues.

Short Response Times Required

Time is money. Every user has this saying in the back of their minds when things get stuck in the system. At the heart of rapid troubleshooting and root cause analysis is the Customer Connect Center system, in which each customer is routed to the right advisor. Dragan Klisaric, Global COC Manager and thus responsible for all Collaborative Operations Centers worldwide, describes the structure: “Comparable to our COC here in Baden, there are six other centers that are located in the different time zones in such a way that our experts are available around the clock. In the support network, everyone works together, we exchange know-how with each other and work together according to the follow-the-sun concept.”

Many customers, especially those in critical infrastructure, use service level agreements that define very fast response times. Depending on the contract, this can be one or two hours, up to a first response of 15 minutes. “In order to achieve such response times, various conditions must be met. First of all, we work together with the local units. You already know the systems very well and do not have to spend a lot of time familiarizing yourself with them. When a customer calls us, we don‘t have to look up what they might have bought from us. Instead, we know exactly who is on the other side, what their system is and where the problems could lie,” says Klisaric.

> “We used to stand in the control room to get to the networks. Today, everything is recorded digitally and access is done via the Internet with the help of intelligent security solutions such as genubox.”
>
> Michael Joos, Chef des Collaborative Operations Center, Hitachi Energy

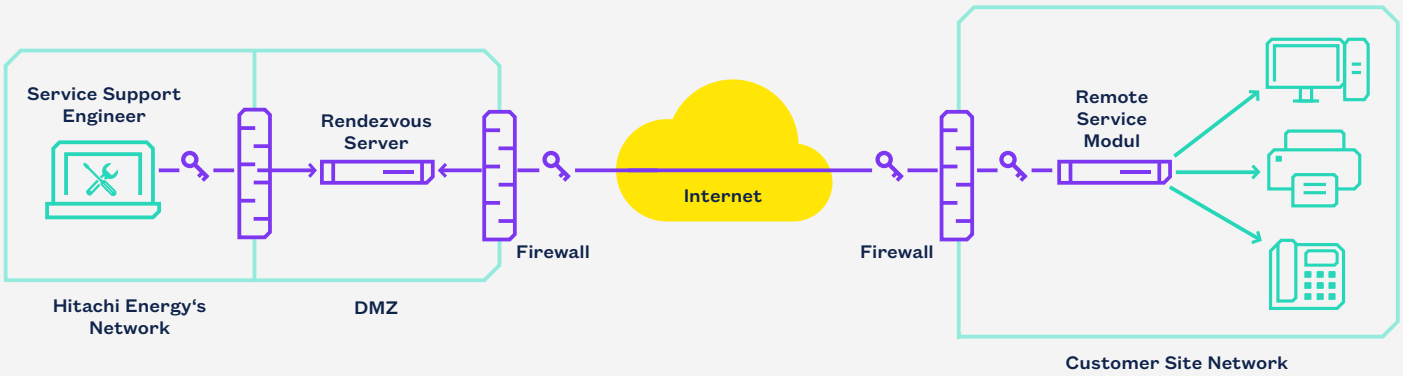
The View into the Complex

In order to be able to help users quickly in the event of an emergency, the engineers and technicians in support depend on getting information very quickly. What does it look like in the system, what alarms are there, how loud events in logbooks, can information be downloaded quickly, log files, fault recorder entries – these are typical questions that used to have to be clarified by phone and e-mail. “Fortunately, those days are over,” says Joos, adding: “The crucial thing is that we now have a secure way to access the customer system directly. Our service level agreements define who can access, when can be accessed, which systems can be accessed. Our partner genua ensures that the whole thing runs safely with the genubox.”

The subsidiary of the German Bundesdruckerei Group is an IT security company and expert when it comes to protecting complex and critical digital infrastructures. In addition to consulting and software applications, it is also special hardware that can be used to securely implement remote access to systems.

“genubox is the answer to our customers‘ legitimate security questions,” says Joos. “It solves our challenges in terms of remote engineering, cybersecurity, remote asset access, or connection to the Internet. We use it as a service box and as a platform for different functionalities.”

If all maintenance connections run through genubox, the system is safe and users retain full control. Access from the outside is carried out on a port- or application-specific basis to the target system, which is isolated from the rest of the system. Dedicated rendezvous points are available. They are located, for example, in the cloud or in the so-called demilitarized zone. These are computers that lie between two networks and separate them from each other by strict access rules.



Remote maintenance at Hitachi Energy: Without the genua solution, secure external access to the customer systems would not be possible. Between 80 and 100 support cases are processed each month – around 5 % of them remotely.

All Accesses Always at a Glance

Nevertheless: “When talking to customers, the question arises again and again: Is this safe enough? Even in cases where we have been able to convince our partners that the system is secure and that there are significant benefits, uncertainty often remains. This goes so far that plant access is limited to individual Hitachi Energy colleagues, otherwise no one is allowed to enter the plant remotely,” says Joos. Here, too, the software and authentication logic used offers a solution: Common identity and access management systems can be connected and thus users and their rights can be managed easily and centrally.

In addition to connection control, monitoring is helpful for very sensitive areas: With the help of genubox, users can follow all maintenance work live via the user interface and create video recordings for revision-optimized documentation. This means that the maintenance action, access time, destination and accessing instance are monitored in real time and documented at all times.

“We are very satisfied with the genua technology and the cooperation with our colleagues. By using it, we ensure to our customers that remote access is only provided by authorized personnel and can show a rapid response that deserves the name ‚rapid response‘,” says Klisaric.

With the help of genubox, Hitachi Energy‘s Grid Automation business unit can tailor its service agreements to the needs of its customers. In emergencies or planned business interruptions, repairs are carried out quickly so that the affected system can quickly take its place in the power grid and the energy transition.

“It’s not just service that we stand for, we are also driven by the topic of sustainability.”

Dragan Klisaric, Global COC Manager,
Hitachi Energy

Secure Remote Maintenance – IT-Security made in Germany

Different Scenarios Possible

genubox combines remote access, VPN access and firewalling. The solution is centrally manageable and allows the user to have complete connection control to their network. The basic module secures the essential types of access with its basic cryptographic functions. The application module as an application platform optimizes secure system access with the help of individual settings. This enables scenarios of machine monitoring, remote diagnostics or remote access. Complex tunnels for application service providing such as preventive maintenance systems are also conceivable. Measured values and status information can be recorded, encrypted and sent to the maintenance service provider at certain intervals.

Further Information:

www.genua.eu/genubox

0325-03-E

About genua

genua GmbH secures sensitive IT networks in the public and enterprise sectors, at KRITIS organizations and in the classified industry with highly secure and scalable cyber security solutions. The company focuses on comprehensive network protection and internal network security for IT and OT. The range of solutions includes firewalls and gateways, VPNs, remote maintenance systems, internal network security, and cloud security through to remote access solutions for mobile working.

genua GmbH is a company of the Bundesdruckerei Group. With more than 400 employees, it develops and produces IT security solutions exclusively in Germany. Since the founding of the company in 1992, regular certifications and approvals from the German Federal Office for Information Security (BSI) provide proof of the high security and quality standards of the products. Customers include, among others, Arvato Systems, BMW, the German Armed Services, THW as well as the Würth Group.

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim, Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu