[Automation System XY]

Note to the editor: Please check if you are using the latest version of this document (refer to BASF Technical Rules). Please insert the description of the automation system to be purchased in the headline above, change the document file name and update the footnote accordingly.

Contents

1 Purpose

This document describes general requirements regarding automation security (also referred to as “OT–security”) for process automation systems. Typically, this document is part of a user requirement specification (URS) that serves to specify the properties of a process automation system that a customer wants to purchase from a vendor. Since this document is general, project-specific URS documents supersede this document if requirements are conflicting.

BASF is aware that security of the production plants is important regarding availability, confidentiality and integrity of automation systems. This document defines general cyber security requirements, taking into account the security requirements set forth in G-R-OT 860 M as well as recommendations described in G-P-EI 860, 861, 862 and 863.

The following objectives are key for all automation systems. It must be checked if appropriate measures are implemented protecting:

- Availability (highest priority)
- Data integrity (subordinate priority)
- Confidentiality of created, processed and stored data (subordinate priority)

of the automation system. Please note that this document only describes requirements that are not covered by the BASF information protection requirements, which apply as well. Internal regulations regarding information protection are covered by other internal documents.

The requirements described in this document are categorized as follows:

- **Network** (Section 2) is dealing with the network architecture and the network device management of the automation system.
- **System Hardening** (Section 3) describes the requirements how an automation system should be modified to reduce the attack surface of the system.
- **Malware Prevention** (Section 4) gives security measures for the protection against viruses and other software threats.
- **Backup and Restore** (Section 5) introduces concepts for automation systems necessary for disaster recovery.
- **Remote Access** (Section 6) describes procedures for BASF and external staff to improve the response time of service personnel.
- **Others** (Section 7) includes topics not covered by the previous chapters.
- **Organizational** (Section 8) deals with non-technical requirements.

This document may be used for all types of automation systems. However, common types of automation systems are individually addressed:

- D – Distributed Control Systems (DCS)
  This category refers to computerized control systems for the process industry. It includes all components beginning with sensors at the field level up to the operator supervisory control and supporting systems.
- U – Package Units (Unit)
  This category refers to all systems related to the production process which are provided off the shelf by the unit vendor. These may be dosing systems, packaging machines, analysis equipment etc.
- S – Safety Instrumented Systems (SIS)
  A safety instrumented system consists of an engineered set of hardware and software controls which ensure safety integrity of the production process at all times. An exact definition is given in the G-P-EI 201 M.
- V – Vertical Integration (VI) System
  VI systems are linking process control systems, such as DCS, Scada and other automation systems, and business applications, such as ERP systems. VI solutions typically ensure data connectivity (including data processing, archiving and analyzing), take coordinative action between connected systems and provide interfaces for user interaction. VI solutions are considered Level 3 applications and can be hosted either centrally (data center) or locally (on premise).

The applicability for each of the above–mentioned systems is marked on the right side of the page using the abbreviations D for DCS, U for Unit, S for SIS and V for VI system as shown below. The character in the table marks the relevance for the system type of the respective column. Mandatory measures are marked **M**, recommended measures are marked **R**. Measures which are not applicable are marked by a hyphen (**–**).

Example:

		D	U	S	V
1)	Mandatory measure for DCS which shall be implemented.	M			
2)	Recommended measure for Units which should be implemented.		R		
3)	Measure is not applicable for SIS and cannot be implemented.			–	

All measures must ultimately form a comprehensive security concept that protects the automation system. If a mandatory measure (M) cannot be met for technical reasons, compensating controls may still fulfil the protection goal. In this case, an individual review of the security concept by the gETAS is required.

Note to the editor: All requirements that are preselected as mandatory (M) in this document are derived from mandatory statements in G-R-OT 860 M. In particular, they are mandatory for all BASF plants that are subject to “BSI-Gesetz”. If you delete or make any change to such requirements in this document (e.g., due to project-specific reasons) the obligation to demonstrate compliance to G-R-OT 860 M (and BSI-Gesetz, if applicable) remains with the system owner. Additional requirements or changes that increase the measures to meet the mandatory requirements are not affected by the aforementioned disclaimer.

2 Network Security

This section describes the minimum requirements for a secure network architecture. Additional controls may be implemented by the vendor and should include a proper description.

2.1 Network Topology

The BASF Network Design Concept is followed.

		D	U	S	V
1)	Direct communication between two devices which are more than one security level away is not allowed. E.g., a device located at L2 is only able to communicate with a device located at the same level or an adjacent level. In particular, the aforementioned requirements imply that connections to public networks like the internet are prohibited (e.g., mobile connections for maintenance).	M	M	M	M
2)	Network segmentation into different levels is done by BASF firewalls. If the automation system consists of components located at different levels (e.g., server in L3 and client in L2), then a list of network protocols and ports must be provided, so that BASF can implement the according firewall rules, which follow a strict whitelisting approach.	M	M	M	M
3)	Network segmentation at the same level into zones must be performed where feasible. At level 1 and 2, the necessary firewall or router is to be provided by the vendor.	M	M	M	M
4)	For SIS, a clear zone concept (e.g., as introduced by NA 163) is presented. Network connections from and to an SIS (zone A) or related components (zone B) to other components (“peripherals” as per NA 163) shall be limited to the absolute minimum.	–	–	M	–
5)	The core SIS (logic solver, actuators, sensors) continues to operate as designed even if all connections or data exchange with its environment or peripherals become unavailable.	–	–	M	–
6)	Data and signal connections are appropriately secured (e.g., encrypted, monitored, physically protected).	R	R	M	R
7)	Unused network interfaces (Ethernet, Wi-Fi, Bluetooth, etc.) are logically disabled or physically blocked.	R	R	R	R

More detailed recommendations are specified in G-P-EI 861. If cloud services are part of the automation system, the G-P-EI 861 is to be consulted and the security concept to be aligned with the customer.

2.2 Network Device Management

As the ethernet network of a DCS system consists of several devices such as switches and firewalls, for each device the security measures regarding network device management need to be defined. Therefore, a network management solution has to be implemented.

	D	U	S	V
1) Capability of network infrastructure components (e.g., routers, firewalls, switches) to report their status to a central system (e.g., using SNMP, Syslog).	M	M	M	M
2) The configurational interface is protected.	M	M	M	M
3) It should be possible to configure a secure password as well as session timeouts	R	R	R	R
4) A central management for administrative users is in place (e.g., RADIUS authentication).	R	R	R	R

2.3 Network Monitoring / Alarming

Automation networks are a critical part of the whole automation system. Therefore, it is necessary to monitor the behavior of the network. The vendor should provide a solution which covers the following.

	D	U	S	V
1) Detection of topology changes due to new devices connected to the network or lost connections to previously connected devices is implemented.	R	R	R	R
2) Visualization of device status are possible at least for switches and routers. The status includes operational state (OK/NOK) and can include additional information (MAC- and IP-address, firmware version).	R	R	R	R

2.4 Virtualization

For improved hardware resource utilization and easier management, virtualization is a common method. If the vendor employs virtualized systems of any kind, the following requirements on the separation of network levels must be fulfilled.

	D	U	S	V
1) The installation of virtual systems belonging to different levels on one physical hardware is not allowed.	M	M	M	M
2) Management interface is separated in dedicated zones on the same level. 1) The vendor must implement an audit trail, named accounts and strong authentication for privileged access. 2) The patch management process (see Section 3.5) must include all systems. This includes also all virtual systems and host systems. 3) For virtual clients, all appropriate security requirements must be applied	M	M	R	M

3 System Hardening

All devices within an automation system need to be hardened to increase their cyber resilience. This means that all unnecessary functions must be disabled and available build in security measures must be enabled if applicable. In order to ensure consistency throughout different installations, hardening shall be implemented according to a hardening guideline or templates (e.g., group policy objects).

3.1 Deactivation of Unused Services and Functions

Services of devices which are not needed for the proper function of the automation system are a possible thread for the system. To reduce possible weak spots the number of services and software on devices should be kept to a minimum.

		D	U	S	V
1)	Standard software which is not necessarily needed (e.g., Microsoft games on computers) is uninstalled.	M	M	M	M
2)	Services which are not needed for proper functionality (e.g., webserver on controller, telnet on network switch, printer interface, file share functions) are deactivated.	M	M	M	M
3)	Functions and programs relevant to the security of the automation system which cannot be disabled are documented. Legacy and settings for downwards compatibility (e.g., SMB V1, CIFS Null-Sessions, weak cipher suites) must be avoided	R	R	M	R
4)	Measures are in place to manage Security Policies on end point devices (as described in G-P-EI 862).	R	R	R	R

3.2 Removable Media Controls

For a secure use of portable media, the following measures have to be in place.

		D	U	S	V
1)	Unused USB ports, CD/DVD drives are disabled or physically locked.	M	M	M	M
2)	Autorun is disabled on all stations, i.e. programs on removable media are not automatically executed.	M	M	M	M
3)	Ports for keyboard, mouse and other necessary peripherals are configured that only authorized devices can be used.	M	R	R	M
4)	Devices which allow usage of portable media have malware protection enabled (see also Section 4).	M	M	M	M
5)	A technical solution (quarantine station) regulates the data transfer from and to the system	R	R	R	R

3.3 Physical Access Control

The physical access to automation systems must be restricted to authorized personal. Therefore, the following requirements have to be covered.

		D	U	S	V
1)	Cabinets which are not located in an area with restricted access (e.g., control room) are lockable by an internal keylock or a padlock. The lock does not accept standard keys but requires unique keys.	M	M	M	M
2)	Unused ports of network devices are disabled or physically locked.	R	R	R	R

3.4 Identity, Access and Account Management

Automation systems offer different ways of access control.

For the segregation of duties and a consistent management of rights a management solution for users and accounts is a precondition. The following requirements must be covered.

		D	U	S	V
1)	Hardcoded passwords for any device or account are not allowed.	M	M	M	M
2)	Default users, accounts and passwords are changed at least after the implementation of the automation system.	M	M	M	M
3)	A password consists of a minimum length of eight characters, including at least i) one upper case letter, ii) one lower case letter, iii) one digit. Passwords must not be visible upon typing.	R	R	R	R
4)	Management of accounts and passwords is possible by BASF. Any possible exception must be approved upfront by BASF.	M	M	M	M
5)	Access controls are based on defined roles. Where feasible, personal accounts are used instead of functional accounts.	M	M	R	M
6)	The vendor must implement and document a role-based authorization concept following the BASF requirements on Identity and Access Management.	R	R	R	R
7)	Additional access control functions (e.g., ACL–-lists) are implemented.	R	R	R	R
8)	Technical measures support the implementation of Segregation of Duties (SoD), i.e., responsibilities for managing similar tasks must not be overlapping or shared. Different responsibilities must be established e.g., for access -requests, -authorization, and administration.	R	R	R	R
9)	The vendor sets a BIOS password in accordance with the BASF password policy.	R	R	R	R
10)	Unused accounts must be deactivated upon delivery of the system (e.g., Test accounts, etc.) Systemwide (e.g., Unit, DCS, SIS) management of users accounts is implemented at least for the operator and engineering stations.	M	R	–	M
11)	Accounts and users which are able to change variables require at least a single factor authentication (e.g., password, RFID-card).	M	M	M	M
12)	Accounts and users which are able to change programs or screens require a two-factor authentication (e.g., Smartcard + PIN).	R	R	R	R
13)	Authentication attempts (successful or not) are logged for Windows machines.	M	M	M	M
14)	Authentication attempts (successful or not) are logged for controllers and embedded devices.	R	R	R	R
15)	Technical means are provided that support a password policy.	R	R	R	R
16)	Accounts with configurational access are locked automatically after 5-15 min inactivity.	M	M	M	M
17)	Accounts and passwords that exist already when the system is installed, least-privilege and need-to-know should be followed as far as possible.	R	R	R	R
18)	Automatically started applications (e.g., user interface of an operator station) must run with restricted user rights. Please refer to E-P-EI 401 0701, Section 2.8.	R	R	R	R

Please refer G-P-EI 862 and G-P-EI 863 for detailed Information.

3.5 Patch Management Solution

Automation systems cannot be handled like IT-systems. While there are major differences between IT and OT systems, updates and patches reduce the attack surface by closing known vulnerabilities. To ensure the handling of updates the Vendor has to provide a procedure for updates and patches.

		D	U	S	V
1)	All software (BIOS/UEFI, firmware, operating system, applications, etc.) should be system-tested and up-to-date when the system is installed.	M	R	M	M
2)	Patches and Updates include operating System, the vendor software and installed 3rd party software (examples: Java, PDF viewer, Office suite).	M	R	R	M
3)	Vendor provides updates and patches during the entire life-cycle of the product A description on how patches (both OS and software) are assessed (criticality), tested, delivered and installed is provided.	R	R	R	R
4)	Installation of patches is not done automatically. Vendor provides a managed patch process which is used for easy deployment and reporting (e.g., WSUS concept, approved update bundles provided by the vendor for installation via removable media).	M	R	M	M

4 Malware Prevention

Due to the need of data transfer from and to automation systems it is necessary to implement measures for protection against malware such as viruses or trojans. The vendor should provide or at least recommend a solution dealing with this.

4.1 Anti-Virus Solution

The antivirus solution refers to the application installed on all computer devices of the automation system to protect them against malicious software.

		D	U	S	V
1)	Antivirus Software must be installed on critical stations. Stations which are used for file transfers and the engineering/maintenance are defined as critical.	M	M	M	M
2)	The vendor provides or recommends an antivirus solution which is system-tested (antivirus software does not interfere with the operation of the plant) and compliant to the vendors software and systems. Also, a user manual (e.g., on access scanning, heuristics) is provided to the customer.	M	M	M	M
3)	A solution how the customer makes sure that noncritical stations without AV are protected is provided (e.g., whitelisting and/or data execution prevention).	M	M	M	M
4)	The vendor describes how to test, qualify and roll out AV signatures. Virus signatures have to be up-to-date.	M	M	M	M
5)	Technical measures for alarming responsible persons when a virus is detected are to be implemented.	M	M	M	M
6)	Where it is not possible to install an AV-solution, an application whitelisting solution alternatively is recommended	R	R	R	R

4.2 Security Monitoring

If necessary, please refer to the following document “URS_Security_Monitoring”.

4.3 Handling of Data Transfers

A methodology to verify integrity of media before use in an automation system is necessary to ensure security measures are not bypassed. Besides organizational measures (e.g., standard operating procedures by BASF) the automation security concept of the vendor shall offer a technical solution for secure data exchange. If the transfer of data from and to the automation system is necessary, the following requirements have to be covered.

	D	U	S	V
1) Technical measures are in place to handle the usage of removable media at the plant. This measure can be a single point of entry to the automation system with an antivirus software and distribution platform inside the system (e.g., fileserver).	M	M	M	M
2) Portable media that are used in an automation system shall be exclusively used for this purpose. The devices have to be labeled accordingly and encrypted if confidentiality needs to be enforced.	R	R	R	R
3) The transfer of a new application program on the controller or logic solver is physically protected, e.g., with a key switch.	R	R	M	R

5 Backup and Restore

More information on how an advanced backup solution may be designed can be found in the G-P-EI 850.

6 Remote Access

More information on how using Remote Access can be found in the G-P-EI 864.

7 Others

Additional topics not handled before are to be found at this section.

7.1 Dedicated Use of Components

Regarding Safety Instrumented Systems (SIS) a dedicated use of equipment is required. See G-P-EI 201 M for more SIS specific details.

	D	U	S	V
1) The automation system components are used solely for the intended purposes, e.g., an SIS engineering station may only be used for configuring and engineering the SIS.	–	–	M	–
2) Engineering stations are connected to the respective automation network they belong to (e.g., safety network). They are never connected to any other network, not even temporarily.	–	–	M	–

7.2 Event Logging / Event Management

Events are signals which support the security management of an automation system and help to analyze incidents. The event message should be clear, easy to understand and should guide the user towards appropriate actions. Regarding event logging the following requirements must be covered.

		D	U	S	V
1)	All security-related hard- and software creates logfiles. A centralized solution (e.g., syslog server) is preferred. Logging best practices (which event types should be logged) for Windows systems are provided in the BASF hardening guideline (G-P-EI 863).	M	M	M	M
2)	The logfiles (at least Application, Setup, System, and Security event logs) must be stored for at least 90 days (under consideration of data protection regulations). Automated retention period (90days) must be ensured.	R	R	R	R
3)	Capability to actively notify security events (e.g., virus found, network topology change, anomalies of authentication attempts, IDS system detection, etc.) e.g., via E-Mail or event forwarding to a SIEM	R	R	R	M

7.3 Interface to BASF security solutions

For a holistic approach, it should be possible to integrate the vendor concept into the automation security landscape of BASF. One part of this landscape is BASF SIEM (security incident and event management).

		D	U	S	V
1)	The automation system provides the possibility to use the logfiles and events for analyzing behavior and activities at the global SIEM system. The SIEM is provided by BASF.	R	R	R	R
2)	The vendor describes the according IP addresses, ports and protocols for collecting the data.	R	R	R	R

The related firewall rules to allow the communication from the automation system to the SIEM will be implemented by BASF.

7.4 Mobile Solution

If the vendor provides a solution for a mobile DCS-/SCADA-Client on a BASF-Internal device (connected to an Automation - WLAN) or an external device (connected over public mobile network) the following requirements shall be covered.

		D	U	S	V
1)	Mobile devices are configured the way not to connect to unknown or untrusted networks.	M	M	–	M
2)	Wireless networks are separated to other networks by a firewall	M	M	–	M
3)	Mobile devices are encrypted to protect the data stored on the device.	M	M	–	M
4)	A device and user management are in place.	M	M	–	M
5)	In wireless networks all connections are authenticated and encrypted (e.g., WPA2). End to end encryption is implemented.	M	M	–	M
6)	Use of Wireless frequencies is authorized by the local responsible BASF employee for frequency management.	M	M	–	M
7)	Use of wireless devices follows Best Practices for Wireless Security.	R	R	-	R

7.5 Additional services

If a vendor offers security services that provide added value to BASF, they should be described.

Possible examples are:

- Detailed risk assessments
- On-demand remote support
- Cyber security monitoring services and cyber forensics
- Specific trainings

7.6 Scalability

Because of the variety of systems and the different complexities it is necessary to be able to adjust an automation security concept to special requirements in a single automation system. So, the concept can be adopted to huge plants or small sites with minor changes. Vendors should show possibilities how their concepts can be scaled up or down to the size of the requested solution.

7.7 Documentation

Precondition for a proper protection against cyber threads is a well-known system. Additional to the standard documentation the vendor should provide a detailed documentation of the plant assets. Regarding automation security the following minimum requirements must be fulfilled.

		D	U	S	V
1)	A complete, accurate, and up-to-date hardware inventory list is provided by the vendor. This includes descriptions of type and model, firmware version, etc.	M	M	M	M
2)	A complete, accurate, and up-to-date software inventory list is provided by the vendor.	R	R	M	R
3)	A complete, accurate, and up-to-date inventory of all data related to an Automation System is provided by the vendor. Data may include, depending on the individual case, e.g., user programs, configuration files and data, risk analyses, function blocks, operating procedures, software and tools, training material, or wiring diagrams.	R	R	M	R
4)	The documentation includes the available CPE (Common Platform Enumerations) of the assets.	R	R	R	R
5)	A graphical overview for the logical structure of the automation system is provided.	M	M	M	M
6)	The connections and interactions to and with other systems (IT or OT) is documented.	M	M	M	M
7)	A logical network diagram / data flow diagram is provided. It must contain IP addresses and should contain communication protocols and data flow directions. A network level model template is contained in G-P-EI 861.	M	R	R	M
8)	The requested inventories conform to the G-P-EI 202 M.	–	–	M	–

7.8 Lifecycle

		D	U	S	V
1)	The vendor provides a description how the security and functionality of the proposed security concept can be maintained during the entire lifecycle of the system (design, test, commissioning, operation, maintenance, decommissioning). If this requires updates, patches, etc. these should be system-tested.	M	M	M	R
2)	If services by the vendor are necessary to achieve 1), then all services are to be described and offered	M	M	M	M

7.9 Design and Engineering

		D	U	S	V
1)	Throughout the engineering and specification phase of the automation system a dual control principle (4-eyes, separate roles, segregation of duties) is applied.	R	R	M	R
2)	Cyber security aspects have already been taken into account during the plant's design and engineering phase (applies to updates, larger system changes and for new plants).	R	R	M	R
3)	State of the art technology is used for cryptographic measures (e.g., key exchange, encrypted communication, password hashes, etc.).	R	R	R	M

8 Organizational

This topic belongs to non-technical requirements.

8.1 Incident Handling Process

The vendor should outline its internal process for Incidents which also identifies key global and regional (Asia/Pacific, EMEA, NA, SA) contacts for incident response support from the vendor to BASF.

		D	U	S	V
1)	The vendor must support BASF during the treatment of an incident within the BASF incident management process.	R	R	R	R
2)	The vendor must inform BASF about security incidents, which impact the operation of the plant.	R	R	R	R
3)	The vendor should offer on demand remote incident handling.	R	R	R	R

8.2 Change Management Process

The vendor should describe the process for JML process for systems access such as any cloud or portal services offered by the vendor to BASF.

		D	U	S	V
1)	The vendor must support BASF employees during a change within the BASF change management process	R	R	R	R
2)	The change management process must take into account: reasoning of the change, authorized change requests, request for change, security risks of the change, approvals, documentation, testing, implementation and communication	R	R	R	R
3)	Changes must be tested before the implementation.	R	R	R	R

8.3 Certifications Regarding Automation Security

It would be appreciated to know about certifications hold by the vendor regarding OT and IT security. The certifications are not a minimum requirement.

		D	U	S	V
1)	Appropriate OT and IT security certificates or adequate substitution must be demonstrated by the vendor.	R	R	R	R
2)	The vendor must transmit existing and renewed certifications regarding OT and IT security to BASF.	R	R	R	R
3)	Ending certifications, including a reasoning, must be communicated to BASF timely.	R	R	R	R

8.4 Data Sanitizing

	D	U	S	V
1) The vendor must ensure the requirements of BASF regarding the secure disposal of media.	R	R	R	R

8.5 Inclusion of Sub-Suppliers

All security regulations need to be passed on to sub–suppliers (if applicable).