Release Note CODESYS V3.5 SP16 Patch 5

25.05.2021

1 Release Notes

Key	Summary	Release Note	Component/s
CDS-57116	**Compile:** There should be a possibility to clearly detect new instances	**[[COMPATIBILITY_INFORMATION]]** There might now be more calls to FB_Init and less calls to FB_Exit of a function block when inserted via online change. The first call to an instance should be a FB_Init(bInCopyCode = FALSE) and the last call to an instance should be a FB_EXIT(bInCopyCode = FALSE). [[GENERAL]] During Online Change: The FB_Init-method of a newly inserted instance of a function block in another Function block instance will now be called one initial time with bInCopyCode = false. If the change triggers an online change of the existing (outer) function block, the newly inserted inner function block will be called a second time with bInCopyCode = true. Analog, if an inner function block is deleted FB_Exit on the inner function block will be called with bInCopyCode = false. If the deletion triggers an online change of the outer function block, the inner function block will get a call of FB_EXIT with bInCopyCode = true before the final call with bInCopyCode = false.	CODESYS
CDS-63205	**CrossRef:** Possibility to see all references of a single array element	**[[GENERAL]]** Won't fix, because accessing an array with a constant index indicates a bad software design. There are several possibilities to avoid such an index access, e.g.: 1.) Enumerations An enum type can be introduced. The names reflect the numeric value of the enum values and can be used directly for an index access. The occurrences of such an enum member can be browsed in the crossreference view.	CODESYS

		2.) Structure instead of an array A structure can be used instead of an array and the structure components can get meaningful names. The occurrences of such a structure component can be browsed in the crossreference view. Both possibilities lead to better readable source code. 3.) Filter The filter functionality (introduced with V3.5 SP13) allows to filter only the accesses with a given (constant) index. With V3.5 SP16 this will also work for ARRAY OF INT because the filter can be applied to the text showing the context of the array access.	
CDS-65129	**Online Device:** Unencrypted password transmission in special cases	**[[GENERAL]]** Solved as part of CDS-63951. For more details see **Advisory 2019-08**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=	CODESYS
CDS-65917	**Compiler:** Input expression of "AnalyzeExpressionCombined" containing several parts leads to incorrect/not working analyzation result sOutString with too many brackets	**[[GENERAL]]** The Output string and the table treat the variables differently. So the String is not just a string display of the table content. The table treats OR similar to AND and interprets the content of OR, whereas the String interprets OR like a > b. If the a OR b is FALSE, the whole expression will be part of the string. If a OR b is TRUE, the expression will not be part of the string. The table used to handle OR just in the same way as AND: so that for a(TRUE) OR b(FALSE), the variable b would be part of the table, even if the expression does not produce FALSE. The logic for the analyzation in the table is now: - for exp1 AND exp2: both expressions will be tested for FALSE, and be part of table, if they are false - for exp1 OR exp2:	CODESYS

		We first test whether the OR is FALSE, and only if it is, then both expressions will be tested for FALSE, and be part of table, if they are false - NOT (exp1 AND exp2) will be treated like NOT exp1 OR NOT exp2 - NOT (exp1 OR exp2) will be treated like NOT exp1 AND NOT exp2 XOR will be treated like a > b: the whole expression is part of the table or the string, if it produces FALSE. String and Table will always be empty, if the tested expression evaluates to TRUE. The change in behavior is best demonstrated with an example: In the table: a=FALSE AND (b=FALSE OR c=FALSE) old: a | b | c new: a | b | c a=TRUE AND (b=FALSE OR c=FALSE) old: b | c new: b | c a=FALSE AND (b=TRUE OR c=FALSE) old: a | c new: a a=TRUE AND (b=TRUE OR c=FALSE) old: c new: empty a=FALSE AND (b=FALSE OR c=TRUE) old: a | b new: a a=TRUE AND (b=FALSE OR c=TRUE) old: b new: leer a=FALSE AND (b=TRUE OR c=TRUE) old: a new: a a=TRUE AND (b=TRUE OR c=TRUE) old: empty new: empty String: a=FALSE AND (b=FALSE OR c=FALSE) old: a | (b OR c) new: a | b OR c a=TRUE AND (b=FALSE OR c=FALSE) old: (b OR c) new: b OR c a=FALSE AND (b=TRUE OR c=FALSE) old: a new: a a=TRUE AND (b=TRUE OR c=FALSE) old: empty new: empty a=FALSE AND (b=FALSE OR c=TRUE) old: a new: a a=TRUE AND (b=FALSE OR c=TRUE) old: empty new: empty a=FALSE AND (b=TRUE OR c=TRUE) old: a new: a a=TRUE AND (b=TRUE OR c=TRUE) old: empty new: empty	

CDS-66210	**Visu:** Only configured startvisualizations should be accessible	**[[GENERAL]]** For more details see **Advisory 2020-04**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13136&token=c267875c01ea70bc9613bc39c684eedc17f55420&download= For security reasons only the configured start visualizations (in the visualization clients below the Visualization Manager) are allowed to be accessed when using a visualization profile >= V3.5.16.0. The previous behavior can be restored by setting the compiler define VISU_NO_STARTVISU_CHECK. However, this should be used only if necessary for compatibility reasons to prevent opening this security problem for the application. Instead of this compiler define consider if adding additional start visualizations by adding additional visualization client objects is an option.	CODESYS
CDS-67481	**Core Separation:** Merge branch into trunk	**[[GENERAL]]** The Core interface component has been refactored. The interfaces from Core have been swtiched to: - Commands - Compiler (was already existing) - ComponentModel - ComponentModelWin - DeviceIdentification - Engine - EngineWin - External - Help - MessageService - MessageServiceWin - MessageStorage - Objects - ObjectsWin - Online - OnlineWin - OptionStorage - OptionStorageWin - Printing - Security - SecurityWin - SystemInstances - TargetSettings	CODESYS

		- UndoManager - Views **[[COMPATIBILITY_INFORMATION]]** The "old" Core.dll is now a compatibility interface which has to be present in "Common" and the new "CompatibilityInterfaces" folder, which is located beside the Common directory. Using remote calls in CODESYS Test Manager prior version 4.3.1.0 may cause an exception because a *.profile could not be found. A valid workaround is creating an empty dummy *.profile file with the required name. It is no longer possible to install CODESYS SVN < 4.2.6.0 into CODESYS Development System >= 3.5.16.0.	
CDS-67819	**InputAssistant:** Javascript code from libraries can be executed.	**[[GENERAL]]** For more details see **Advisory 2019-05**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12940&token=7723e5ed99830656f487e218e73dce2de751102f&download=	CODESYS
CDS-67992	**NetVars:** Setting for packet size	**[[GENERAL]]** Compiler Version >= 3.5.16.0 and Runtime Identification >= 3.5.16.0. The packet size for UDP telegrams is no longer hardcoded in the NetVarUdp library. Instead the packet size can be configured in a new parameter list contained in the library. The value of the packetsize target setting must not be greater than the value configured in the library, otherwise the netvars refuse to initialize with a corresponding error code set in the diagnosis data.	CODESYS
CDS-69841	**WinCE:** Reading/Writing 64 bit values to Cortex devices is incorrect	**[[COMPATIBILITY_INFORMATION]]** On Windows Embedded Compact 2013 devices with Cortex CPU, the 64 bit integers are no longer atomically accessed. This affects monitoring, and online writing/forcing of values.	CODESYS

CDS-62813	Weak protection for **transmitted passwords**	**[[GENERAL]]** Solved as part of CDS-63951. For more details see **Advisory 2019-08**, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-08_CDS-62813.pdf	CODESYS Control
CDS-62814	Use of weak hashing algorithm for **online passwords**	**[[GENERAL]]** Solved as part of CDS-63951. For more details see **Advisory 2019-08**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=	CODESYS Control
CDS-63766	**FixedPinned-Tasksgroups** should be assigned to different cores	**[[COMPATIBILITY_INFORMATION-EndUser]]** If you use several taskgroups with the specifier "FixedPinned", every taskgroup is bound to one core, but to different cores for every taskgroup (beginning with the first core beneath the "system" core!). So typically we start with core1 for the first taskgroup, second taskgroup on core2 and so on. So the core assignment is quite similar to the "SequentialPinned", but here it is used on taskgroup layer!	CODESYS Control
CDS-64207	Setting a new **password** does not request the old one	**[[GENERAL]]** Solved as part of CDS-63951. For more details see **Advisory 2019-08**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=	CODESYS Control
CDS-64209	**Online UserManagement:** Login tries are counted only for existing user names	**[[GENERAL]]** Solved as part of CDS-63951. For more details see **Advisory 2019-08**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=	CODESYS Control
CDS-65602	**CmpLog: Logger Messages** are not written to disk at once even if LT_DUMP_ALWAYS is set	**[[COMPATIBILITY_INFORMATION-OEM]]** To flush every logger entry directly into the logfile, there is a new option for the logger: LT_DUMP_SYSFILE_FLUSH	CODESYS Control

		So this performs a SysFileFlush for every log entry intependently, if the logger has the additional option LT_DUMP_ASYNC or LT_DUMP_ALWAYS.	
CDS-65675	Setting a new **password** does not request the old one - runtime system part	**[[GENERAL]]** Solved as part of CDS-63951. For more details see **Advisory 2019-08**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=	CODESYS Control
CDS-66949	**ComponentManager:** Create a SysTask as main thread of the runtime system	**[[COMPATIBILITY_INFORMATION-OEM]]** There are new options for CMInit3() to execute CH_INIT_XXX, CH_EXIT_XXX and CH_COMM_CYCLE hooks in own SysTask (see CMItf.h for details): - RTS_CMINIT_OPTION_INITTASK - RTS_CMINIT_OPTION_COMMCYCLETASK - RTS_CMINIT_OPTION_EXITTASK	CODESYS Control
CDS-67291	**RTS VxWorks:** Runtime crashes after PlcExit->PlcStart	**[[COMPATIBILITY_INFORMATION]]** Once the CODESYS runtime (VxWorks) has been stopped with PlcExit( ) it cannot be started anymore with PlcStart( ). In this case a reboot (PowerOff/On) of the target system is recommended, before starting the CODESYS runtime (VxWorks) again.	CODESYS Control
CDS-67591	**WinCE:** improve comm cycle handling thread	**[[COMPATIBILITY_INFORMATION-OEM]]** From version 3.5.16.0 on, the Windows CE runtime system can handle the startup, shutdown and cyclic handling of low priority stuff in different ways. The default behaviour is different from past versions: the runtime system calls CMInit3 for creating a system task doing all these things. If the OEM wants to go back to the old behaviour, he can #undef USE_CM_TASKS in SysWinCE.h and re-compile CeWin.c and Maince.c. In this case, the Windows CE specific part of the RTS calls CMInit as in the past, and creates its own task for the comm cycle handling. For headless systems, the defines NoTargetVisu and _3S_HEADLESS_	CODESYS Control

		must be used as before, in the Visual Studio project settings (the new define USE_CM_TASKS should be modified in SysWinCE.h, however). Recommendation: set USE_CM_TASKS. In this case, initialization, shut down and comm cycle are protected through exception handling, without any code required from the OEM side. As before, these two C files are delivered as source code, so the OEM can modfiy and extend if needed or wanted.	
CDS-67596	**CmpItf.h :** Due to removed CMPID's for IEC code components customer builds fail	**[[COMPATIBILITY_INFORMATION]]** Component IDs of IEC libraries are removed from the runtime system with CDS-65850, because they are managed in other scopes. So: If you need the component ID of an IEC library, it can be retrieved in the runtime system by: CMPID cmpId; CMItf .h:: CMGetCmpId(<ComponentName> &cmpId); The prerequisite for that is that the corresponding library have to register itself at the component manager with the CmpComponentManager.library with the function: CMAddComponent2(<ComponentName>, <Version>, ADR(<ComponentId>), ADR(result));	CODESYS Control
CDS-68341	**Webvisu, Webserver:** PLC crashes with crafted request	**[[GENERAL]]** For more details see **Advisory 2019-10**, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-10_CDS-68341.pdf	CODESYS Control
CDS-68651	**CODESYS Control VxWorks:** Support LLVM compiler	**[[GENERAL]]** With Service Release 6.00 of VxWorks 7 WindRiver replaced the toolchain based on GNU by LLVM (clang) for the Hardware architectures ARM and X86. Starting with version >= V3.5.15.40 CODESYSControl also supports LLVM (clang).	CODESYS Control

		Please note that the CODESYSControl built with GNU is not able to run on a VxWorks Image built with LLVM and vice versa, which means that users have to order a new Runtime Tool Kit based on LLVM, if they upgrade their ARM or X86 based systems to a newer VxWorks version (VxWorks7 SR6.00 or newer).	
CDS-68816	**VxW7_0620 / LLVM:** Add check for INCLUDE_DATA_NO_EXEC in VxWorks kernel	**[[GENERAL]]** With VxWorks 7 SR0620 the VxWorks Core OS kernel hardening features are enabled by default. One of the hardending features is INCLUDE_DATA_NO_EXEC. With this feature it is not possible to run generated IEC (machine) code from memory of the target. At startup of the VxWorks CODESYS runtime a check for this feature will be performed and if present, the startup of the VxWorks CODESYS runtime will abort.	CODESYS Control
CDS-69663	**CmpRouter/CmpRouterEmbedded:** Crafted packet may cause a DoS	**[[GENERAL]]** For more details see **Advisory 2020-02**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=	CODESYS Control
CDS-69698	**CmpRouter/CmpRouterEmbedded/CmpBlkDrvTcp:** Crafted packets may cause a DoS	**[[GENERAL]]** For more details see **Advisory 2020-02**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=	CODESYS Control
CDS-68994	**ChannelServer:** Memory allocation DoS	**[[GENERAL]]** For more details see **Advisory 2020-01**, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	CODESYS Control, Gateway Server
CDS-68635	Remove dependencies to +SubVersionIntegration and upgrade to +RevisionControlSystemHooks	**[[COMPATIBILITY_INFORMATION-OEM]]** This ticket introduces support for the following new IRcs hooks IRcsStatusUpdateOverride and IRcsObjectSerializationCustomizationHook. Those hooks can be used with CODESYS SVN as follows (but are not	CODESYS, CODESYS SVN

		restriced to usage with SVN): - To suspend status updates of SVN during rich project transactions, we now offer an implementation of the interface IRcsStatusUpdateOverride (introduced with SDK V3.5.15.30), which can be instantiated using the type guid "{B953FED2-2AD3-4383-A511-5717C832092B}". Note: Since this interface is an IDisposable, a rich transaction could easily be scoped with the "using" keyword. - To set the "ignore on commit" in the SVN Working Copy for an object, implement a IRcsObjectSerializationCustomizationHook. In the method InterceptWrite(IRcsInterceptWriteArguments2 arg) you can request to set the ignore flag by setting IRcsInterceptWriteArguments2.IgnoreOnCommit. For further information see the CODESYS Developer Network: https://dn.codesys.com/news/details/s28-svn-git-migrate-hooks-from-svn-specific-to-independent-revision-control-systems-rcs-hooks/	
CDS-64429	**Profibus** (CIFX) Redundancy	**[[KNOWN_LIMITATIONS]]** - Timeout must be set to 100ms to stay in sync at reset. - Output data is not bumpless (see CDS-68794). As a workaroud %Q-Data can be manually added to the "Registered Areas" (in Redundancy Configuration Object)	Driver
CDS-31507	**OPC-Configurator:** Interfaces Gateway and ARTI:Support V2 PLC password	**[[COMPATIBILITY_INFORMATION-EndUser]]** In older versions the texts for user name and (PLC) password of a connection could only be entered in the Expert settings dialog. Now these parameters are in the PLC settings.	OPC Server
CDS-68412	**WebServer:** Heap Buffer overflow vulnerability	**[[GENERAL]]** For more details see **Advisory 2019-10**, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-10_CDS-68341.pdf	Web Visualization
CDS-69655	**Webserver:** Remote heap buffer overflow vulnerability	**[[GENERAL]]** For more details see Advisory 2020-03, which is available on the CODESYS website: https://customers.codesys.com/index.php?	Web Visualization

		eID=dumpFile&t=f&f=13078&token=de344ca65252463cc581ef144e0c53bd97b8f211&download=	
CDS-71491	**VisuServer:** Possible uncontrolled memory allocation	**[[GENERAL]]** For more details see Advisory 2020-05, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	CODESYS Control
CDS-71393	**CmpRouter/CmpRouterEmbedded:** Crafted packet may cause a DoS	**[[GENERAL]]** For more details see Advisory 2020-02, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=	CODESYS Control
CDS-70662	**Multiclient:** A login of a second instance of CoDeSys on the same application must be avoided	**[[COMPATIBILITY_INFORMATION]]** From now on, only one programming system can log in to an application. The second login from a programming system to the same application is refused with the client information of the client that is currently logged in.	CODESYS, CODESYS Control
CDS-72739	**CodeMeter:** Update to current version 7.10a	**[[GENERAL]]** For more details see Advisory 2020-06, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13245&token=12e702eb28edb2de082dc2f5e1375bea35c2fd1d&download=	CODESYS, CODESYS Control, CODESYS Control RTE, OPC Server
CDS-72324	**CodeMeter:** Update to current version 7.00b	**[[GENERAL]]** For more details see Advisory 2020-06, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13245&token=12e702eb28edb2de082dc2f5e1375bea35c2fd1d&download=	CODESYS, CODESYS Control, CODESYS Control RTE, OPC Server
CDS-72315	**ResetOriginDevice:** Should be configurable	**[[COMPATIBILITY_INFORMATION]]** The reset origin device can now be configured to keep dedicated objects during the reset. If the reset origin device is triggered by an old client (e.g. a CODESYS IDE <= V3.5.16.0) all objects for which the current user has the needed rights will be deleted. This behaviour does already apply for the UserManagement since V3.5.12.0 (only if an administrator executes the reset origin device, the user management is deleted)	CODESYS Control

		and is now extended for all new options (e.g. certificates).	
CDS-72930	**CODESYS Control for Linux (and ARM) SL:** update wibu codemeter package to 7.10a	**[[GENERAL]]** For more details see Advisory 2020-06, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13245&token=12e702eb28edb2de082dc2f5e1375bea35c2fd1d&download=	CODESYS Control
CDS-73294	**CmpOpenSSL:** improve interface for native OpenSSL implementation	**[[COMPATIBILITY_INFORMATION-OEM]]** If an OpenSSL version lower than 1.1.0 is used, the scrypt algorithm is not available. Therefore, the user management of the CODESYSControl Run-Time System is not available as well in this case.	CODESYS Control
CDS-76459	**VxWorks:** OPCUA port 4840 down on max. concurrent connection scan	**[[GENERAL]]** For more details see Advisory 2021-10, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14806&token=637e12e86301b83beac1653bd88da3aa5aa3f51b&download=	CODESYS Control
CDS-76460	**VxWorks:** OPCUA port 4840 down on stress test (TCP) on another port	**[[GENERAL]]** For more details see Advisory 2021-10, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14806&token=637e12e86301b83beac1653bd88da3aa5aa3f51b&download=	CODESYS Control
CDS-76457	**Web server** crashes when subjected to HTTP header memory exhaustion attack	**[[GENERAL]]** For more details see Advisory 2021-09, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14805&token=f0b86f99bb302ddd4aadec483aed5f5d3fddbf1a&download=	CODESYS Control

2 Known Limitations

None

3 OEM information from JIRA

To read up on implemented features and changes you can use your JIRA account. Please find some **example** filters below.

List of features and changes:

fixVersion = "V3.5 SP16 Patch 5"

fixVersion = "V3.5 SP16 Patch 5" AND issuetype = "New Feature"

List of features and changes since CODESYS V3.5 SP16:

fixVersion IN ("V3.5 SP16 Patch 5", "V3.5 SP16 Patch 4", "V3.5 SP16 Patch 3", "V3.5 SP16 Patch 2", "V3.5 SP16 Patch 1")

List of issues with compatibility information and known limitations:

fixVersion = "V3.5 SP16 Patch 5" AND (text ~ COMPATIBILITY_INFORMATION OR text ~ KNOWN_LIMITATIONS)

4 History

Created:	Bianka Jödicke (Quality Assurance)
Reviewed:	Rico Ottliczky (Quality Assurance)
Released:	Rico Ottliczky (Quality Assurance)