

# Secure Remote Access to Safety Systems

Process Safety Congress, Dordrecht, NL

Alexander Horch

VP R&D

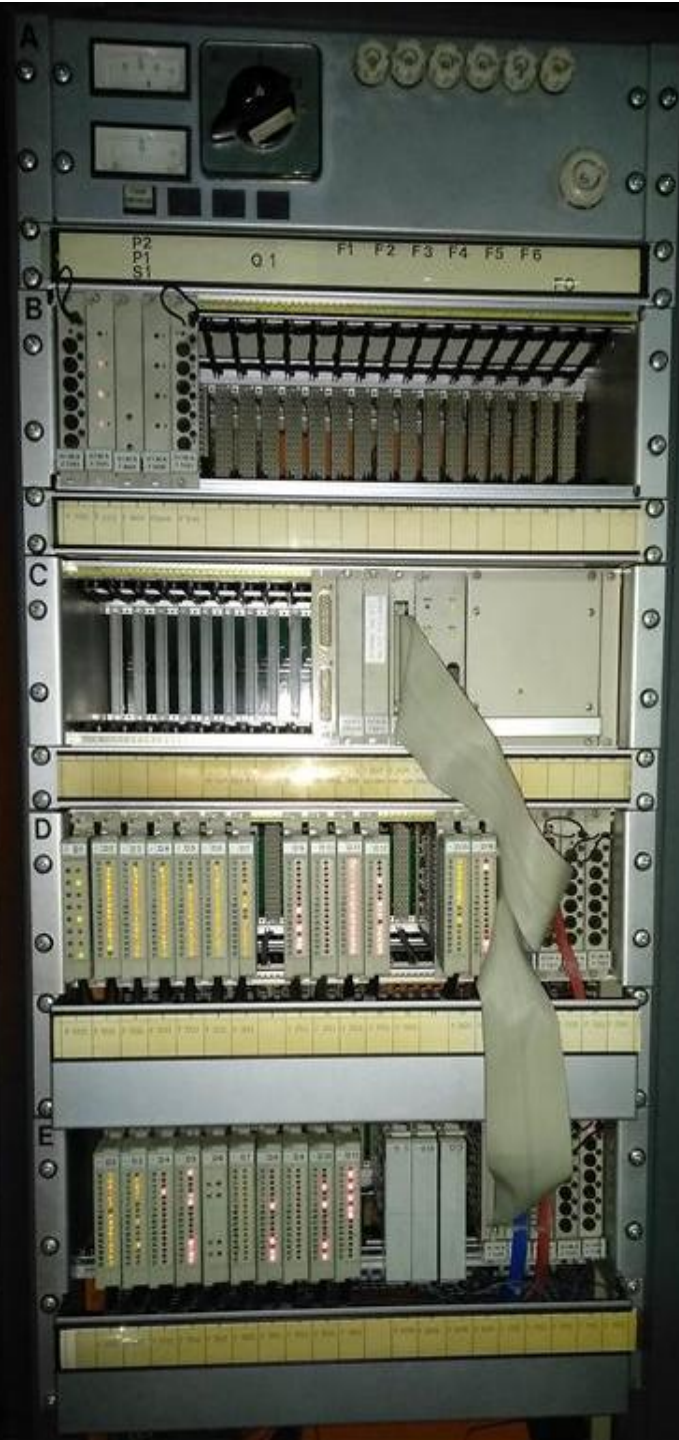
HIMA Group



SMART  
SAFETY.









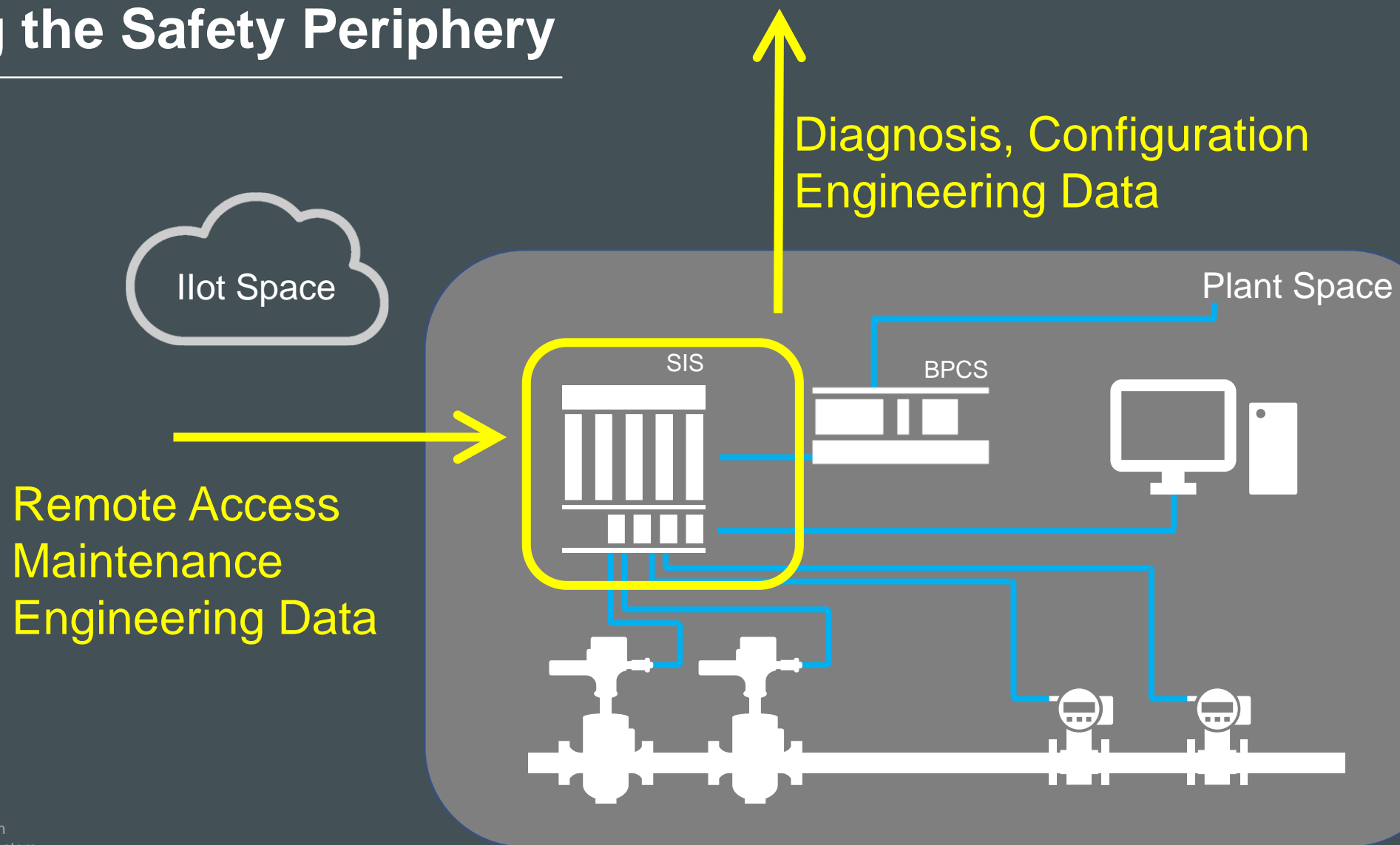
# How to secure a system that knows nothing about security



- HIMA H50 – System, still in operation since ~1986!
- Cyber Security for Control Systems and Safety Systems means securing systems that are in operation for decades!
- It is unrealistic to believe that 500.000 – 1.000.000 safety systems will be upgraded to 2021 state-of-the-art technology only because of security concerns.
- Many of those systems are islands. This is not true any more for more modern control systems.



# Securing the Safety Periphery



SIS – Safety Instrumented System  
BPCS – Basic Process Control System



# Challenges of Industrial Remote Solutions



Steady increase in digitization and networking of products/services



Shorten downtimes, reduce cost



Changing threat situation, increased security requirements



Effective, global use of resources / ageing workforce / shortage of experts



Regulatory requirements



# Challenge #1: Access to Critical Systems



Systems classified as critical are important for the maintenance of public order and basic services (electricity, water, transportation etc.)

This also includes large parts of the process industry


- Oil and gas production
- Chemical industry and subsequent industries



# Challenge #2: Threats & Countermeasures

## Industrial Control System Security (ICS) Top 10 Threats and Countermeasures 2019

Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	→
Intrusion via Remote Access	→
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	→

 Federal Office  
for Information Security

RECOMMENDATION: Secure use of IT IN PRODUCTION

Remote maintenance in industrial environments

Systems for process control, production and automation, subsumed under the term "industrial control systems" (ICS), are meanwhile exposed to the same threats as conventional IT systems. Due to operational or economic reasons, it is often required to be able to perform remote maintenance of the systems via public networks. Remote maintenance accesses designed in such a way mean that industrial systems are exposed much more and thus at the same time lead to an increased threat situation. Today, industrial remote maintenance components must therefore reach an adequate security level.

The range of available solutions on the market for remote maintenance in the industrial environment is very wide. The offers range from VPN solutions via cloud-based approaches to provider solutions in the field of machine-to-machine (M2M). There are significant differences between the product features of individual solutions. This recommendation provides an overview of the generic requirements for industrial remote maintenance according to the state of the art. It is explicitly pointed out that established solutions on the basis of analogue or ISDN modems as well as the direct Internet connection of components such as programmable logic controllers (PLCs) do not comply with the state of the art.

1 Architecture

The following requirements should already be taken into consideration when planning and integrating a remote maintenance solution:

- ✓ Consistent solution: Especially in larger infrastructures, a consistent solution should preferably be used. This reduces both the number of attack vectors and the complexity (no "uncontrolled growth").
- ✓ DMZ: The remote maintenance component should preferably be in a separate zone (DMZ) and not localised directly in the production network. Remote maintenance accesses must not lead to existing firewalls being bypassed. Rather, firewalls are suitable to define, for example, allowed IP address ranges for remote maintenance.
- ✓ Granularity of the communication connections: The remote maintenance access should preferably not be performed generally per (sub)network, but rather it should be possible to control remote maintenance access per IP and port in a fine-grained manner. This minimises the "range" of remote maintenance accesses and thus also limits the consequence of compromising. One possible approach is for example to establish 1:1 connections by means of SSH instead of coupling entire networks by means of IPsec.
- ✓ Connection establishment: remote access should, if possible, only be initiated from the company (outbound). There should be no open ports for establishing a connection from outside. As an alternative, remote maintenance accesses can be activated temporarily. This requires adequately secure authentication and an up-to-date patch level as well as organisational processes to ensure subsequent deactivation.
- ✓ Dedicated systems: The components used for remote maintenance should only be used for this application purpose and not be mixed with other functionalities.

BSI publications on cyber security

BSI-CS 108 | Version 1.00 - 12/01/2015

Page 1 of 3

[https://www.bsi.bund.de/EN/Topics/Industry\\_CII/ICS/recommendations/ICS-Operators/recommendations-operators\\_node.html](https://www.bsi.bund.de/EN/Topics/Industry_CII/ICS/recommendations/ICS-Operators/recommendations-operators_node.html)



# Challenge #3: Supplier Warranty Cases



- High hurdles for the end user in supplier requirements for warranty claims.
- A lot of suppliers with various good solutions create complexity that could lead to high failure rate and increasing risk.

This contradicts the basic principle of K-I-S-S -> Keep it simple, stupid



# How to design remote access solutions

- Architecture
- Secure communication
- Authentication mechanisms
- Organizational requirements
- Others (e.g. Scalability)



Federal Office  
for Information Security

## RECOMMENDATION: Secure use of IT IN PRODUCTION

### Remote maintenance in industrial environments

Systems for process control, production and automation, subsumed under the term “industrial control systems” (ICS), are meanwhile exposed to the same threats as conventional IT systems. Due to operational or economic reasons, it is often required to be able to perform remote maintenance of the systems via public networks. Remote maintenance accesses designed in such a way mean that industrial systems are exposed much more and thus at the same time lead to an increased threat situation. Today, industrial remote maintenance components must therefore reach an adequate security level.

The range of available solutions on the market for remote maintenance in the industrial environment is very wide. The offers range from VPN solutions via cloud-based approaches to provider solutions in the field of machine-to-machine (M2M). There are significant differences between the product features of individual solutions. This recommendation provides an overview of the generic requirements for industrial remote maintenance according to the state of the art. It is explicitly pointed out that established solutions on the basis of analogue or ISDN modems as well as the direct Internet connection of components such as programmable logic controllers (PLCs) do not comply with the state of the art.

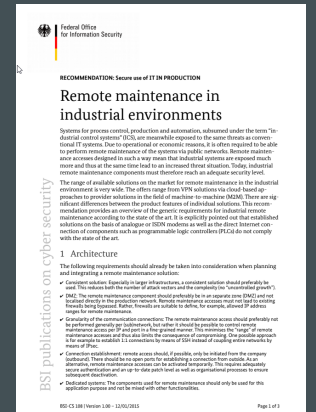
(BSI-CS 108, Recommendation by German BSI, Federal Office for Information Security)



# Remote Access for Industrial Environments



BSI recommendation	genua/HIMA Solution
<b>Architecture</b>	
Uniform solution (no "uncontrolled growth")	All remote maintenance cases can be covered uniformly as well as central management solution
Remote maintenance components in the DMZ	Dedicated server as central remote maintenance gateway in the DMZ
Connections not per (sub)network but fine-granular per IP and port	Remote maintenance relationship always per IP and port
Connection setup from inside to outside, no open ports	Machine operator controls remote maintenance channel (four-eyes principle)
Dedicated systems for remote maintenance	Dedicated system: Remote maintenance appliance genubox



(BSI-CS 108, Recommendation by German BSI, Federal Office for Information Security)



# Best of Breed: Safety & Security

German companies HIMA and genua forge strategic partnership for security.



Pioneer and technology leader in  
**Functional Safety** since >50 years.  
Focus: Safety Automation Systems



Pioneer and technology leader in  
**Cybersecurity** since >25 years.  
Focus: Automation Networks, Security Zones



Secure the safety automation networks and offer a comprehensive portfolio

- Encryption / Decryption devices
- Data diodes
- ...
- Remote access
- Firewalls



# Securing the Safety Periphery and Security Services



## High Resistance Firewall:

Firewall solutions of the highest quality for secure zone separation according to Common Criteria (CC) EAL 4+

## Secure Engineering Station:

Secure Windows environment incl. monitoring, hardening, encapsulation and controlled data transfer

## Encryption:

Secure data exchange through the establishment of Virtual Private Networks (VPN)

## Remote Access:

Highly secure remote maintenance access at almost any location incl. monitoring and recording

## Demilitarized Zone:

Zone separation of the highest quality by building a so-called demilitarized zone

## Data Gateway:

Safe entry and exit of permitted and malware-free data

## Network Analysis:

Comprehensive system survey and analysis of existing automation network (OT)

## Network Segmentation:

Segmentation of the automation network (Zones & Conduits according to ISA/IEC 62443)

## Anomaly Detection, Monitoring und SIEM:

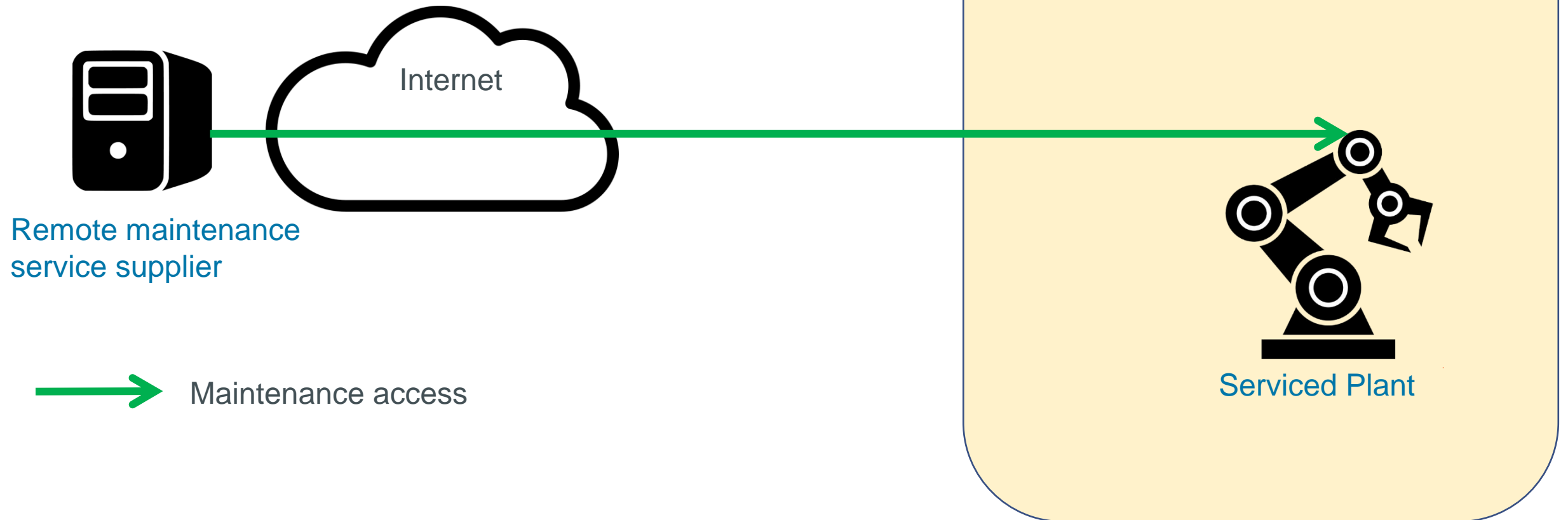
Recording and evaluation of network activities

## Managed Services:

Patching, update and monitoring services

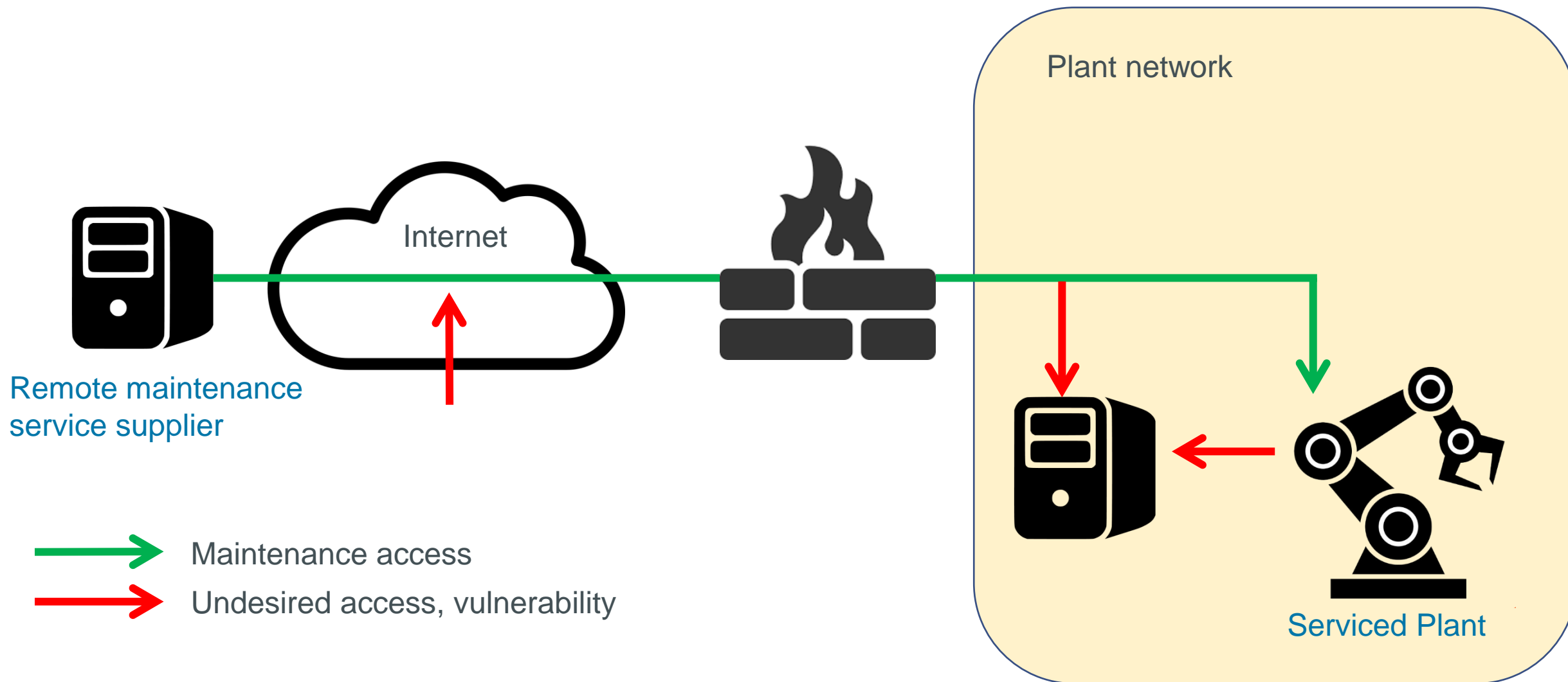


# Inbound Data – Remote Access





# Inbound Data – Remote Access

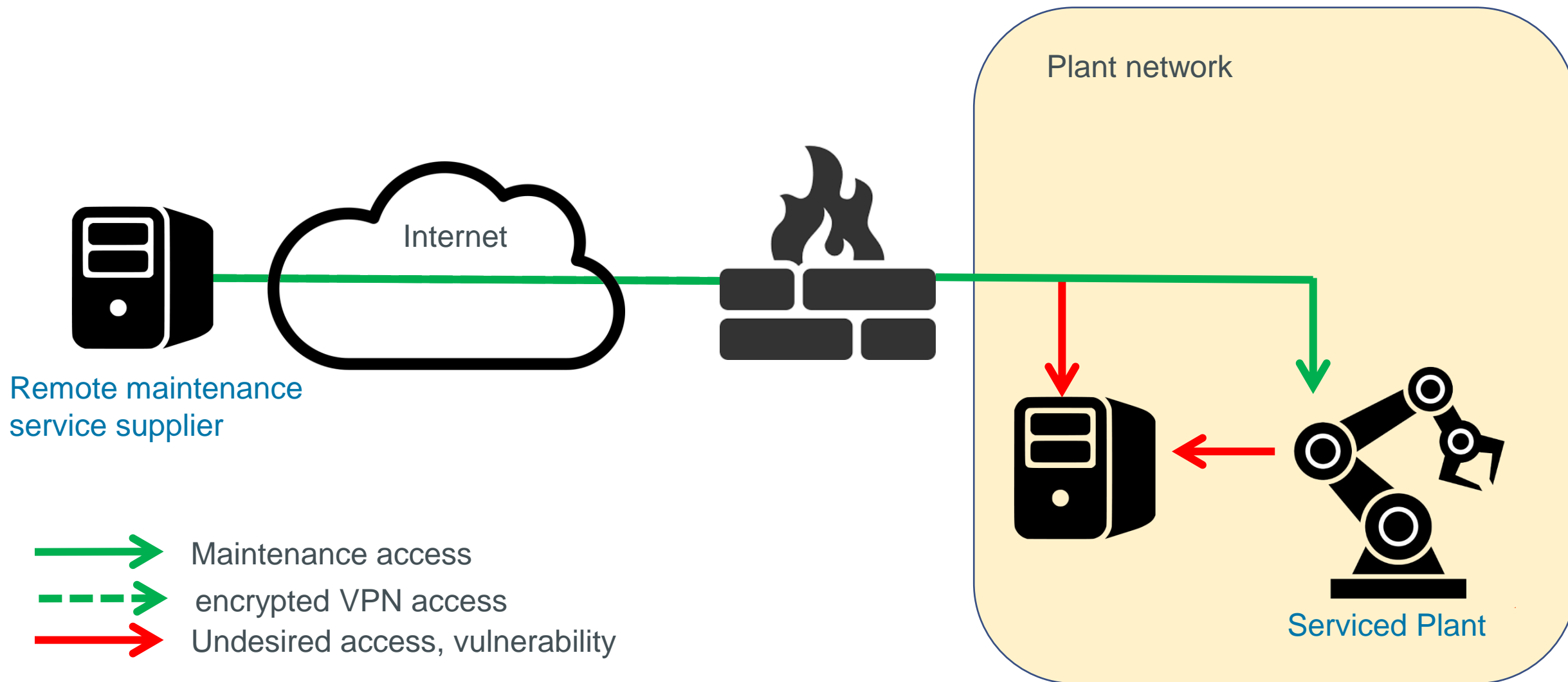






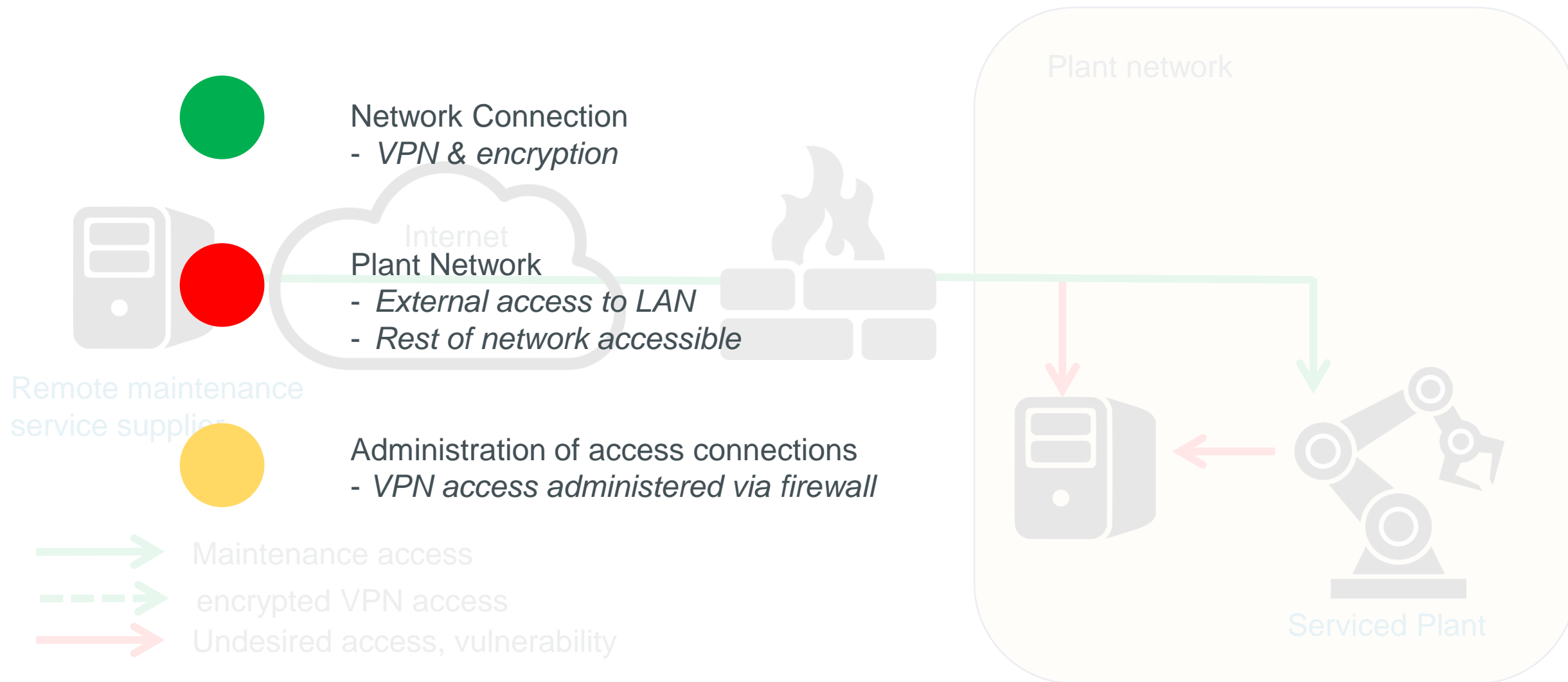


# Remote Access – but Secure!



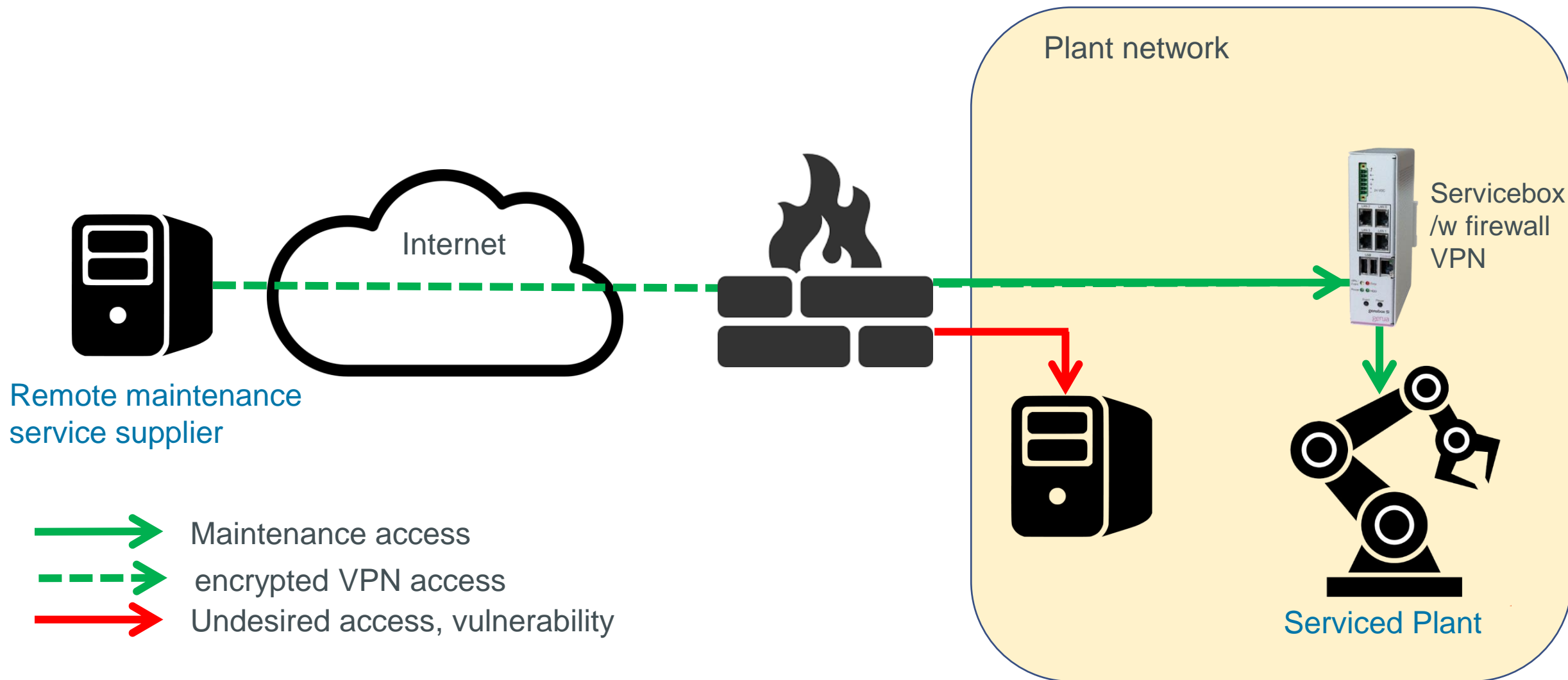


# Remote Access – but Secure!



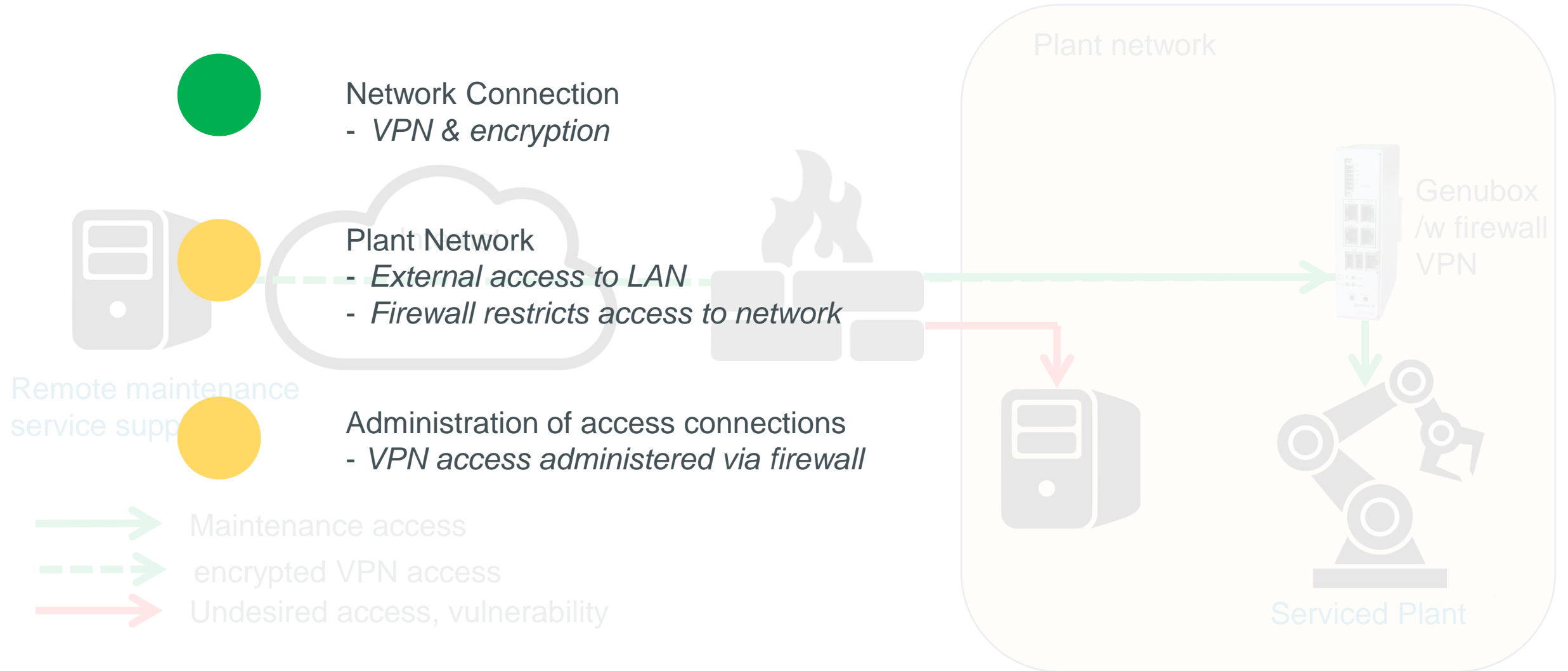


# Remote Access – but Secure!



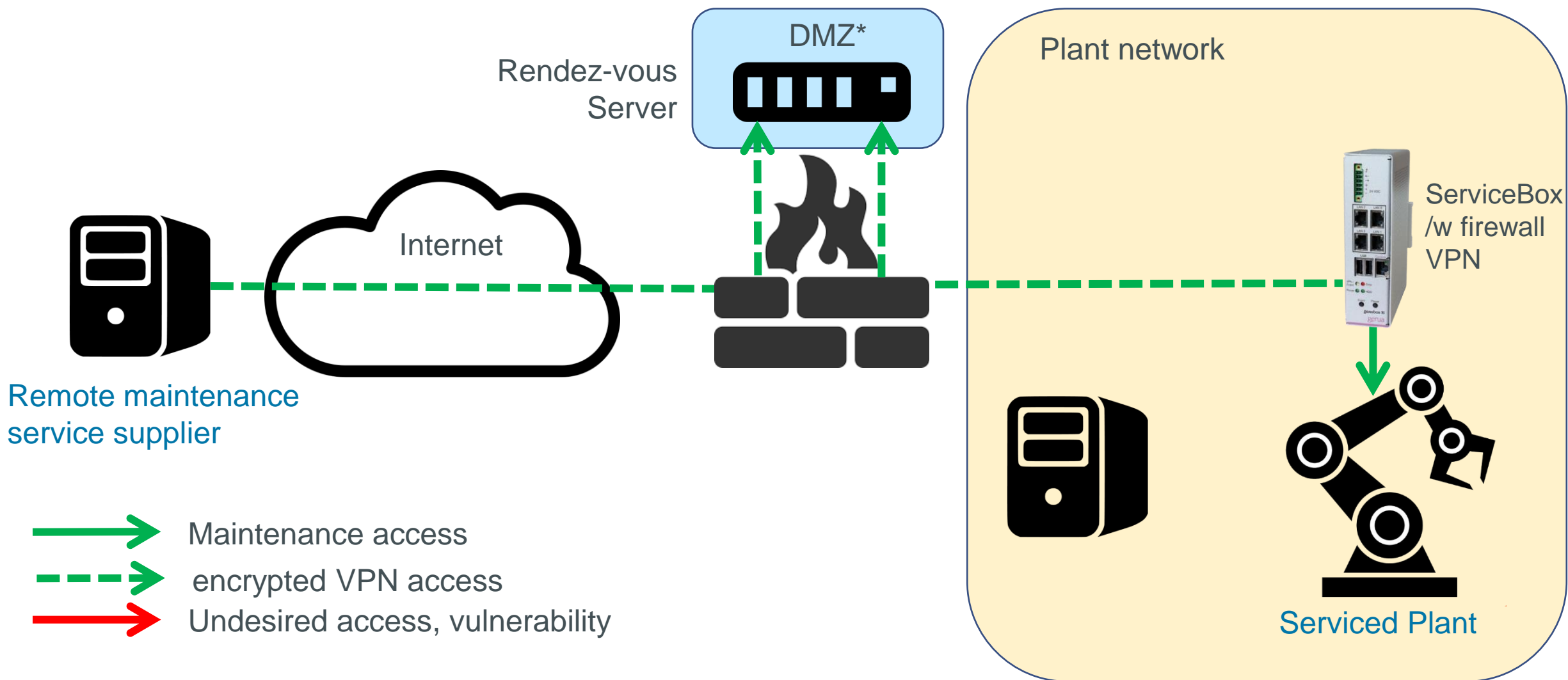


# Remote Access – but Secure!



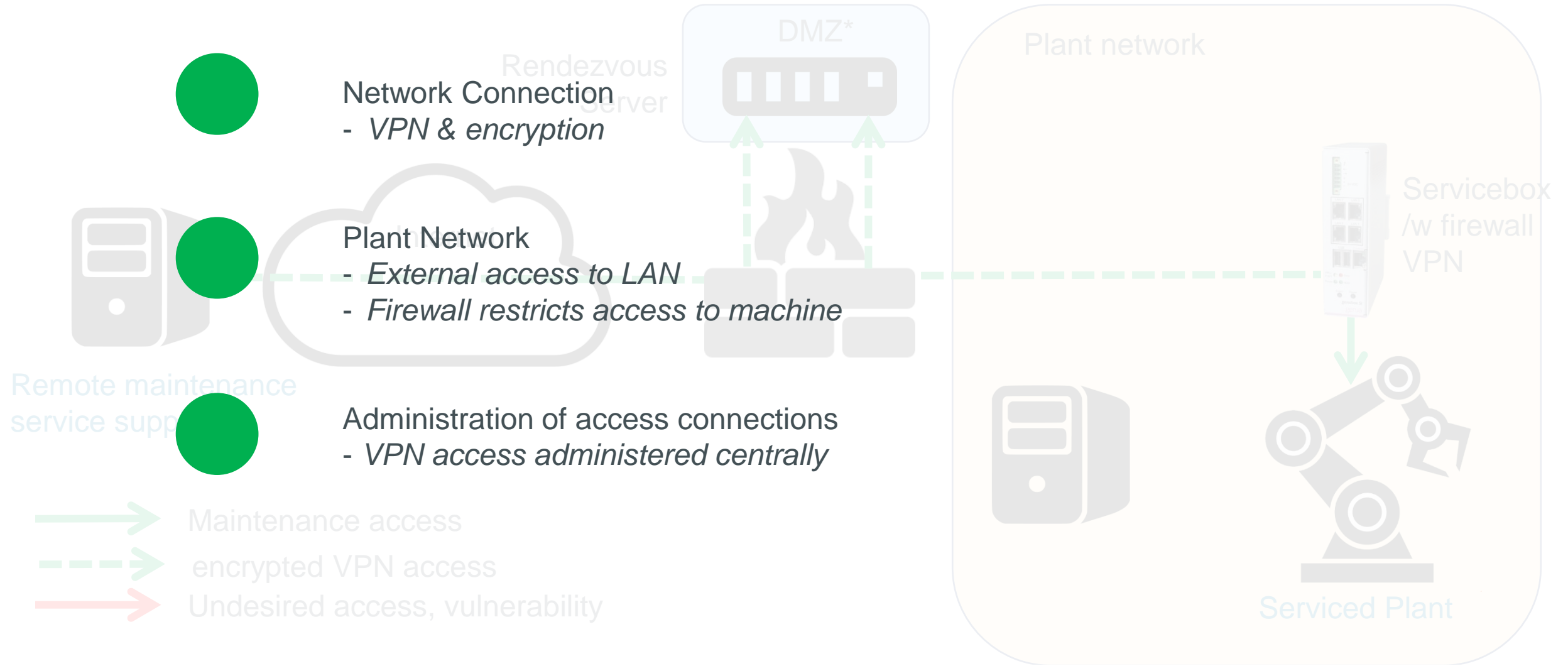


# Remote Access – but Secure!



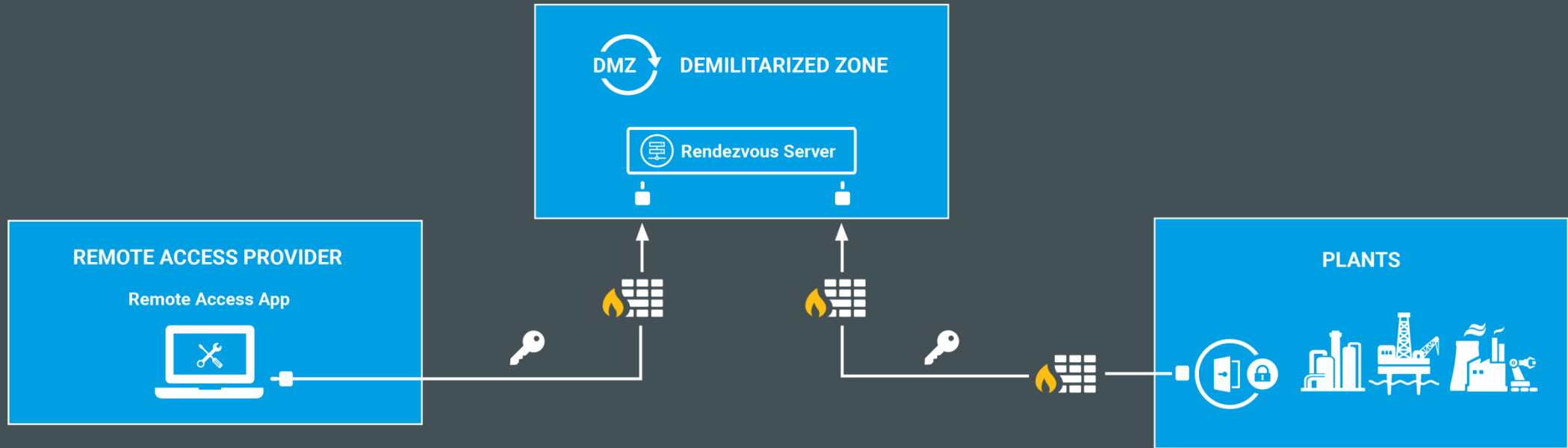


# Remote Access – but Secure!



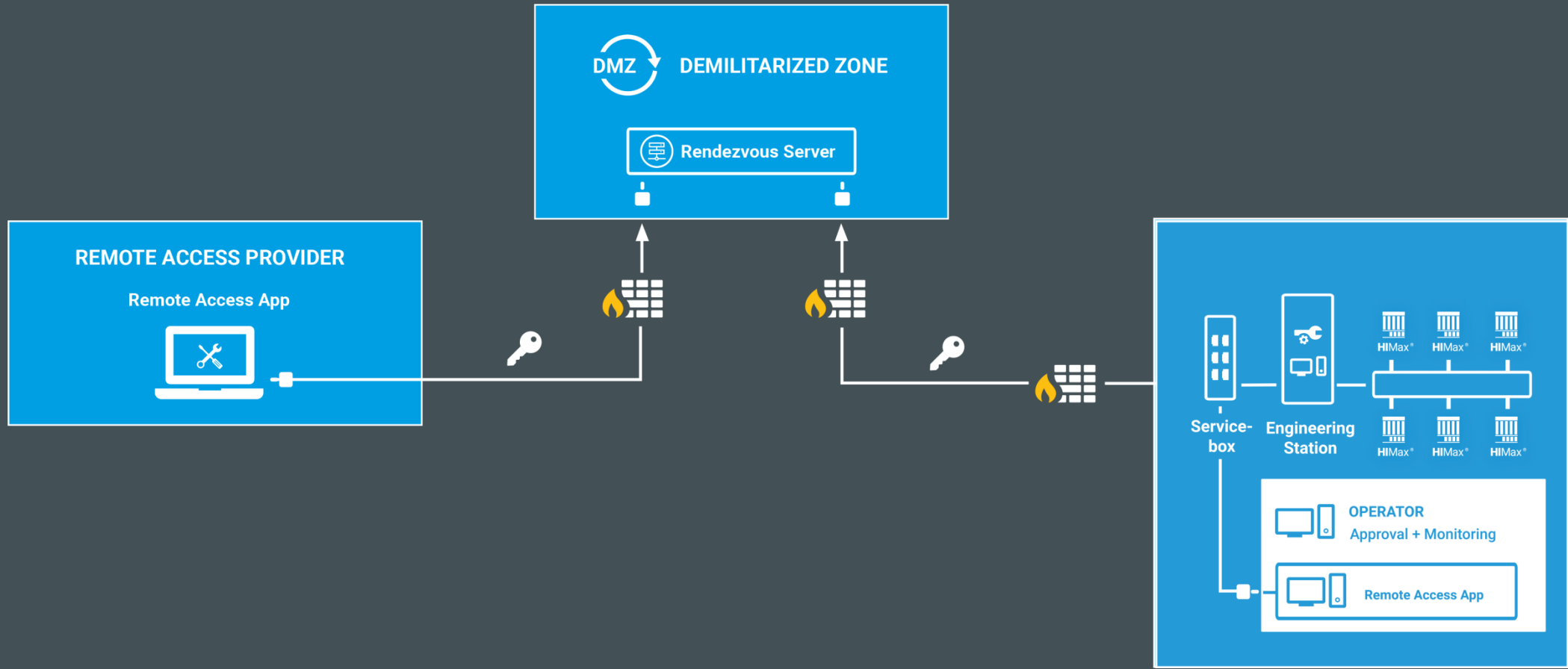


# Secure Remote Access Solution



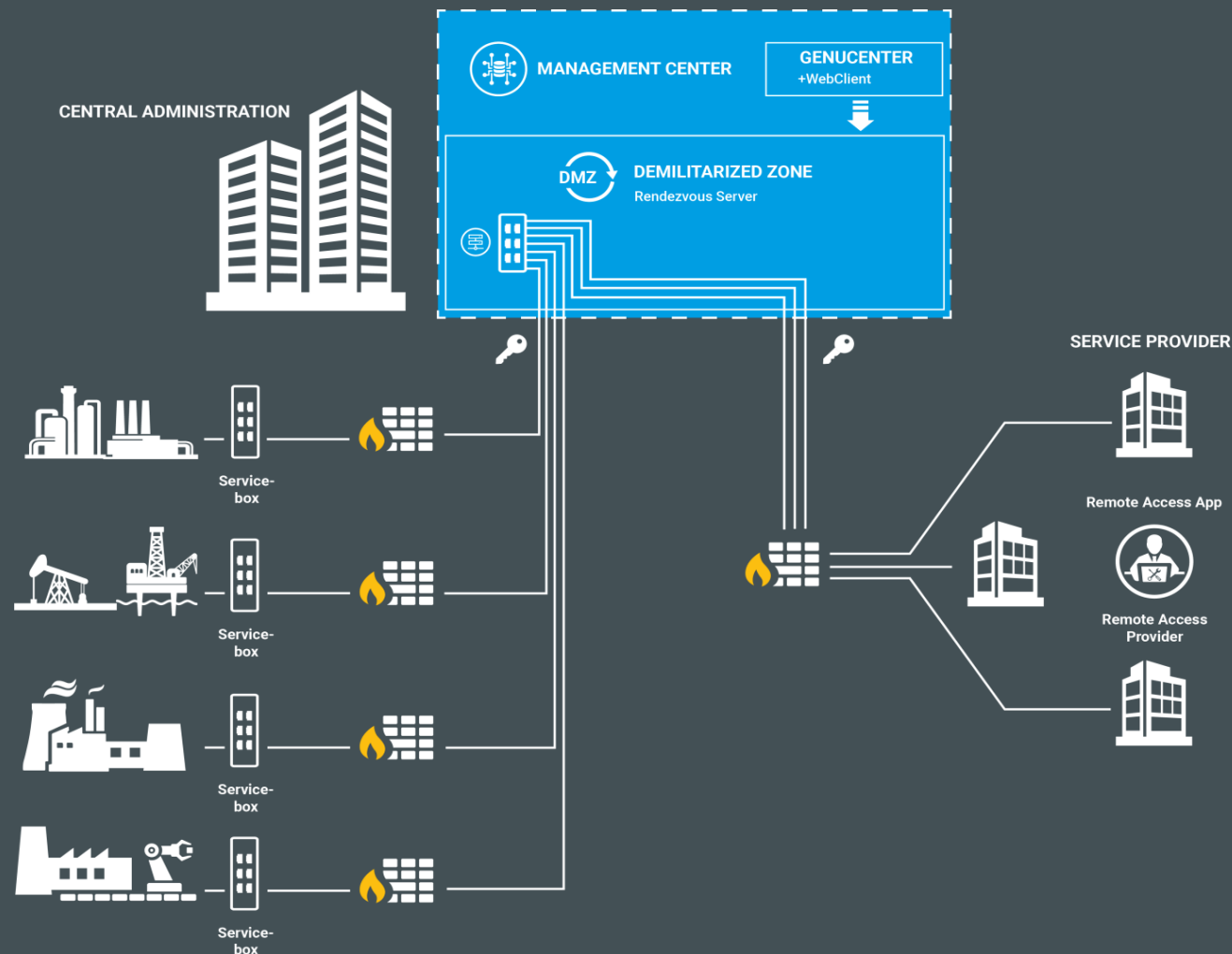


# Secure Remote Access Solution



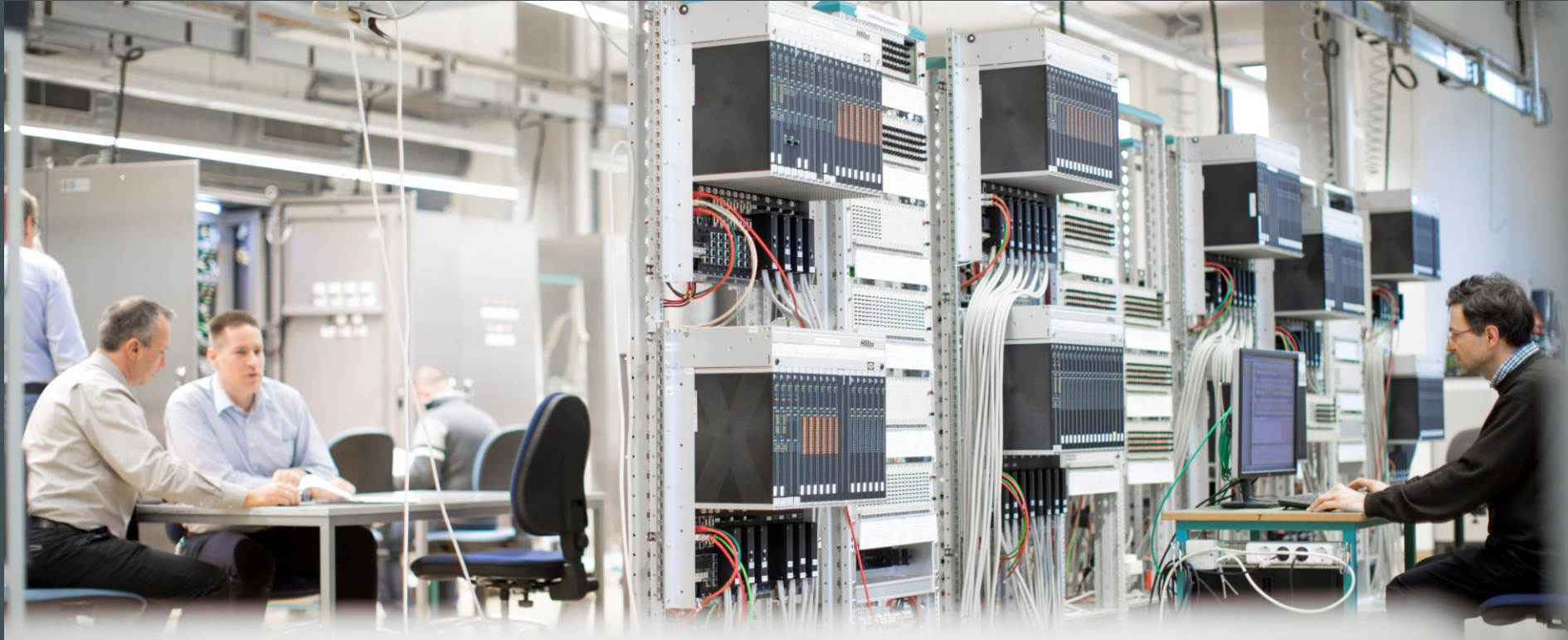


# Secure Remote Access Solution





# Covid-19: Remote Factory Acceptance Test

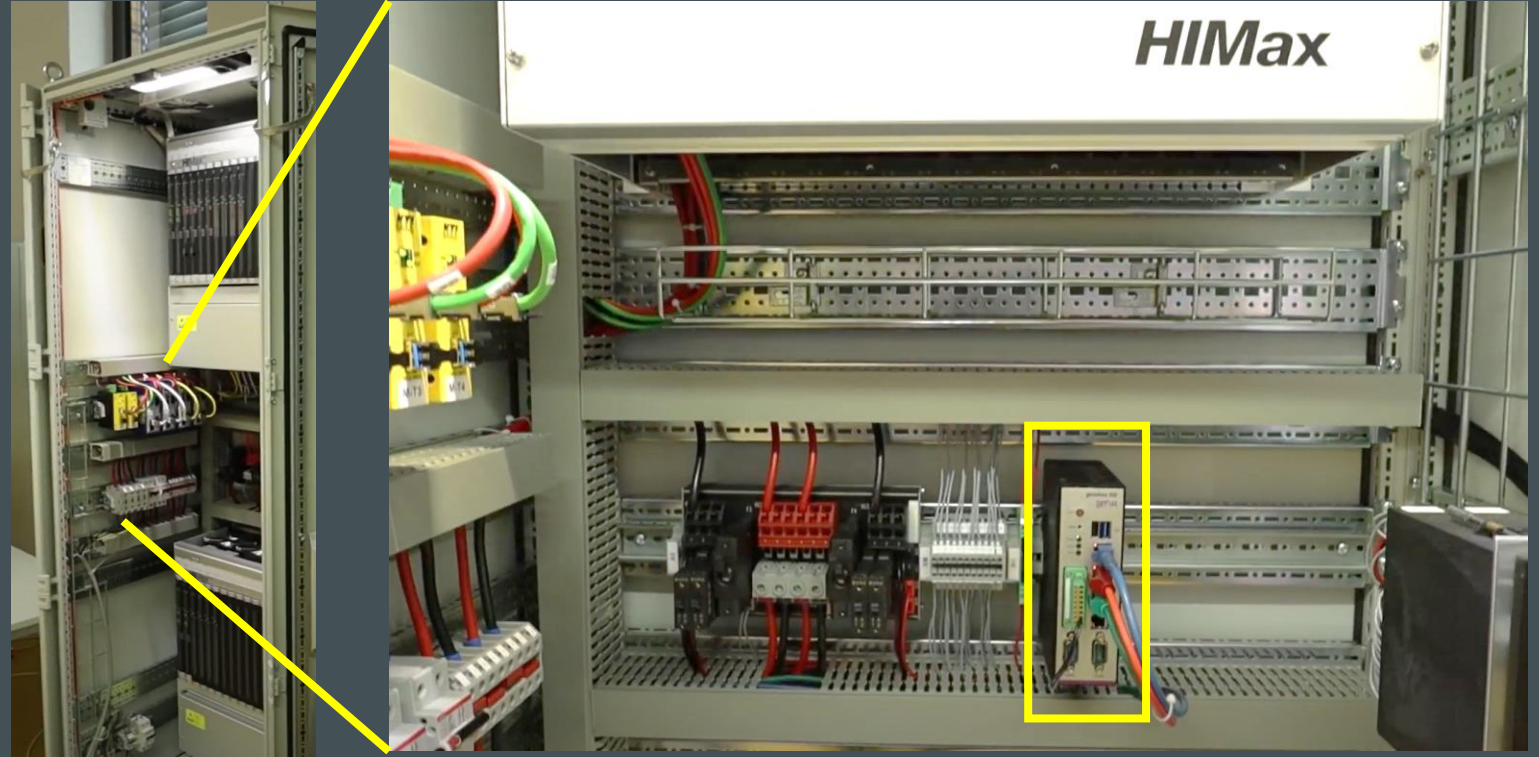




# Remote Factory Acceptance Test

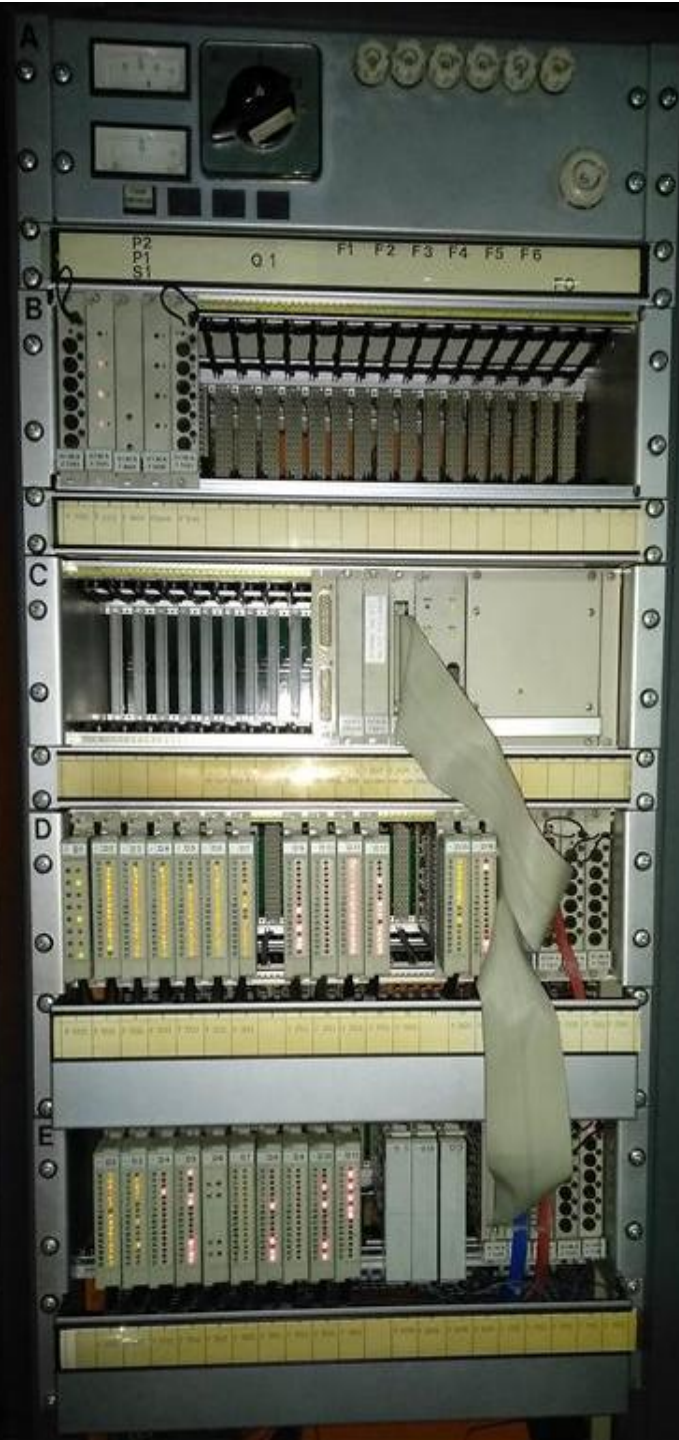


DMZ: Rendez-vous server



Plant site: Controller cabinet /w Service Box









---

# Secure Remote Access

---

- There are good reasons for remote access to plants, also to safety systems.
- It can be done securely, if it is done the right way.
- Benefits are large, one solution can and should be used for all access cases.



---

# Thank You.

---



## Alexander Horch

VP R&D and Product Management

Mobile +49 172 266 24 65

E-Mail [a.horch@hima.com](mailto:a.horch@hima.com)

HIMA Group

Albert-Bassermann-Str. 28  
68782 Brühl, Germany

Website: [www.hima.com](http://www.hima.com)