Features and Recommendations

CODESYS Control – OEM Documentation

Version 3.5.10.0

Content

1 Introduction

In this document in the chapter Features, you find listed all new features and improvements of the current version of the CODESYS Runtime System (CODESYS Control) which are optional and so they must be considered by the OEM customer to integrate in their controller or not. We provide in the subchapters “Recommendations” some hints, in which cases and conditions we recommend to use each feature.

2 Features

Here we describe all optional features, which are available at least with the current version V3.5.9.0. So still existing features are described here too.

2.1 Encrypted CODESYS - RuntimeSystem communication

Available with: V3.5.10.0

With this new feature you can encrypt the communication between CODESYS and the RuntimeSystem via TLS based on X.509 certificates.

For details see the feature description under “Runtime System Documentation/Features/Security/Encrypted communication”.

Recommendations:

We recommend to use this feature, if CmpOpenSSL is integrated in the RuntimeSystem or OpenSSL is available on the OperatingSystems!

2.2 Signed & encrypted IEC application code

Available with: V3.5.10.0

With this new feature you can encrypt and/or sign the IEC application code downloaded to the RuntimeSystem. This covers the download, online change and the bootproject.

For details see the feature description under “Runtime System Documentation/Features/Security/Encrypted communication”.

Recommendations:

We recommend to use this feature, if CmpOpenSSL is integrated in the RuntimeSystem or OpenSSL is available on the OperatingSystems!

2.3 Security manager

Available with: V3.5.10.0

There is a new component in the RuntimeSystem called CmpSecurityManager. This component specifies the security level of all available security features.

For details see the feature description under “Runtime System Documentation/Features/Security/SecurityManager”.

Recommendations:

We recommend to use this component, if CmpOpenSSL is integrated in the RuntimeSystem or OpenSSL is available on the OperatingSystems!

2.4 X.509 certificate management

Available with: V3.5.10.0

There is a new feature to manage X.509 certificates on a RuntimeSystem. For this the CmpOpenSSL component must be integrated in your RuntimeSystem. The configuration can be managed via PlcShell commands yet.

For details see the feature description under “Runtime System Documentation/Features/Security/Certificate handling”.

Recommendations:

We recommend to use this component, if CmpOpenSSL is integrated in the RuntimeSystem or OpenSSL is available on the OperatingSystems!

2.5 Supervisor

Available with: V3.5.10.0

There is a new component in the RuntimeSystem called CmpSupervisor. This component can be used to support a hardware watchdog available on the controller or to use for a hardware watchdog on a Hilscher CIFX card.

For details see the feature description under “Runtime System Documentation/Features/Supervisor” and for an example “Runtime System Documentation/Examples/RtsHardwareWatchdog.c”.

Recommendations:

We recommend to use this component, a hardware watchdog is available on the controller and/or a Hilscher CIFX card could be used on the target!

2.6 New scan information in the communication dialogue in CODESYS

Available with: V3.5.10.0

There are new scan information available in the communication dialogue in CODESYS. For example the SerialNumber, TLS supported/not supported or the number of available channels is displayed in the dialog as additional information.

Recommendations:

- none -

3 General Recommendations

3.1 Integration of OpenSSL

To realize most of the security features, you need a crypto component. In the runtime system we use OpenSSL by default. The integration of OpenSSL can be done in 2 ways:

1. Operating system integrated OpenSSL:

   If your operating system contains an implementation of OpenSSL, you can use the CmpOpenSSL component of the runtime system without the OpenSSL implementation. In this case you have to defined the compiler switch CMPOPENSSL_USE_SYSLIB building the runtime system.

2. Using the OpenSSL source components shipped with the runtime system:

   If your operating system does not contain an implementation of OpenSSL, you can use the CmpOpenSSL component of the runtime system with the OpenSSL implementation. In this case you must not define the compiler switch CMPOPENSSL_USE_SYSLIB building the runtime system! Additionally you have to include all OpenSSL modules into your build environement specified in CmpOpenSSLDep.h.

For details see the feature description under “Runtime System Documentation/Features/Security/OpenSSL”.

3.2 Target Serial Numbers

There are 2 different serial numbers provided in the runtime system for different needs. These are described in the following chapters.

3.2.1 Official Serial Number

This is the official serial number of the device, typically visible on a label on the controller. This serial number is used e.g. to identify a target with the “interactive login” feature or to use if for a unique nodename for the communication.

Recommendations:

So we recommend to support this official serial number on every target! For this you have to implement the interface function SysTargetGetSerialNumber() in your SysTargetOEM component. This serial number is additionally used for the “New scan information in the communication dialog in CODESYS” since v3.5.10.0!

3.2.2 Secure Serial Number

This is the secure serial number that based on hardware characteristics of the device. This serial number is used e.g. to bind licenses at this single device and so this feature must be implemented with a higher security level. So this secure serial number must not be modifiable e.g. like retrieving from a local file.

Recommendations:

We recommend this secure serial number for targets, that intend to use WIBU CodeMeter softcontainer support and for targets, that has the possibility to use secure hardware characteristics for this secure serial number.

Version History

Version	Description	Author	Date
0.1	Creation	AH	28.11.2016
1.0	Review and Release	TZ	06.12.2016