

Appendix D: Service Guide

The service portfolio listed below is regularly adapted and further developed to meet customer needs.

For services not listed in the Service Guide, clarification is required between the customer and the handling service unit of ProLeiT/Schneider Electric.

1 Definitions

1.1 ITIL

In providing its services, ProLeiT is guided by ITIL (IT Infrastructure Library), the world's best practices for IT service management.

1.2 Service Request

A service request is a request from a customer that does not require the rectification of malfunctions. The service request defines a formal customer request to provide information or support as well as consulting services.

Examples related to automation systems and manufacturing execution systems (MES):

- Providing patches and/or installation media
- Project planning support
- Advice on the software components
- Standard changes (password changes, etc.)
- Information requests (manual requirements, consultation requests, etc.)
- Creation of reports

1.3 Incident

An incident defines an unplanned interruption of an IT service or a reduction in the quality of an IT service.

Examples related to automation systems and manufacturing execution systems (MES):

- Failure / disruption of communication between server and PLC (DCS)
- Hardware component failure
- Long response times for system operation

The classification of the incidents (disruptions) is carried out by ProLeiT with appropriate consideration of the urgency and the impact of the reported errors or disruptions on the customer's business operations. The following matrix applies:

	Effect			
		high	medium	low
Urgency	high	Priority 1	Priority 2	Priority 3
	medium	Priority 2	Priority 3	Priority 4
	low	Priority 3	Priority 4	Priority 4

Urgency: Measure of the speed with which a fault must be resolved

Impact: Extent of a disruption: Who or what is affected and to what extent?

Within the framework of this service agreement, ProLeiT distinguishes the incidents into:

- "Major Incident" = Priority 1 or 2 IncidentA "Major Incident" is a fault that causes the failure of essential system components or the entire system, so that use is completely prevented and immediate troubleshooting is unavoidable. A non-production system (e.g. test system) cannot trigger a "major incident". Examples:
 - Priority 1: Plant shutdown, production can no longer be carried out.
 - Priority 2: Production is significantly impaired or production downtime is imminent.
- "Minor Incident" = Incident of Priority 3 or 4A "Minor Incident" is an indirect impairment of production or an error or disruption without impairment of production.
 - Priority 3: Indirect effect on production
 - Priority 4: An error message appears, but after confirming it, work can continue normally.

1.4 Event

An event is a status change as well as an alarm or notification generated by Event Management.

1.5 Problem

A problem is the cause of one or more incidents. By means of a problem ticket, the causes of disruptions are analysed and measures are developed to prevent or eliminate them.

1.6 Change

The Change defines an adding, modifying, or removing hardware or software components or parts thereof.

Examples related to automation systems and manufacturing execution systems (MES):

- Replacement of hardware
- Installation of new software components or software updates or other patches
- Changes in project planning

In general, a distinction is made between 'Normal Change', 'Standard Change' and 'Emergency Change':

- **Normal Change**
Normal changes are, for example, extensions, changes or optimizations of the project planning, installation of patches of the operating system, the SQL Server or third-party software that also affect ProLeiT software. Every Normal Change goes through the usual approval process.
- **Standard Change**
Standard Changes are changes for which there are usually precise procedural instructions: Since they are associated with only low risk, they do not require any (further) approval processes. If the impact is high and the urgency is high, the Request for Change (RfC) also has a high priority and vice versa.
- **Emergency change**
The emergency change does not go through the usual process, but is carried out immediately, if necessary at considerable risk and without further approval, usually to avert greater damage.

1.7 Patch

A patch is a correction delivery for software or data from the end user's point of view in order to fix errors – usually to close known security gaps – or to retrofit previously non-existent functions. A distinction must be made between brewmaxx / Plant iT patches and 3rd party patches.

1.8 Service time

The service time describes the period of time in which the services offered by ProLeiT are provided. The service time depends on the selected contract model.

1.9 Business hours

ProLeiT's business hours at the Herzogenaurach site (Bavaria, Germany) apply.

Business hours are on weekdays from **Monday to Friday between 9:00 a.m. and 5:00 p.m. (CET)**, excluding public holidays, as well as Saturdays and Sundays.

Another regulation (e.g. business hours of a subsidiary at a different location) must be described in **Appendix A – Chapter 7**.

1.10 Reaction time

The response time is the time span from the receipt and recording of an incident to the first contact by ProLeiT with the customer. The response can be made by phone or email.

The response times apply exclusively to systems in productive use.

The initial reaction by ProLeiT to major incidents is always by telephone.

The fault report outside business hours must be made by telephone with the note that processing as a major incident is desired. Outside of business hours, ProLeiT will only handle major incidents. ProLeiT assesses and processes this fault in accordance with Chapters 1.2 Service Request and 1.3 Incident, the selected services from **Appendix A** and the corresponding response times from **Appendix C**.

Response times depend on the selected service model.

1.11 Service Delivery Point

The Service Delivery Point is the physical location from which the Service is provided.

The contact details will be communicated after the conclusion of the contract via an SLA certificate, which contains all the necessary information of the service contract.

1.12 Correspondence language

All communication, written and oral, is in German or English. Deviating regulations must be contractually agreed, see **Appendix A – Chapter 7**.

The documentation in the ticket system and the Health Check Report (see chapter 2.4.2.1 Remote Health Check and Chapters 2.4.2.2 On-Site Health Check) are written exclusively in German or English.

2 Services

2.1 Request Management

ProLeiT has qualified service personnel for the provision of the services described. Customer inquiries are forwarded by phone or e-mail to the central helpdesk in Herzogenaurach or to the **Appendix A** – and recorded in the ProLeiT ticket system. After categorization and prioritization (see chapter 1.2–Chapter 1.6), further processing is carried out in accordance with the ProLeiT processes for:

- Incident Management
- Service Request Management und
- Escalation Management

For this purpose, ProLeiT relies on remote dial-up to the customer system (see chapter 2.4.1). In addition, ProLeiT operates system environments of the appropriate version of Plant iT / brewmaxx for error analysis.

The monitoring system (see chapter 2.4.2.3) supports the determination of causes of malfunctions.

2.1.1 Incident Management

Elimination of unplanned incidents through manufacturer expertise by:

- Procedure according to ITIL-based standard process
- Fault analysis including support for the restoration of operational readiness triggered by malfunctions or the failure of components of the DCS/MES according to Appendix A
- Collection of diagnostic data to narrow down the cause of the error
- Assistance in troubleshooting or circumventing the error through a workaround
- Ticket documentation including changes made to the configuration / installation
- Notification of processing status
- Transfer to Changes / Problems if necessary
- Provision of patches and updates for bug fixes for the contractually defined computer programs (ProLeiT system software) in accordance with Appendix A.
- If troubleshooting via remote dial-in is not possible, on-site support can be arranged after consultation with ProLeiT. If there is a travel warning from the Federal Foreign Office of the Federal Republic of Germany, ProLeiT is not obliged to provide on-site support. The exact provisions for on-site support are agreed in Appendix A, Chapter 7.

2.1.2 Escalation Management

In coordination with the customer, ProLeiT offers priority escalation management. Depending on the categorization of the incident, expert support is ensured. Examples of escalations include:

- Application Support: Further support from the project team
- Product Support: Escalation to the Head of Support
- IT Support: ProLeiT IT department or manufacturer

2.1.3 Service Request Management

Response to customer enquiry by

- Consulting Services (Service Request)
- Processing Service Requests (Service Request, Change)
- Advice and information by telephone on all functions of the ProLeiT software
- Support in the adaptation of hardware and software configurations by qualified personnel with experience in the project planning of ProLeiT software as well as plant experience by telephone / remote access
- Optimizations, e.g. additional reporting texts and queries
- Notification of processing status
- Transfer to Changes / Problems if necessary

2.1.4 Self-Service-Portal

Every SLA customer receives web access to the mySchneider portal. This provides the following functions, among others:

- Create tickets and add notes, comments and queries about the ticket
- Overall overview of all tickets of your own company and thus avoidance of duplicate inquiries on one and the same topic
- Viewing ticket status

- Overview of Credit Postings
- Documentation of all services provided
- With the self-service portal, the customer has transparency about the services provided.

2.2 Product Support

ProLeiT offers product support for the software products Plant iT and brewmaxx as well as their add-ons and modules.

The processing of the customer enquiry is carried out in accordance with Chapter 2.1 and is provided by the central helpdesk in Herzogenaurach.

2.3 Application Support

ProLeiT offers support for customer-specific applications of the Plant iT / brewmaxx software according to the following regulation:

- Engineering by ProLeiT:
Application Support can include incident, problem, and change management (see Appendix C).
- Third-party engineering:
Application support includes incident management exclusively.
The processing of the customer enquiry is carried out in accordance with Chapter 2.1 and is provided by the central helpdesk in Herzogenaurach. Another arrangement (e.g. provision of the service by a subsidiary at a different location) must be described in Appendix A – Chapter 7.

2.4 Business Continuity

ProLeiT supports its customers in the development of strategies, technical measures and processes to enable the continuous operation or the rapid resumption of operation of the customer's system after a malfunction.

2.4.1 Remote dial-in

2.4.1.1 Scope

Remote Access includes the following services:

- Operation of a centrally managed dial-up environment with currently patched operating system and virus protection at ProLeiT
- Initial setup and documentation of remote dial-in to the customer's system
- Ensuring the function of remote dial-up to the customer's system by means of regular connection tests (2x annually)
- The following points with regard to remote dial-in are agreed in Appendix A:
 - Dial-in Methods
 - Remote Access Software
 - Accounts (personal if applicable)

2.4.1.2 ProLeiT standard dial-in

The currently supported standards are published on the ProLeiT Support Website <http://www.proleit.de/support.html>.

2.4.1.3 Special dial-in

All deviating dial-in options count as special dial-in options (see point 2.4.1.2)

The use of the constellations listed here must be examined by ProLeiT on a case-by-case basis and requires the explicit consent of ProLeiT.

Changes to the dial-in must be agreed between ProLeiT and the customer immediately.

2.4.2 Preventive services

ProLeiT offers its customers services that minimize the risk of production downtime.

2.4.2.1 Remote Health Check

ProLeiT checks the condition of the system by means of a remote health check. The results are summarized in a health check report and communicated to the customer. The health check via remote access takes place during ProLeiT business hours (after prior agreement with the operator) once per calendar year.

If services have not been provided or not completely provided by ProLeiT for reasons for which ProLeiT is not responsible, there is no right to compensation.

For brewmaxx / Plant iT software not planned by ProLeiT, an inventory will be carried out after the start of the SLA. The results and measures are summarized in a System Check Report and communicated to the customer. This inventory replaces the remote health check to be carried out in the first year of the contract.

Scope

The Remote Health Check includes the following services for the **components listed** in Appendix A:

- Server
 - Check Disk Capacity
 - Check memory and CPU usage
 - Evaluation of log files (Windows event logs and ProLeiT logs)
 - Database consistency check
 - Audit of the archiving function
 - Check the time synchronization between server and PLC(s)
 - Checking the parameterized connections between server and PLC(s)
 - Performing a Basic Backup, see chapter 2.4.3 Basic Backup
 - Hardware diagnostics using the manufacturer's software tools (e.g. HP Management Tools, Dell Server Administrator, etc.)
 - Recording and logging of the installed ProLeiT software
 - Diagnosis of the redundancy and/or virtualization solutions used (e.g. Stratus Avance, Stratus ft), if supplied by ProLeiT
 - Determination of index fragmentation
 - Checking SQL query execution times
 - Checking Agent Job Execution Times
 - Data volume control
 - Determining the Need for Optimization for SQL Query Plans
- Engineering station
 - Functional Testing of the Engineering Environment (Step7, ProLeiT Software)
- PLC

- Scanning disk space
- Cycle time check
- Evaluation of the PLC diagnostic buffer
- Creation of a standardized Health Check Report: The Health Check Report will contain the following information in particular:
 - List of all detected values for memory allocations, cycle times, etc.
 - List of all errors, problems and dangers identified with information on how to eliminate them
 - Summary assessment of the availability of the process control system with regard to trouble-free production operation
 - Indications of possible measures to increase the availability of the process control system
 - If possible, the Health Check log is extended by screenshots from system monitoring (e.g. development of the memory used, CPU utilization, ...)

Workstations are not covered by the Health Check.

Depending on the results, change-relevant measures (e.g. re-indexing / re-build of indexes) may have to be provided for optimization in consultation with the plant operator. These are recorded and processed via Changes.

2.4.2.2 On-Site Health Check

The on-site health check takes place during ProLeiT business hours (after prior consultation with the operator) and includes in addition to the information listed in chapter 2.4.2.1 the following services:

- Visual inspection of the server, the engineering station and the PLC(s)
- Inspection and renewal of the buffer batteries of the PLC(s)

2.4.2.3 System Monitoring

Due to the increasingly complex IT infrastructure, ProLeiT uses monitoring solutions. The monitoring system makes the operational behavior of an IT infrastructure and its individual components transparent. It provides information about the current state, the history, shows trends and tendencies and alerts the system managers when critical situations occur.

Scope of services for local system monitoring

The customer receives reading and purely informative access to the system monitoring via web frontend. The monitoring system is installed locally at the customer's premises. It can thus monitor the status of its systems 24/7, research historical data and view accumulated warnings and alarms. The local system monitoring does not send any warning or warning messages. Alert notifications via email. The following services are included in the operation of System Monitoring as a local instance:

- Pre-configuration and provision of the software appliance by ProLeiT
- Installation, configuration and testing of the system
- Initial system-specific configuration of warning and alarm thresholds of the included checks
- A one-time readjustment of the warning and alarm thresholds

The monitoring system then provides the following functions:

- Monitoring of preconfigured checks
- Overall view of the status of key system functions in one dashboard
- Overviews and statistics on the utilization of the connected components
- Long-term trends of data

Scope of services for system monitoring as a managed service

In addition to the services described above, the following services are provided by ProLeiT if there is a direct connection to the customer system via site-to-site:

- Proactive detection of faults, failures and overload situations in software and hardware
- E-mail alerting to monitoring@proleit.com
- Transfer of the fault report to ProLeiT's event management
- Monitoring of the operational readiness of the system monitoring by ProLeiT
- The customer is also automatically alerted by the monitoring system by e-mail and can initiate further steps to rectify the fault

Optional services

The monitoring system as a managed service can be expanded to include the following services:

- Monitoring of other IT services
- Monitoring of other hardware, such as UPS or network components (switches) used, if checks from the manufacturer are available or have been developed by ProLeiT. An up-to-date list of possible checks can be found on the product website (<https://checkmk.de>)

These optional services are agreed in Appendix A – Chapter 7.

Technical framework

The system monitoring solution "checkMK" is operated on an appliance in addition to the PLS / MES (i.e. standalone virtual server).

The following requirements are required on the customer side:

- Provision of the necessary device data, network addresses and information
- Provision of resources for the operation of the appliance, if it is operated on the customer's IT infrastructure
- Fixed internal IP address for the monitoring appliance
- Access rights of the monitoring solution to the systems to be monitored (e.g. SNMP or ESX users with sufficient authorizations)
- Access of the Monitoring Appliance to a mail server
- DNS servers and time servers
- Read access to the interfaces of the systems to be monitored
- Support from customer IT in configuring, updating and installing the monitoring solution

Limitations of System Monitoring

The monitoring system monitors the components of the DCS / MES supplied by ProLeiT as well as any IT infrastructure, hardware and third-party software that are part of the PLS / MES. Pure monitoring does not mean a 100% guarantee of detecting all failures. However, it can make a decisive contribution to increasing availability and protecting against system failures and performance losses.

If the IT infrastructure is provided by the customer or a third-party company, ProLeiT's scope of services is limited to the initial analysis with subsequent consulting. The customer or the third-party company is responsible for rectifying the fault.

The responsibility for the operation of the production plant remains fully with the customer and ProLeiT cannot be held liable for any damage caused by the failure to report by the monitoring system.

Changes and Enhancements

Expenses for adjustments to checks and extensions of the system monitoring functions as well as the change of warning thresholds are treated and charged as change (RFC) or service requests.

2.4.2.4 Event Management

Event Management ensures that configuration items (CIs) and services are continuously monitored. The process filters and categorizes events to take appropriate action if necessary.

- CIs to be measured and their limits are defined with the customer
- Events that occur are detected by monitoring systems, logged and forwarded to the helpdesk after an initial correlation.
- There is a second-level correlation
- If necessary, a transfer to downstream processes to eliminate malfunctions or initiate changes / problems

Event management is provided exclusively during ProLeiT's business hours at the Herzogenaurach (Bavaria, Germany) location (see chapter 1.9 Business hours). Outside of business hours, the data from the system monitoring provides additional information to solve a major incident.

2.4.2.5 Customer-specific system monitoring reports

The Monitoring system can send automatically created and preconfigured reports to any e-mail address. Such a report can contain several graphical evaluations of any checks. The report is automatically sent as a pdf file at a desired time (e.g. every day at 7:00). A typical report used is the compilation of data that describes the stability of a production environment. The configuration of the reports is billed via a service request.

2.4.3 Basic Backup

At the beginning of the contract, a project backup is stored on the ProLeiT servers. This includes the system configuration (database backup) and the PLC project. It does not contain any movement and archive data.

At every health check (see chapter 2.4.2.1) a basic backup is again performed and stored on the customer server.

2.4.4 Advanced Backup Disaster Recovery Concept

ProLeiT offers its customers advice and support in backup and disaster recovery, and based on the customer's requirements for maximum permissible downtime and maximum permissible data loss, a concept for rapid recovery of operations is created. As a result, an individual service is developed that is tailored to the customer's IT infrastructure and IT processes.

The concept includes the following points:

- Creation of a concept based on customer requirements, e.g.
 - Recovery Time Objective (RTO) and Recovery Point Objective (RPO) values
 - Defining the IT architecture: shared backup or dedicated environment
 - Scope and frequency of disaster recovery tests
 - Backup reporting requirements
 - Determination of the software / hardware to be used
- Optional implementation of the concept
 - Optionally, provision of a test environment to simulate the customer's system (see chapter 2.5.4)

The exact agreements are set out in **Appendix A** – Chapter 7.

2.4.5 Patch Management

ProLeiT offers its customers support in regularly updating the customer's system with security patches for Microsoft operating systems to ensure IT security. This includes the provision of individual patch lists, consulting services and recommendations for action individually tailored to the system configuration.

The ProLeiT scope of services includes consulting services on

- Security Patches for Microsoft Operating Systems

- Security Patches für Microsoft SQL Server
- in the context of the Plant iT / brewmaxx system software used.

For the introduction of a patch management process, ProLeiT recommends the following prerequisites and procedures.

Preconditions:

- Suitable tools for:
 - Determination of patch requirements (e.g. by a vulnerability scanner)
 - Automated distribution of patches (e.g. Matrix42 Empirum)
- Introduced change process
- An Advanced Backup Disaster Recovery Plan has been defined and successfully implemented (see chapter 2.4.4 Advanced Backup Disaster Recovery Concept)
- The products used (e.g. Microsoft SQL Server, Microsoft Windows, ...) are in the support lifecycle and compatible with the Plant iT / brewmaxx version used according to the ProLeiT Release Notes

Approach and assumptions:

- Within a workshop, an overall concept is developed in which processes, tasks and the time frame are defined. The workshop is organized by ProLeiT and lasts eight hours, with representatives of ProLeiT application and IT specialists.
- The time windows for the distribution of the patches (core maintenance time windows) are jointly agreed between the customer and ProLeiT (patch calendar). The customer ensures that the patches can be rolled out in the agreed time windows. Depending on the items to be patched, this may require downtime for production.
- Clarification of the scope of the systems / devices to be patched (ProLeiT scope of delivery or beyond). This requires the use of a Configuration Management Database (CMDB) for the hardware and software items used by the customer. Updating this database is the responsibility of the customer.
- Based on the patch matrix for Plant iT / brewmaxx software published by ProLeiT in conjunction with the Microsoft operating system and SQL Server, ProLeiT makes patch recommendations for the respective customer system. These recommendations, resulting from a general smoke test, mainly include security patches. The customer derives his need to patch his systems from this recommendation.
- If the Plant iT / brewmaxx version used is subject to on-demand support in accordance with the ProLeiT lifecycle, the plant-specific test is extended to include the components of the smoke test.
- Before the rollout on the production system, a test of the patches in the test system (see chapter 2.5.4 Test system and virtual factory). For this purpose, corresponding test scenarios and fallback scenarios must be developed and documented for each test case. Only after successfully passing the test may the rollout to the productive system take place.
- The release for the rollout to the productive system is given by the customer.
- The rollout to the productive system is carried out by the customer.
- After the rollout, appropriate functional tests must be carried out by the customer (see SLA chapter Tests). In the event of a negative functional test, it is up to the customer to decide whether the fallback scenario is applied.
- After the rollout, a ProLeiT employee with plant experience is available to the customer remotely for eight hours during business hours during a hypercare phase in order to be able to clarify any issues that arise directly and efficiently.
- The production release after the successful functional test is carried out by the customer.

Demarcation:

- Minor and major releases (e.g. operating system updates or Plant iT /brewmaxx version upgrades) are not part of patch management, but are to be handled as projects
- Patching of third-party software is not included, unless specific software has been named in the scope of Patch Management, see **Appendix A** – Chapter 7.
- No warranty claims can be derived from patch management

2.4.6 Hardware Support

ProLeiT provides support for hardware included with ProLeiT.

This includes, for example: manufacturer support from HP, Dell, Stratus or VMware. The prerequisite is a valid service contract with the manufacturer of the respective product. The customer is responsible for any necessary extensions of the service contract for the respective product, alternatively this service can be included as a special agreement, see **Appendix A** – Chapter 7.

ProLeiT, for example, offers services defined as a Stratus reseller, so that the ProLeiT Helpdesk acts as the first point of contact in the event of disruptions.

2.4.7 OT Cybersecurity First Level Assessment

Needs in the business environment

More than ever, organizations are working to modernize and digitize their operations to gain greater visibility and efficiency from their OT (Operational Technology) assets. Nevertheless, many organizations classify their control network as an insignificant risk. Recent cyber incidents and attacks are proof that OT attackers are far more sophisticated, insidious, and brazen than ever before. And apart from malicious attacks, many OT security issues are random in nature.

ProLeiT's OT Cybersecurity First Level Assessment assesses the strength of customers' OT cybersecurity defenses and policies, providing guidance to help executives make prudent cybersecurity decisions and ensure that cybersecurity investments pay off in the form of increased awareness and preparedness for attacks.

Solution

The OT Cybersecurity First Level Assessment provides customers with a non-invasive analysis of their OT cybersecurity profile led by Schneider Electric's cybersecurity experts. The service provides a clear view of the customer's cyber status and a path to achieving cybersecurity goals, whether it's following industry best practices or complying with guidelines and standards such as ISA-62443, NIST, NERC CIP, CFATS, and ISO27001.

Upon completion of the assessment, auditors deliver an OT cybersecurity report with remedial steps to provide customers with an actionable roadmap to improve their OT cybersecurity.

This assessment is manufacturer-independent and is carried out once a year. In this way, the OT cybersecurity situation is continuously improved.

This service is aimed at the complete OT and does not only look at the Plant iT / brewmaxx system.

Scope of delivery

The solution described is made up of 2 key elements:

1. Telephone interview on the cybersecurity situation
 - Planning - The client's goals are captured and rules of engagement are established.
 - Discovery procedures – conducting virtual interviews to identify potential vulnerabilities, weak areas, and security vulnerabilities. No access to the site is required.
 - Duration approx. 4 hours

2. OT Cybersecurity Report

- Cyber classification profile and recommendations for remediation

Details

The aim is to provide customers with a profile of the cybersecurity posture of control systems based on expert analysis of data collected through interviews. Within the interview, the following points are addressed:

- Network Architecture
- PCS System Components
- Cybersecurity Procedures and Policies
- Physical Security Procedures
- Cyber Training Level of PCS Personnel
- Documented incident response procedures
- Lifecycle-Management
- Role-based security practices

The interviews are usually conducted virtually and within a single working day. Upon completion of the interview component of the review, Schneider Electric's cybersecurity experts will prepare and deliver a summary report with the cybersecurity findings, gaps, and recommended mitigations for the OT control network based on ISA 62443 standards. Schneider Electric's resources are well qualified to perform this service, with their background and advanced training in operational cybersecurity, as well as their extensive industry experience in control systems and electrical engineering processes.

The following list defines severity levels that are used throughout the document to assess impact:

- **Critical:** Exploitation is easy and usually results in system-level compromise. It is recommended to create an action plan and patch it immediately.
- **Important:** Exploitation is more difficult, but can lead to elevation of privileges and potentially data loss or downtime. It is recommended to create an action plan and patch it as soon as possible.
- **Moderate:** Vulnerabilities exist but are not exploitable or require additional steps. It is recommended to create an action plan and install patches after the high-priority issues are resolved.
- **Low:** The vulnerabilities are not exploitable, but would reduce an organization's attack surface. It is recommended that you create an action plan and patch it during the next maintenance window.

The OT Cybersecurity Report provides remedial recommendations for the findings. These remediation recommendations are recorded and processed via Changes.

Preconditions

To ensure that auditors can deliver a complete and actionable summary report, they need to learn as much as possible about the client's OT systems before conducting interviews. Therefore, the following information, if available, should be provided:

- OT network diagram with PCS layers/zones and labels showing the locations of critical assets on the network.
- Identify personnel who are most familiar with building and managing OT networks and can answer detailed technical questions about the OT devices/assets used in the customer network.
- Information on current cybersecurity policies, including existing cybersecurity tools/technologies, key standards/goals, and roles/responsibilities related to an existing cybersecurity program.

Delivery

Upon completion of the interview component of the assessment, Schneider Electric's cybersecurity experts prepare and deliver a cybersecurity assessment report with insights on the evaluated cybersecurity policies, gaps, and recommended mitigation actions based on ISA 62443 standards. This report provides a priority-

based list of actionable cybersecurity insights and expert recommendations based on the customer's control network and ISA 62443 standards.

2.4.8 Installation Services

ProLeiT has trained personnel for the installation and safe operation of hardware and software.

In the event of malfunctions or failure of a device, ProLeiT supports the installation, configuration and testing of the hardware with the appropriate technical expertise in compliance with the respective manufacturer's specifications.

ProLeiT supports the installation of the necessary software. This includes, for example, the Plant iT / brewmaxx basic installation, the application software required for operation and the complete restoration of data from backups.

2.5 Business Improvement

ProLeiT offers its customers services to continuously improve the effectiveness and efficiency of business processes.

2.5.1 Service Manager

ProLeiT offers its customers regular and individual support from a service manager as a dedicated contact person. The latter performs the following tasks:

- Dedicated contact person for all topics in the field of service management
- Online meeting with the customer's contact person
 - Verification of the processing of all open tickets of the customer.
 - Creation of statistics and overviews
 - Proof of SLA deliverables
- Ability to escalate incidents through the Service Manager
- Discussion of individual incident/problem reports
- Initiation of the investigation of complex or multiple problems that have occurred or existed over a longer period of time with the aim of developing sustainable solutions (problem management)
- Leading communication in the area of problem and change management, if included in the contract
- Initiation of contract adjustments in consultation with the ProLeiT key account / sales representative, e.g. in the event of new customer requirements, changes in quantity structures, exceeding or falling short of quotas

2.5.2 Problem Manager

The Problem Manager works in close coordination with the Service Manager. He is familiar with the customer's production processes and the project planning of the Plant iT/brewmaxx application. It serves the customer as a technical contact for the sustainable solution of malfunctions that occur in a standard process based on ITIL. The area of responsibility includes:

- Monitoring the sustainable resolution of incidents
- Proactively investigate complex, multiple or long-term problems with the aim of developing sustainable solutions
- Creation of workaround descriptions to solve known errors
- Professional exchange with the development and project planning departments of ProLeiT
- Creation of statistics and reports

2.5.3 Change Manager

ProLeiT offers its customers the processing of changes. These can be specific change requests or result from other services.

In coordination with the customer, the change manager develops the process for implementing changes on the customer's productive system.

The change manager evaluates the necessary or desired adjustments according to the following criteria: feasibility, effort estimation, test descriptions and risk assessment. An evaluated change is submitted to the customer as a Change Request (CR).

After appropriate approval and commissioning by the customer, the implementation of the change takes place according to the coordinated process for the respective categories of the change, see chapter 1.6. The change manager organizes the necessary measures.

All expenses (see above) of change management are billed over an hourly quota, see chapter 3.4. The quota size is defined in Appendix A – Chapter 7.

2.5.4 Test system and virtual factory

ProLeiT offers its customers the option of simulating the productive system in a comparable engineering environment.

In this system, changes can be tested in advance. Possible scenarios can be tested in a realistic environment. The system can be extended with additional hardware and software to implement a kind of virtual factory.

A typical setup of a test system includes the functionalities of the database server, the PLC, at least one operator station and, if necessary, associated peripherals (e.g. scanners, card or chip readers).

The infrastructure required for this purpose and the detailed scope of services are set out in **Appendix A**, Chapter 7.

2.5.5 On-site software optimizations

ProLeiT offers its customers to carry out minor optimizations of the software on site. In most cases, this optimization is carried out in the temporal context of a health check on-site (see chapter 2.4.2.2 On-Site Health Check). These include, for example, improvements in operator guidance or the optimization of automated process flows.

The aim is to open a dialogue with the operating personnel and make adjustments for optimisation on site. Any adjustments require a specification, return to the plant documentation and subsequent acceptance.

The provisions of Chapter 5 apply

Customer's obligation to cooperate. ProLeiT recommends a standardized change process for this.

2.5.6 Knowledge Management for Applications

ProLeiT offers its customers to create special knowledge articles on an agreed platform. These knowledge articles could include instructional videos, troubleshooting recommendations, decision trees, etc. The scope of the services is agreed in Appendix A – Chapter 7.

2.5.7 Training

ProLeiT offers its customers training courses for various target groups such as administrators, project planners and operators.

2.5.7.1 Standard training

The standard training courses are offered at the Herzogenaurach site in the current Plant iT / brewmaxx version in German and English. The current training offer is published on <https://www.proleit.de/training.html>.

2.5.7.2 Customer-specific training

On request, customer-specific training courses (e.g. operator training on site) can be offered by ProLeiT. For example, customized training can be delivered at the customer's site, in the customer's specific application, or in other languages.