Features and Recommendations

CODESYS Control – OEM Documentation

Version 3.5.9.0

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 Configurable Filepaths

Available with: V3.5.8.0

The general intention of this feature is to group and redirect files on the PLC and completely separate them from runtime sytem kernel files, i.e., files and folders that are created and accessed via SysFile/SysDir or CAA File interface functions.

For Details a new documentation is provided under Runtime System Documentation/Tutorials/FilePaths and Placeholders.

Recommendations:

- none -

2.2 Backup/Restore IEC Applications

Available with: V3.5.8.0

The new feature of V3.5 SP8 “Backup&Restore of application related files” has the aim to backup and restore all files an application deals with, i.e., the application itself and all files it reads or writes, such as visu files, data base files, the retain variable file, and all files accessed via IEC.

For Details and requirements a new documentation is provided under Runtime System Documentation/Tutorials/FilePaths and Placeholders.

Recommendations:

The main requirement is the PlcLogicPrefix=1 setting which introduces a new folder and file structure. Please take note of the chapters ‘Backup&Restore’ and ‘New folder structure via PlcLogicPrefix’ in the new documentation under Runtime System Documentation/Tutorials/FilePaths and Placeholders.

2.3 Coredump

Available with: V3.5.5.0

A core dump is a memory snapshot of the application data. In case of an exception error, runtime systems that support this feature automatically store a core dump file (<application name>.core) in the application directory on the controller.

This feature is available in 2 different manners: 1. Online Mode: you can also generate a core dump explicitly if the application is currently stopped at breakpoint or if an exception has occurred. In this case, CODESYS stores the core dump file in the project directory and not on the controller. 2. Offline Mode, you can load the core dump from the controller to the project. An online view of the application is then displayed with the data and values at the time of the exception.

To use this type, the runtime component CmpCoreDump must be available in the runtime system.

Recommendations:

We recommend this feature for all targets to have a possibility to investigate seldom exceptions or difficult errors in machine environments! So if there are no resource limitations to integrate CmpCoreDump, you should integrate this component.

2.4 OPC UA Server

Available with: V3.5.7.0

The OPC UA Server is protected by an OEM license on 3S.dat, so the OPC UA Server must be purcahsed for your target. The OPC UA Server is scalable in its feature set to adapt to the resource consumption as best to the target.

Recommendations:

But we don't recommend the OPC UA Server for very low perfromant embedded targets, because the OPC UA Server doubles nearly the resource consumption of the runtime system. Additionally if you intention to use X.509 encrypted communication, you need the CmpOpenSSL component on the runtime system which increases the resource consumption once more.

2.5 OpenSSL + Certificate Management

Available with: V3.5.9.0

For every X.509 certificate that is used in the runtime system, we need the CmpOpenSSL or the integrated OpenSSL library in the operating system. Actually we use X.509 certificates for the https communication for the WebServer and in the future for different usages (encrypted CODESYS and OPC UA communication, signing/encraption bootproject, User-Identification, etc.).

Recommendations:

So we recommend to integrate CmpOpenSSL in your target, if it is not still avaialble in the operating system on the controller.

2.6 C-Code Integration

Available with: V3.5.7.0

C-Code Integration for end users is supported with CODESYS V3.5.7.0 or newer. Of course, OEMs can still integrate own C-Code functions as runtime components. C-Code Integration for end users allows to download components dynamically, together with the application download. The package includes the development of a AP PlugIn, that works together with the OEMs toolchain for the device (C compiler).

Recommendations:

- none -

2.7 Consistent Monitoring

Available with: V3.5.9.0

With this new consistent synchronized access feature, you can read/write a variable list consistent online via the CmpIecVarAccess component. Currently this feature can be mainly used by the PLCHandler. For synchronous consistent access, the communication task in the runtime system, which handles the symbolic client request, waits when processing a read or write request until a time is found when no IEC task is executed. As soon as this gap is found, the restart for the IEC tasks is prevented until all values are copied from/to the variables list. Then all IEC tasks are scheduled as usual. Thus this synchronized consistent access may lead to the delayed starting of the IEC tasks what is reflected in a higher jitter. As all applications are administrated by a common scheduler in the runtime system, this potential deterioration of the real-time behavior affects all applications on the device. So all applications of the device are affected, independently of whether they contain a symbol configuration or whether they are loaded to the controller from one or from several CODESYS projects. Therefore the runtime system only allows the synchronized consistent access if all applications, that are loaded on the controller at the time of access, allow this access. This can be configured in the CODESYS IDE for each PLC device using the device properties or the symbol configuration dialog.

Caution! On the basis of the increased jitter the synchronized consistent monitoring is unsuitable for motion and real time-critical applications. For these reasons the synchronized consistent access should only by activated and be used, if it is absolutely necessary. For many clients this in genaral not the case (e. g. visualization clients) or there exist already other synchronisation means between IEC application and the symbolic client (PLCHandler, OPC Server) using for example handshake variables.

To use this new feature CODESYS, PLCHandler und CODESYS runtime version >= V3.5.9.0 is required.

For more information see also the CODESYS online help object Symbol configuration “Configure synchronisation with IEC tasks”.

Recommendations:

- none -

2.8 Interactive Login and Wink

Available with: V3.5.5.0

The interactive login and wink feature is a security feature to prevent a user from login to a wrong controller and to identify a single controller. There is a feature description and an example in the RTS-OnlineHelp that describes this feature in detail.

Recommendations:

We recommend this feature for all targets to support a more secure way for the users to login.

3 General Recommendations

3.1 WIBU CodeMeter

CodeMeter is a product from WIBU-Systems to us a hardware device (USB-Dongle, CF-card, etc.) or a softcontainer to manage software licenses or decryption/encryption of the bootproject. For this feature, the CmpCodeMeter must be integrated in the runtime system. For the softcontainer, on the controller there must be a secure serial number to bind the container.

Recommendations:

We recommend this feature for every target, because this is the requirement to use e.g. features from the CODESYS Store. The usage of the CmpCodeMeter component depends on the hardware and operating system, and so please check first, if CmpCodeMeter is available for your target.

3.2 Target Serialnumbers

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 Serialnumber

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.

3.2.2 Secure Serialnumber

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.

3.3 Node Name

The NodeName, which is displayed in CODESYS in the communication dialog scanning all targets, should be unique by default. That means the NodeName can contain the official serial number in the NodeName (e.g. “MyController_1234-5678”) or the IP-Address of the controller, which is most of the time unique (e.g. “MyController_192.168.123.234”). This requirement focused on the use case where an end user takes several identical controllers of one vendor and plugs at once into his plant or machine. And so every controller should show up in the commuication dialog at a scan with a unique nodename. Furthermore this is important to allow a client to connect by using the nodename and not the variant logical CODESYS address.

Recommendations:

We recommend that the NodeName should be unique by default on all targets of an OEM vendor.

3.4 Redundancy

The CODESYS Redundancy Toolkit includes two additional runtime components, that have to be added to the runtime configuration. For the programming system, the configuration editor is included in the CODESYS setup. The runtime components are CmpRedundancy and CmpRedundancyConnectionIp. CmpRedundancyConnectionIp can be replaced by a OEM specific implementation of the connection. CODESYS Redundancy allows to synchronize two controllers. The bood application files are synchronized. In operation, both controllers monitor each other, and take over control over the IO system if the other controller fails. CODESYS Redundancy is available for Windows, RTE, WinCE, Linux and VxWorks. It is not available for embedded systems. Fieldbusses supported is EtherCAT, others are possible. With SP8 or newer, files needed for visualization are synchronized, too.

There is a separate OEM documentation available.

Recommendations:

- none -

Version History

Version	Description	Author	Date
0.1	Creation	AH + TZ	24.05.2016
0.2	Features documented	AH	13.06.2016
1.0	Review and Release	TZ	14.06.2016
1.1	Added legal note	RT	23.08.2016
2.0	Release	MaH	23.08.2016

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