
Reliance SCADA

Design, configuration, and operation of a SCADA system with regard to cybersecurity

- Date created: 9/2026
- Relevant Reliance SCADA version: 5.0.3

1. Introduction

The purpose of this document is to establish recommendations for the design, configuration, commissioning, and maintenance of a SCADA system with regard to cybersecurity and to provide system integrators with practical information for decision-making when designing a specific solution. The document covers two areas. The primary area comprises the security features and settings of the Reliance SCADA project itself (Chapters 3 and 4); the second area is the surrounding IT/OT (Information Technology/Operational Technology) infrastructure within which the SCADA system is operated (Chapter 5).

The target audience for this document consists primarily of Reliance SCADA system integrators, as well as SCADA/OT solution designers and architects and IT administrators.

The purpose of this document is not to provide step-by-step instructions for configuring a Reliance SCADA project or a complete list of recommended settings. Each project may be operated in a different technological environment, in a different country with different legislation, and under different customer requirements, so the requirements and objectives may vary. However, the document should provide the target audience with supporting information and summarize the tools that enable them to design, create, and operate a project as effectively as possible from a cybersecurity perspective.

When preparing this document, emphasis was placed on interpreting the recommendations in the context of the IEC 62443 series of standards, which takes into account the specific requirements of OT environments, particularly availability, integrity, security, and operational continuity.

2. Reliance SCADA

2.1 Reliance SCADA development

Reliance SCADA is developed by GEOVAP, spol. s r. o., in the Czech Republic. Development places emphasis on the cybersecurity of the resulting product and on taking into account the relevant requirements of the IEC 62443 series. The security properties of Reliance SCADA are designed with regard to the requirements and recommendations relevant to the operation of SCADA systems in critical and significant environments.

2.2 Operation and maintenance

An application in Reliance SCADA is typically developed by a system integrator and operated at the end user's site in a production environment. As part of operation and maintenance, it is **recommended** to use a supported and current version of Reliance SCADA, provided that its compatibility with the specific project and operating environment has been verified. Responsibility for updates should be assigned to the system integrator or operator according to contractual arrangements and the allocation of responsibilities. GEOVAP, spol. s r. o. regularly releases new versions and updates of Reliance SCADA. Information about new versions is available on the [website](#) or through the manufacturer's official communication channels.

3. Recommendations for a Reliance SCADA project

3.1 Project

The SCADA application itself is defined and configured in a project that is created and managed in the Reliance Design development environment. The project consists of a main file and additional files arranged in a directory structure.

3.2 Project access

It is **recommended** to protect the project at two levels:

- *file level*: The principle is to ensure, at the level of the Windows operating system and its file system, that only authorized users have access to the relevant files (typically administrators and accounts under which the relevant Reliance SCADA modules are operated),

- *project encryption*: This is a built-in feature of the Reliance Design development environment that encrypts project files using a password and limits the possibility of unauthorized access to and modification of the project. Encryption can be turned on in the New Project Wizard or later turned off/on using the corresponding commands in the *Project* menu of the Reliance Design development environment. Note: The password is required only when opening the project in the development environment or opening one of the project files using the appropriate viewer.

3.3 Target object security settings

This refers to the *Secure target objects* option in the *Project Options – Security – Checking* dialog. This option determines how and where the required permissions are checked. If turned on, permissions are checked at the target (e.g., permissions for writing a tag value that are defined for the given tag). Otherwise, permissions are checked at the source (e.g., permissions on a Button component linked to a tag).

It is **strongly recommended** to keep this option turned on. In projects created in Reliance 5, this option is turned on by default. In projects created in older versions of Reliance, it is turned off for backward compatibility. Warning: Simply turning on the option in an older project is not sufficient; the required permissions throughout the entire project must be reviewed and, if necessary, configured again.

3.4 User authentication

A user's identity is verified by entering a logon name and password.

User authentication can be performed using various methods:

- *Reliance*: user identities are authenticated directly by Reliance SCADA. The advantage is simplicity and independence from external services. The password policy defined in the project can be applied to user passwords. This is the most common method of user authentication.
- *Active Directory*: users must be defined with corresponding names in the Reliance SCADA project, but their identities are authenticated by an Active Directory server or LDAP (Lightweight Directory Access Protocol) server. The policy configured in Active Directory is used for user passwords. In the Active Directory server definition, it is **recommended** to use a secure connection and SSL encryption (*Project Options – Security – Active Directory*).
- *Windows*: users must be defined with corresponding names in the Reliance SCADA project, but

their identities are authenticated by the Windows operating system on the local computer. The policy configured in the Windows operating system is used for user passwords.

- *OpenID Connect*: users must be defined with corresponding email addresses in the Reliance SCADA project. Their identities are authenticated by an external identity provider through OpenID Connect, which is an authentication layer on top of OAuth 2.0. An example of an identity provider may be Microsoft AD FS, provided it is configured for a supported OpenID Connect scenario. The policy configured in the authentication service (e.g., ADFS) is used for user passwords. This is a modern logon method whose security depends primarily on the configuration of the identity provider, the flows used, and client protection. Its disadvantage may be a relatively demanding configuration process.

Each user can have a different authentication method configured. It is not possible to state unequivocally which method is recommended. In general, the method that meets the customer's requirements or specifications is used. An advantage of the *Active Directory* and *OpenID Connect* authentication methods is the use of centralized user management within the organization. This makes it possible, for example, to centrally block a user in all systems used within the organization, including Reliance SCADA.

Note: If user identities are authenticated using an external authentication service (*Active Directory*, *OpenID Connect*), it is **recommended** to have at least one emergency account (user) in the project that is authenticated by Reliance. This is a suitable fallback solution for situations in which the authentication service becomes unavailable.

3.5 Password policy

When checking passwords of users authenticated by Reliance SCADA or other passwords entered in the Reliance SCADA project, it is **recommended** to enable a secure password policy. This encourages users and project developers to use secure passwords. The feature can be enabled in the *Project Options – Security – Passwords* dialog, and the following properties can be configured for passwords:

- *Minimum length,*
- *Minimum digit count,*
- *Minimum special character count,*
- *Maximum number of consecutive identical characters,*
- *Password must contain letters in mixed case,*

- *Password must not match any property of user or project,*
- *Password must not be well-known weak password* (the source of the list of such passwords is the file "C:\Program Files (x86)\GEOVAP\Reliance5\Config>PasswordBlackList.txt")

The following properties also apply to user passwords:

- *Enforce password history* (the password must be changed several times before the same password can be used again),
- *Set maximum password age* (after the specified number of days since the password was changed, the user will be prompted to set a new password).

The meaning of the parameters is described in detail in the Reliance Design development environment help.

For password hashing (hash calculation), it is recommended to use the *Script* algorithm. The *Hashing function* parameter is therefore **recommended** to be set to *Script*. Note: The change will take effect only when the user subsequently logs on or when the existing password is changed in the *User Manager*.

3.6 Two-factor authentication (2FA)

To increase the security level, user authentication can be extended with a second factor. Two-factor authentication (2FA) can be enabled for each user in the *User Manager*. After entering a name and password, the user is then prompted to enter a numeric code displayed in an authentication application on a mobile device. It is **recommended** to enable 2FA for applications where reliable authentication is emphasized (i.e., where it is essential to verify that the person logging on to the system is actually the specified user). The feature can be enabled in the *Project Options – Security – 2FA* dialog, and its configuration is described in the Reliance Design development environment help.

3.7 User management

User management is performed in the *User Manager*. It allows the following objects to be defined:

- *Permission*: an object specifying an operation or command that may be performed by a user who has this permission,
- *Role*: a group of permissions suitable for easily assigning the same permissions to multiple

users,

- *User*: an object to which permissions or roles can be assigned; both options cannot be used simultaneously.

It is **recommended** to name permissions and roles appropriately, which makes them easier to understand later. Permissions should be named according to the operation (e.g., "Set tag values", "Acknowledge alarms"). Roles should be named according to the user's function (e.g., "Operator", "Process Engineer", "Administrator"). It is **recommended** to define a sufficiently granular set of permissions and roles so that user permissions can be configured as precisely as possible. Otherwise, some users may be able to perform operations that are outside their responsibilities.

3.7.1 User

A user's *Logon name* may differ from both the *Name* and the *Alias* (display name). Using a logon name that cannot be easily derived from publicly known information can reduce the likelihood of it being guessed. However, this measure does not replace a strong password, multi-factor authentication (MFA), or protection against brute-force attacks.

- Logon name: X951753
- Name: jdoe
- Alias (display name): John Doe
- Password: *****

When managing users and designing a project where security is emphasized, it is **recommended** to:

- turn on the *User must change password* option for a newly created user (so that the user cannot continue using the default password for an extended period) and turn off the *Password never expires* option. Exceptions may include service accounts (accounts used, for example, for machine logons via REST API) or emergency accounts established for situations such as unavailability of the user authentication service),
- turn on the *Enable user administration* option only for a very limited set of responsible users,
- assign the predefined *S* permission only to a very limited set of responsible users,
- assign users only the permissions they actually need (this is particularly important for service and emergency accounts),
- connect users only to those computers in the *Project Structure Manager* on which they should

be able to log on (this is particularly important for service and emergency accounts),

- turn on the *Log user logon* and *Log user logoff* options,
- not use the *Code* property (it allows logon by passing the logon name and code to the corresponding function in scripts),
- not use user logon through scripts (by passing the logon name and password to the corresponding function in scripts),
- not store passwords or other secret information in tags in any way,
- not use the *Web key* (it allows logon to the server web page by entering a key in the URL without having to know the password),
- configure *Restrictions* strictly but appropriately. This is a group of options that prevent the user from accessing certain system areas and functions of the runtime software and operating system (e.g., *Disable minimizing main window*, *Disable 'Start' menu*).

It is **strongly recommended** not to replace user management and authentication with a custom solution in any way (e.g., in scripts).

Working with the *User Manager* is similar to working with the other managers in Reliance SCADA and, like all user properties, is described in the Reliance Design development environment help.

3.7.2 Automatic user logon and logoff

It is **strongly recommended** not to use automatic logon for a user who has permission to perform privileged operations. It is **recommended** to enable inactivity checking and automatically log the user off after a specified period of inactivity. The relevant settings are available in the *Project Options – Runtime – User Inactivity* dialog.

3.8 Web server

The web server is built into Reliance SCADA runtime software and forms the basis for many of its functions. The web server may represent a significant attack surface, especially if it is accessible from remote or less trusted networks. This should be taken into account when configuring it.

The web server properties are configured in the project in two places:

- *Project Options* dialog: common project settings
- computer in the *Project Structure Manager*: settings specific to the relevant computer

3.8.1 Web server – common project settings

Common settings are configured in the *Project Options – Web* dialog.

On the *Server* tab, it is **recommended** to consider turning off the *Enable CORS (Cross-Origin Resource Sharing)* option. Turning it on is meaningful only if this part of the website is to be accessible to other domains. For example, if you embed the page in a third-party website (e.g., using the HTML *iframe* object) or call this server's REST API from *JavaScript on another* web page, you must turn on the option. Otherwise, it is **recommended** to leave the option turned off for security reasons.

On the *Headers* tab, it is **recommended** to retain the default headers. These are mostly so-called security HTTP headers, which are special instructions that the web server sends to the client (browser) with each response. They can, for example, enforce the use of HTTPS, restrict the execution of external scripts, or prevent the page from being loaded within a third-party website. The default headers are preset to provide appropriate default security parameters for the web page. The headers need to be modified only when you need to embed a page from a different web domain into the page (e.g., a window in the Smart Client module; in this case, this concerns the *Content-Security-Policy* header) or in other similar cases. More information about security headers can be found, for example, on the [Security Headers](#) or [Security headers quick reference](#) pages.

On the *Security* tab, it is **recommended** to turn on the *Secure Project section* option and select the corresponding permissions to prevent users who are not logged on from accessing project information (e.g., viewing tag values, generating reports). It is also **recommended** to turn on the *Secure server administration* option and select the corresponding permission (one available only to administrators). A user with permission to administer the web server has access to low-level diagnostic information and can perform significant operations (project restart, deployment of a new project version, logging changes, etc.).

On the *DoS Attack Protection* tab, an option can be turned on to provide basic defense against DoS (Denial of Service) attacks. If full protection against DoS attacks is required, it is **recommended** to use a professional solution or service.

On the *Internet of Things (IoT)* tab, it is **recommended** to enable the feature only if messages are actually received from the IoT network. The option is also conditional on the web server role.

On the *API* tab, it is **recommended** to enable the feature only if the API actually needs to be called from a client application. The API is very powerful and can easily be misused if insufficiently

secured. It is **recommended** to use REST API (SOAP API is retained in Reliance SCADA for backward compatibility with older projects). It is **strongly recommended** not to use REST API with security turned off (the *Secure with HMAC authentication* option or the *Secure with permissions* option). The *Publish interface description and documentation* option is **recommended** to be turned on only temporarily (to make the interface description and documentation available to client application developers during testing) and turned off before deployment to the production environment. The *Enable setting tag values* and *Enable alarm acknowledgement and reset* options are **recommended** to be turned on only if the client application actually requires these operations. The API is also conditional on the corresponding web server roles.

Tags can be accessed through the API (both read and write). Only tags shared with the API will be available in the API. These are tags for which the *Share through REST API and SOAP API* option is turned on on the *Sharing* tab in the *Device Manager*. It is **strongly recommended** to minimize the number of shared tags.

3.8.2 Web server – settings specific to the relevant computer

The computer's web server settings are configured in *Project Structure Manager – computer – Web tab*.

For computers that are not intended to provide web server functionality, it is **recommended** to consider disabling the web server completely using the *Start Web server* option. However, it must be taken into account that the *System Information* window in the visual runtime software (Reliance View, Reliance Control, Reliance Control Server) depends on the local web server. If this service is disabled, system information will not be displayed.

It is **recommended** to select the server role carefully. Use only the roles that the web server on the given computer actually needs. Removing unnecessary server roles also eliminates the possibility of exploiting the corresponding web server functions. Note: Client runtime software (Reliance View, Reliance Control) always has only the *Server Web Page* role.

It is **strongly recommended** to use HTTP only in the following cases:

- project preparation (a certificate may not be available to operate HTTPS)
- encryption (HTTPS) is provided by a reverse proxy server that communicates with the client using HTTPS, converts all of its communication to HTTP, and forwards it to the local Reliance server, and performs the reverse operation in the opposite direction. This principle is described in the *Data Servers* manual.

In all other cases, it is **strongly recommended** to operate exclusively using *HTTPS* (disable *HTTP*). The *SSL version* property is **recommended** to be set to *TLS 1.2* (until Reliance SCADA supports TLS 1.3). Certificates for HTTPS encryption can be stored in various locations. For many reasons, it is **recommended** to specify them in the *Project Structure Manager* for the relevant computer. How to enable HTTPS and work with certificates is described in detail in the *Data Servers* manual.

3.9 Project Export Wizard for Remote Users

The wizard allows the thin clients of Reliance SCADA (the Web Client and Smart Client modules) to be configured. Both clients use the web server as a data source, so the recommendations for the web server provided in Chapter 3.8 also apply to them.

It is **recommended** to enable in the wizard only the types of thin clients that are to be used. If neither Web Client nor Smart Client is to be used, both options must be turned off and the export completed.

It is **strongly recommended** to consider turning off the *Enable sending commands to devices* and *Enable alarm acknowledgement, reset, and notes* options. If these options are turned off, thin clients will not be allowed to perform these operations even if their users have the required permissions.

For the Smart Client module, it is **strongly recommended** to require *Permissions*.

It is **recommended** to turn off the *Enable running Web Client as applet* option.

3.10 Ensuring high availability of the application

To ensure high availability of the application, it is **recommended** to consider using data server redundancy (if the primary server fails or undergoes maintenance, the secondary server can take over its function). Reliance SCADA provides this functionality. More information about data server redundancy is provided in the article [Reliance 4 Data Server Redundancy](#)

3.11 Communication drivers and OPC UA

When configuring communication with devices such as PLCs or telemetry stations, it is **recommended** to use only the necessary communication channels. If the configuration in Reliance SCADA allows it and the given device supports it, it is generally **recommended** to:

- use authentication,
- use encryption,
- enable data integrity checking,
- prefer secure protocol variants over their unsecured variants

It is advisable to configure timeouts, retries, and responses to communication failure carefully so that unsafe process behavior (looping) does not occur. Encryption on the device side may be slow, so it must not be introduced without verifying compatibility and its impact on performance, latency, and availability.

For OPC UA (Open Platform Communications Unified Architecture) devices in the Device Manager, it is **recommended** to set:

- the *Security mode* property to *Digital signature and encryption*
- the *Security policy* property to *Basic256Sha256*
- the *Authentication* property to *Name and password* or *Certificate*

As part of certificate management (Trust Management), it is **recommended** to use a strict whitelist (the server must not automatically trust new clients; each new certificate must be manually approved by an administrator). If there is a large number of OPC UA servers, deployment of GDS (Global Discovery Server) for centralized certificate management can be considered.

3.12 Additional important recommendations

It is also **recommended** to:

- disable remote project management if it is not used. This is the *Enable remote control* option in the *Project Options – Runtime – Other* dialog. If remote control is used, it is **strongly recommended** to configure required permissions that are available only to administrators,
- require corresponding permissions for all privileged operations,
- secure the execution of scripts that perform privileged operations (i.e., any user action that invokes such scripts must require the corresponding permission),
- require corresponding permissions for access to parts of the project in which privileged operations can be performed (e.g., process control windows, service windows),
- require corresponding permissions for the acknowledgement (or reset) of critical alarms,

- minimize the number of shared tags (shared with OPC clients and through the API).

3.13 Logging

Logging is the recording of information about the operation of Reliance SCADA and about events that may be significant from an operational or security perspective. Log records generally serve the following purposes:

- Reliance SCADA developers use them to check application operation and identify possible software errors,
- security analysts use them to perform offline analysis of recorded events,
- online monitoring by specialized software, such as SIEM (Security Information and Event Management), which automatically and immediately evaluates abnormal behavior (e.g., an unauthorized access attempt) based on recorded events and informs the appropriate personnel about the situation.

Logging is important today and it is **recommended** to perform it. It is advisable to log all security- and operation-relevant event types and to configure the logging level appropriately. The logging level has a major impact on the number of log records and therefore on processing capabilities.

Records can be stored in files (text files in the project directory) and/or sent to a *Syslog* server. Both methods can be used simultaneously, and a different set of logged event types and a different level can be configured for each. Software for online monitoring of log records generally requires Syslog as the source of log records.

Logging to files is configured in the *Project Options – Runtime – Logging* dialog. Syslog servers are defined in the *Project Options – Runtime – Syslog* dialog. For a computer in the *Project Structure Manager – Other tab*, the Syslog servers to which records are to be stored are then specified.

3.14 Built-in project checking tools

The Reliance Design development environment contains the following tools for checking a project from a cybersecurity perspective:

- Security audit,
- Project diagnostics.

It is **recommended** to use both tools during project creation and before every deployment of a new project version or Reliance SCADA version to the production environment.

3.14.1 Security audit

The *Project – Perform Security Audit* command is available in the main menu of the Reliance Design development environment. This command generates a report (text file) that summarizes all Reliance SCADA project settings that affect security. It also contains information about all network connections (remote IP addresses, numbers of open TCP ports) on individual computers defined in the project. The report can be used for the following purposes:

- checking whether the project is configured in accordance with this document,
- supporting information for IT administrators for configuring server and workstation security, establishing the required network access paths, and other related settings.

3.14.2 Project diagnostics (security)

Project diagnostics is a very useful project checking tool that makes it possible to identify errors and inconsistencies in a project. It can also check security. When a problem is identified, it is easy to navigate directly to the relevant property in the user interface and correct the problem.

More information about project diagnostics can be found in the article [Project diagnostics helps find problems and inconsistencies in a visualization project](#).

3.14.3 Scripts for Microsoft Defender firewall

Another useful tool is the *Project – Generate Firewall Scripts* command, which generates *PowerShell* scripts for automatically creating rules for the required ports. This enables IT administrators to automatically open the required ports that Reliance SCADA will need. Note: Only Microsoft Defender firewall is supported.

4. Recommendations for application development

For secure application development, it is **recommended** to:

- record requirements, changes, tests, errors, and approvals,

- separate the permissions of the developer, tester, and approver,
- manage the application's source and configuration files using a version control system, such as Git or SVN (Subversion). Reliance SCADA includes the *RDTMerge.exe* tool for easy comparison and merging of files in RDT (Reliance Data Table, binary format),
- back up and retain a functional version of the project,
- regularly test negative scenarios (invalid input, loss of communication, invalid user, repeated command, database unavailability, recovery from backup),
- regularly update project documentation.

To ensure maximum continuity and minimize outages, it is **recommended** to follow the points below so that application unavailability is as short as possible:

- plan all maintenance carefully and prepare for it,
- before deploying a new project version or a new Reliance SCADA version, test it in a relevant test environment,
- have a functional project backup and the Reliance SCADA installer available in case a rollback is required,
- have up-to-date documentation available for the procedure for deploying a new version to production.

5. Recommendations for the external environment

This chapter provides only a general framework. Detailed designs of the network architecture, operating systems, and security products must be addressed in separate documentation.

5.1 Network environment

In the network environment, separate corporate IT, SCADA, and OT networks. Use segmentation according to function and criticality. Control communication between zones using firewalls with explicitly permitted rules. Disable unnecessary routing and direct interconnection between the IT and OT networks. Ensure separate management of network devices. Restrict access from standard user segments to the SCADA environment. Use network traffic monitoring and detection of unusual behavior. Document network topology, addressing, and communication rules.

In the core network, separate operational and administrative communication. Restrict access to

critical VLANs (Virtual Local Area Network) and routed segments. Use redundancy where availability is required. Ensure access control for switches, routers, and management interfaces. Prevent unauthorized devices from connecting.

Place in the DMZ (demilitarized zone) only services that must mediate communication between zones. Prevent direct communication flow from IT to the SCADA network. For remote access, prefer a bastion host / jump server in a controlled zone. Separate data services from administrative remote access. Consider unidirectional gateways or other communication direction restrictions for highly critical systems.

5.2 Remote access and service

Allow remote access only for a specific purpose, for a specific user or supplier, for a limited period, and through an approved entry point. Require multi-factor authentication (MFA) where technically possible. Use a secure VPN (Virtual Private Network) or bastion host / jump server. Prohibit direct supplier connections to the internal SCADA network. Log logons, session start and end, and changes performed. Require operator approval for critical interventions. Remove temporary permissions after the service intervention is completed. Do not use permanently active shared accounts for service. Prohibit uncontrolled use of common remote desktop tools. Minimize and secure network connections, use segmentation, controlled remote access, backup, patch testing, and monitoring of the OT environment.

5.3 Workstations and servers

Maintain supported versions of operating systems. Verify updates in a test environment first. Coordinate updates with operational outages. Record exceptions and systems that cannot be updated. Use compensating measures for unsupported systems.

Use malware protection according to compatibility with Reliance SCADA. Verify the impact of antivirus scanning on performance and timing. Consider application whitelisting or similar control of permitted software. Regularly update security signatures if the operating mode allows it. Use scanning exclusions only when justified and documented.

Keep the host-based firewall active if it is compatible with Reliance SCADA. Allow only necessary inbound and outbound communication. Manage rules centrally or through a controlled procedure. Record and test rule changes.

Disable unnecessary services, ports, and protocols. Restrict local administrative privileges. Disable automatic execution from removable media. Control the use of USB devices. Secure BIOS/UEFI and boot devices. Restrict interactive logon for service accounts. Configure security policies appropriate to the criticality of the system. Ensure physical protection of servers, workstations, and network devices.

5.4 Monitoring and detection

Centrally collect selected system, network, and application events. Monitor configuration changes, failed logons, new accounts, network traffic changes, communication failures, connection of unknown devices, unauthorized file changes, and remote service sessions. Assign responsibilities for evaluating alerts. Protect monitoring systems against compromise. Configure OT monitoring so that requirements for low load and operational stability are met.

5.5 Physical security

Restrict entry to server rooms, electrical cabinets, control rooms, and process areas. Control access by service personnel. Record physical interventions on devices. Protect backup media and documentation. Ensure adequate power supply, UPS (Uninterruptible Power Supply), air conditioning, and protection against fire or water.

5.6 Operation, maintenance, incident response, responsibility, and documentation

Before putting the application into the production environment, perform security tests, acceptance tests, and hand over the documentation.

The documentation should define routine system administration, adding and removing users, change approval, updates, backup, recovery, service interventions, outage resolution, log review, and escalation of security events.

In the event of an incident, define who reports, evaluates, and manages the incident. Define contacts for the operator, integrator, manufacturer, and security team. Prepare scenarios for account compromise, ransomware, SCADA system unavailability, unauthorized configuration manipulation, communication failure, remote access compromise, and loss of historical data.

Always preserve evidentiary information and audit records.

Do not perform an uncontrolled restart or recovery without assessing the impact on the process. After an incident, perform root cause analysis and update the measures. Regularly test the incident response plan.

Regularly train operators in the secure use of the SCADA system, administrators in accounts, logs, backups, and changes, and personnel in remote access rules; remind them of the risks of phishing, removable media, and password sharing.

The document should clearly specify who is responsible for SCADA project configuration, security architecture, network infrastructure, operating systems, antivirus protection, identity management, backup, updates, monitoring, incident response, supplier security, and approval of exceptions.

The documentation may specify exceptions to responsibility. Each deviation from the recommended setting should include a description of the requirement or limitation, the affected system or component, the security risk, the reason why the recommended measure cannot be used, the compensating measure, the risk owner, operator approval, and the date for re-review.

6. Other

6.1 False positive detection by antivirus software

The entire Reliance SCADA package consists of a number of software modules based on different development platforms and developed in different programming languages and environments, which is also related to the use of corresponding protection mechanisms. For example, the core modules are native Windows applications (x86/x64) in PE (Portable Executable) format and are protected by an external tool to make them resistant to reverse engineering. Due to the advanced nature of this protection, antivirus software may incorrectly identify a protected file as malicious (a so-called *False Positive* detection). The procedure for resolving this situation is described in the article [What to do if antivirus software reports that a Reliance program file contains a virus](#)

6.2 Concerns about using the Web Client module because of the Java platform

The Web Client module is based on the Java platform. During deployment, this fact may raise concerns among security specialists. The fact that the module uses the Java environment does not

in itself have to represent a security problem if the module is operated in a supported and controlled manner. It is true that certain vulnerabilities were identified in the past when running Java applets or applications using Java Web Start. Both execution methods require installation of the Java Runtime Environment (JRE) in the operating system. These mechanisms have historically been associated with security risks. However, the Web Client module can also be launched in another way, using Web Client Launcher. It includes JRE but does not require installation in the operating system. The JRE used is optimized only for the Web Client module, and other applications normally cannot use it as they could a system-installed JRE. The JRE is based on OpenJDK (an open-source project), so this method of operating Web Client may eliminate the need to use Oracle's commercial JRE. It is therefore **recommended** to launch Web Client using the launcher. More information about Web Client Launcher can be found in the article [Reliance Web Client Launcher](#)

6.3 SBOM

SBOM (Software Bill of Materials) is a formal list of all components, libraries, modules, and dependencies that make up a given software product. An up-to-date SBOM is created for the main program modules for each new version of Reliance SCADA. GEOVAP, spol. s r. o. may provide these files to the customer based on an individual agreement.

7. Conclusion

The security of Reliance SCADA cannot be ensured solely by configuring a firewall or installing antivirus software. The foundation is a combination of a securely configured project, a well-designed user permission system, secure communication, defined rules for development, deployment, and backup, secure remote access, and appropriately segmented network infrastructure. This document focuses primarily on the security capabilities of a Reliance SCADA project, its creation, deployment, and operation. Other areas are described only at a high level as necessary context, not as a detailed administrative guide.
