RECOMMENDATION: IT IN PRODUCTION

Recommendations for further education and qualification measures in the ICS environment

The urgent need for action to protect industrial control systems (ICS), i.e. in the field of factory automation and process control, against cyber threats is increasingly recognised by the industry. In this respect, the BSI offers an abundance of information materials, best practices and other resources. However, it is essential, in addition to these offers, that companies train and qualify their employees accordingly. Whereas specific awareness-raising measures are suitable for employees, such as system operators, other target groups must obtain more in depth training. This applies in particular to those employees who are responsible for planning, development, integration or installation, operation and maintenance or are significantly involved in these activities and thus actively shape cyber security in this respect. The management or persons responsible for production should also be qualified to an appropriate extent which goes beyond typical sensitising.

The need for such further education and qualification measures is constantly growing. Accordingly, there are more and more service providers who address this need. Especially with respect to the growing number of offers, it is important that an adequate, content-related minimum level is ensured. This document is an orientation guide for two training types:

1. Management and persons responsible for production
2. Employees with responsibility and/or potential influence on cyber security of an ICS.

This means that experts from the factory automation and process control areas who want to extend their qualifications by cyber security for their own area of responsibility are in the focus of this document. General awareness-raising measures as well as qualification measures for IT and/or IT security experts who want to become familiar with the ICS field of application (administrators, service providers, consultants, auditors) will not be covered in this document. These target groups are taken into consideration in a revision of this recommendation where applicable.

This recommendation of the BSI is not related to certification. This is only a non-binding recommendation for training content.
1 General requirements

The structure of the qualification measures is only to be seen as a suggestion which is based on empirical values and has proved to be successful in the past. As an alternative, however, other structures or procedures can also be used. This applies in particular when qualification measures are tailored to individual industries or to specific company sizes.

With respect to the individual topics to be covered, it is recommended to implement the suggestions presented in this document as a training provider or to actively demand them as a customer.

The temporal expenditure suggested in this document is also only a reference value. Training for ICS experts may have another scope for employees of SMEs, and thus another in-depth expertise, than for employees of large corporations.

In addition to a theoretical part, the qualification measures should also necessarily have a practical part in order to promote a long-lasting learning effect. This includes for example exercises based on the example scenarios or the testing of software tools. The latter should be performed, where appropriate, on simplified, but necessarily representative platforms so that transfer into one’s own company is preferably given.

The speakers or trainers of the qualification measures should be familiar from practice with the contents they convey. Especially experts with several years of experience in operating industrial systems are suited. IT security experts are also suited provided that they do not only have theoretical basic ICS knowledge, but have actively worked there for at least five years as consultants or in IT security projects. A cooperation of two speakers, one from the industry and one from IT security, also makes sense. Providers should make the respective profiles of their speakers transparent in this respect.

2 Training for management

Target group: Persons responsible for production, management (C level), where applicable (new) employees with operative relevance for security as an introductory safeguard

Timeframe: 6-7 hours (net)

Objectives:
✔ Showing the threat situation,
✔ Illustrating the need for action,
✔ Basic understanding of fundamental terminology and systematic approaches,
✔ Knowledge of the most important organisational and technical safeguards on an abstract level,
✔ Establishing the conditions to initiate projects and measures and be able to understand them on the management level
<table>
<thead>
<tr>
<th>Topic</th>
<th>Contents</th>
</tr>
</thead>
</table>
| **Basic information**<br>1h | ✓ Common terminology in the field of ICS  
✓ Basic network knowledge: Routers, switches, firewall, WiFi, mobile communications etc.  
✓ Basic cryptographic knowledge (symmetrical vs. asymmetrical cryptography, hash algorithms, certificates (e.g. SSL, S/MIME, PGP), benefits and disadvantages for ICS)  
✓ Legal framework: German IT Security Act [IT-SiG] (reference to KRITIS if applicable, law as role model function), manager liability, product liability, industry standards and standards landscapes etc. |
| **Threat situation**<br>1h | ✓ Protection objectives  
✓ Forms of attack (e.g. DDoS, APT, malware, MITM, spoofing etc.)  
✓ Picture of the situation: most common attacks, statistics, examples if necessary  
✓ Collateral damage in ICS caused by non-targeted malware  
✓ Targeted attacks: typical procedures / anatomy of a targeted attack (via IT) on ICS  
✓ Gathering of information and social engineering (e.g. FOCA tool or OSINT)  
✓ Security of partners, customers, third-party companies (supply chain)  
✓ Spreading in the company (lateral movement)  
✓ Insecurity of industrial protocols  
✓ Exfiltration, manipulation, sabotage in ICS  
✓ Damage consequences  
✓ Other threats (e.g. remote maintenance, industrial wireless etc.)  
✓ If necessary, practical demonstration based on Metasploit, SET or the like |
| **Security management and comprehensive organisational safeguards**<br>2h | ✓ Idea / procedure and structure of an ISMS  
✓ Operation of an ISMS  
✓ Fundamental terms: Asset, vulnerability, threat, risk etc.  
✓ Standards  
✓ Defense in depth  
✓ Basic safeguards in the security management (especially organisational safeguards)  
✓ Network plan  
✓ Tendering, procurement, security in the context of FAT/SAT  
✓ Initial operation  
✓ Contingency planning, BCM, incident response |
| **User-centred safeguards**<br>1h | ✓ Policies with examples (essential topics include the use of mobile data media, external companies and the connection of new components and/or systems to the network)  
✓ Sensitising / awareness |
| **Technical measures**<br>1.5h | ✓ General clarification of terminology: Firewall, AV, AWL, SIEM, IDS, IPS etc.  
✓ Firewall / industrial firewall  
✓ Remote access / VPN  
✓ System hardening  
✓ Log data – collection, analysis  
✓ Monitoring (traffic, system properties)  
✓ AV protection, airlock for removable media  
✓ Vulnerability scanner (outsider view, e.g. using the example of OpenVAS)  
✓ Industrial wireless |
When describing the threat situation, it is important to keep in mind that attacks are often initiated in the office network from where they spread into the operational network. Protecting the office and/or at the outer perimeter of the company alone is not enough protection. The description of the safeguards should focus on ICS and address the special requirements. General IT should be addressed only where it is necessary.

In the last section, the participants should be given concrete recommendations (action items) how the knowledge conveyed can be implemented in practice their own companies.

## 3 Training for production experts

**Target group:** Production CISO, engineers, infrastructure operating personnel, maintenance technicians, maintainer – i.e. persons with a technical background in ICS and in charge of planning, development, integration/installation, operation or maintenance/servicing.

**Timeframe:** 21-35 hours (net) / 3-5 days

**Objectives:**

✔ Basic understanding of relevant terminology, technologies and elements of IT / IT security,

✔ Sound understanding of the threat situation in order to assess the personal concerns and dangers,

✔ Conveying the basic principles of ISMS,

✔ In-depth knowledge of organisational and technical safeguards,

✔ Concrete approaches for the implementation during operation / when planning new systems / when managing security projects (where applicable, with external commissioning),

✔ The purpose of this qualification measure is not that the participants are able to independently handle all topics covered as an operative task without any support by third parties or further education measures.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic information</td>
<td>✔ Common terminology in the field of ICS</td>
</tr>
<tr>
<td>2h</td>
<td>✔ Basic network knowledge: Routers, switches, firewall, WiFi, mobile communications</td>
</tr>
<tr>
<td></td>
<td>✔ Network protocols and services (from conventional IT)</td>
</tr>
<tr>
<td></td>
<td>✔ Basic cryptographic knowledge (symmetric vs. asymmetric encryption, signatures, hash algorithms, certificates (e.g. SSL), S/MIME, PKI, PGP, benefits and disadvantages for ICS)</td>
</tr>
<tr>
<td></td>
<td>✔ Legal framework: German IT Security Act [IT-SiG] (reference to KRITIS if applicable, law as role model function), manager liability, product liability, industry standards and standards landscapes etc.</td>
</tr>
</tbody>
</table>
## Topic Contents

### Threat situation

- 4–6h
- ✔ Protection objectives
- ✔ Forms of attack (e.g. DDoS, APT, malware, MITM, spoofing etc.)
- ✔ Overview of the situation: most common attacks, statistics, examples
- ✔ Collateral damage in ICS caused by non-targeted malware
- ✔ Classification of attackers
- ✔ Targeted attacks: typical procedures / anatomy of a targeted attack (via IT) on ICS
- ✔ Security of partners, customers, third-party companies (supply chain)
- ✔ Gathering of information and social engineering (e.g. FOCA tool or OSINT)
- ✔ Spreading in the company (lateral movement)
- ✔ Typical scope of functions of ICS components
- ✔ Typical vulnerabilities in ICS components
- ✔ Typical vulnerabilities in the concept/architecture
- ✔ Insecurity of industrial protocols
- ✔ Vulnerability of safety systems
- ✔ Exfiltration, manipulation, sabotage in ICS
- ✔ Damage consequences
- ✔ Other threats (e.g. remote maintenance, industrial wireless etc.)
- ✔ Practical part on attacks, lateral movement and manipulation of ICS components; e.g. using tools such as nmap, metasploit, snmpcheck, sqlmap, plcscan etc.
- ✔ Where applicable, practice: Tabletop exercise, specific scenario

### Security management and comprehensive organisational safeguards

- 6–11h
- From here, focus on safeguards in ICS and/or at the interfaces to the outside world
- ✔ Idea / procedure and structure of an ISMS
- ✔ Fundamental terms: Assets, vulnerability, threat, risk etc.
- ✔ Standards
- ✔ Defense in depth
- ✔ Basic safeguards in the security management (focus on organisational safeguards)
- ✔ Network plan (incl. gathering, discovery, forms of representation)
- ✔ Configuration/change management
- ✔ Security of partners, customers, third-party companies (supply chain)
- ✔ Tendering, procurement, security in the context of factory and/or site acceptance tests (FATs/SATs)
- ✔ Initial operation
- ✔ Vulnerability & patch management
- ✔ Using up-to-date information (advisories, warnings etc.)
- ✔ Practical example incl. recording assets, drawing up a network plan, assessment of protection requirements, modelling, deriving safeguards, ...
- ✔ Certification

### User-centred safeguards

- 1–2h
- ✔ Policies with examples (essential topics include the use of mobile data media, external companies and the connection of new components/systems to the network)
- ✔ Sensitising / awareness
<table>
<thead>
<tr>
<th>Topic</th>
<th>Contents</th>
</tr>
</thead>
</table>
| Technical measures | ✔ General clarification of terminology: Firewall, AV, AWL, SIEM, IDS, IPS, honeypot etc.  
✔ IT / ICS interface  
✔ Zones & conduits, protection of network transitions, ICS DMZ  
✔ Firewall / industrial firewall incl. important aspects to be taken into account, such as impacts on real-time requirements or latency periods  
✔ Remote access / VPN; incl. practical part where applicable  
✔ System hardening (general); where applicable, practical part for example regarding group policies; PLCs, HMIs, historians/DB  
✔ Security of ICS server components, HMI, PLC  
✔ Access management – access models, directory services, management of roles and rights  
✔ 3rd party devices (e.g. service technician)  
✔ Log data – collection, analysis incl. practical part where applicable  
✔ Monitoring (traffic, system properties)  
✔ Protection of databases and historians  
✔ AV protection, airlock for removable media  
✔ Vulnerability scanner (outsider view)  
✔ Industrial wireless  
✔ Mobile devices in the field |
| Audit, revision, penetration test  
0.5–2h | ✔ Basic information  
✔ Procedures, standards  
✔ Particularities in the case of ICS, e.g. necessary rules of engagement  
✔ Example of practical implementation |
| Contingency planning, BCM, incident handling  
0.5–2h | ✔ Backup & recovery, testing Backups, different backup methods  
✔ Basic information about contingency planning, BCM, incident response  
✔ Procedures and standards  
✔ Forensics  
✔ Practical example: Contingency planning, BCM, incident response |
| Final discussion, next steps, summary  
1–2h | ✔ Suggestions/courses of action as well as their efforts and potential  
✔ Initial organisational safeguards (roles, responsibilities, cooperation IT, initial processes etc.)  
✔ Checklist (e.g. BSI Top 10 self-check)  
✔ Creating and analysing the network plan; establishing this as an ongoing task  
✔ Simulation games (e.g. BSI tabletop exercise)  
✔ (Brief) revision |

For this qualification measure, a continuous scenario by way of illustration and as a basis for practical exercises would be desirable. Thus, a simplified scenario can be protected successively without security safeguards.

Additional alternatives for a practical part include, among other things,

✔ system hardening using the example of a PLC that is common or used in the respective company
✔ Configuration of a firewall for industrial scenarios
✔ Configuration of a VPN
✔ Configuration of a VLAN for an industrial application case
4 Outlook

There is increasing demand for further education and qualification measures in the context of cyber security for industrial control systems on the part of the operators in the field of factory automation and process control. This document should be used as an orientation guide for the relevant contents in this respect. As a further basis for designing such training courses, the publications and resources of the BSI¹ in this area can be used.

For feedback, suggestions and collaboration when developing recommendations for additional target groups, the BSI can be contacted using the email address ics-sec@bsi.bund.de.