CODESYS Security

Whitepaper

Version: 8.0
Template: templ_tecdoc_en_V1.0.docx
File name: CODESYS Security Whitepaper.docx

CONTENT

1 Security in industrial control applications

1.1 Introduction

Even as the IT security of commercial computers is a common task, the protection of industrial control applications against unauthorized access or even violent attacks has not been a major topic in the past. At least since the well-known Stuxnet attack, this situation has changed. Governmental institutions, such as ICS-Cert or the German Federal Office for Information Security (BSI, *Bundesamt für Sicherheit in der Informationstechnik*), note a drastic rise in security incidents in factories, plants, and other industrial automation applications.

Meanwhile, vulnerabilities are systematically searched and detected by security consultants. Today, protection against these kinds of incidents is inevitable for the automation equipment of industrial machines, factories, and plants to protect the following:

- availability of controller functionality
- application function
- confidentiality of the application and the application source code
- integrity of the application function, the development system function, and employed components
- handling of the entire function
- authenticity of controllers and their data

In addition to functional improvement, security improvement needs to be continuously developed further. Despite this, it is not possible to achieve 100% security. Even when designed with state-of-the-art security measures, a system may still be vulnerable via connections to the networks of suppliers, contractors, and partners.

1.2 Areas of application and aim of this whitepaper

This document will enable manufacturers of intelligent automation devices, system integrators, and operators of industrial control applications to protect their installation by means of integrated security measures within the IEC 61131-3 compliant automation software CODESYS. It provides an introduction to security topics in industrial automation and control systems, points out the responsibility of involved parties, and shows which present and future CODESYS measures assist in creating the desired level of security protection. Furthermore, it presents the handling of detected CODESYS vulnerabilities.

1.3 Consequences

Regardless of threats due to unintentional misuse or intentional attacks with different severity and effort, the security of an automation system is a task which concerns all parts of an industrial control application (e.g., in machines or plants and which cannot be guaranteed through a single measure).

Furthermore, security requires a certain effort:

- Physical access control to security critical installations
- Additional processing power on devices
- Configuration effort for the application programmer and operator
- Loss of convenience in operation and maintenance
- Security training for system integrators and operators

Each operating company must evaluate for itself how much security it needs and how much it is prepared to spend on that goal.

Therefore, manufacturers of automation products have to provide appropriate means of protecting critical parts of their automation system to the system integrator and operator of such industrial applications.

The IEC 61131-3 automation software platform CODESYS offers several such measures as described in Section 0. These measures do not replace the responsibility of the system integrator or operator of the industrial control application of the security tasks, such as the indication of threats and the definition of necessary measures in order to achieve the desired level of security. But they do help.

2 Terms and definitions

2.1 Asset

The purpose of industrial automation environments is to produce goods or to maintain machine functions or process flows, for example. Different parts of the industrial environments are threatened by security risks, which can harm or prohibit this purpose. With reference to Figure 1, the assets of an industrial automation environment are the controller, the application executed on the controller, the development system used for the application development, and the handling of the whole system.

2.2 Vulnerability

Typical automation environments can be harmed at different locations:

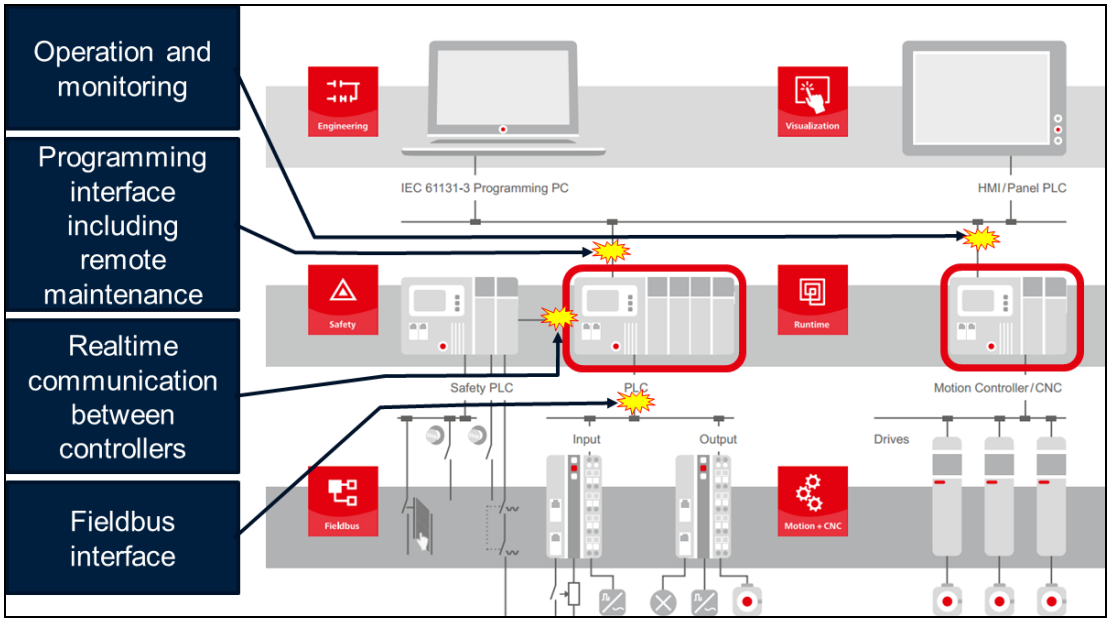

Figure 1: Possible vulnerabilities in a typical automation environment

2.3 Protection levels

The IEC 62443 international standard defines different protection levels:

- Level 1: Occasional and accidental threat
  Examples: Hard disk failure, operating error
- Level 2: Intentional threat by simple means
  Example: Password guessed correctly
- Level 3: Intentional threat by highly developed means
  Example: Hacker tools
- Level 4: Intentional threat by highly developed means and extended resources.
  Examples: Specific development, knowledge of the application, or corruption of insiders

The order of the level corresponds to their likelihood that the described threats will actually occur.

2.4 Controller

The industrial computer that controls an automation installation may be called a PLC[1], PAC[2], Motion Controller[3], ECU[4], DCS[5], PCS[6], or with any other technical term. In any case it executes the automated function. This programmable intelligent device is thus the major target for security attacks. **Furthermore, these controllers[7]**

[1] PLC = Programmable Logic Controller
[2] PAC = Programmable Automation Controller
[3] Motion Controller = PLC / PAC for dedicated motion control tasks
[4] ECU = Electronic Control Unit
[5] DCS = Distributed Control System
[6] PCS = Process Control System
[7] In the following text all the mentioned different devices are meant when talking about “controller”

need to be programmed for their designated use. This means that they all contain a programming interface which can be abused easily. Due to this designated use, it is not possible to categorically prevent an access for programming or reprogramming of applications that are executed on the controller. Therefore, the protection of these controllers and their communication interfaces has a high priority for both the system integrator and the operator of such devices.

2.5 Application

The operational function that is executed on the controller represents the functional description of the purpose of industrial automation environments in software. It is loaded to the controller through its programming interface.

2.6 Threat

The operational function of an industrial automation system can be damaged or interrupted in various ways. Mostly intentional threats, such as sabotage, vandalism or spying, are discussed as the focus of security measures. Nevertheless, up to now unintentional malfunctions due to faulty hardware and software, faulty operation during commission, or in service more often lead to the harm of the assets.

2.7 Protected environment

All industrial automation systems are required to be executed in environments that disable intended or unintended faulty operation and thus the risk of harm of assets. Nevertheless, every system needs access during installation, commissioning, operation, or maintenance. Thus, splitting the whole system into subsystems is required to enable controlled access to every subsystem only for authorized personnel. See Section 3.1 for more information.

3 General means for protecting industrial control applications

In the first step, **all commonly known security measures for standard PCs should be applied in networks with industrial automation equipment**, such as

- Virus protection
- Strong and regularly changed passwords
- Firewall protection
- Use of VPN tunnels for inter-network connections
- Careful contact to removable data carriers, such as USB flash drives

Furthermore, a well-defined user and permission management for the access to the controllers and their interconnecting networks is mandatory.

In addition, several additional general measures are required for each machine or plant builder:

3.1 Usage in a protected environment

Locating the controller in a protected environment is absolutely required in order to avoid accidental or intended access to the controller or its application, which is executed for the function of the machine or plant.

Such a protected environment can be, for example, within

- locked, electric control cabinets without communication access from outside,
- an intranet network with well-defined user rights without access from outside, or
- a network with internet access only through a well-maintained firewall via a VPN tunnel.

Obviously, the degree of protection decreases in this list.

For creating such a protected environment, several rules have to be followed:

- Keep the trusted network as small as possible and independent from other networks.
- Protect the cross-communication of controllers and the communication between controllers and field devices via standard communication protocols (fieldbus systems) by appropriate measures.
- Lock such networks and strictly separate them from commonly used access.
- Use fieldbus system only in protected environments. They are not protected by additional measures, such as encryption. An open physical or data access to fieldbus systems and their components is a serious security risk.

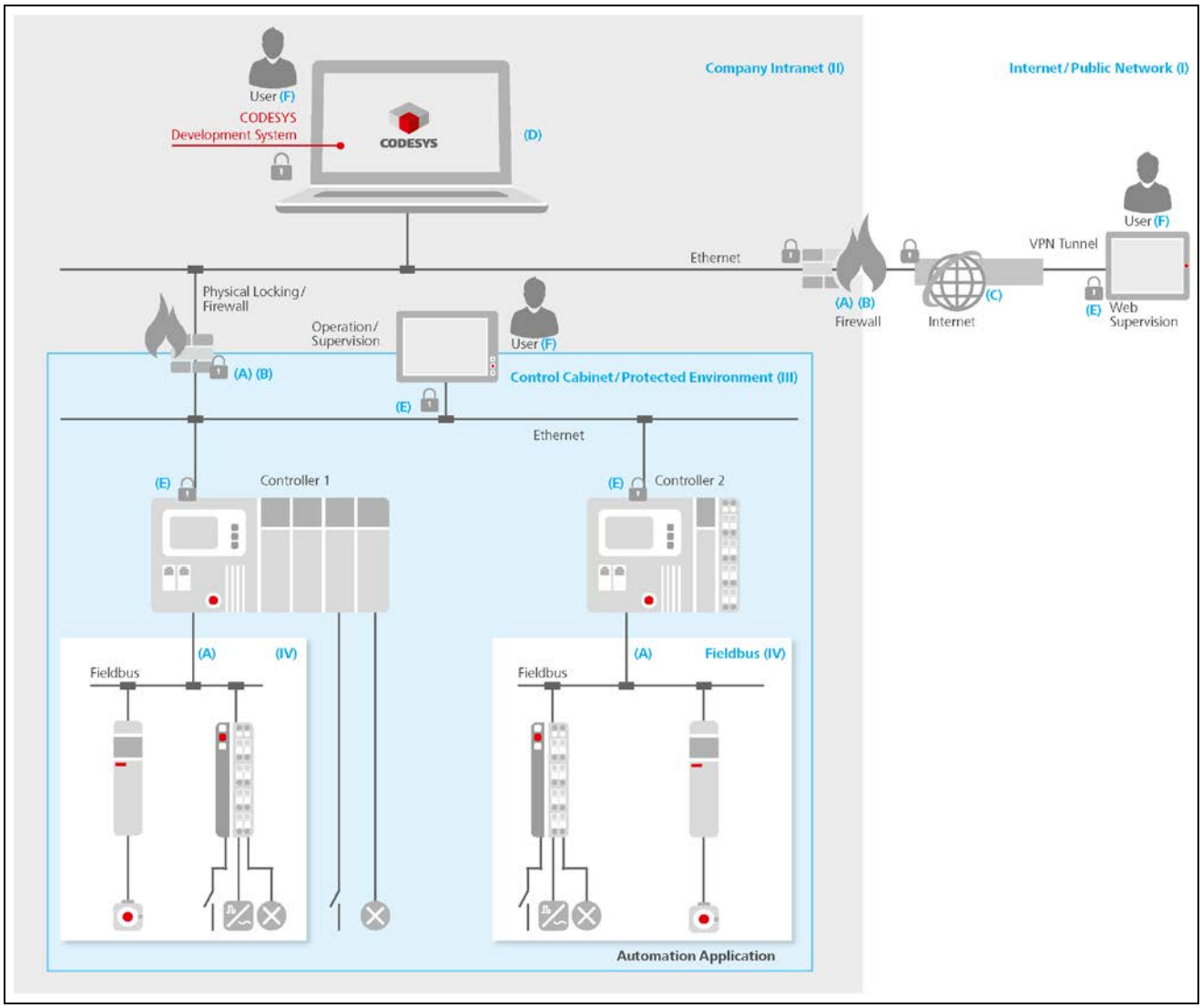

Figure 2: Typical environment in automation applications with areas of different protection level

Explanation / legend for Figure 2:

Separated networks (completely separated or connected via secure Firewall):

I. External network, e.g. Internet, dial-up connection
II. Company network
III. Machine / production site network
IV. Fieldbus

Protection of the infrastructure

A. Mechanical access protection (e.g., locked control cabinet)
B. Firewall[8]
C. Virtual Private Network (VPN)
D. Virus protection, network / Windows user administration
E. User management with appropriate authentication method (e.g., dongle, password)
F. Employee training concerning security measures

[8] The firewall between the networks II and III must protect in both directions. Malware in the company network might affect the production site network and vice versa.

3.2 Users with awareness for security

As most of the reported security incidents occurred without intention due to handling or device errors, the user of industrial controllers has a crucial role concerning the security protection. Thus, it is required for both, machine / plant builders and operators alike to know about the possible threats and the infrastructural measures which are necessary to avoid these threats.

Users of the CODESYS Development System and programmable controllers should furthermore know about the available security features and are required to consider them when programming the control application. In order to achieve this goal, it is advisable to join special training from security specialists either within a company or from externals.

4 Security responsibilities in industrial control applications

In the setup of industrial control applications, several active parties and suppliers are involved: the suppliers of software and hardware components, the system integrator or builder of the industrial control applications, and the operator. As IT security is a comprehensive task, all of the aforementioned parties have to make a certain effort in order to protect the application against attacks.

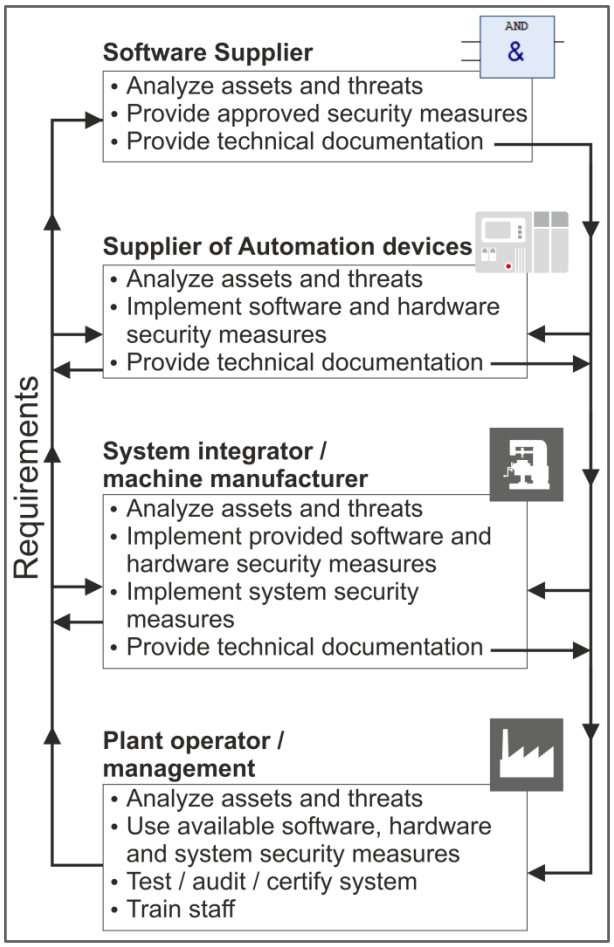

Figure 3: Relation between different parties in industrial control applications concerning security

Further details of the different responsibilities and the roles within the parties are explained in the VDI/VDE2182 standard.

5 Available onboard security measures within CODESYS

It is the objective of 3S-Smart Software Solutions, the manufacturer of the IEC 61131-3 automation software CODESYS, to offer measures which assist the user in the task of protecting his application concerning availability, integrity, and confidentiality. These measures tackle protection level 1 and 2 threats (see Section 2.3). On a long-term basis, also level 3 threats will be covered.

The CODESYS architecture contains two main parts: the integrated development environment (IDE - the CODESYS Development System) running as the user interface on the workstation computer, and the runtime system (CODESYS Control) on the programmable device that executes the application code. Both parts operate together seamlessly when programming an industrial automation application. Therefore, the security measures also influence these main parts. In addition, CODESYS provides such measures that can be activated by the user from the programmed application code. As the CODESYS Development System integrates multiple visualization functions that enable security-critical access to the control application and thus the machine/plant, the system also provides security measures for this aspect.

The following sections describe measures and features which are or will be available in the latest generation of CODESYS (V3). In order to protect the application and the controller, using the latest version of the CODESYS Development System is required. It can be downloaded free of charge at www.codesys.com. Furthermore, using the appropriate runtime system on the controller is also required. As described in Section 7, detected vulnerabilities will be fixed in patch versions. Thus, it is always highly recommended to use the latest software versions with these patches.

The tables below provide an overview on the measures, their locations within CODESYS, and for whom they are intended. Each measure is explained. For technical information about the realization of the described measures, it is recommended to look into the CODESYS Online Help, installed with the CODESYS Development System.

CODESYS Development System

Measure	Explained in Section (Page)	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Encryption of the source code of the application	5.1.1 (12)		X		Occasional/unintentional threats and attacks
User administration on project level	5.1.2 (12)		X		Occasional/unintentional threats and attacks
Sign and encrypt CODESYS-related files	5.1.3 (13)	X	X	X	Attacks
Signing of compiled IEC libraries	5.1.4 (13)	X	X	X	Attacks

CODESYS Runtime System

Measure	Explained in Section (Page)	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Access to the runtime system with authentication / permission management	5.2.1 (13)	X	X	X	Occasional/unintentional threats and attacks
Encryption and signing of the executable application code	5.2.2 (13)	X	X		Attacks
Controller operation mode	5.2.3 (14)		X		Occasional/unintentional threats and attacks
Interactive login	5.2.4 (14)	X	X		Occasional/unintentional threats
Disaster recovery	5.2.5 (15)	X	X	X	Occasional/unintentional threats
Communication encryption between the IDE and the controller	5.2.6 (15)	X	X	X	Attacks
Secure OPC UA Server	5.2.7 (15)		X	X	integrity and/or confidentiality of data
Configurable symbols sets via user management / Symbolconfiguration	5.2.8 (15)		X	X	confidentiality of data

IEC 61131-3 Application code

Measure	Explained in Section (Page)	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Access restrictions out of the application / library	5.3.1 (16)	X	X		Occasional/unintentional threats and attacks
Unlocking additional functions	5.3.2 (16)	X	X		Occasional/unintentional threats and attacks

CODESYS Visualization

Measure	Explained in Section (Page)	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Visualization User Management	5.4.1 (16)		X	X	Occasional/unintentional threats and attacks
Communication encryption for the CODESYS WebVisu	5.4.2 (16)	X	X	X	Attacks

5.1 Available onboard security measures of the CODESYS Development System

5.1.1 Encryption of the source code of the application

Measure for system integrators

The application source code contains the detailed information on the function of the machine/plant and thus the intellectual property of its manufacturer. Therefore, protecting the application source code has a high priority whenever it contains confidential information.

In the CODESYS Development System, the entire project can be encrypted either via password or optionally with a workstation hardware USB dongle (CODESYS Security Key). The password solution uses the AES algorithm, the hardware dongle is based on a proprietary solution from the company WIBU Systems. Without the password or the bound security key(s), it is not possible to open or edit the project source file.

The advantage of password protection is the absence of additional hardware, whereas protection with the hardware key has a much higher protection level, as a password can be hacked or published. The project can be bound to multiple different such keys at the same time. Thus, access to source code can be limited to the number of security keys and therefore passed to multiple users at the same time. Furthermore, the risk of losing the access to source code due to a destroyed or lost key can be minimized by binding it to at least one more key than necessary.

Starting in CODESYS V3.5 SP10, the source code can also be protected using X.509 certificates. In this scenario, the source code will be encrypted symmetrically (AES algorithm). The symmetric key will then be encrypted asymmetrically (RSA algorithm) using the public key of each user sharing the source code. Optionally, the source code can also be digitally signed using the private key associated with the X.509 certificate of the current user. The signature will be saved side-by-side with the source code in a file with the extension ".p7s" following PKCS#7 format for digital signatures.

This measure protects the confidentiality of intellectual property.

5.1.1.1 Secured project file with integrity check

If encryption is not an option, the project file is saved in a proprietary format and its integrity will be checked each time the project is loaded. This integrity check is active by default. It may be incompatible with older versions of the programming system.

For a better protection of the application data, the activation of one of the above mentioned encryption features is recommended.

This measure protects the integrity of the project file and is available since version V3.5 SP13 of CODESYS.

5.1.2 User administration on project level

Measure for system integrators

In addition to the protection of the entire application source code, CODESYS provides the capability of read/write protection of individual objects in the project with a user administration. Such a protection can be defined for menu commands as well as for specific object types (e.g. creation of tasks, POUs, Methods, GVLs etc.) or existing objects in the project (like project settings or dedicated POUs or tasks).

By the means of this user administration, it is furthermore possible to limit the range of functionality in a very fine granular manner. So the access rights can be adapted to specific security needs (e.g. security critical functions, such as the use of scripting options, can be restricted to users with explicit permissions).

The measure protects the confidentiality of intellectual property as well as the integrity of the application code.

5.1.3 Sign and encrypt CODESYS-related files

Measure for suppliers of automation components, system integrators and operators

Any file access by the CODESYS Development System can be authenticated. Thereto an X.509 signature is checked when reading any file and a X.509 signature is created on writing a file. When the signature is invalid or not existent a meaningful error message can be reported by the PlugIn which tried to access the file.
CODESYS-related files are:

- Libraries/Projects
- Device Descriptions
- All .dll and .exe files of the Standard CODESYS setup
- GACs

5.1.4 Signing of compiled IEC libraries

Measure for system integrators and operators

Since CODESYS V3.5 SP15 an IEC library can be signed with an X.509 certificate if it is stored as compiled library.

While compiled libraries ensure the protection of the source code, the signature allows a verification of the authenticity of the library. Signed libraries are explicitly indicated in the library manager of the CODESYS project.

5.2 Available onboard security measures of the CODESYS Runtime System

5.2.1 Access to the runtime system with authentication / permission management

Measure for suppliers of automation components, system integrators and operators

There are different phases of an industrial application: from the start of the development of the control source code to its commissioning up to the production with the machine or plant and its maintenance. These phases are commonly operated by different technicians with appropriate qualification levels.

With the consideration of these qualification levels as well as the threats of a possible use beyond task or competence, it makes sense to limit the use for certain user groups.

CODESYS supports such an authentication and permission management with a user and user group administration. It depends on the security policy of the runtime system, if the user management is enforced by default or not.
If it is not enforced, everyone is a member of the administrator group and has unlimited rights on the controller until the user management is activated.
If it is enforced, then it has to be activated during the first login by specifying an administrator user (if no user has already been predefined by the device manufacturer).

With corresponding commands in the CODESYS Development System, the current administrator of the controller can easily add or delete online users. Furthermore, the administrator may combine users to a user group to limit permissions. A predefined permission system is already available and can be adapted to the requests.

As soon as at least one new user is added, all users have to authenticate with their usernames and passwords for each online connection to the controller. Passwords are transferred encrypted (by default using asymmetric cryptography) and stored encoded as scrypt hashes on the runtime system.

In accordance to protection level 1 and 2, this measure reduces the threat of accidental or intended access to the running controller concerning availability and somehow the integrity of the compiled application executed on the controller.

5.2.2 Encryption and signing of the executable application code

Measure for suppliers of automation components and system integrators

The application development is terminated as soon as the executable application code is running on the controller and the function of the industrial application is released, except for further maintenance. Even if the application code is available in a compiled and thus non-readable and editable binary, there is a certain security

threat for the manufacturer of the application. The entire control system, including the executable application code, could be reproduced and used without permission.

5.2.2.1 Encryption with CodeMeter®

In order to avoid these threats, the executable application code can be encrypted by a hardware dongle with the CodeMeter® technology from the company WIBU Systems. This hardware dongle can be either a USB key (CODESYS Runtime Key), for instance for PC-based systems running Windows® or Linux, or a special preprogrammed flashcard offered by WIBU Systems. Each of these keys has a unique serial number. During the encryption of the executable application code, the binary code is linked exclusively to the key.

This means that the encrypted binary code cannot be reverse engineered. As a result of binding the binary code, the application cannot be executed on this or any controller without the bound key. Thus, the threat of unauthorized reuse on plagiarized applications is avoided and the confidentiality of the application is protected.

5.2.2.2 Encryption and signing with X.509 certificates

Since CODESYS V3.5 SP10 it is also possible to use X.509 certificates to encrypt the executable application code instead of using the above mentioned CodeMeter® technology. So the code is only executed on a runtime system that owns the private key of a certificate to which the application has been bound to. It is also possible to bind the application to different controller certificates. In this case, the code is executed on every controller that is the private key owner of at least one of those certificates.

Additionally to the encryption, the application can also be signed with a X.509 certificate. The result is that the application is only executed if the specified certificate of the originator is registered as trusted in the runtime. This measure protects the controller against execution of code from unauthorized/untrusted originators.

The management of X.509 certificates within the CODESYS Runtime System can be done using the CODESYS Security Agent. See https://store.codesys.com/codesys-security-agent.html and the corresponding Documentation[9]

5.2.3 Controller operation mode

Measure for system integrators

A controller does not distinguish between productive operation, commissioning, and development. This leads to a security risk which can be avoided by introducing an operation mode.

CODESYS provides the capability of assigning three different operating modes to the controller. The “Debug” operation mode is the default and allows all online commands, including deleting, changing, and updating the application. The “Locked” mode protects the developer from unintended access to controller (e.g., while simultaneously programming several controllers). As soon as the application commissioning is terminated, the controller can be switched to “Operational” mode which prevents all unintended access to the running application. Thus, this mode ensures that the controller loads the correct application after rebooting and that no more debugging measures are activated.

In combination with the user management on the controller (see Section 5.2.1), switching the operation mode can be limited to certain users.

With the controller operation mode, the integrity and availability of the device is protected from unintended external data access.

5.2.4 Interactive login

Measure for suppliers of automation components and system integrators

Unintended access to the incorrect controller in a network with multiple devices can harm the machine or the production. CODESYS supports an interactive login to avoid this threat. The login can be either confirmed by pressing a button on controller, by entering the serial number of the dedicated controller, or by a blinking of the controller. This security level 1 protection is already implemented in the CODESYS Development System. As this measure depends on the hardware functionality of the controller, it is a task of the controller manufacturer to implement the appropriate interaction in his device.

The interactive login protects the availability and reliability of the downloaded application and thus the controller.

[9] https://help.codesys.com/webapp/_csa_f_codesys_security_agent;product=codesys_security_agent;version=1.1.0.0

5.2.5 Disaster recovery (Backup / Restore)

Measure for suppliers of automation components, system integrators and operators

Even if there are already measures to protect the executed application code on the controller against unintended harmful access, such a harmful access could nevertheless happen e.g. especially due to a breakdown of the controller itself. In order to reduce the consequences of this threat, a comprehensive backup and disaster recovery function is available. In case of an unexpected damage, it will be possible to restore the complete backup of the controller application with simple procedures.

5.2.6 Communication encryption between the IDE and the controller

Measure for suppliers of automation components, system integrators and operators

Even if there is an authentication for the access to the controller available, communication between the CODESYS Development System and the CODESYS Control runtime system could be hacked and thus harm the application. A TLS 1.2 encryption of the communication between the CODESYS IDE and the controller is available and can be activated in the CODESYS IDE.

This protects the integrity and confidentiality of the complete online communication between the CODESYS IDE and the controller, containing the application code as well as all exchanged data (e.g. monitored values).

It depends on the security policy of the runtime system, if encrypted communication is possible or not. The runtime system can be configured with one of the following security levels for encrypted communication:
- No encryption: no encrypted communication is possible
- Optional encryption: encrypted or unencrypted communication is possible
- Enforced encryption: only encrypted communication is possible

See chapter 5.2.2.2 how to manage the X.509 certificates within the CODESYS Runtime System.

5.2.7 Secure OPC UA Server

Measure for system integrators and operators

OPC UA is an industrial communication protocol for interoperability developed by the OPC Foundation. The CODESYS Runtime System can optionally be equipped with an OPC UA Server functionality in order to provide access to the controller and the application on the controller. Several security measures are provided as follows:

5.2.7.1 OPC UA Server: Support of X.509 based communication

One feature of the OPC UA Server is to operate with an encrypted communication based on X.509 certificates. The different security profiles are defined by OPC Foundation.

Depending on the profile this protects integrity (for signed only profiles) or integrity and confidentiality (for signed and encrypted profiles) of the data that is exchanged with the connected clients.

This measure is available since version V3.5.11.0 of the CODESYS OPC UA server.

See chapter 5.2.2.2 how to manage the X.509 certificates within the CODESYS Runtime System.

5.2.7.2 OPC UA Server: User management available

With an activated user management for OPC UA the establishment of a session is restricted to dedicated users.

This measure protects the confidentiality of the data that is exchanged with the connected clients and is available since version V3.5.13.0 of the CODESYS OPC UA server.

5.2.8 Configurable symbols sets via user management / Symbolconfiguration

Measure for system integrators and operators

Within the Symbolconfiguration one can collocate subsets of all the defined symbols (symbol sets). With an activated user management these symbol sets are assignable to dedicated users for visibility and the determination of the read/write access rights.

This measure protects the confidentiality of the data that is exchanged with the connected clients and is available since version V3.5.13.0 of the CODESYS Symbolconfiguration.

5.3 Security measures that can be activated out of the CODESYS application code

5.3.1 Access restrictions out of the application/library

Measure for suppliers of automation components and system integrators

The CODESYS application programmer can restrict the access to the controller and the application by the application code itself. A special library offers commands which may deactivate security critical access to the controller, such as online program changes, breakpoints, stopping the application, file transfer, or access to variables. Typically this measure is used to prevent code or configuration changes during the execution of time critical application code.

The measure protects the integrity of the application code.

5.3.2 Unlocking additional functions

Measure for suppliers of automation components and system integrators

If the application code may contain additional functions (e.g., for service or maintenance tasks), these functions may be locked for the standard operation. By the means of hardware dongle (e.g., CODESYS Security Key, CODESYS Runtime Key), such functions may be unlocked for authorized staff.

The locking function may be programmed within the application source code and protects the application from level 1 and level 2 threats.

5.4 Security measures with CODESYS Visualization

5.4.1 Visualization User Management

Measure for system integrators and operators

The integrated CODESYS visualization enables a direct operation of the controller respectively the application and thus the entire machine or plant. It is highly recommended to separate the operation into different parts or screens according to their level of functional and security influence. CODESYS provides the capability of protecting individual visualization elements as well as entire visualization screens of the project by the means of a special visualization user management. This user management enables the limitation of the range of functionality for certain operators. Security-critical operation modes, such as the export of production data, the start/stop process of the machine/plant, and the access to dedicated service functions, can be restricted to operators with explicitly assigned permissions.

The measure protects the confidentiality of intellectual property, as well as the availability and reliability of the machine or plant process.

5.4.2 Communication encryption for CODESYS WebVisu

Measure for suppliers of automation components, system integrators and operators

In order to prevent the hacking of the communication between a CODESYS compatible controller, which supports the CODESYS WebVisu, and an internet browser on a PC or mobile device, an HTTPS connection with encryption is available. It protects the integrity of the displayed data.

See chapter 5.2.2.2 how to manage the X.509 certificates within the CODESYS Runtime System.

6 Scheduled and future additional on-board security measures of CODESYS

In addition to the already available security measures, there are several measures that will or may be implemented in CODESYS. Similar to the measures already available, they are listed below in a table and explained.

Measure	Explained in Section (Page)	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Easier authentication	6.1.1 (17)		X	X	Occasional/unintentional threats
Configuration of programming and operating interfaces	6.1.2 (17)		X		Occasional/unintentional threats and attacks
Support for the security feature settings	6.1.3 (18)	X	X	X	Occasional/unintentional threats and attacks
Read only mode	6.1.4 (18)		X		Occasional/unintentional threats and attacks

6.1 Future additional on board security measures of CODESYS

In addition to already available or scheduled security measures, further measures are possible and taken into account:

6.1.1 Easier authentication

Measure for system integrators and operators

As already pointed out, the increase of protection by the means of security measures (e.g., by entering an access code is only gained with a loss of convenience). Thus, there is certain likeliness that measures are avoided. With an optional mapping of the authentication on a hardware dongle or on LDAP as the user management of the IT system, this loss of convenience can be compensated. Thus, such a mapping may have a positive effect on the use of the protection measures and on the protection of the application.

This effect can be achieved by an easier authentication on the workstation level and the controller level.

Examples:

- The workstation dongle (CODESYS Security Key) contains the user information for the access the controller.
- The runtime dongle (CODESYS Runtime Key) bound to the controller activates the operation mode “Debug”.

6.1.2 Configuration of programming and operating interfaces

Measure for system integrators

So far there is no limitation concerning the programming and operating interfaces to the controller. This means that CODESYS does not check the IP address of a user accessing the controller.

Certain profiles could restrict the access to the controller (e.g., for programming, operating or read-only debugging). These profiles will define a set of permissible IP addresses (IP white-listing) for the mentioned tasks. Furthermore, such a profile can disable the routing option.

This measure will prevent unintended access to controllers within an open network.

6.1.3 Support for the security feature settings

Measure for suppliers of automation components, system integrators, and operators

All described security features request their configuration and a certain experience how to do it correctly. To support that work, various options are taken into consideration:

- Security wizard for an overall setup of all features
- Security feature documentation including user guidelines and checklists, more than already available in the CODESYS online help
- Training module covering the topic “Security” will be added to the basic training course. Part of the training will be the display of general vulnerabilities, the connection of a controller to the internet (e.g., firewall and VPN configuration and the disconnection from open networks)
- Training and certification for base knowledge security in automation systems

6.1.4 Read-only mode

Measure for system integrators

When opening a project, the user can set the option that neither the project nor the application on the controller can be changed. This protects the application source code and the controller against unintended changes.

7 Networks ports used by CODESYS

As described, controllers are designated to be programmed. Thus, CODESYS compatible controllers need certain open network ports for their designated use. The default communication ports are listed below.

Ports	Communication purpose	Reconfiguration possible?
1740 – 1743	UDP Runtime communication	No
11740	TCP Runtime communication	Yes
1217	TCP Gateway communication	Yes
8080	CODESYS WebServer	Yes
443	CODESYS WebServer (SSL)	Yes
4840	CODESYS OPC UA Server	Yes (since of CODESYS V3.5 SP7)

In addition to these ports, system integrators or operators may open communication ports for other purposes (e.g., FTP server, maintenance or diagnostic shells, terminal applications, etc.) System integrators or operators are fully responsible for the protection of these ports against unauthorized access.

8 Handling of security vulnerabilities in CODESYS

CODESYS is developed under consideration of security aspects. Product security is of utmost importance to 3S-Smart Software Solutions. Nevertheless vulnerabilities may be detected.

Vulnerabilities are handled accordingly to the 3S-Smart Software Solutions Coordinated Disclosure Policy.

This policy describes the complete process of receiving information, internal handling and disclosure of vulnerabilities in CODESYS products.

All security issues reported to 3S-Smart Software Solutions are thoroughly investigated, assessed and prioritized. Goal is to identify all possibly affected products, determine the root cause of the vulnerability, and develop a resolution or remediation. As part of this 3S-Smart Software Solutions also searches for security vulnerabilities in the vicinity of the reported issue, also in other CODESYS products and protocols.

In general security patches are released for the latest version of the affected CODESYS products. Once a resolution (usually software update) or mitigation is available, 3S-Smart Software Solutions will release a security advisory.

The advisories and further security documents are published on the CODESYS security web site https://www.codesys.com/security.

As each security vulnerability case is different, we may take alternative actions if necessary, including accelerate or delay the release of an advisory or not issue a notice at all. If the disclosure is limited to a specific group of customers, we may contact customers directly and/or publish it limited to OEM customers only.

For manufacturers that have implemented the CODESYS runtime system as the programming interface on their controllers (OEM customers), 3S-Smart Software Solutions provides an additional security page in the customer area of the CODESYS web site. Beside OEM relevant security information there is also a registration form for a security mailing list. In case of detected vulnerabilities, OEM customers registered for this mailing list are informed via email as soon as possible.

9 Conclusion

The security of control systems in industrial automation applications becomes increasingly critical as different networks are connected and systems are integrated. Accordingly, system integrators and users of industrial automation applications need to pay increased attention to these issues. Security needs to be a continuous activity accompanied by systematic risk assessment, similar to functional and safety improvements. Even if security can never be 100% effective, implementation of available security measures as well as careful planning can bring security up to a level that is adequate for any particular application and installation.

10 Disclaimer

3S-Smart Software Solutions GmbH assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided on good faith by 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact support@codesys.com.

11 Bibliography

The latest version of this document can be found here:
https://customers.codesys.com/fileadmin/data/customers/security/CODESYS-Security-Whitepaper.pdf

Standard	Title
IEC 61131-3 ed3.0	Programmable controllers – Part 3: Programming languages
IEC 29147	Information technology – Security techniques – Vulnerability disclosure
IEC 30111	Information technology – Security techniques – Vulnerability handling processes
IEC 62443	Industrial communication networks – Network and system security
VDI/VDE 2182	IT-security for industrial automation

Change History

Version	Description	Date
1.0	First Release	21.04.2014
2.0	Feature Disaster Recovery in CODESYS V3.5 SP8 added	28.01.2016
3.0	- New security features in CODESYS V3.5 SP10 added - Handling of security vulnerabilities updated - Smaller corrections	02.01.2017
4.0	Handling of security vulnerabilities updated, Disclaimer added, Bibliography extended	26.04.2017
4.1	Security measure: Sign & encrypt CODESYS-related files	09.05.2017
5.0	OPC UA secure communication updated.	27.06.2017
5.1	CODESYS Security Agent added	12.12.2017
6.0	Release	09.01.2018
6.1	- Minor corrections - Added chapter 5.1.1.1 Secured project file with integrity check - Updated: 5.2.7 Secure OPC UA Server - Added chapter 5.2.7.2 OPC UA Server: User management available - Added chapter 5.2.8 Configurable symbols sets via user management / Symbolconfiguration	28.06.2018
7.0	Release after formal review	02.07.2018
7.1	- Chapter 5: added / corrected references - Updated: 5.2.1, 5.2.6 - New: 5.1.4	04.05.2020
8.0	Release after formal review	10.06.2020