Release Note CODESYS V3.5 SP12 Patch 6

18.09.2018

1 Release Notes

Key	Summary	Release Note	Component/s
CDS-57549	**Compile, IO Config:** Wrong Task deployment for function blocks used in initial values	**[[COMPATIBILITY_INFORMATION]]** With compiler version >= 3.5.12.0 only those tasks will be used as update task for instances with IOs in which an Access to the IOs can be detected, or in which the instance is called directly. The behaviour is now again the same as with versions < V3.5.10.30. Beginning with this version for the fix of CDS-53189, we also used the declaration position for updating IOs. That could mean, that an Output was in unexpected tasks. For example, if two instances with mapped IOs are declared in one GVL, and one of the instances is called in a task X, the output of the other instance would also be updated in task X. The new behaviour, and the pre V3.5.10.30 behaviour could lead to less updates of Outputs as in the versions in between. For example, if an instance of a function block is declared in Program, but there is no direct call of the instance, there will be no update in the task in which the Program is called. Direct call means in this case, that a call via an interface is not enough. A workaround for this problem is to manually edit the tasks in which to update IOs in the IO-Configuration.	CoDeSys

CDS-56472	**Using functions with big return values** causes stack overflow / watchdog error	**[[GENERAL]]** Stackoverflow cannot be corrected in the runtime system! Typically a reboot of the controller is the consequence on that or a hardware exception is generated to halt the application. . The only way to inhibit this error during compile time of the IEC application is to specify the stack size in the device description of a target (see following OEM note). **[[COMPATIBILITY_INFORMATION-OEM]]** Every device description should specify the limit of the stack size with the following target setting. Then the compiler checks during the compile time the stack usage and generates an error, if the stack usage exceeds this limit: <ts:section name="memory-layout"> <ts:setting name="max-stack-size" type="integer" access="visible"> <ts:value>0</ts:value> </ts:setting> ... </ts:section>	CoDeSys
CDS-59141	**Compiler:** Unexpected online change in specific project with new CODESYS version	**[[COMPATIBILITY_INFORMATION]]** The problem only occurs for persistent variable lists that are decorated with an attribute. The problem was introduced with Codesys Version 3.5.10.0. With this version the internal order of a list of attributes of an object might change, without respect to the compiler version. Therefore projects with CODESYS Version > 3.5.10.0 may produce a language model for Persistent vars (with additional attribute) that is different to previous versions. We now generate for projects with compilerversion < 3.5.10.0 a compatible the same list as with codesys < 3.5.10.0. Projects with compilerversion < 3.5.10.0, that were created with codesys versions >= 3.5.10.0 may now be different! This is a problem that we can't avoid since we only know the compiler version and not the codesys version of the created project. For CompilerVersion >= 3.5.12.20 the order of the attributes is always fix (sorted lexically).	CoDeSys

CDS-52387	**CmplecTask:** IecTasksWaitForStop() should be improved to be more tolerant for longer running tasks	[[**COMPATIBILITY_INFORMATION-EndUser**]] 1. The timeout to wait for a timeout is changed from: PREVIOUS: - Timeout is calculated from all IEC Tasks: Timeout = 2 * MAX(<Last IECTask Cycletime>, <Configured IECTask Interval>); - WaitTimeout = MIN(Timeout, <Setting: CmplecTask::WaitForStopTimeoutMs>); <Setting: CmplecTask::WaitForStopTimeoutMs>: By default = 10000ms CURRENT: - Timeout is calculated from all IEC Tasks: Timeout = 2 * MAX(<Maximum IECTask Cycletime>, <Configured IECTask Interval>); - WaitTimeout = MIN(Timeout, <Setting: CmplecTask::WaitForStopTimeoutMs>); <Setting: CmplecTask::WaitForStopTimeoutMs>: By default = 10000ms 2. We splitted the RUN/STOP transition in 2 phases: - PHASE 1: This is the phase at the RUN/STOP transition until the safe state of the application/machine will be reached. In this pahse, we wait only on IEC tasks, wich uses mapped outputs! - PHASE 2: This is the phase at the RUN/STOP transition after the safe state of the application/machine was be reached. In this pahse, we wait only on IEC tasks, wich don't use mapped outputs! For this phase, there is a new setting for the timeout: [CmplecTask] WaitForStop.TimeoutMs_2=25000 Reason for this feature: - This is because typically non IO tasks (AlarmTasks, TrendTasks, etc.) need a lot more time for the RUN/STOP transition as the tasks which reference IOs. And so sometimes a watchdog error occurred at this non IO tasks during normal RUN/STOP transition.	CoDeSys Control

		NOTES: - To disable this feature, you can use the following new setting in the cfg-file: [CmpIecTask] WaitForStop.SkipTasksWithoutOutputs=0 - If the plc does not use the standard CODESYS IO-configuration/IO-mapping, you have to switch off this feature!	
CDS-4238	**OnlineUserManagement**	**[[COMPATIBILITY_INFORMATION-EndUser]]** 1. With a CODESYS Version < v3.5.12.0 there is no more the possibility to activate simple UserManagement (menu command "Online / Security / Add device user ...") on a runtime system >= v3.5.12.0 ! 2. We recommend to create a new UserManagement configuration (users and groups) and RightsManagement configuration, if the UserManagement was created with/on a previous runtime system version or if you import existing UserManagement files! This is because the default rights of the corresponding default usergroups has changed to cover more strict the user roles!	CoDeSys, CoDeSys Control
CDS-54404	**Online User Management:** Limit number of invalid login tries	**[[COMPATIBILITY_INFORMATION-EndUser]]** Failed user authentication are now limited. After the third (default) failed user authentication an error box appears: "Operation aborted, too many retries". The user is then excluded from login for 60 seconds (default), i.e. the described error box appears. **[[COMPATIBILITY_INFORMATION-OEM]]** Limit number of invalid login tries In CmpUserMgrItf these two settings configure this feature: USERMGR_NUM_OF_LOGIN_RETRIES USERMGR_TIMEOUT_OF_LOGIN_RETRIES In case USERMGR_NUM_OF_LOGIN_RETRIES is set to 0 this security feature is disabled. The maximal timeout value for user exclusion is 4233600 seconds which is equivalent to 49 days. But this is not persistent, i.e. a restart of the runtime resets the exclusion. Control of these settings by the Security Manager is prepared.	CoDeSys, CoDeSys Control

CDS-48900	**Online User Management:** Split of CmpUserDB interface and implementation into 2 parts necessary	**[[COMPATIBILITY_INFORMATION-OEM]]** With the splitting of CmpUserDB into CmpUserDB and CmpUserDBObjects it is necessary to include both components into runtime builds and initialization lists. It is easier now to replace the user management and authentication part (CmpUserDB) while the object rights management part (CmpUserDBObjects) works as it is.	CoDeSys Control
CDS-51587	**CmpApp:** Memory allocation / recycling on Application Download (possible "out of memory")	**[[COMPATIBILITY_INFORMATION-EndUser]]** The download with online change uses an extra area to manage the online change. This area is now freed when it is no longer needed. But this may not help if the allocation of areas defragments the available memory so that only (too) small blocks of memory are left. In this case a download of an application fails and a restart of the PLC is necessary.	CoDeSys Control

CDS-53424	**CmplecTask:** Watchdog should not be disabled during IO-Update to detect deadlocks in IO-driver	**[[COMPATIBILITY_INFORMATION-EndUser]]** Watchdog remains activated now during an IO-update within a IEC task cycle! So a watchdog error can be detected additionally in this sequence. In this case we try to run out of this IO-update before suspending the IEC-Task. If the task does not run out if the IO-update within the specified setting "WaitForStopTimeoutMs", the supervisor vital operation RTS_OPID_IecTask_WatchdogInIO will fail and so a hardware watchdog could expire. **[[COMPATIBILITY_INFORMATION-OEM]]** This new behaviour can be deactivated with the following setting / preprocessor define (so the behaviour is as before v3.5.12.0): [CmpIecTask] EnableWatchdogDuringIOUpdate=0 /** * <category>Settings</category> * <type>Int</type> * <description> * Setting enables the feature to fire a watchdog during an IO-update in an IEC task! * Can be disabled if this causes problems in IEC applications and so the behaviour is similar to the runtime system before v3.5.12.0. * </description> */ #define IECTASKKEY_INT_ENABLE_WATCHDOG_DURING_IOUPDATE "EnableWatchdogDuringIOUpdate" #ifndef IECTASKVALUE_INT_ENABLE_WATCHDOG_DURING_IOUPDATE #define IECTASKVALUE_INT_ENABLE_WATCHDOG_DURING_IOUPDATE 1 #endif	CoDeSys Control
CDS-54951	**CmpApp / InitArea:** Prevent the initialization of the area on AllocArea event	**[[COMPATIBILITY_INFORMATION-OEM]]** EVTPARAM_CmpAppArea structure is expanded now with a result which defaults to ERR_APP_DONT_INIT_AREA, i.e. the returned area is not initialized. In order to initialize the returned area, the result has to be set to ERR_OK explicitely in the event callback function.	CoDeSys Control

CDS-52311	**WinCE:** Change the CE5 project files to VS 2008 compiler	**[[COMPATIBILITY_INFORMATION-OEM]]** There are now Visual Studio 2008 project files for Windows CE 5 runtimes.	CoDeSys Control
CDS-55069	**RTE Setup:** Remove data files from installation dir (similar to Control Win)	**[[COMPATIBILITY_INFORMATION]]** CODESYS Control RTE V3 and CODESYS Control RTE 64: - The working directory and the configuration files of the runtime product are moved to %ProgramData%\CODESYS\CODESYSControl RTEV3 - If a configuration file from former installations exists in the installation folder and the user confirms to use it (against our recommendation), the working directory will remain in the installation directory.	CoDeSys Control RTE
CDS-59323	**WinCE:** Generate lists of source files and components dynamically from selected features	**[[COMPATIBILITY_INFORMATION-OEM]]** WinCE runtime toolkits: Some of the .c files which used to be in the VC project of the CODESYS runtime system have now been replaced by .obj files. The .c files are still part of the delivery and can be used instead of the .obj files if needed	CoDeSys Control
CDS-58875	**WinCE:** Separate SysReadWriteLock and SysCpuMulticore	**[[COMPATIBILITY_INFORMATION-OEM]]** Windows CE 7 and 8 runtimes now have dynamic SysReadWriteLock and SysCpuMultiCore components. Implementation of ReadWriteLocks is native.	CoDeSys Control
CDS-59658	**Visu:** No login without change when using compiler versions < 3.5.9	**[[COMPATIBILITY_INFORMATION]]** To fix this issue it was necessary to introduce a minor incompatibility under special circumstances when using target- or webvisualziation within a project. It will no longer be possible to login to applications without change under the following circumstances: * a project containing target- or webvisualization was downloaded * a compilerversion >= 3.5.7 and < 3.5.9 was used during this download * the download was done using a programming system >= 3.5.12 and < 3.5.12.30 This is a problem that we can't avoid since we only know the compiler version and not the codesys version of a downloaded project.	CoDeSys

CDS-59793	**CmpFileTransfer:** Possibility of unauthorized file access to all system files	**[[GENERAL]]** For more details see Advisory 2018-04, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-04_CDS-59017.pdf **[[COMPATIBILITY_INFORMATION]]** A new security feature is implemented to secure online file and directory access. It is represented by two new settings in [SysFile] section: ForceOnlineFilePath=1 (default) Setting to force the configured file path to every online file access. If an absolute file path is requested, which is not a configured path, or a directory traversal path an error is returned at this operation (ERR_OPERATION_DENIED). NOTE: ForceFilePath=1 dominates this setting. DenyOnlineAccessCfgFile=1 (default) Setting to deny online access to all configuration files. If a configuration file is requested, an error is returned at this operation (ERR_OPERATION_DENIED). NOTE: This setting is independent of any Force settings. To restore the old behaviour these settings may be configured as follows: [SysFile] ForceOnlineFilePath=0 DenyOnlineAccessCfgFile=0 BUT WE HIGHLY RECOMMEND, TO LEAVE THESE SETTINGS AT THEIR DEFAULT VALUES! For more information about configuration of filepath and placeholders see our corresponding tutorial as part of the CODESYS Control Runtime System Toolkit.	CoDeSys Control

CDS-56915	**Compiler:** A Bit assigned to a REFERENCE TO BOOL should produce an error in any case	**[[GENERAL]]**
		Compilerversion >= 3.5.12.0
		There will be now new error messages when trying to a assign a boolean variable located on a bit address to a REFERENCE TO BOOL.
		If such a reference was written, the whole byte was written, which could lead to unintended consequences.
		
		As a workaround, use copy and restore
		b := bit;
		bref REF= b;
		// do whatever you have to do
		bit := b;
			CoDeSys

CDS-54199	**Data breakpoints** on RTE	**[[GENERAL]]** Data breakpoints now implemented on RTE, according to release of CODESYS 3.5.11.0	CoDeSys Control RTE
CDS-55941	**OPC UA Server:** Crash if subscription is active and connection was lost.	**[[GENERAL]]** For more details see Advisory 2017-07, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2017/Advisory2017-07_CDS-55941.pdf	CoDeSys Control
CDS-58572	**OPC UA Server:** Crash when invalid request is sent	**[[GENERAL]]** For more details see Advisory 2018-02, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-02_CDS-58208.pdf	CoDeSys Control
CDS-57676	**Webserver:** Crafted request can cause shutdown of plc in some states	**[[GENERAL]]** For more details see Advisory 2017-09, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2017/Advisory2017-09_CDS-57676.pdf	CoDeSys Control

CDS-57679	**Webserver:** Connection channels might be lost	**[[GENERAL]]** For more details see Advisory 2017-09, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2017/Advisory2017-09_CDS-57676.pdf	CoDeSys Control
CDS-57141	**MemGC: Cyclic check** should be configurable via setting	**[[GENERAL]]** New runtime setting for enabling a cyclic check for overwrites on dynamic memory: [CmpMemGC] EnableCyclicMemGcCheck=1 Default value: 0 Before enabling the option, consider that this check is done very often! In case of heavy usage of dynamic allocation (using SysAlloc functions) or a memory leak, CPU load and application/runtime performance will degrade very quickly. This option is to be used for error detection and not in normal daily production.	CoDeSys Control
CDS-59781	**CmpWebServer:** Possible run out of file descriptors	**[[GENERAL]]** For more details see Advisory 2018-05, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-05_CDS-58820.pdf	CoDeSys Control
CDS-59783	**Webserver, SSL:** Connections can be blocked by a client	**[[GENERAL]]** For more details see Advisory 2018-05, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-05_CDS-58820.pdf	CoDeSys Control

2 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 SP12"

fixVersion = "V3.5 SP12" AND issuetype = "New Feature"

List of features and changes since CODESYS V3.5 SP12:

fixVersion in ("V3.5 SP12 Patch 6", "V3.5 SP12 Patch 5", "V3.5 SP12 Patch 4", "V3.5 SP12 Patch 3", "V3.5 SP12 Patch 2", "V3.5 SP12 Patch 1")

List of issues with compatibility information and known limitations:

fixVersion in ("V3.5 SP12 Patch 6", "V3.5 SP12 Patch 5", "V3.5 SP12 Patch 4", "V3.5 SP12 Patch 3", "V3.5 SP12 Patch 2", "V3.5 SP12 Patch 1","V3.5 SP12") AND (text ~ COMPATIBILITY_INFORMATION OR text ~ KNOWN_LIMITATIONS)

3 History

Created:	Rico Ottliczky (Quality Assurance)
Reviewed:	Benedikt Brückmann (Quality Assurance)
Released:	Rico Ottliczky (Quality Assurance)