Bosch-Norm

N51M M27

2022-05-16

Delivery instructions for IT-Security of machines, installations and production equipment (MAE)

Document part number:	4 497 040 708
Technical responsibility:	hlo2fe C/TED1 (400)
Replaces edition:	2019-05-14
Changes:	Chap. 3 “General” and chap. 4 "Technical specifications and requirements" updated; Chap. 5 "Using the Bosch-Norm" renamed and updated In chap. 9 "Normative references" annexes 4, 5 and 6 added Former Attachment 1: IT-Security questionnaire has been split into Attachment 1: Supplier self-disclosure and Attachment 3: Inventory list and network planning of the machine; Attachment 2: Agreement to Security specification sheet and Attachment 4: OT security acceptance protocol supplemented; Attachment 5: User documentation updated Editorial changes
Change information:	AEN 4497R31714 (internal document of the Bosch Group)

SNT1FE 2022-05-19 NormMaster

Area of validity, binding force, freedom to disclose	
Valid for	Bosch Group
Binding for	Bosch Group
Binding due to	SC-ITM decision:2015-02-25
Recommended for	Not applicable
Disclosure	No restrictions

This Bosch-Norm is binding for suppliers if it is part of the order.

© Robert Bosch GmbH. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of application for industrial property rights.

General information	
Series	N51M Machine tools, delivery instructions
Bosch-Norm standardization expert	snm1si C/TED6 (497)
Document language	en
Original language	de

Translation			
Release date	Source language	Target language	Author
2022-05-16	de	en	C/TED6 (497)

In case of doubt, the original language edition of this Bosch-Norm applies.
The comma is used as the decimal marker.
Valid edition only in NormMaster. No change service for copies.

1 Scope

This Bosch-Norm specifies the IT-Security requirements for machines, installations and production equipment (MAE).

2 Transitional regulation

This Bosch-Norm will become binding with a transitional period of 3 month.

This Bosch-Norm has to be binding during Post Merger Integration (PMI) of new divisions with a transitional period of 12 months.

3 General

The Bosch-Norm N51M M27 is binding for all machine types around the world.

Deviations from the N51M M27 should be coordinated with the responsible plant-representative for IT in manufacturing (Local-ITM).

The following standards and guidelines serve as basis for the supplier self disclosure, the security specification sheet, the sheet for agreement to the Security specifications, the list of all OT-components, the acceptance checklist/protocol, **in the version valid at the time of order acceptance respectively:**

- VDI/VDE 2182 BLATT 3.3 IT-security for industrial automation - Example of use of the general model for plant managers in process industry - LDPE-plant
- IEC 62443-3-3 - Network and system security
- VDMA - Supplier self-disclosure

The supplier is obliged to apply these instructions. The suppliers have to change deviations **that do not have our approval** for us **free of charge**. Machines shall only be considered accepted if the **OT-Security acceptance protocol** has been completed and countersigned by the asset owner or purchaser.

The cooperation of the customer in the technical solution or the approval of design characteristics does not relieve the supplier of the sole responsibility for flawless function and do not restrict the assured properties in any way.

SNT1FE 2022-05-19 NormMaster

© Robert Bosch GmbH. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of application for industrial property rights.

4 Technical specifications and requirements

The following technical specifications should be considered and adhered to, the asset owner or orderer has to be informed in case of deviations.

1. Authentication measures

In case of new installations, authentication information's must be transmitted exclusively via secure protocols or through a transport encryption.

2. Machine internal network

The machine-internal network must be divided into different network zones (segmentation). The security- and real-time network must be separated from the asset owner network.

3. Data protection

If the data has a protection class **greater than** C-SC1(confidentiality - internal) or I-SC(integrity - internal) or A-SC1(Availability - internal) is transferred to a higher-level system (e.g., ERP, MES, SCADA, ...), encryption is mandatory.

4. IP-based communication within the machine

For IP-based, machine-internal communication, addresses from the private network area 192.168.x.x must be used. These addresses must not be directly accessible from the asset owner's network. Direct transitions or connections between two machines are not allowed. The machine safety network and the asset owner's network must be separated from each other. The real-time network and production network must be separated.

5. General hardening measures

Unnecessary software applications and services that are not required for operation should be removed or disabled.

6. Avoid potentially risky services

Insecure protocols and variants are not permitted. Any deviations must be documented and explicitly approved by the asset owner.

7. Vulnerability management

Critical vulnerabilities of the OT components must be closed before delivery or before acceptance of the MAE. Information on vulnerabilities of the installed OT components must be forwarded to the asset owner during the warranty period.

8. Port scan

Open ports and discovered services represent the so-called 'network footprint' of the MAE. These are to be reduced to the necessary level for operation and listed.

9. Software inventory

The integrator creates a list of the software required for the maintenance, repairs and operation of the machine. This includes per OT component with reference to the version used (patch level) minimal data of the firmware and/or operating system, application software, third-party software and the documentation of the necessary software licenses.

10. Verification of being free of virus

At the time of delivery as well as after commissioning, the machine must be free of virus.

11. Data backup of the automation system

In the process of delivery, it is mandatory to create and maintain a virus-free emergency image (backup) of the entire system, that the system can be reset to the delivery state (see N51M M20, folder 6 Electrical documentation). This also includes, among others, configuration and production data.

12. Wi-Fi

If Wi-Fi should be used for point-to-point connections, then channels 36 and 40 in the 5 GHz band have been reserved for this purpose. An authentication is required for a Wi-Fi point-to-point connection in the manufacturing zone. A spectrum

SNT1FE 2022-05-19 NormMaster

© Robert Bosch GmbH. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of application for industrial property rights.

analysis has to be carried out before starting a Wi-Fi connection. The requirements have to be coordinated with the local ITM.

13. Export control

IT-Software and technologies have to adhere to the Export Control (CD 03402) for foreign trade.

14. Remote access/remote maintenance

If a remote maintenance is necessary, then the use of the Bosch-internal solution Remote Shopfloor Access is mandatory for the remote maintenance.

15. Verification

The transmission of the security requirements can be carried out by using a security specification sheet and is to be agreed with the integrator. The acceptance of the technical specifications and requirements must be verified with the help of an acceptance protocol.

5 Use of the Bosch-Norm

The annexed appendix and the **CGP-04602-003** **(OT Security Specification Sheet Template)** are to be used as follows:

- At the time of creation of the security specification sheet, a **CSRS** (Cyber Security Requirements Specifications) must be created based on the security specification sheet template.
    - Specified security specification sheet IT-Security (based on the template **CGP-04602-003** **OT-Security Specification Sheet Template**)
- At the time of preparing the offer, the proofs:
    - **Attachment 1 Supplier self-disclosure**
    - **Attachment 2 Agreement to security specification sheet**

  have to be filled out by the supplier of the MAE (integrator).
- At the time of order receipt, the:
    - **Part B - Installed IT-devices** of N51M M27
      Attachment 3 Inventory list and network planning of the machine

  has to be filled out and made available latest at the pre-acceptance.
- At the time of delivery, the entire inventory list and network planning of the machine shall be provided:
    - **Attachment 3 Inventory list and network planning of the machine**
- At the time of the start of production (SOP), the signed **OT-Security acceptance protocol** is exchanged between the asset owner or purchaser of the machine. The security specifications are only deemed accepted with the signature of the asset owner or purchaser.
    - **Attachment 4 OT security acceptance protocol**
- The following document serve to simplify the use of the Bosch-Norm:
    - **Attachment 5 User documentation**
- The following appendix serves as a guideline for external service providers
    - **Attachment 6 IT-Security Guidelines for external service provider**

The **inventory list and network planning** of the machine is used both upon delivery of the machines for network planning and documentation, as well as for IT risk assessment of the OT systems deployed in the MAE.

By default, it is sufficient to provide the above-mentioned proof for each order (e.g., per machine line). However, at the request of the operator, a proof may also be required for **each machine.**

If necessary, the supplier properties can be used as a basis for supplier development.

SNT1FE 2022-05-19 NormMaster

© Robert Bosch GmbH. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of application for industrial property rights.

6 Documentation

The inventory list and network planning of the machine with a list of all OT components can be used as basis of a technical IT-documentation and is part of the installation documentation (see N51M M20, chap.10, folder 6, Electrical documentation) and is handed over to the orderer latest at the time of the MAE delivery.

Within the EU, the N51M M20 is considered part of the documentation. Outside the EU, at least the proof of the used OT components and the configuration description must be signed and deposited with the orderer.

The documents are available in the NormMaster as an attachment to the Bosch Norm N51M M27.

7 Pre-acceptance and final acceptance

The **Attachment 4 OT-Security acceptance protocol** is to be checked by the orderer during the pre-acceptance (FAT) and final acceptance (SAT) in the plant. He can be supported by the local-ITM or the IT-planner.

8 IT-Security guidelines for external service providers

During the assignment by the assigning technical department, the **Attachment 6 "IT-Security guidelines for external service providers"** should be handed over to the service provider is available in NormMaster in PDF format as an attachment of the Bosch-Norm N51M M27.

SNT1FE 2022-05-19 NormMaster

9 Normative references

The following documents are applicable for using this Bosch-Norm. With dated references, solely the edition referred to applies. With undated references, the last edition of the indicated document applies (including all revisions). Intentionally cited historical documents are additionally identified as "H" in the column "Type."

No.	Document number (edition date)	Title	Type
1	N51M M27 Attachment 1	Supplier self-disclosure	M
2	N51M M27 Attachment 2	Agreement to Security specification sheet	M
3	N51M M27 Attachment 3	Inventory list and network planning of the machine	M
4	N51M M27 Attachment 4	OT security acceptance protocol	M
5	N51M M27 Attachment 5	User documentation	M
6	N51M M27 Attachment 6	IT-Security Guidelines for external service provider	M
7	CGP 4602 003	OT-Security Specification Sheet for use in MAE purchasing	Z
8	N51M M20	Machine tools, delivery instructions, General delivery instructions for machines, installations and production equipment (MAE)	Z
9	VDI/VDE 2182 BLATT 3.3	IT-security for industrial automation - Example of use of the general model for plant managers in process industry - LDPE-plant	Z
10	IEC 62443-3-3 * CEI 62443-3-3	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	Z
11	CD 03402	Central Directive Export Control	Z
12	CD 04602	Central Directive IT in Manufacturing	Z

Type M = document to be supplied; Z = cited document; H = historical document

© Robert Bosch GmbH. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of application for industrial property rights.