Manual

Automation Security

HIMA Security

Contact

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Document designation	Description
HI 801 372 E, Rev. 2.01 (1844)	German original document
HI 801 373 E, Rev. 2.01.00 (1844)	English translation of the German original document

Table of Contents

1 Introduction 5

1.1 Structure and Use of This Manual 5

1.2 Target Audience 5

1.3 Writing Conventions 6

1.3.1 Safety Notices 6

1.3.2 Operating Tips 7

2 Introduction to Safety and Security 8

2.1 Distinction between Safety and Security 8

2.1.1 Safety (Functional Safety) 8

2.1.2 Security (Automation Security, IT Security or Cyber Security) 8

2.2 Security Threats 9

2.3 Measures for Preserving Security 9

2.3.1 Awareness 9

2.3.2 Good Engineering Practice 9

2.4 Security as a Process 10

2.4.1 Analyze Risk 11

2.4.2 Protect 11

2.4.2.1 Organizational Measures 11

2.4.2.2 Technical Measures 11

2.4.3 Detect 11

2.4.4 React 11

3 Product Properties to Support Security 12

3.1 Overview of HIMA Systems 12

3.1.1 Relay Logic (VPS, Planar4 Systems) 12

3.1.2 HIQuad 13

3.1.3 HIMatrix Remote I/Os 13

3.1.4 HIMatrix F*02 13

3.1.5 HIMax, HIQuad X, HIMatrix F*03 13

3.2 Protective Measures 14

3.2.1 Protection at Network Level 14

3.2.1.1 HIMatrix Remote I/Os 14

3.2.1.2 Ethernet Interface 14

3.2.1.3 Ethernet Settings 14

3.2.1.4 Network Segregation and Physical VLAN 15

3.2.1.5 Use of safe**ethernet** 16

3.2.1.6 Use of OPC 17

3.2.1.7 System Bus Module (HIMax X-SB) 17

3.2.1.8 Use of Non-Safety Protocols 17

3.2.1.9 Remote PES Access 18

3.2.1.10 Link Layer Discovery Protocol (LLDP) 18

3.2.1.11 Mirroring 18

3.2.1.12 Simple Network Time Protocol (SNTP) 18

3.2.1.13 Ethernet Ports Used 19

3.2.1.14 Firewalls Controlling the Data Traffic 20

3.2.2 Integrated Protective Mechanisms 20

3.2.2.1 Operating System State 20

3.2.2.2 Access Restrictions 20

3.2.2.3 Reading Back and Changes to Program Parts 21
3.2.2.4 PES User Management 21
3.2.2.5 System Monitoring 22
3.2.2.6 Protecting the Operating Systems 22
3.2.3 Protection When Connecting the PC for Programming 22
3.2.3.1 Installation (SILworX) 23
3.2.3.2 SILworX PADT 23
3.2.3.3 User Management in SILworX 24
3.2.3.4 Backup Recovery Strategy 24
3.2.3.5 SILworX Code Comparator 24
3.2.3.6 Know-How Protection 25
3.2.3.7 Preferred PADT Connection 25
3.2.3.8 Diagnosis in SILworX 25
3.2.3.9 Remote Access to the PADT 25
3.2.3.10 Passwords 25
3.2.4 Protection When Connecting the OPC Server 26
3.2.5 Configuration of PCs 27
3.2.5.1 BIOS Settings 27
3.2.5.2 Interface Protection 27
3.2.5.3 Reducing Rights (Least Privilege) 27
3.2.5.4 Patches 28
3.2.5.5 Antivirus Software 28
3.2.5.6 Application Whitelisting 29
3.2.5.7 General Information on Protecting PCs 29
3.2.6 Further Protective Measures 29
3.2.7 Tests by an Independent Authority 29
4 Further Information 30
4.1 HIMA Information 30
4.2 External Information Sources 30
Appendix 31
Glossary 31
Index of Figures 32
Index of Tables 32

1 Introduction

HIMA safety products feature essential technical properties that can significantly reduce security risks in plants. However, proper implementation of the HIMA safety products is key, in particular, in terms of their network structure, parameter setting and programming. This manual describes the automation security aspects that must be taken into account when using HIMA safety products.

The main focus is on the HIMax, HIQuad X and HIMatrix systems.
HIMA recommends structuring the systems for practical application. Typically, the individual structure has to be adapted to the operator's overall concept.

The suggested structure does not eliminate the need for a risk analysis.

If an individual risk analysis results in a different concept, the structure should be set up in line with the result of this risk analysis.

Further external measures can additionally be implemented to reduce risks. However, this manual does not contain any recommendations for using third-party products, such as, e.g., infrastructure components. Any mention of products is meant to be exemplary and has no recommendatory character.

1.1 Structure and Use of This Manual

This manual contains the following main chapters:

- Introduction.
- Introduction to safety and security.
- Product properties to support security.
- Further information sources.

The current manual can be obtained upon request by sending an e-mail to: documentation@hima.com. The documentation is available for registered HIMA customers in the download area https://www.hima.com/en/downloads/. Here, customers can also register for the Document Info Service (DIS) to obtain information on updated documents.

The revision index in the footer can be used to compare the manuals in use with the Internet edition and determine if they are up to date.

1.2 Target Audience

This document is aimed at the planners, design engineers and programmers of automation systems as well as the persons authorized to start up, operate and maintain the devices and systems concerned.

HIMA offers a training course in security. For further information, refer to the HIMA website at: https://www.hima.com/en/products-services/seminars/ (→ Other)

Contact

For questions regarding security, please contact support@hima.com or security@hima.com. HIMA is continuously looking to improve its products. Please send us your feedback, particularly if something is not clear, if you have any suggestions for improvement, or if you notice any system responses that do not seem plausible.

For current information, refer to the HIMA website at:
https://www.hima.com/en/industries-solutions/cybersecurity/.

1.3 Writing Conventions

To ensure improved readability and comprehensibility, the following writing conventions are used in this document:

Bold	To highlight important parts. Names of buttons, menu functions and tabs that can be clicked and used in the programming tool.
Italics	Parameters and system variables, references.
`Courier`	Literal user inputs.
RUN	Operating states are designated by capitals.
Chapter 1.2.3	Cross-references are hyperlinks even if they are not specially marked. In the electronic document (PDF): When the cursor hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are specially marked.

1.3.1 Safety Notices

Safety notices must be strictly observed to ensure the lowest possible risk.

The safety notices are represented as described below.

- Signal word: warning, caution, notice.
- Type and source of risk.
- Consequences arising from non-observance.
- Risk prevention.

The signal words have the following meanings:

- Warning indicates hazardous situations which, if not avoided, could result in death or serious injury.
- Caution indicates hazardous situation which, if not avoided, could result in minor or moderate injury.
- Notice indicates a hazardous situation which, if not avoided, could result in property damage.

SIGNAL WORD

Type and source of risk!

Consequences arising from non-observance.

Risk prevention.

NOTICE

Type and source of damage!

Damage prevention.

1.3.2 Operating Tips

Additional information is structured as presented in the following example:

i The text giving additional information is located here.

Useful tips and tricks appear as follows:

TIP The tip text is located here.

2 Introduction to Safety and Security

2.1 Distinction between Safety and Security

The terms safety and security describe a state of freedom from unacceptable risk.

It is always necessary to implement both technical and organizational measures to reduce risks.

2.1.1 Safety (Functional Safety)

Functional safety describes the part of safety of a system that depends on the proper function of the safety-related system and other measures aimed at minimizing risk.

Safety in this context relates to avoiding systematic faults (management of functional safety) as well as reducing and controlling random faults (component faults - this is achieved through a failsafe design, the creation of hardware fault tolerances and the use of diagnostics).

HIMA develops, produces and supplies safety controllers that are used to increase plant safety. The controllers from HIMA help to reduce process risks to an acceptable level.

2.1.2 Security (Automation Security, IT Security or Cyber Security)

The term describes security in terms of data confidentiality, integrity, and availability. In contrast to safety, security presumes systematic external influences (e.g., hackers).

Safety can only be ensured based on correct data. For this reason, safety conditions can only be guaranteed if the corresponding security measures were implemented.

Which priority is to be associated with the aforementioned protection targets, i.e., confidentiality, integrity and availability, depends on the application.

Data confidentiality is usually the most important issue for information technology (IT), whereas availability has usually the highest priority in operational technology (OT). For complying with safety requirements, data integrity is usually key.

Every system to be protected must be considered and assessed on an individual basis.

Other (minor) protection targets are authentication, authorization and non-repudiation.

Organizational protective measures are supported by technical measures. Technical measures on their own are not sufficient.

i The previous considerations not only apply to programmable systems, but also to every technical system over the entire lifecycle. As such, the modification of design documentation can cause significant risks.

2.2 Security Threats

Automation components have already been suffering from the consequences of malware for many years. These were often not targeted at automation systems. Meanwhile, however, targeted attacks on automation systems have emerged. Stuxnet is the first known malware that specifically interfered with the function of automation components. (For further information, refer to https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, for example.) Meanwhile, TRITON has also been used to attack a safety system.
(For further information, refer to https://www.hima.com/en/about-hima/news/article/hima-security-advisory-trisistriton-1/.)

This scenario shows that both the threat (interest) and the vulnerability (known, useful gaps) of systems are continuously changing. Consequently, the achieved level of security can only be maintained for a certain period.

2.3 Measures for Preserving Security

2.3.1 Awareness

Standards and publications on security deal with security awareness in detail. This is the basis of security. Any technical measure can only be successful if company personnel are sufficiently aware of security. This applies throughout the planning phase, start-up, operation and decommissioning.

2.3.2 Good Engineering Practice

Security is strictly related to the way of thinking of the parties involved. For this reason, the basic security principles presented by Viega and McGraw can be mentioned as a good example. This list was compiled in 2002 and is still valid today. These principles do not provide 100 % protection. They should help to achieve 80 % of the possible risk reduction using 20 % of the effort.

1. **Secure the weakest link** (i.e., identify and strengthen the weakest link.)
   Attackers look for simple ways to influence a system and will try to identify the weakest link for an attack. Therefore, the weakest link in the chain should be secured first.
2. **Practice defense in depth** (i.e., counteract software risks by implementing multi-layer security solutions.)
   To overcome a weakness, attackers cannot impact the entire system, but only a part of the system. Attackers also run an increased risk of detection. In safety, this is referred to as *layer(s) of protection*.
3. **Fail securely** (i.e., make sure that if the system fails, it only does so in a secure manner.)
4. **Follow the principle of least privilege** (i.e., do not grant more privileges than required, and do not extend privileges longer than necessary.)
   If it is not permitted, it is forbidden. Only the minimum needed permissions should be granted for the minimum possible time. So, if read-only access is required, only this permission should be allowed.
5. **Compartmentalize** (i.e., try to constrain faults in a system part to prevent them from having an impact on the rest of the system.)
6. **Keep it simple & stupid** (KISS)
   KISS should be in good balance with *defense in depth*. Easy to see through, reuse of well-tested components, creation of individual, controllable data channels (conduits).
   Security by design. Speak with the users applying it most and take account of their requirements.
7. **Promote privacy** (i.e., do not disclose any unnecessary information.)
   Data should be handled sensitively. It also does not hurt to provide false information.
8. **Remember that hiding secrets is hard**
   Secrets are not secure just by using a format that is not obvious (e.g., binary file). This is called *security by obscurity* and does not work.

9. **Be reluctant to trust**
   Even manufacturers of secure software are not infallible. Do not put unconditional trust on anybody, even on yourself or your company, but involve independent third-parties, if required.
10. **Use your community resources** (i.e., describe your security measures.)
    If they withstand third-party scrutiny, they can be assumed to be fairly secure. If you are uncertain whether your design is secure, get help.

For further information, also refer to:
http://searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security

2.4 Security as a Process

Security risks keep changing. It is therefore necessary to set up a continuous process to achieve and maintain the required security level. Similar to the continuous improvement process in quality management or functional safety management, security must be actively and continuously maintained. This is best supported by a management system.

The security process can be divided into the following four steps, for example:

- **Analyze risk (Plan)**: Determine and evaluate the assets worthy of protection.
- **Protect (Do)**: Protect the assets in accordance with the needs.
- **Detect (Check)**: Integrate and assess measures for detecting the system's gaps.
- **React (Act)**: After detection of a gap, react accordingly.

After expiration of a given period, identification of a threat or detection of an event, the process starts from the beginning. This process is also referred to as PDCA model (**P**lan, **D**o, **C**heck, **A**ct).

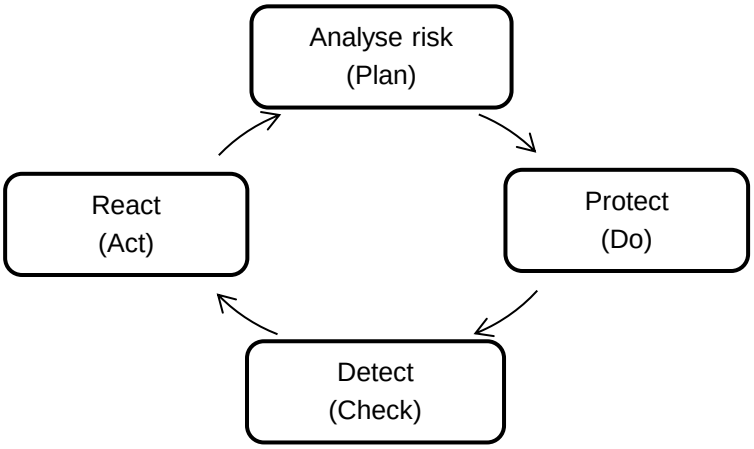


Figure 1: PDCA Cycle

In change management, both safety and security characteristics of a system must be considered.

TIP The illustrated PDCA cycle is just one option. For further information, refer to standards such as ISO 27000 and later, IEC 62443-2-1, VDI 2182 and NIST SP 800-37.

2.4.1 Analyze Risk

In addition to implementing basic protection, a risk analysis should be performed to determine the risk.
During the risk analysis, the entire system is systematically examined. This includes the identification of potential threats and vulnerabilities as well as the extent of potential damages. This serves to draw up suitable solutions for individual plants.

TIP Risk analyses are described in several standards, including IEC 62443-3-2, NA163, ISO 27005 and BSI 200-3.

HIMA offers risk analysis for safety and security as a service.

2.4.2 Protect

2.4.2.1 Organizational Measures

It is a widespread view that security measures are inevitably linked to high investments in security technology and the employment of highly qualified personnel. However, this is not the case. The most important success factors are common sense, well thought-out organizational regulations as well as reliable and well-informed employees who are disciplined and routinely aware of safety requirements. Creating and implementing a capable and effective information security concept does not necessarily have to be expensive. The most effective measures are surprisingly simple and often free of charge! (Source: BSI IT-Security Guidelines)

2.4.2.2 Technical Measures

Technical measures support the organizational measures.

Multiple layers of defense (*defense in depth*) are currently approved as the most effective measure to minimize risk. Multiple layers of protection should be implemented in industrial automation systems.

HIMA systems are equipped with an operating system specifically developed for safe automation. The safety controller therefore represents the best possible last line of defense.

2.4.3 Detect

HIMA products extensively utilize standard technologies. Programming systems are based on current Windows operating systems. Default communication is based on standard Ethernet. This way, additional technical measures, such as the use of honeypots or IDS, can help detect irregularities in the network or in the overall system.

2.4.4 React

An adequate response must be given for any irregularity detected within the system. The cause must be eliminated. An examination should show if and how to prevent such events in the future. The process begins anew.

3 Product Properties to Support Security

This chapter describes the use of HIMA systems. Figure 2 provides an overview:

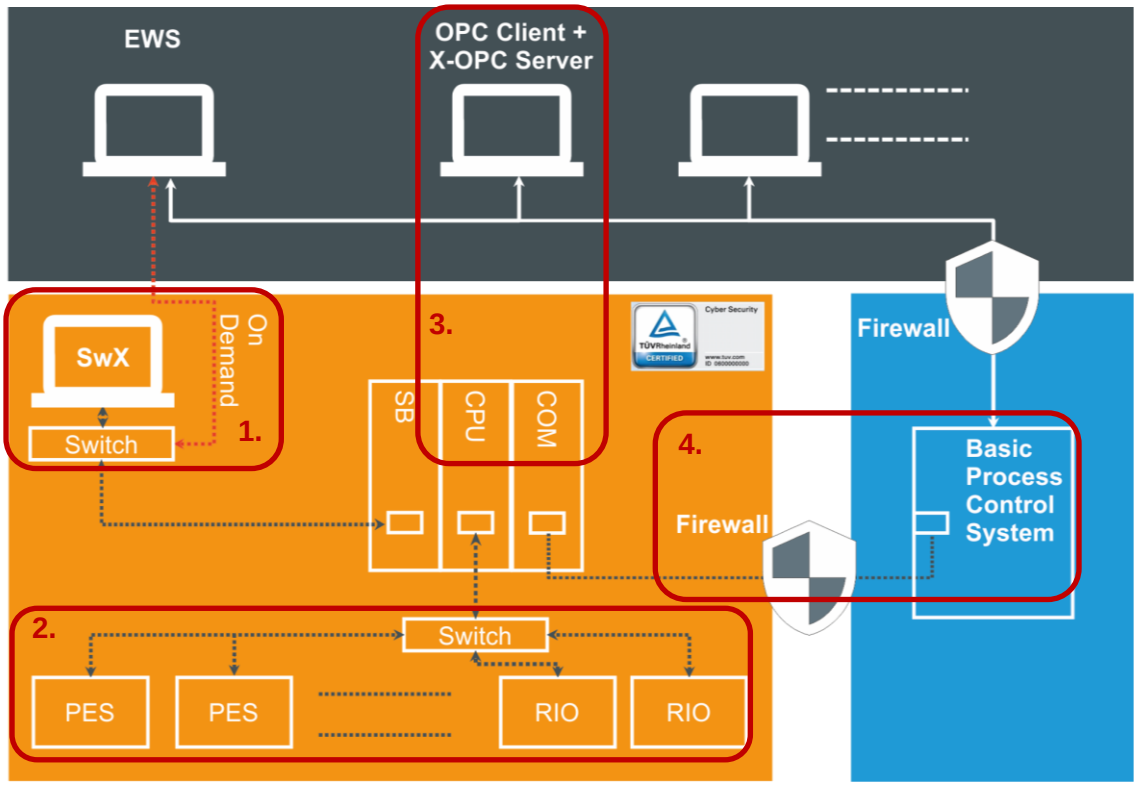


Figure 2: Overview of Safety Controller and Surrounding Systems

Explanation: A safety controller, such as HIMA PES, (nearly) always has to be viewed in the context of other systems. These mainly include

1. PADT (Windows PC with SILworX or ELOP II).
2. Connection to other safety systems (HIMA PES and RIO).
3. Connection to third-party systems, e.g., via OPC.
4. Connection to a control system (BPCS, DCS, PLS).

This overview illustrates typical use of the HIMA products which will be explained in more detail below. All information is also available in other HIMA documents. This document summarizes the information relevant to the security of all HIMA systems.

3.1 Overview of HIMA Systems

This document refers to the products contained in the current price list.

3.1.1 Relay Logic (VPS, Planar4 Systems)

The Planar4 system should be taken into consideration whenever the requirements for safety (SIL 4) and security are high. Planar4 systems become functional through their hardware wiring. This type of programming is extremely robust and **immune** to any malware.

3.1.2 HIQuad

HIQuad is a programmable system developed at a time in which security was not considered in automation technology. It is programmed with the ELOP II programming tool. The system does not have any explicit security properties. However, it features very stable operation and can be operated securely through suitable organizational and application measures. Especially the access protection is crucial (separate networks, locked cabinets, operation without connected PADT …).

i Plants equipped with HIQuad that have to comply with new security requirements should be modernized using HIQuad X systems, thus making the latest HIMA technologies available.

3.1.3 HIMatrix Remote I/Os

HIMatrix remote I/Os are non-programmable, safety input and output modules that can be connected to HIMax, HIQuad X and HIMatrix systems. The configuration must be defined in the programming tool and is adopted from the PES when it is started.

i HIMatrix remote I/Os for ELOP II Factory are in the *legacy* phase. In case of a PES upgrade, the HIMatrix remote I/Os should be modernized by updating the operating system to achieve compatibility with SILworX.

3.1.4 HIMatrix F*02

This programmable electronic system is in the *legacy* phase. If offers basic security mechanisms, such as user management. However, the system is no longer maintained.

i Plants equipped with HIMatrix ELOP II Factory that have to comply with new security requirements should be modernized using current HIMatrix SILworX systems, thus making the latest HIMA technologies available.

3.1.5 HIMax, HIQuad X, HIMatrix F*03

HIMA products help to prevent systematic faults. Their high quality supports the protection of plants also in terms of security.

Considering security aspects is an integral part of the development of these programmable electronic systems. For example, all revision states of all PES are checked for their behavior in the event of an attack.

3.2 Protective Measures

The following chapter describes functions to increase the security of HIMA systems. This evaluation encompasses the network level through the switch and controller to the programming tool (PADT, SILworX) and the connection to third-party systems.

3.2.1 Protection at Network Level

3.2.1.1 HIMatrix Remote I/Os

The remote I/Os have been developed for simple point-to-point connections. If the network load is high, the remote I/Os may reboot. For this reason, they must be protected from excessive network loadThis can be achieved by segregating the systems from potential sources of disturbances (see Chapter 0).

3.2.1.2 Ethernet Interface

A physical protection should be used to block unused Ethernet interfaces. This prevents accidental use. Physical protection is available in the form of locks with keys (e.g., from Tyco Electronics) or as plastic caps with a special tool to open them (e.g., from Panduit or Lindy).

This applies to all devices with Ethernet ports.

3.2.1.3 Ethernet Settings

1. Default Gateway

   The default gateway is 0.0.0.0. Routing is not possible.

2. ARP Aging and MAC Learning

   If *MAC Learning* is set to *Tolerant*, new addresses are learned immediately and can be easily overwritten by attackers.
   The default setting for *MAC Learning* is therefore *Conservative*. If the ARP cache already contains MAC addresses of communication partners, these are locked for 1 to 2 *ARP Aging Time* periods and cannot be replaced by other MAC addresses.

3. ICMP Mode

   The default setting is *Echo Response*. This is the preferred setting for monitoring the device for communication capability. The setting is a good compromise between ease of use and security. The setting should be changed to *No ICMP Responses* if the devices should be hidden in the network.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

i In case of a DoS attack, the PES may temporarily not respond to ARP or ICMP requests. This does not affect the PES functionality.

3.2.1.4 Network Segregation and Physical VLAN

Creating zones and the associated segregation of networks is the basis for the *defense in depth* concept. This is universally regarded as an important security concept. IEC 62443 explicitly specifies this concept. Figure 3 shows an example of a sensible zone structure. The example clearly shows that a transition from one individual zone (orange: safety, blue: control, gray: IT) to another zone is only possible at a single, explicitly defined point. These transition points are clearly defined and can therefore be protected effectively.

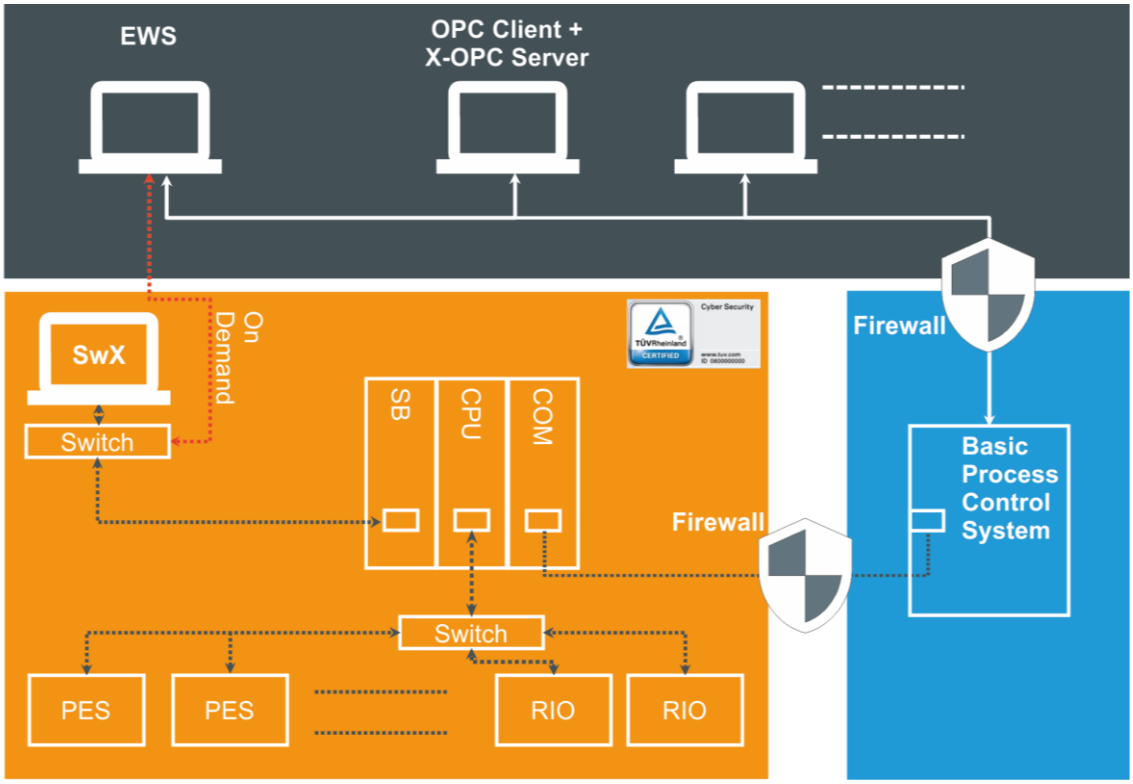


Figure 3: Example of Zone Structuring

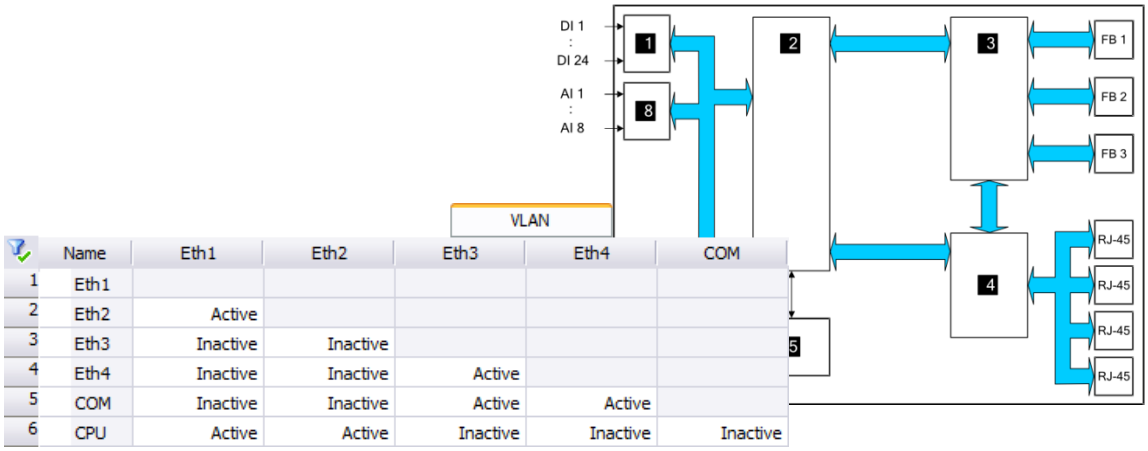
HIMax and HIQuad X: CPU and COM communicate via the backplane. COM has no direct access to the CPU. It can only read data from and write data to a COM memory. The CPU has read and write access to this memory via the system bus.

To communicate with the outside world, CPU and COM are both equipped with an Ethernet switch. These switches are completely independent from each other.

A subscriber (e.g., BPCS) that is connected to a COM module has read and write access to this COM. However, the BPCS has no access to the CPU or any devices connected to the CPU.

TIP HIMA recommends using this system property to reduce security risks. A safety network should be set up via the CPU, and a separate network for connection of non-safety components, such as the BPCS.

HIMatrix PES: HIMatrix also has an internal CPU (2) and a COM ( ). These are directly connected with one another and via the internal switch ( ).



	Name	Eth1	Eth2	Eth3	Eth4	COM
1	Eth1					
2	Eth2	Active				
3	Eth3	Inactive	Inactive			
4	Eth4	Inactive	Inactive	Active		
5	COM	Inactive	Inactive	Active	Active	
6	CPU	Active	Active	Inactive	Inactive	Inactive

Figure 4: Network Segregation in HIMatrix

The connection of each port to any other port can be configured via the VLAN settings for this switch. As illustrated in the matrix, the switch can thus be divided into 2 separate switches. This also prevents devices connected to the COM from accessing devices connected to the CPU.

TIP HIMA also recommends closing off unused HIMatrix ports.
CAUTION: If all ports are closed, the system can only be accessed again after initialization.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	-
COM	X	X	X	

TIP It is additionally possible to use infrastructure components where unused physical ports can be closed. This limits access options for unauthorized users and reduces risks.

3.2.1.5 Use of safe**ethernet**

safe**ethernet** is used for safety communication between HIMA safety systems. This should be operated in a separate network via the CPU, which is independent of the non-safety communication. In terms of security, this measure achieves effective physical segregation. If the CPU load has to be reduced further to increase availability, it is possible to use further COM(s) exclusively for safe**ethernet**.

3.2.1.6 Use of OPC

PES/SERVER connection

safe**ethernet** is also used to connect the OPC server. While the communication itself is not safe here (the PC used for running the OPC is not a safety device), the reliability of safe**ethernet** applies. To achieve segregation from the safety part, the connection should always be made via a COM. For separate zones, HIMA recommends integrating a firewall in this connection.

CLIENT/SERVER connection

In accordance with the OPC Foundation's specification, DCOM is used here. For increased protection requirements, HIMA recommends using an additional firewall here. To this end, specific firewalls are available that are able to follow DCOM communication.

3.2.1.7 System Bus Module (HIMax X-SB)

The PADT port of the module is suitable for connecting to the programming system.
All other ports (UP, DOWN and DIAG) may only be used for connecting to other HIMax X-SB. Any external influences are to be avoided. HIMA recommends the mechanical protection of unused connections. The possible line and network structure variants are described in the HIMax system manual.

3.2.1.8 Use of Non-Safety Protocols

ETHERNET

Non-safety protocols, such as Modbus TCP, should always be connected via COM. This enables segregation from the safety network.

FIELDBUS

Generally, fieldbuses can be manipulated the same way as Ethernet protocols. For increased protection requirements, HIMA also recommends considering the implementation of protection measures.

HART

When using HART, write access to parameters can be prevented. Field devices can thus be managed from a central location. Manipulating field devices is not possible in this set-up.

WARNING

Using HART handheld devices, the HART device can be reprogrammed through a direct connection, thus, e.g., changing parameters that would be required for shutdown. This can be detected in the application program, but it cannot be prevented by the control system due to the electrics. To protect end devices from this scenario, field devices themselves must be provided with write protection.

GENERAL

It is only possible to read defined read variables and to write defined write variables. Access requests to variable areas that are not explicitly defined are rejected.

It is generally sensible to check values that are written to the HIMA system by non-safety protocols, e.g.:

- If an input value is outside the reasonable limits, it could be an attempted attack.
- If a value changes a lot quicker than expected by the process, a sensor might have been reconfigured.
- If the correlation between two process parameters is no longer valid, this could be a sign of manipulation.

3.2.1.9 Remote PES Access

As a principle, remote maintenance systems should not be used in connection with safety systems.

A remote maintenance system for a safety controller should only be used in case of a justified need and after a thorough risk analysis has been carried out.

The same applies to safety communication via untrusted networks. If an insufficiently separated network or wireless link has to be overcome or even a public network (e.g., Internet) has to be used, adequate protection must be provided. This protection must at least correspond to the state of the art.

3.2.1.10 Link Layer Discovery Protocol (LLDP)

LLDP is a protocol that enables the exchange of information between neighboring devices. In HIMA products, LLDP is exclusively used for the legacy PROFINET protocol. It should otherwise be switched off (this is the default setting).

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	n.a.	X	n.a.
COM	X	n.a.	n.a.	

3.2.1.11 Mirroring

In contrast to hubs, switches forward data traffic to the destination port only. To analyze the data traffic (e.g., with Wireshark), it must be routed to a different port. *Mirroring* allows this routing. *Mirroring* is switched off in the default setting, but it can be switched on for network monitoring or troubleshooting purposes. After monitoring/troubleshooting, *Mirroring* should be reset to **Deactivated**.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	-
COM	X	X	X	

3.2.1.12 Simple Network Time Protocol (SNTP)

SNTP is a simple protocol used for transferring and synchronizing time in devices. It is applied in a client/server structure.

HIMax, HIQuad X and HIMatrix use SNTP to allow synchronization with HIMatrix remote I/Os. SNTP cannot be switched off.

HIMax, HIQuad X and HIMatrix can also perform time synchronization, e.g., with a GPS time server. The listed controllers can also be time servers themselves. Both SNTP server and SNTP client can be switched on and off. They are off in the default setting.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

3.2.1.13 Ethernet Ports Used

HIMA products are based on standard Ethernet protocols that can be used with any firewall. Safety communication via safe**ethernet** also makes use of the common Ethernet UDP framework and can therefore be allowed through or blocked by any firewall in accordance with the requirements.

	HIMax, HIQuad X, HIMatrix PES SILworX	**HIQuad ELOP II**	**HIMatrix PES ELOP II Factory**	**PADT**
HIMax HIQuad X HIMatrix PES (SILworX)	**UDP 6010**	**UDP 6010**	UDP 6010	**UDP 8000**
HIQuad	**UDP 6010**	**UDP 6005 UDP 6010 UDP 6012**		**TCP 6034**
HIMatrix PES (E2F)	UDP 6010		UDP 6010	UDP 8000
HIMatrix Remote I/O	**UDP 6010 UDP 8004 UDP 123**		UDP 6010 UDP 8001 UDP 123	**UDP 8000**
(X-)OPC Server DA	**←UDP 15138 (var) → UDP 6010**	**UDP 6005 UDP 6010 UDP 6012**	UDP 6005 UDP 6010 UDP 6012	**←UDP 25138 (var) → UDP 6010**
(X-)OPC Server A&E	**←UDP 15138 (var) → UDP 6010**	**TCP 502**		**←UDP 25138 (var) → UDP 6010**
Modbus	**TCP 502 UDP 502 (var)**	**TCP 502 TCP 8896**	TCP 502 UDP 502 (var)	
HART over IP (HIMax only)	**UDP 5094 TCP 5094 (var)**			
Send Receive	**TCP (var)**		TCP (var)	
CUT	**TCP (var) UDP (var)**		TCP (var) UDP (var)	
SNTP	**UDP (var)**		UDP (var)	
ISOfast	**UDP (var) ***			
COMeth		**UDP 6011 UDP 6031 UDP 6032**		
safe**ethernet Token**		UDP 6005 UDP 6010 UDP 6012	UDP 6005 UDP 6010 UDP 6012	
PROFINET	UDP 49152 UDP 49153 UDP 34964		UDP 49152 UDP 49153 UDP 34964	
EtherNet/IP			TCP 44818 UDP 44818 UDP 2222	

Table 1: Ethernet Ports Used by HIMA Products

Information about the table content:

- The interfaces in the matrix indicate the ports used, e.g.,
  HIMax to X-OPC uses UDP 15138, X-OPC to HIMax uses UDP 6010.
  HIMatrix PES (SILworX) to HIMatrix Remote I/O uses UDP 6010, UDP 8004 and UDP 123 in both directions.
- (var)…Ports can have a variable configuration
- Several OPC servers can run on one PC. The ports can therefore be configured. The default value is documented.
- All Ethernet-based communications require ARP.
- DCOM for data exchange between (X-)OPC Server and OPC Client requires UDP 135 or higher.
- UDP port 8001 is needed for search via MAC.

* ISOfast is only available in HIMatrix. The required UDP port can be configured freely. If ISOfast is not used, no port is opened for it.

i The matrix listed above contains a complete list of all available ports. No further services, such as DHCP, DNS, priority, FTP, etc., are offered.

i A PC with SILworX (PADT) has no specific source port, but selects it autonomously.

3.2.1.14 Firewalls Controlling the Data Traffic

HIMA (communication) is always based on standards. Standard security measures (e.g., firewalls) can thus be used. Firewalls are used to segregate (internal and external) networks and reduce data traffic to required, configured access.

The range of functions varies, and may include:

- The aim is to relieve the protected network.
- Only specific ports (protocols) may be used.
- Only the configured communication from a given subscriber to another given subscriber is permitted.
- Only responses to requests to the external network may be responded.
- Known protocols can be checked and filtered in accordance with specific rules.

Processes such as requests for unauthorized communications are usually logged as well and provided to a central management system.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

3.2.2 Integrated Protective Mechanisms

3.2.2.1 Operating System State

HIMA recommends keeping the PES operating systems up-to-date.
Redundant systems enable operating system updates during operation.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

3.2.2.2 Access Restrictions

To protect the user program, the following system variables should be used:

- *Force Deactivation*
- *Read-only in RUN*
- *Reload Deactivation*

This protection should be active in daily use. This prevents direct impact on the program and PES. HIMA recommends connecting a key switch to an input and mapping it to a system variable. A good solution is to map *Force Deactivation* to one key switch and to map *Read-only in Run* and *Reload Deactivation* to another key switch.

This applies to	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
	X	X	X	n.a.

TIP HIMA recommends using 0 V as logical 1 for the system variable. This means that the system is protected in case of a wire break.

To exclude the possibility of a "forgotten" key switch, an appropriate program should be written. The rising edge of the input signal (key switch) should trigger a timer that sets the system variables to 0 for an appropriate time (e.g., 1 working day, 8 hours). This could also be used to allocate different times to different users with different key switches.

In combination with user management, key switches help to implement the "least privilege" concept.

HIMA recommends indicating the position of the key switch in the control center (hard-wired). This allows monitoring to check if changes can be made to the safety controller.

3.2.2.3 Reading Back and Changes to Program Parts

Reload processes require the complete, original SILworX project. Only a limited circle of users should be granted access. This supports the concept of "least privilege". If an attacker gains access to the PES, it will not be possible to read out the program or reload parts of it. Both processes are not supported by the system.

3.2.2.4 PES User Management

Before the acceptance test is performed, PES passwords must be changed for the last time. Otherwise, the CRC will change. HIMA passwords are transmitted and stored encrypted. (The default setting is User: *Administrator*, Password: *Administrator*)

WARNING

Changing the passwords is essential to ensure secure operation.

Default passwords should not be used for start-up, and definitely not during operation. The optimal approach is to change passwords directly the first time contact with the PES is initiated.

The passwords required for operation should be set by the end user (see Chapter 3.2.3.10).

User accounts that are no longer required should be removed.

i If the user happens to be locked out from the PES, a new access is only possible by switching the controller (or the remote I/O) off and on again. To do so, observe the following when booting the different HIMA systems:

- HIMatrix: Actuate the reset button under the top of the enclosure.
- HIQuad X CPU: Set the mode switch on the front plate rear side to INIT.
- HIMax CPU: Set the mode switch on the front plate to INIT.

3.2.2.5 System Monitoring

System variables can be used to identify the first cycle after a download or cold start (*start cycle*) or after a reload (*reload cycle*). CRCs are mapped in variables as well.

Both can be changed by performing a reload if a suitable project is available. Monitoring projects and operations using these variables shows whether someone has modified a program since a target variable can only be overwritten at one position.

Using multitasking, an individual checksum is created for each user program.

As an additional measure, a variable incrementing at each reload process can be created in the user program. A specific system variable (*Reload Cycle*) that is active during the first cycle after a reload exists for this purpose. This variable is available to the entire system and to each individual user program.

3.2.2.6 Protecting the Operating Systems

All safety CRCs and MD5 (secure checksum) are made available in the TÜV version list. This ensures that the proper operating systems are used after the download.

3.2.3 Protection When Connecting the PC for Programming

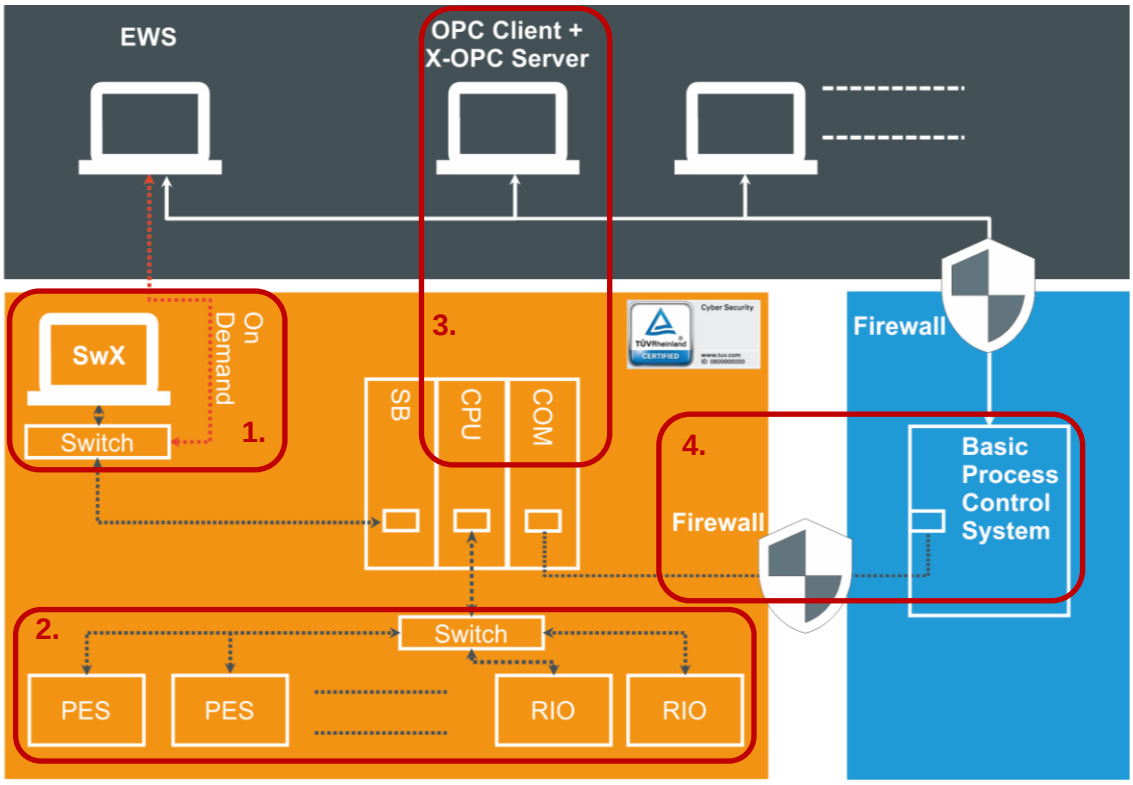


Figure 5: PADT on the Safety Controller

No. 1 in this overview.

3.2.3.1 Installation (SILworX)

The MD5 checksum of the installation file (setup.exe) is included in the HIMA DVD in the same directory as the installation file, and it is also documented in the TÜV version list. This ensures use of the correct installation version.

Depending on the individual installation, the user can create a cryptographic checksum. To detect modifications to the SILworX installation, this checksum can be evaluated on a regular basis. Alternatively, this can also be performed automatically using an application whitelisting program (see Chapter 3.2.5.6).

3.2.3.2 SILworX PADT

When developing SILworX, strict attention was paid to remaining as independent as possible of the Windows operating system.

In particular, this means that the safety of the user programs created with SILworX does NOT depend on the Windows operating system used or is not influenced by it.

Update cycles for HIMA software are subject to time constraints due to the required TÜV certifications. This does not make it possible to follow the ever-shorter Windows operating system cycles and to test all Windows versions, variants and combinations of hardware and software. HIMA has had very positive experience with Windows updates. All service and engineering employees work with current Windows operating systems and thus test HIMA software in a real environment. Simple tests suffice to confirm proper function in the individual environment:

1. Perform installation (if not yet performed).
2. Activate the license (if not yet activated).
3. Open the online help.
4. Create or open a project.
5. Generate code (in the test project!).
6. Establish the connection to the controller.

HIMA recommends only using the PADT PC to program and maintain the safety system.

If an OPC server is used, it should be operated on a different PC.

TIP HIMA PES are standalone systems. HIMA strongly recommends operating them with no PADT connected. The PADT should only be connected if it is truly required, e.g., for start-up or maintenance.

3.2.3.3 User Management in SILworX

The offered user management scheme should be used to protect SILworX projects and the access to the PES.

WARNING

Setting passwords is essential to ensure secure operation.

The optimal approach is to set up user management directly when creating a project.

The passwords required for operation should be set by the end user (see Chapter 3.2.3.10).

i Only one SILworX can have write access to a HIMA PES, independently of user rights. Any other SILworX connecting to the PES only has read access.

SILworX passwords can be changed by the security manager at any time without affecting the project in the controller or the checksums. These passwords should be changed in accordance with individual password guidelines, but at the latest when an employee leaves the company.

SILworX projects can be protected with a password for opening in SILworX. For higher security requirements, the project file (*.e3) can be cryptographically encrypted with a suitable tool (e.g., veracrypt).

Encryption of the project file is not only important for know-how protection. HIMA PES can receive a new user program during operation, without stopping. This process is called "reload". A program that is loaded into the controller by performing a reload has to be based on the version currently in use on the controller. If the previous version is not available, the reload cannot be performed. The controller then has to be stopped, which can be determined during operation if the system is monitored.

3.2.3.4 Backup Recovery Strategy

SILworX are stored in databases (one file per project). When possible, a backup of this project file should be created. It is also possible to automatically save a copy of the project at every download process.

In addition to the project file, HIMA recommends storing the SILworX and OPC installation, as well as all the operating systems used for the controllers.

If PCs are delivered by HIMA as part of a project, they also contain recovery CD, SILworX and the project as delivered by HIMA.

i Complete backups should be stored in a safe place (safe from fire, water, unauthorized access). Access to these backups should be quick and easy in case of an emergency.

3.2.3.5 SILworX Code Comparator

SILworX also includes a code comparator which compares two project versions and shows the differences. It is important to ensure that only deliberate changes were made when a new user program was loaded.

3.2.3.6 Know-How Protection

To ensure know-how protection, HIMA recommends locking the relevant function blocks. SILworX supports two types of protective measures:

1. Function blocks can be protected against modification (*Read-only* in the properties).
2. Access to function blocks can be completely blocked (*Know-How Protection* in the properties)

WARNING

When using know-how protection, it is no longer possible to access this function block. Even HIMA cannot use this code to create a function block that can be read. Any later modifications are impossible. The user must therefore ensure that a backup of the function block is created before protection is applied.

3.2.3.7 Preferred PADT Connection

The choice to connect to a PADT (PC with SILworX programming tool) must be made systematically. Depending on the overall constellation, the following order applies:

HIMax	HIQuad X and HIMatrix
A PADT port of an X-SB which is not *Responsible*.	Ethernet port of a COM
Ethernet port of a COM	Ethernet port of a CPU
Ethernet port of a CPU	
A PADT port of an X-SB which is *Responsible*.	

Table 2: Priority When Connecting a PADT

For HIMatrix segregation, VLAN should be set in accordance with Chapter 0.

i The PADT should be located in the same security zone as the PES.

3.2.3.8 Diagnosis in SILworX

SILworX allows users to read diagnostic information from within the controller. This information cannot be deleted by the PES. Information such as PES login or changes to the safety-related parameters, are therefore permanently available. For traceability purposes, this information is provided with a timestamp.

3.2.3.9 Remote Access to the PADT

Remote access to the PADT corresponds to direct access to the PES and has to be avoided (see Chapter 3.2.1.9).

3.2.3.10 Passwords

Generally, suitable passwords are to be used. They are composed of more than 12 characters and contain numbers, special characters, capital and lowercase letters.
Individual passwords have to be allocated to segregate roles.

HIMA recommends using a password manager to manage a multitude of passwords.

3.2.4 Protection When Connecting the OPC Server

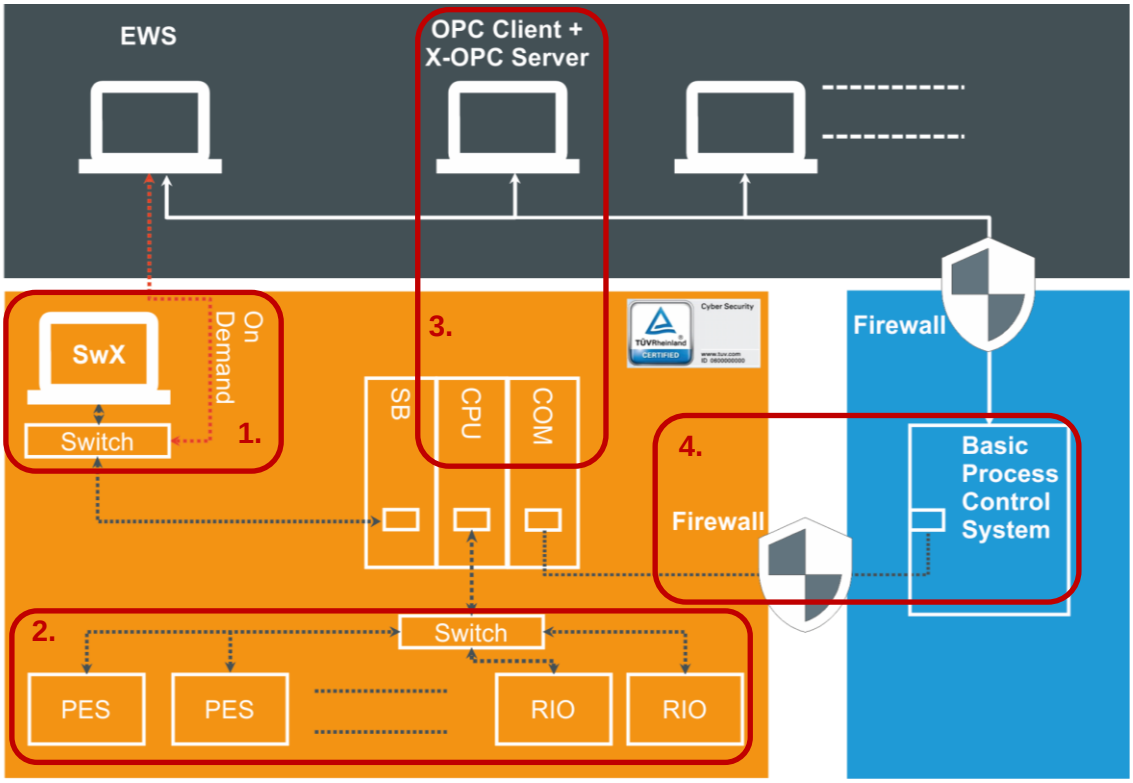


Figure 6: OPC Server on the Safety Controller

No. 3 or No. 4 in this overview, depending on where the OPC server runs.

The MD5 checksum of the installation file (setup.exe) is included in the HIMA DVD in the same directory as the installation file, and it is documented in the TÜV version list. This ensures use of the correct installation version.

The X-OPC Server for systems programmed with SILworX (HIMax, HIQuad X and HIMatrix) runs as a service. This has the advantage that the X-OPC Server is active, even if no user is logged in. Even changes can be performed using SILworX, without having to log in to Windows.

For increased protection requirements, HIMA recommends using an additional firewall between the X-OPC server and the HIMA PES that only serves to open the required ports for this communication.

TIP The PC used for the OPC server should not be used as a programming station. This way, the programming station can usually be switched off, which reduces the possibility of attacks due to the limited time of use alone. Additionally, the OPC is typically connected to a parent network with increased risk.

3.2.5 Configuration of PCs

HIMA offers a hardened PC, which corresponds to the current state of the art for protection.

This chapter provides information on how to configure a secure PC. Experience shows that Windows systems are rarely exactly the same. Only the typical features can therefore be described.

In automation technology, PCs do not typically change during operation. No additional software must be installed. If so, this is seldom the case. Additionally, regular updates are assumed to be very difficult. Daily updates of virus signatures can be taken into account in the rarest cases. HIMA recommends setting up a multi-stage protection concept, see Chapter 2.3.2.

- BIOS password protection.
- Interface protection.
- Reduction of Windows rights to the minimum requirements.
- Reduction of the number of programs to a minimum.
- Use of protection software.
- Project protection.
- Recovery strategy.

3.2.5.1 BIOS Settings

If possible, BIOS passwords should be used.

The boot sequence must be set so that first the internal hard disk is used and then all other media.

If allowed by the workflow, all unneeded interfaces, such as wireless, USB or FireWire, must be switched off in the BIOS.

3.2.5.2 Interface Protection

The interfaces cannot be switched off in the BIOS, they must be closed in the operating system through suitable measures.

The Windows firewall must be activated to protect the interfaces. Windows must be locked so that access to external media is only allowed with administrator rights. Before allowing connection, the administrator must check all media using a current virus scanner.

USB interfaces must be switched off in the BIOS or be software-protected. USB blockers, which only allow access to approved USB devices, may be used.

3.2.5.3 Reducing Rights (Least Privilege)

A basic security principle is to reduce the attack surface as far as possible. The rights provided by Windows must be reduced to a minimum.

Since SILworX V4.X, softlocks or hardlocks can be used. Administrator rights are only required for installation. HIMA recommends using Windows with user rights in everyday use.

Generally, any software can represent a flaw that may be used as a gateway into the system. For reasons of security, no additional software should be installed on the PC in use. HIMA does not prohibit the installation of other software, but cannot make any statement on its behavior, in particular in terms of security.

Further protection of Windows PCs can be adjusted to individual needs. It is possible, for example, to disable all USB ports on the PC, operate SILworX with a softlock and use PS2 mouse and keyboard. HIMA recommends setting up and activating time-controlled screensavers and the Windows firewall.

CAUTION

Windows firewall settings can be affected by the installation of patches. Protection may be impaired as a result. Firewall settings have to be checked after a patch or an update.

Windows screensavers with password can be used as additional protection. Depending on the individual needs, the employees should be instructed to lock their PCs when leaving (shortcut: Windows+L) or even to exit the project.

Password administration of the active domain (AD) can principally be used for access to the PC. However, SILworX cannot be linked to the AD. In addition, an AD in the security zone only makes sense in terms of safety in exceptional cases.

3.2.5.4 Patches

HIMA software is a platform-independent development. However, HIMA software cannot be tested on all platforms with any type of third-party software and combinations.

Additionally, regular (offline) updates (patches) are required for most protection products (antivirus software). This can cause the platform to change and thus the system to modify its behavior (e.g., resulting in decreased speed or blocked functions).

At present, all known protection programs can be used (e.g., antivirus software).

HIMA recommends performing (offline) updates in non-critical situations as patches and signatures can always result in changed behavior. Interactions in terms of availability cannot be completely excluded.

HIMA engineering department and service always use the latest patches and signatures.

Despite of all protective measures, the necessity for connecting to the Internet should be carefully considered. If a PC was connected to the Internet, HIMA recommends performing a complete virus scan.

i Safety is not affected by patches and new signatures.

3.2.5.5 Antivirus Software

HIMA recommends using protection software in PCs in accordance with the customer-specific security policy. The use of antivirus software is common here, which can detect known malware using signatures and heuristics.

TIP HIMA does not specify any special antivirus software. There should be no direct Internet access in the direct safety environment. It must therefore be ensured that an offline update of signatures is possible (e.g., via CD).

3.2.5.6 Application Whitelisting

Some HIMA customers are already successfully using application whitelisting (AWL).

Especially in environments where updates are difficult to implement, not advisable or not possible at all, alternatives or additional options to popular antivirus software should be considered. In addition to access restrictions within the operating system, application whitelisting can provide the required protection.

Application whitelisting is now recognized as equivalent to antivirus software.

3.2.5.7 General Information on Protecting PCs

Protecting a Windows PC

The following sources provide some descriptions of how to protect Windows 7 (articles in German):

- BSI, Anleitung zur Installation und Minimierung eines Arbeitsplatz-PCs mit Windows 7:
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-client-Anleitung_Windows-7.pdf?__blob=publicationFile
- c't 2011/Issue 3, *Der öffentliche PC*:
  http://www.heise.de/artikel-archiv/ct/2011/03/114_Der-oeffentliche-PC

Protecting a Windows 10 PC

The following sources provide some descriptions of how to protect Windows 10 (articles in German):

- BSI, IT-Grundschutz:
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_2_3_Clients_unter_Windows_10.html

3.2.6 Further Protective Measures

HIMA systems mostly use standard technologies and can be protected with standard measures of your choice. In addition to hazard avoidance, hazard identification is an important step against malware. This includes the development of an action plan defining which action should be taken after a hazard.

- Honeypots can be useful, are relatively easy to use and provide good detection rates. In this context, secXtreme provides an industrial solution called honeyBox.
- The use of intrusion detection and intrusion prevention systems can be very useful, but it currently requires expertise in this field.

3.2.7 Tests by an Independent Authority

HIMA systems must meet high quality standards to ensure compliance with the safety requirements. The high-quality implementations result in increased stability and, consequently, in lower vulnerability to cyberattacks. This has been since proven several times over since the first HIMax Achilles certificate in 2009.

A basic principle is that only planned functions are implemented, i.e., no backdoors. This can be verified by the TÜV during the security certification process.

Exemplary certification according to IEC 62443-4-1 and IEC 62443-4-2 for SL1 was carried out for HIMax and HIMatrix F35 03. Corresponding development processes and functionalities have therefore been taken into account in the product.

4 Further Information

4.1 HIMA Information

With security topics in particular, it is important to stay up to date with the latest information. HIMA recommends registering with DIS, HIMA's Document Info Service. The DIS will inform you about new documentation (including new versions of this manual) at the desired intervals. For registration, go to: https://www.hima.com/en/downloads/

4.2 External Information Sources

The following contains a list of standards and possible sources of information on the topic of security. Due to ongoing dynamic changes, different local conditions and the variety of applications, this should be understood as a basis for further research.

- **IEC 27000 and higher** *Information technology — Security techniques*:
  This is the generic international standard for office IT. It describes an ISMS (information security management system). Sector-specific extensions are being developed. One example is ISO 27019 which was published in 2013 for the energy industry.
- **IEC 62443 family**: In close cooperation with the ISA 99 (mainly driven by the United States), the IEC 62443 is intended as an international standard (currently 13 parts).
- **IEC 63074** *Security aspects related to functional safety of safety-related control systems*
  IEC TR 63069 *Industrial-process measurement, control and automation-framework for functional safety and security*
  These describe the interaction of safety and security.
- **VDI/VDE 2182**: *IT security for industrial automation*
  The GMA technical committee has developed these guidelines. The first part presents a generic procedural model. The following 3 sheets with 2 parts each are sample sheets for different scopes. From the perspective of manufacturers, integrators and end users, the directive is applied in process and factory automation. Sheet 4 is currently being prepared and represents a "roadmap".
- **NAMUR** has released Namur Worksheet NA 163 *Security Risk Assessment of SIS* on the assessment of safety systems.
- The **BSI** has been active in the field of industrial IT security since 2013. Several documents have been published and can be downloaded from the BSI website.
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/international.html
- The Department of Homeland Security and NIST are very active and offer a range of excellent documents for download free of charge, e.g., *Seven Steps to Effectively Defend Industrial Control Systems*.

A complete list would be far too extensive.
Such a list is maintained here: https://www.security-standards.de/ITSecurityGrid.html.

Appendix

Glossary

Term	Description
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses
AWL	Application whitelisting
BPCS	Basic process control system
BSI	Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security
COM	Communication module
CRC	Cyclic redundancy check
CVSS	Common vulnerability scoring system, industry standard for describing the severity of vulnerabilities in computer systems
DCS	Distributed control system, process control system
DCS	Distributed control system
DMZ	Demilitarized zone
DoS	Denial of service
EN	European standard
EWS	Engineering workstation (see also: PADT)
FAT	Factory acceptance test, functional testing of an installation at the manufacturer's site
ICMP	Internet control message protocol, network protocol for status or error messages
ICS	Industrial control system, automation system
IDS	Intrusion detection system, system for detecting attacks
IEC	International Electrotechnical Commission, standards committee for electrotechnologies
IP	Internet protocol
ISMS	Information security management system
IT	Information technology
LLDP	Link layer discovery protocol
MAC Address	Media access control address, hardware address of one network connection
NAT	Network address translation, generic term for procedures that automatically replace address information in data packets to connect different networks. It is typically used in routers.
OPC	OLE for process control, standard for data and information exchange of software components
OT	Operational technology
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX or ELOP II Factory
PES	Programmable electronic system
RIO	Remote I/O (extension unit with inputs and outputs)
SIEM	Security information and event management
SIL	Safety integrity level (in accordance with IEC 61508)
SNTP	Simple network time protocol (RFC 1769)
SQL	Structured query language, database language
SwX	SILworX (see also: PADT)
TCP	Transmission control protocol
UDP	User datagram protocol
VPS	Relay logic
XSS	Cross-site scripting

Index of Figures

Figure 1: PDCA Cycle 10
Figure 2: Overview of Safety Controller and Surrounding Systems 12
Figure 3: Example of Zone Structuring 15
Figure 4: Network Segregation in HIMatrix 16
Figure 5: PADT on the Safety Controller 22
Figure 6: OPC Server on the Safety Controller 26

Index of Tables

Table 1: Ethernet Ports Used by HIMA Products 19
Table 2: Priority When Connecting a PADT 25

MANUAL
Automation Security
HI 801 373 E

For further information, please contact:

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone +49 6202 709-0
Fax +49 6202 709-107
E-mail security@hima.com

Learn more about HIMA solutions online:

www.hima.com/en/industries-solutions/cybersecurity/

www.hima.com