RECOMMENDATION: PRODUCT SUPPLIERS

Requirements for Network-Connected Industrial Components

Programmable logic controllers (PLCs) and similar network-compatible components for industrial use increasingly feature services also found in server systems. Given the increasing interconnectedness of these components, these general services as well as specific functions of automation technology require a sufficient level of security. The present document provides product suppliers with an overview of the essential best practices for components of this type. In addition, the BSI offers a guide for manufacturers of industrial components which is intended to support the setup of product tests and security analyses. Mechanical engineers and integrators can use this document in the context of their product development to address security-related requirements.

1 Organisational Safeguards

1.1 Product lifecycle & internal processes

Establishing a secure software development lifecycle can fundamentally improve the security of a product. The questions below offer some guidance in this context.

- Do consistent and mandatory, state-of-the-art guidelines exist for secure implementation (development policies)?
- Are mandatory test stages (security gates) required within the development cycle, including e.g. a review of the application logic or a comprehensive security review?
- Do automated code analyses form a permanent part of the development cycle, as far as technologically and economically feasible?
- Are security analyses addressing threats and risks performed and are countermeasures defined as a part of the development cycle?
- Is final cleaning of products performed, ensuring that no test code from the development process remains?
- Are technical security analyses (penetration and vulnerability tests) performed, checking not only for known weaknesses, but also for new vulnerabilities (e.g. by fuzz testing)?
- Are additional security mechanisms e.g. protection against malware, encouraged (e.g. certification) instead of prohibiting their use e.g. by exclusion of liability?
- Do uniform regulations exist for the handling of weaknesses (see BSI recommendation "How to handle vulnerabilities")?

1 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/programmierung/BSI-CS_019.html
• Have you established suitable processes to track vulnerabilities in the used operating system, third-party components and products developed in-house in order to draw conclusions on whether your own product may be affected and react accordingly?

• Are patches and updates for products available over a sufficiently long period and as soon as possible in order to correct any discovered vulnerabilities? Can customers perform the update process as efficiently as possible? Do you test updates and patches before they are made available and do you guarantee that the basic functionality of devices is maintained? Do you inform your customers which patches have to be assessed with which criticality?

For additional useful requirements to be considered in the context of a secure development process see, among others, the BDEW white paper\(^2\), with WIB\(^3\), in DIN SPEC 20009\(^4\) or IEC 62443-2-4\(^5\).

1.2 Communication

In many fields of application, such as factory automation or process control, it is important to provide suitable information comprehensively and as soon as possible to integrators and end-users. In many cases, information about a weakness can be much more important than providing a patch. For this reason, the following essential issues have to be addressed.

• Do you, as a product supplier, strive to communicate as openly as possible concerning the security of your products?

• Have you appointed points of contact or other contact options for security questions / incidents, preferably with 24/7/365 availability? In addition, have you defined response times and emergency procedures (cf. BSI recommendation "How to handle weaknesses")?

• Are customers informed as effectively as possible in case a weakness in a product becomes known?

• Do you gather information from different communication channels, such as hotline, support, forums etc., which could indicate potential weaknesses or incidents (e.g. messages such as "A .dll file was changed on my system")?

2 Product Features

The following minimum requirements for the product features of network-compatible industrial components should be understood as generic recommendations. Adaptations are required depending on a component's specific range of functions, e.g. if no web server or web-based interface exists in a component.

2.1 Documentation

The documentation of the product is of particular importance for secure operation by the customer or further use by integrators. The following questions can offer guidance for compilation and review of the product documentation. For further requirements concerning this, see VDI/VDE 2182,\(^6\) among others.

1. Are the integrator's or user's target audiences named which should be advised of the information contained here for security-specific reasons?

\(^2\) http://www.bdew.de/internet.nsf/id/212E01B4E0C52139C1257A5D0429968/$file/2008-06-10_Whitepaper_Sichere%20Steuerungs-Telekommunikationssysteme.pdf

\(^3\) http://www.wib.nl/

\(^4\) http://www.beuth.de/de/technische-regel/din-spec-27009/151100155

\(^5\) http://webstore.iec.ch/

\(^6\) http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/richtlinien/
2. Is sufficient attention drawn to the necessity to change default passwords during commissioning?

3. Are the security properties and/or features of the component described?

4. Do you outline which risks / threats are addressed by the component itself?

5. Are all the interfaces, access points and features documented?

6. Does the documentation include information the customer can use to create a security concept?
   a) Are the threats documented which have to be considered in the context of a security assessment or security management?
   b) Have you documented which measures can be taken to counter these threats?
   c) Have you documented which services (including the mechanisms integrated into the product) cannot be secured and therefore require additional technical or organisational security measures?

7. Do any recommendations exist concerning the configuration for secure operation (e.g. guideline for system hardening)?
   a) Are the instructions on how to change default passwords and deactivate unnecessary accounts sufficient?
   b) Are the security-specific consequences of the potential configuration options / alternatives documented?
   c) Are there any indications which settings should be considered critical and could potentially lead to increased vulnerability?
   d) Does a checklist exist offering an overview of the configuration and its security-specific implications?

8. Do references exist indicating additional information on protection and/or safe operation?

2.2 Product configuration

The configuration options are particularly important for the security of a component, as they are used to control and parametrise security mechanisms, among others. The following central questions have to be considered in this context.

1. Is the product delivered in a secure basic configuration?

2. Can services considered insecure / not required be deactivated?

3. Are the passwords, certificates etc. for all services replaceable?

4. Can the configuration be modified only following prior authentication?

2.3 Technical product features

Secure operation is the responsibility not only of end-users, but also of product suppliers. Practical security-specific product features are an important component of comprehensive protection.

1. Logging
   a) Is the distribution or exposure of critical information via logging data (e.g. login data) prevented?
b) Are all potentially critical actions recorded in log files, e.g. changes to the configuration, failed logins, removal or replacement of CF cards or connection of a USB device?

2. Login / Authentication

a) Do fine-grained access control and sufficient user administration (i.e. several users with different roles and privileges) exist?

b) Are login data (particularly passwords) stored in encrypted form instead as plaintext according to the state of the art (e.g. no use of MD5)?

c) Following a failed login, are only general error messages displayed, e.g. not offering any clue that the user name was correct and the password was incorrect?

d) Do sessions time out or can timeouts be configured?

e) Is it possible to limit network access to specific MAC addresses or IP addresses and/or IP address ranges?

f) Are additional mechanisms in place securing user access, e.g. “four-eyes principle”?  

g) Is access (temporarily) blocked, an SNMP alert or the like triggered if a brute force attack on a login mechanism is performed?

3. Authorisation

a) Does the product prevent potentially critical actions from being performed without the required privileges?

4. Web interface

a) Are technical controls in place impeding or preventing Cross Site Scripting (XSS) or Cross Site Request Forgery (XSRF)?

b) Is it possible, at least as an option, to always use HTTPS to access the web interface?

c) Is critical information always transmitted in encrypted form?

d) Have you ensured that passwords are never displayed as plaintext in the configuration and when logging in?

e) Is a current version of the SSL/TLS protocol used in a current implementation? In particular, refrain from using TLS 1.0.

5. Network services

a) Can services (e.g. HTTP(S), FTP, etc.) and interfaces (e.g. WLAN) be switched off if they are not required by the integrator or end-user?

b) Have the privileges used to run services such as FTP or the web server been minimised?

c) Has the implementation, in particular of the basic communication protocols, been tested with regard to fault tolerance and robustness (cf. ISA 99)?

d) Do provisions exist to impede attacks on the availability of services by opening a large number of connections or sessions?

e) Are all the interfaces of the device secured by sufficient input validation in order to prevent any manipulation?

f) Do you refrain from error-prone self-implementation of services (e.g. Embedded Web Server)?
6. Miscellaneous

a) Can remote maintenance or write access of the component only be performed after it has been explicitly enabled – e.g. via a key or flip switch?

b) If available, are secure alternatives for common industry-specific protocols used, e.g. Secure DNP3 instead of DNP3 or OPC UA instead of OPC?

c) Has the used operating system been subject to fundamental system hardening?

d) Have you ensured that the fundamental functionality of the component is maintained in case of a denial-of-service attack and the component resumes normal operation with the entire functional range following such an attack?

e) Are secure and user-friendly mechanisms for backup and recovery implemented?

f) Are updating mechanisms (e.g. for firmware updates) performed via the network instead of locally on the device sufficiently secured? In addition to integrity checks using checksums, you should in particular provide for suitable authentication or protection using signatures.

g) Are commonly accepted algorithms and implementations for encryption procedures used instead of developing them in-house?

h) In addition to web communication, XML-based file formats are commonly used for storing data such as product configuration. Is a secure XML parser used with a restrictive configuration? Are additional checks of XML files performed in order to prevent XML-specific attacks?

i) Does the option exist for automatic triggering of an alarm in case of critical system events or states?

For additional recommendations – in particular for HTTP(S) interfaces (web interfaces) – see BSI recommendation "Development of Secure Web Applications", in particular the section "Development stage".

2.4 Implementation options for selected features

Particular care should be taken when designing the specific implementation of security-specific product features. In addition to sufficient quality of the implementation and the achieved security level, aspects such as the consequences with regard to the effort by integrators and end-users are of particular importance.

Please note: The following sections explain some of the specific security-specific product features and their implementation options. These are selected examples which will be gradually expanded in cooperation with industry partners. You can send your suggestions and additions to the authors at ics-sec@bsi.bund.de.

Default passwords

Delivery of a product with default passwords always poses a security risk. There are several possible solutions for this, e.g.

- Indication in the documentation – in a prominent place if possible – that a default password has been defined and that it is imperative to change it.
- Indication in the administration interface that a default password has been set.
- Mandatory change of password during installation or initial configuration.
- Delivery already with an individual password (e.g. derived from serial number and MAC address) which will be reset after a factory reset.

---

7 http://www.ws-attacks.org
In addition to the stated implementation options, there are more additional measures, e.g. recommendation of requirements for secure passwords in the documentation or technical enforcement of such password policies.

FTP and alternatives
Conventional FTP for file transfer does not include any security mechanisms and is therefore not recommended for secure applications. Among the potential alternatives are e.g. the Secure File Transfer Protocol (SFTP) or FTP over SSL or TLS (FTPS). SFTP is based on SSH and, to be precise, is a subfunctionality of SSH for file transfer. Other than the purpose of exchanging files, it has nothing in common with the FTP protocol proper. Accordingly, SFTP differs from FTP in that it only requires one connection and – like SSH – it runs via port 22, making it substantially simple when compared to FTPS (see below) concerning the transfer of data through a Firewall. The essential security mechanisms – encryption of the entire communication (credentials and payload) as well as authentication – are provided by SSH. Extensive guidance concerning these encryption functions is provided by the BSI, see Technical Guideline TR-02102⁹.

However, SFTP has never been officially defined as an Internet standard. In contrast, FTPS was specified in RFC 4217. FTP, which differs from SFTP in that it is a native protocol, is supplemented by TLS-based encryption and authentication features. As FTP requires at least two connections, as already stated above, this solution is not very "firewall-friendly", because several ports have to be opened for data transfer. In addition, only authentication data, but not content data (!) are encrypted in different implementations. Depending on the configuration of clients and servers, this can lead to incompatibilities which may go as far as to prevent successful connection. Therefore, SFTP is to be preferred for operability reasons.

SCP is another secure alternative to unencrypted FTP in addition to FTPS and SFTP. See also TR-02102 cited above.

Managed devices
SNMP (Simple Network Management Protocol) is a common protocol for centralised monitoring and control of devices connected to a network. SNMPv2, or more precisely SNMPv2c, is particularly common at the moment. The problem is, however, that SNMP up to SNMPv2(c) does not feature any encryption, i.e. all data are transferred as plaintext, which can be read by any person. In addition, practically anyone participating in the network can read system information and can potentially obtain critical information. As SNMPv1 and SNMPv2 are based on UDP, they are stateless, increasing their susceptibility to IP spoofing.

SNMPv3 (version 3) introduced functions such as encryption and improved authentication. For this reason, it is recommended to generally implement SNMPv3 and to enable this in the default configuration, if possible. Regarding compatibility with existing systems, SNMPv2(c) can be implemented additionally, but should then require enabling by the end-user.

Please note that certain residual risks remain also with SNMPv3. In particular, brute force and dictionary attacks on authentication are possible. Therefore, it is sensible to incorporate a suitable detection mechanism for this kind of attack. In addition, write access should be implemented only if required and there should be the option to disable it.