DAIMLER

Powertrain Requirement Specifications 2021 Part VI IT Security Specifications for Production Facilities

Version 2021

Version	2021	Number of pages	12
Last revised	12.03.2021		
File	01_LH6_PT_v2021_v2.2_en.docx		

Author	Passenger car planning approval	Truck planning approval
PP/PT4.0, Benjamin Müller	PP/PT, Dr. Messelken	TG/MP, Dr. Juergen Betz

Table of Contents

1. GENERAL INFORMATION

1.1. INFORMATION SECURITY REQUIREMENTS

One of the main objectives of information security is to ensure the availability, trustworthiness and integrity of the production facilities. The implementation of a comprehensive security strategy based on the requirements and measures described in this document is required for this purpose. In addition to the implementation of suitable measures directly in the components (hardware and software) used, the integration in the central security and operational tools is a decisive step in constantly maintaining the security level.
The Daimler requirements with regard to the IT security for systems and machines are highlighted and an inspection process according to the IT security criteria is defined in the following sections.

1.2. VALIDITY AND OBLIGATIONS

The present document defines the IT security requirements for suppliers of production facilities for all production locations and centers in the divisions of Daimler where standardization of production planning for major assemblies (SPPA) is employed as an automation standard.

Compliance with the IT security specifications for production facilities is binding and shall be confirmed in the bids. The security measures to be implemented shall be defined in the course of the design run-throughs for systems and documented.

IT security protection measures shall already be effective in the commissioning (IBN) and warranty phases and also allow continual updating and additions. Daimler ensures cyber-secure operation by connecting the system to the Daimler plant network and accordingly can undertake the necessary security adjustments at any time. The contractor is required to ensure compatibility of the system with the required security mechanisms in the installation through the final operational handover and to carry out post-improvements as required. This does not constitute a passage of ownership of the systems to the client.

1.3. RECORD OF REVISIONS

Version	Last revised	Chapter	Revised by
1.0	19.03.2018	New draft	Michael Günther PP/PT4.0
1.1	14.08.2018	Adaptation to Chapter 7 "Remote Maintenance"	Michael Günther PP/PT4.0
2.0	12.02.2020	Complete rework	Michael Günther / Benjamin Müller PP/PT4.0
2.1	06.03.2020	Section 2.3.4 Application Documentation added	Michael Günther / Benjamin Müller PP/PT4.0
2.2	18.01.2021	Chapter 2.4.5 "Protocols" and Chapter 2.5.2 Password protection added	Michael Günther / Benjamin Müller PT/PP4.0

1.4. CONTACTS

For general, content-related questions regarding understanding of the requirements document, send an e-mail to the following address:

itsec_powertrain@daimler.com

If you have any order-specific questions, please contact the client's representative (as per the plant-contract-compliant procedure).

2. SECURITY REQUIREMENTS

2.1. ORGANIZATIONAL REQUIREMENTS

2.1.1. IT Security Briefing

The contractor is required to train and raise the awareness of all personnel presenting a cyber-security risk potential, owing to their activities related to the delivery, setup and commissioning of a system, using the IT security awareness training videos provided by Daimler on the multiplier principle and to document the details to the client. The awareness video can be accessed through the Daimler Supplier Portal.

The supplier shall define a contact responsible for IT security during all phases of system creation. This encompasses the design phase, delivery, setup and commissioning of the system.

2.1.2. Use of Approved Components

The supplier is required to use only components approved by Daimler. The components to be used in the system are subject to approval by Daimler. Approved components are defined in Material Approval Lists (MFL) from the Material Data Manager (MDM).

For a component connected to the Daimler factory network but not appearing in a MFL, a special approval in accordance with the process-specific implementation shall be requested from the planner responsible during the concept phase of the system.

2.1.3. Physical Security and Access Protection

Physical security measures are implemented to detect, delay and prevent unauthorized access to components. The integrator shall set up components and IT-proximate production terminal devices so that they can be operated in a locked or enclosed condition. The following requirements shall be complied with:

- Peripherals and interfaces that are used for administrative purposes shall be locked and may only be accessed by a limited group of persons. Only the peripherals and interfaces required for normal operation shall be freely accessible.
- Access protection of the system and the system components for non-authorized personnel shall be monitored and ensured throughout the entire setup period, and during commissioning and service activities.

2.2. AWARENESS AND CONDUCT DURING SETUP

2.2.1. Conduct During Commissioning and Service Deployments

All personnel engaged in the setup, commissioning and service deployment of a system shall perform all operations in compliance with the Daimler IT security specifications. The following requirements shall be complied with:

- Handling of hardware and other IT equipment shall comply with the IT security instructions (see Chapter 2.1.1).
- The following rules are absolutely mandatory when handling implements that can access the Daimler network or components in the system and when programming components (e.g. programming units, smartphones, notebooks, etc.):
  - The use of potentially malicious software is not permitted.
  - Accessing unknown, potentially malicious data and Websites outside the Daimler network is prohibited.
  - All system-specific data and programs on the terminal devices shall be protected from unauthorized access (e.g. through encryption).
  - Awareness about informational duties, alerts and conduct regarding security-relevant events or recognized dangers.
- All computers (in particular programming units and notebooks) shall be equipped with an up-to-date virus scanner with up-to-date virus patterns. The equipment shall be checked for malware before being deployed in the Daimler infrastructure. Daimler reserves the right to spot-check compliance with this measure.
- The operating system and the application software of the IT equipment (in particular programming units and notebooks) shall immediately be brought to and maintained at the latest level with available security updates.

2.2.2. Identifying and Reporting IT Security Problems

During commissioning and service activities, any noticeable problems, changes or violations of the IT security specifications should be identified and reported to the local contact. The local contact at the client's end will be designated during the design run-through.

Should there be a potential danger of an incident (e.g. vulnerabilities in products or attacks against suppliers' infrastructures) affecting the information security objectives (confidentiality, integrity & availability) of Daimler, the Daimler CIRC shall be notified at cyber.security@daimler.com.

The following requirements shall be complied with:

- Monitoring of commissioning and service activities for irregularities, including:
  - Loss/theft/destruction of hardware and other IT equipment.
  - Misuse of access data such as user names or passwords.
  - Loss or compromising of access data (e.g. passwords stolen by attackers through social engineering, password cracking, passwords on non-encrypted data storage media).
  - Unusual application behavior or undefined application states (e.g. unusually high data transfer, unusual network traffic, applications responding more slowly than usual).
  - Attacks by malware (viruses/Trojans/spyware, etc.).
  - Process vulnerabilities or reduced performance (e.g. no data backup; data loss after change/migration).
  - Unauthorized access to system area or components, as well as unauthorized access to system components.
- The supplier shall immediately report any detected violations to the pertinent project supervisor or IT security supervisor in the plants.

2.2.3. Handling Storage Media

Any storage media used during setup, commissioning or service deployments shall also be secured. The following requirements shall be complied with:

- Any external storage media (e.g. USB flash drives) employed shall be checked for malware prior to use. This can be done in the following ways:
  - Checking with an up-to-date virus scanner on a terminal device.
  - Scanning shall be repeated following use of the storage medium for another purpose.
- Any malware found on a storage medium shall be immediately reported (contact: see Chapter 2.2.2)
- Media containing stored information shall be protected against unauthorized access, misuse or falsification during transport.
- If storage media are no longer required before and after conclusion of work, all data stored during such use shall be deleted securely, irrevocably and permanently.

2.2.4. Handling Mobile Devices (Smartphones, Tablets, etc.)

The use of mobile devices during setup or commissioning of a system or in service deployments, with access to the Daimler WLAN or internet, is subject to special regulations. Mobile devices shall generally not be used as storage media. It is moreover prohibited to use mobile devices as hotspots for connections between the internet and a plant network or for connections between different plant networks.

2.3. SYSTEM DOCUMENTATION AND CONFIGURATION MANAGEMENT

2.3.1. Asset Documentation

All components of the system shall be documented that are used for communication. This comprises components processing data of the system and performing an essential function (purpose fulfillment, safety and information security) within the system.

The supplier shall document the asset information on the basis of the format specified by Daimler (see Chapter 5.1).

2.3.2. Documentation of Communication Relations

Daimler uses hardware firewalls to protect the production facilities. For communication with systems outside the installation which are not provided by Daimler, the communication relations must be documented as a communication matrix in the format specified by Daimler (see Chapter 5.1) before commissioning. Non-documented communication relations will not be enabled by Daimler.

2.3.3. Documentation of the Plant Network as a Network Diagram

Communication within the plant and with systems outside the plant shall be documented as a graphic network diagram. The overview of all communication nodes and their communication relations shall be documented. The network diagram shall record the actual state of the plant network. The documentation must be provided digitally as a PDF and in editable format (ePlan or Visio) in a clear and complete manner (see Chapter 5.1).

2.3.4. Application Documentation

For each application the system documentation shall describe the following points:

- Specification of the employed application with full designation and version identifier
- Specification of necessary settings (services, firewall settings, etc.) required for regular operation of each application
- Specification of the boundary conditions of the compatibility of the application with Windows updates
- Specification of the procedure for installing updates (this also includes any required other measures such as deactivation of services, uninstalling of the old versions, adaptation of registry entries, etc.)
- Specification of the source of procurement for any other application updates made available during the system's life cycle

If the application manufacturer provides security advisories or alerts via (e.g.) RSS services, the corresponding links shall also be specified

2.4. NETWORK AND COMMUNICATION SECURITY

2.4.1. Integration in the Daimler Factory Network and Central Security Systems

Integration in the Daimler network shall comply with Daimler specifications.

- The integration proceeds via the network transfer points made available by Daimler (RJ45 jack, fiber-optic cable splice box) provided by Daimler. The contractor shall provide corresponding space in the switch cabinet/network cabinet.
- A direct connection of the system to the Internet is not permitted. Access to the internet shall be possible exclusively after approval by Daimler via the internet proxy / the DCN from Daimler. Regular operation of the system must not depend on a permanent connection to the Internet.

2.4.2. Plant Network

The setup, installation and validation of the plant network as well as the network transfer points to the Daimler network shall comply with Daimler specifications. Communication shall be limited to essentials and the communication relations shall be checked for plausibility at commissioning.

The contractor is responsible for the delivery and installation of any local system firewalls at the location. Parameterization is performed at the customer's end by Daimler.
The documentation of the communication relations must be drawn up by the contractor, see Chapter 2.3.2

2.4.3. Use of Wireless Technology

Any use of wireless technology required for production reasons is subject to approval by Daimler.

Only components approved by Daimler and compliant with the requirements of Chapter 2.1.2 may be used.

Wireless technology, however used, shall comply with the following requirements:

- The network shall be set up in its entirety (permissible frequencies, SSIDs, etc.) on the basis of the Daimler WLAN Guideline (GWSA). Use of deviating parameterizations, technologies or functions is not permitted.
- The supplier shall document specific protocols and other detailed information required for communication between wireless devices and the control system network, including other wireless devices that can communicate with the equipment supplied by the supplier.
- Employed security mechanisms and protocols shall comply with the current state of the art for security standards (non non-encrypted communication or unsafe protocols like WEP, WPS, etc.).

The supplier shall document the employed security mechanisms and protocols as well as the specific information required for communication between wireless devices and the control system network, including other wireless devices that can communicate with the equipment supplied by the supplier.

2.4.4. (Remote) Maintenance

The default remote maintenance solution is FastViewer. If the use of FastViewer (see chapter 5.1) is not possible, only solutions approved by Daimler that meet the following requirements may be used:

- The connections of (remote) maintenance access points shall at all times lie under the exclusive control of Daimler.
- Permanent access points are approved by Daimler only in exceptional cases.
- Remote maintenance is initiated by Daimler.
- (Remote) maintenance access is monitored, recorded and documented by Daimler.
- The supplier shall ensure that the approved remote maintenance tool can be installed on the relevant computers.

2.4.5. Protocols

The use of insecure protocols for interfaces that communicate via the Daimler plant network is not permitted (e.g. SMBv1, FTP). Any use of insecure protocols that are required for production reasons is subject to approval by Daimler.

2.5. PROTECTION OF TERMINAL DEVICES

2.5.1. Secure Configuration

The contractor shall ensure that only functions, services and interfaces required for operation are active and documented. In addition, the employed operating systems, firmware and any application software shall have up-to-date security status.

2.5.2. Password Protection

Immediately after commissioning, the contractor shall change all default passwords for the products procured as per Daimler specifications. The new passwords to be used are determined in the regular reporting procedure for the project between the contractor and the client according to the defined specifications.
The following rules shall be complied with for this purpose provided this is technically feasible.

- Passwords for standard users must have a minimum length of 10 characters (at least one upper case letter, one lower case letter, one number and one special character).
- Passwords for administrators must have a minimum length of 15 characters (at least one upper case letter, one lower case letter, one number and one special character).
- Passwords must not contain repeating or continuous characters (e.g. 'aaaaaa', '1234abcd').

2.5.3. Integration in Central Cyber Security Systems

Immediately after coupling of the production system to the Daimler plant network (generally within one week), Windows-based systems are registered in the corresponding central systems (in particular for anti-malware and anti-virus protection, patch management and system hardening), by means of which the former systems can be protected against cyber-security threats. The procedure required for this is to be agreed in advance between the supplier and the relevant Daimler specialist department in the course of the design discussion.

In cooperation with the contractor, the corresponding Daimler department will also carry out the following steps depending on the equipment, if necessary:

- Commissioning of the client with the aid of special configuration tools
- Installation of additional security software (see Chapter 5.1)
- Installation of operating system patches
- Installation of software updates

From this time, the Daimler department will ensure cyber-security operation. That is, one or more of the stated measures will be cyclically repeated. No passages of ownership of the corresponding clients to the client will then occur.

2.5.4. Non-Windows Systems

For non-Windows systems, the requirements of Chapter 2.5.1 apply. In addition, the contractor must change all default passwords as specified in Chapter 2.5.2 immediately after commissioning.

2.5.5. Windows Systems

Daimler will install additional software according to the location-specific operating concept for ensuring compliance with cyber-security requirements. All applicable requirements from Chapters 2.5.1, 2.5.2 and 2.5.3 apply here. The necessary preconditions must be created by the contractor.

The running capability of additional user software shall be verified in reference to the underlying hardware platform, the operating system and the specified default software (see Chapter 2.5.3). The default software is specified in detail during the design run-through. If support or compatibility of the additional user software cannot be guaranteed, suitable measures shall be indicated for enabling safe and robust operation over the entire planned run time of the system

2.5.5.1. Industrial PCs

Only industrial PCs from the currently applicable hardware basket may be used. Only the current "Daimler Blue PC Image" may be used as the operating system. The currently approved operating system image as well as the current hardware basket shall be requested via the Daimler representative (see Chapter 1.4).

2.5.5.2. Control Panels

Only control panels from the MFL (in the MDM) and project books of the component suppliers may be used. Only the operating system of the "Project DVD" from the product partners may be used as an operating system. The currently approved project DVD shall be requested via the Daimler representative (see Chapter 1.4)

3. ADAPTATION OPTIONS WHERE REQUIRED FOR SECURITY PURPOSES

In addition to the secure and robust production facility handover, it shall also be possible to maintain the secure and robust condition. To assess the system's security risk, Daimler can carry out a regular, automatic or manual scan for vulnerabilities in the course of security audits, or have the scan performed by the contractor or a third party according to specifications. The objective is to identify and eliminate security gaps in the IT systems and components of the production facilities. For this purpose, the contractor shall show how and via whom the system shall be restored to the required security level should new vulnerabilities be identified. The contractor shall also explain that Daimler may implement its own measures in the absence of suitable measures by the contractor, in order to ensure the security of the production facilities and connected systems without causing any disadvantages for Daimler (in particular loss of warranty). The contractor shall highlight and explain which systems of the production facilities may not be modified or replaced.

4. ACCEPTANCE

The planning department checks, according to a checklist, compliance with the necessary cyber-security requirements, and transfers the clients of the production cell to the department of the local BISO organization responsible for cyber-security operation.

5. GENERAL INFORMATION

5.1. ANNEXES AND OTHER APPLICABLE DOCUMENTS

- Appendix_01_-_ Use_of_Barracuda_Firewall_W010_v1_1_ENU
- Appendix_02_-_Connection_to_and_System_Requirements_on_Daimler_Cyber_Security
- Appendix_03_-_Remote_Support_-_Fastviewer
- Asset Documentation From Chapter 2.3.1
  05_Part_V_Documentation\02_Forms_and_Lists\05_Powertrain\PT_V2021_IP-adress_template_EN.xlsx
- Documentation of Communication Relations From Chapter 2.3.2
  05_Part_V_Documentation\02_Forms_and_Lists\05_Powertrain\PT_V2021_IP-adress_template_EN.xlsx
- Documentation of the Plant Network as a Network Diagram From Chapter 2.3.3
  05_Part_V_Documentation\02_Forms_and_Lists\05_Powertrain
  \01_example_network_layout_v2021.vsdx
- Application Documentation From Chapter 2.3.4
  05_Part_V_Documentation\02_Forms_and_Lists\05_Powertrain\PT_V2021_IP-adress_template_EN.xlsx

5.2. LIST OF ABBREVIATIONS

Abbreviation	Meaning
AG	Public limited company
BISO	Business Information Security Officer (responsible for IT security in the production environment)
CIRC	Cyber Intelligence Response Center
DCN	Daimler Corporate Network
DNS	Domain Name System
DVD	Digital Versatile Disc
GWSA	Global Wireless Standard Automation (Daimler WLAN specifications)
IP	Internet Protocol
IT	Information Technology
OF	Fiber-Optic Cable
MAC	Media Access Control
MDM	Material Data Manager
MFL	Material Approval List
PC	Personal Computer
PP/PT	Production Engineering / Powertrain
RJ	Registered Jack
RSS	Rich Site Summary
SPPA	Standardization of Production Planning for Major Assemblies
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPS	Wi-Fi Protected Setup

DAIMLER

Powertrain Requirement Specifications 2021 Part VI Appendix 01: Use of Barracuda Firewall W010

Version 1.1

Version	1.1	Number of pages	9
Last revised	26.02.2021		
File	Appendix_01_-_ Use_of_Barracuda_Firewall_W010_v1.1.docx		

Table of Contents

List of Figures

List of Abbreviations

DIN	German Institute for Standardization
FW	Firewall
GB	Gigabyte
GbE	Gigabit Ethernet
IP	Internet Protocol
LC	Lucent connector (connector for fiber-optic cable)
OF	Fiber-Optic Cable
RJ	Registered Jack
SFP	Small Form-factor Pluggable
SKU	Stock Keeping Unit (item number)
USB	Universal Serial Bus
R	Volts

1. General Information

1.1. Preface

The increasing networking of industrial systems affords numerous advantages for automation technology. The integration of Ethernet connections in the system down to the field bus level is the basis for the digitization and paves the way for Industry 4.0. At the same time, the danger also massively increases of the production process being attacked from within and without. The protection of communication relations through measures smoothly integrated in the automation technology is consequently an essential factor in the secure operation of networked systems.

1.2. Scope

Plant 010 (Mercedes-Benz Untertürkheim Plant)

1.3. Record of Revisions

Version	Last revised:	Chapter:	Changed by:
1.0	26.02.2020	*New draft*	Günther, Michael (PP/PT4.0)
1.1	26.02.2021	*Chapter 4.2.3* *Procurement of SFP modules by supplier of the installations (two per firewall)*	Günther, Michael (PT/PP4.0)

1.4. Contacts

For general substantive comprehension questions about this system, please contact the following Mercedes Benz department:
PT/TPD IT Security Automation Technology
Please contact (in accordance with the further processing/data processing-compliant procedure) the representative specified at the client's end in the case of order-specific questions.

2. Hardware

The Barracuda Firewall models **F183R** and **F193** approved for use in Plant 010.

2.1. Product Data

The product data are given in the Material Data Manager (MDM)

2.2. Product Pictures

Modell: F183R

Modell: F193

Figure 1- Barracuda CloudGen Firewalls F183R and F193

2.3. Power Supply

The power supply is 24 V. If multiple self-sufficient system parts are connected to the Daimler factory network via the Barracuda Firewall, it shall be ensured that power continues to be supplied to the Barracuda Firewall in the event of a voltage drop at a system part. A redundant power supply to the firewall is not necessary. Wiring of the message contact is not required.

3. Procurement

The required hardware is procured by the system supplier. Required licenses for operating the firewalls are provided by the client.
Direct procurement of the hardware from Barracuda Networks AG is not possible. The firewalls shall be procured through the suppliers listed in 3.1.

3.1. Suppliers

3.1.1. Computacenter AG & Co. oHG

Contact:	z.Hd. Christian Ziegenhardt
Address:	DE-70469 Stuttgart, Leitzstr. 45
E-mail:	christian.ziegenhardt@computacenter.com
Mobile:	+49 172 845 3732

3.1.2. Bechtle GmbH - Systemhaus Stuttgart

Contact:	z.Hd. Steffen Kleindienst
Address:	DE-70563 Stuttgart, Meitnerstrasse 10
E-mail:	steffen.kleindienst@bechtle.com
Mobile:	+49 151 21456241
Landline:	+49 711 94784 470

3.2. Ordering Information

Order number / SKU:	BNGIF193A-HWO
Description:	Barracuda CloudGen Firewall F193 / F183R Mercedes Benz AG Plant 010
Price:	On request
Average delivery time for low quantities (up to 20 units):	1-2 weeks
Average delivery time for large quantities:	On request

4. Network Integration

4.1. Copper Connections

4.1.1. Schematic Network Integration with Copper Connections

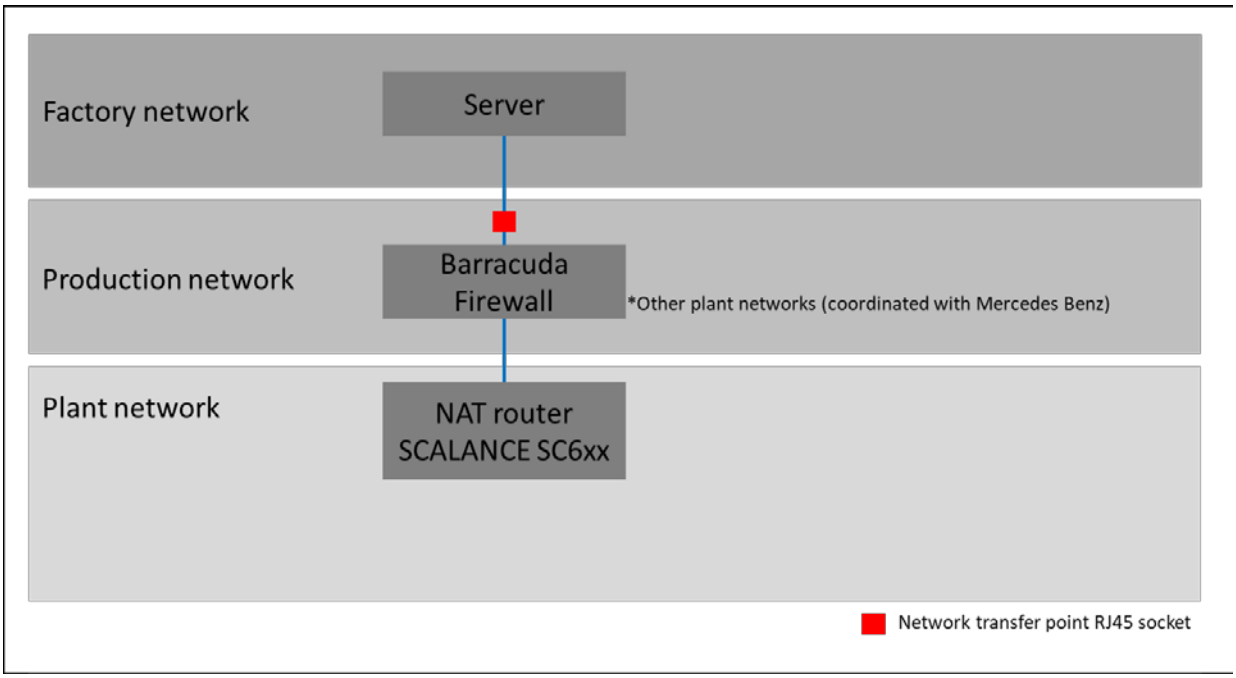

Figure 2 - Schematic of network integration of Barracuda FW with copper connection

4.1.2. Port Assignment with Copper RJ45 Connections

Port	Connection type	Use	Comment
1	RJ45	Connection point to **factory network**	
2	RJ45	**Not used**	Service port
3	RJ45	Connection to **plant network via Scalance S6xx**	
4	RJ45	Connection to **plant network via Scalance S6xx**	
5	RJ45	Connection to **plant network via Scalance S6xx**	
6	SFP	**Not used**	
7	SFP	**Not used**	

Figure 3 - Port assignment with copper RJ45 factory network connections

4.2. Fiber-Optic Cable Connections (Redundant Connections)

In redundant connections of the production facility by fiber-optic cable, the Barracuda Firewall replaces Automation Access Switch XM408-8C.

4.2.1. Schematic of Connections with Fiber-Optic Cable

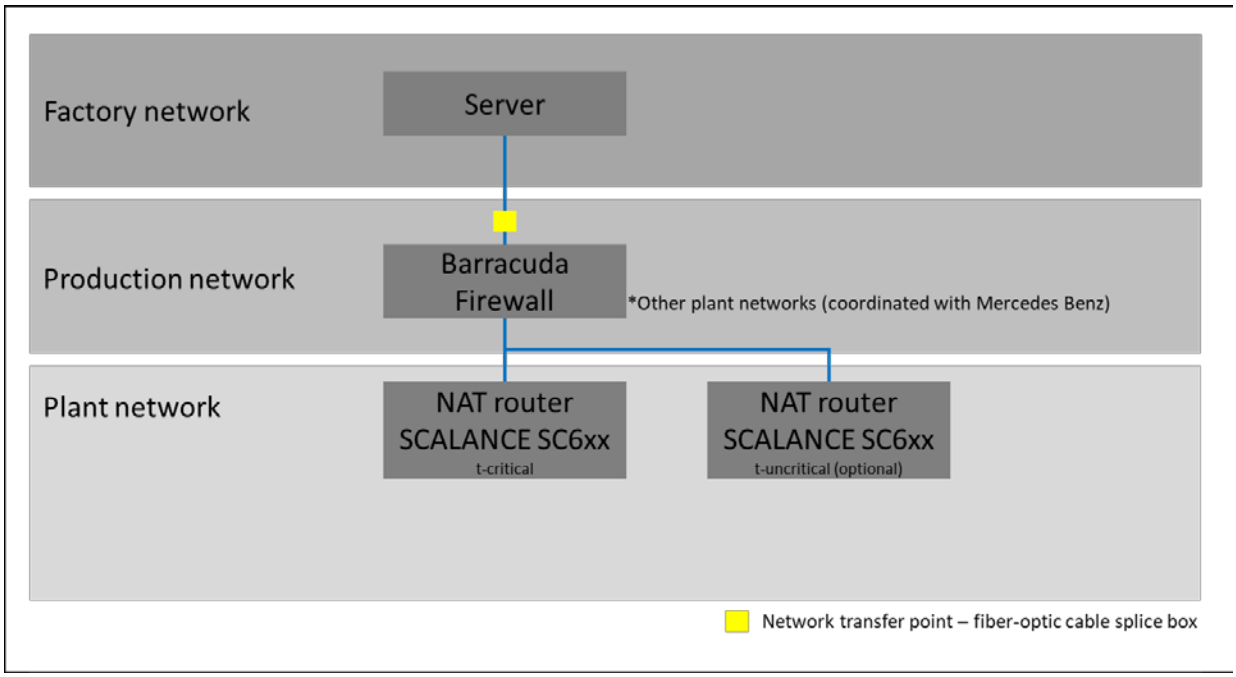

Figure 4 - Schematic of network integration of Barracuda FW with fiber optical connection

4.2.2. Port Assignment with Fiber Optical Connections

Port	Connection type	Use	Comment
1	RJ45	Connection to **plant network via Scalance S6xx**	
2	RJ45	**Not used**	Service port
3	RJ45	Connection to **plant network via Scalance S6xx**	
4	RJ45	Connection to **plant network via Scalance S6xx**	
5	RJ45	Connection to **plant network via Scalance S6xx**	
6	SFP	Connection point to **factory network**	Redundant fiber-optic cable connection
7	SFP	Connection point to **factory network**	Redundant fiber-optic cable connection

Figure 5 - Port assignment for factory network connection with fiber-optic cable splice box

4.2.3. Fiber Optic Media Modules

The following SFP modules from Siemens shall be used. The client's pertinent representative shall be asked about the employed fiber-optic cable fiber type.

The SFP modules (two modules per firewall) are procured by the contractor.

4.2.3.1. Multi-Mode

Designation:	Media module SFP992-1 (plug-in transceiver) 1 x 1000 Mbps LC port, optical for **multi-mode** fiber
Fiber type:	Multi-mode
Article number:	6GK5992-1AL00-8AA0
Manufacturer:	Siemens

4.2.3.2. Single-Mode / Mono-Mode

Designation:	Media module SFP992-1LD (plug-in transceiver) 1 x 1000 Mbps LC port, optical for **single-mode** fiber
Fiber type:	Single-mode / Mono-mode
Article number:	6GK5992-1AM00-8AA0
Manufacturer:	Siemens

5. Commissioning

Installation and power supply of the firewall by the contractor.
The documentation of the communication relations in the factory network must be prepared by the contractor on the basis of the Form Part V (Documentation)/Forms and Lists/Forms 4 Powertrain Plants/02: IP Adress Template.xlsx. The firewall is configured and activated on the basis of the documented communication relations by the Daimler PT/TPD department.
Commissioning and creation of rules and regulations only after coupling with the factory network.
Commissioning of the firewall is coordinated between the contractor and client in the design run-through.

DAIMLER

Powertrain Requirement Specifications 2021 Part VI Appendix 02: Connection to and System Requirements on Daimler Cyber Security Systems

Version 1.1

Table of Contents

1. Preface

One of the main objectives of information security is to ensure the availability, trustworthiness and integrity of the production facilities. This requires the implementation of a comprehensive security strategy. An essential component is the integration into the central security and operational tools in order continuously to maintain the security level.

1.1. Record of Revisions

Version	Last revised:	Chapter:	Changed by:
1.0	15.02.2021	Document creation	Benjamin Müller
1.1	26.02.2021	Revision	Michael Günther

2. Cyber Security Systems

In the Powertrain requirement specifications and in the present document, the following use cases are referred to as cyber security systems:

- Patch management
- Antivirus
- Optional system hardening

3. Connection to Cyber Security Systems

The connection to the central cyber security systems takes place after the shipping acceptance and must be carried out at Daimler no later than five days after connection to the network. The procedure must be agreed and scheduled in advance between the supplier and the Daimler departments involved. A suitable time for this agreement is the design discussion.

The installation of the cyber security software is carried out by Daimler in consultation with the supplier. General inquiries about the connection process can be made through the following non-personal mailbox (NPM) ltsec_powertrain@daimler.com.

4. System Requirements

To ensure smooth operation of the cyber security systems in the Powertrain production environment, we recommend the following minimum hardware configuration for a basic Windows system

Recommended: Quad-core CPU
Use of an SSD for hard disk storage
8 GB RAM
50 GB of free harddisk space

The following cyber security systems are used

- **Patch management and software distribution** through Ondeso Client and Ondeso SR based on central patch repository Microsoft Windows Update Service
- **Antivirus** using Sophos Antivirus – Endpoint Security Management

- **Optional system hardening** through Symantec Critical System Protection (SCSP)

4.1. Patch Management and Software Distribution

Patch management is effected by an Ondeso agent which has to be installed and operated on all Windows client systems. The provision and installation of current patches is carried out by a central patch repository managed by Daimler, which is based on Microsoft Windows update services. Patch installation and software distribution are controlled by a central Ondeso SR.

Notes and hints
Further information is available on the Ondeso homepage under this link
https://www.ondeso.com/produkte-und-services/ondeso-sr/.

4.2. Antivirus Using Sophos – Endpoint Security Management

Sophos Endpoint Protection is used as the anti-virus solution.

Notes and hints
Questions about installation issues can be sent through this non-personal mailbox (NPM): sophos@daimler.com.

4.3. (Optional) System Hardening

Symantec Critical System Protection (SCSP) is used when Ondeso and Sophos cannot be run on the same client.

Notes and hints
Further information can be obtained from the Symantec site under this link
https://help.symantec.com/cs/SESCSP_Help/SESCSP/v99597367_v121007334/Hardware-requirements/?locale=EN_US.

DAIMLER

Powertrain Requirement Specifications 2021 Part VI Appendix 03: Remote Support - Fastviewer

Version 1.0

Table of Contents

1. Preface

The Fastviewer application is used for external remote access to production facilities at Daimler. Fastviewer offers secure remote access to production facilities from external networks (e.g. from the Internet).

1.1. Record of Revisions

Version	Last revised:	Chapter:	Changed by:
1.0	26.02.2021	Document creation	Michael Günther

2. Organizational Requirements

- A Daimler employee is responsible for initiating a session on the machine
- Participants are invited by passing on the session key
- The required functions (activation/deactivation of access to mouse, keyboard and display) are released by Daimler employees

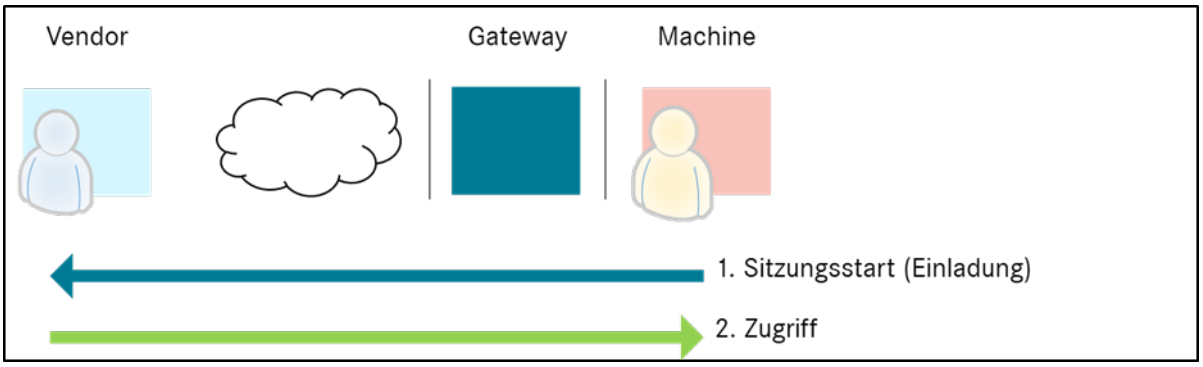

Figure 1- Schematic representation of remote access from an external point

3. Technical Requirements

An HTML5 compatible browser is required to participate in the remote session.

Access is through the Daimler website https://fastsupport.daimler.com/

The session key is provided by the Daimler employee who initiates the remote session.