

Compliant Control Architecture - Bug #1647

Weird component-crashes when wrong converter plugins are loaded

10/22/2013 08:27 PM - C. Emmerich

Status:	New	Start date:	10/22/2013
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:	cca0.5		

Description

Actually I dont know, whether this is more rsb related, cca related or rci-converter related, so I place it here.

When starting a cca node with remote ports for rci data types, and when loading the rsbrstconvertersstable plugin instead of rsbrstconvertersrci plugin, the component crashes with a weird "invalid pointer" error instead of an "wrong or missing converter" error.

Example:

See the [Flexirob open-rave collision checker](#) which has an input port for rci::JointAngles. The rsb.conf is configured such that only the following plugins are loaded:

```
[plugins.cpp]
load = rsbspread:rsbrstconvertersstable:rsbrstconverterssandbox
```

First, the component is running fine, but when I send a joint angle to the related scope, i.e. the component receives the very first joint angle, it crashes:

```
cemmeric@augit:~/Documents/svn/flexirob/modules/lwr-collision/build ./build/runCollisionChecking
[main] Creating collision checking component and configuring ports...
[main] Loading robot from file: /vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/etc/liblwr-rave/kuka_lwr_gripper.robot.xml
[main] Loading scene from file: /vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/etc/liblwr-rave/obstacle_none.env.xml
[LWRRaveEnvironment] creating rave environment...
[LWRRaveEnvironment] creating rave environment... 100%
+---- myLWRRaveCollisionChecker -----+
| Processing strategy: |
| <Port-Triggered, listening to port 'input_angles'> |
| Data input ports: |
| "input_angles"<rci::JointAngles> <cfg:spread,>(/lwr/status/all/position/) [optional] |
| Data output ports: |
| "output_collision"<rst::robot::RobotCollision> <cfg:spread,>(/lwr/status/collisions/) [optional] |
+-----+
| Properties: |
+-----+

[main] Collision checker running...
*** glibc detected *** ./build/runCollisionChecking: free(): invalid pointer: 0x00007fa8540009c8 ***
===== Backtrace: =====
/lib/x86_64-linux-gnu/libc.so.6(+0x7eb96)[0x7fa89b600b96]
/vol/toolkit/nightly/x86_64/successful/lib/librst0.10.so.0.10(_ZN3rst10kinematics11JointAnglesD1Ev+0x24)[0x7fa89af7c154]
/homes/cemmeric/Documents/svn/flexirob/modules/lwr-collision/build/build/liblwr-collision0.1.so.0.1(_ZN8flexirob26CollisionCheckingComp
eckingComponent9onProcessEv+0x100)[0x7fa89cc78d0c]
/vol/toolkit/nightly/x86_64/successful/lib/libcca0.5.so.0.5(_ZN3cca4Node7processEv+0x134)[0x7fa89c373344]
/vol/toolkit/nightly/x86_64/successful/lib/libcca0.5.so.0.5(_ZN3cca4Node13inputCallbackEN5boost10shared_ptrIN3rsb5EventEEEEERKSs+0
EERKSs+0x1cc)[0x7fa89c37604c]
/vol/toolkit/nightly/x86_64/successful/lib/libcca0.5.so.0.5(_ZN5boost6detail8function26void_function_obj_invoker1INS_3_bi6bind_tlvNS_4
d_tlvNS_4_mfi3mf2lvN3cca4NodeENS_10shared_ptrIN3rsb5EventEEEEERKSsEENS3_5list3INS3_5valueIPS8_EENS_3argILi1EEENSH_IS
EEENSH_ISsEEEEEEvSC_E6invokeERNS1_15function_bufferESC_+0x60)[0x7fa89c3779a0]
/vol/toolkit/nightly/x86_64/successful/lib/librsb.so.0.10(_ZN3rsb20EventFunctionHandler6handleEN5boost10shared_ptrINS_5EventEEE+0
ventEEE+0x5b)[0x7fa89b274bab]
/vol/toolkit/nightly/x86_64/successful/lib/libcca0.5.so.0.5(_ZN3cca13InputPortBase12InputHandler6handleEN5boost10shared_ptrIN3rsb5E
```

```
ptrIN3rsb5EventEEE+0xbd)[0x7fa89c392f5d]
/vol/toolkit/nightly/x86_64/successful/lib/librsb.so.0.10(_ZN3rsb15eventprocessing30ParallelEventReceivingStrategy7deliverEN5boost10sh
5boost10shared_ptrINS_7HandlerEEENS3_INS_5EventEEE+0x87)[0x7fa89b2a9e87]
/vol/toolkit/nightly/x86_64/successful/lib/librsb.so.0.10(_ZN5boost6detail8function26void_function_obj_invoker2INS_3_bi6bind_tlvNS_4_m
tlvNS_4_mfi3mf2lvN3rsb15eventprocessing30ParallelEventReceivingStrategyENS_10shared_ptrINS7_7HandlerEEENSA_INS7_5EventE
7_5EventEEEEENS3_5list3INS3_5valueIPSE_EENS_3argILi1EEENSK_ILi2EEEEEEEEvRSC_RKSE_E6invokeERNS1_15function_bufferE
tion_bufferESP_SR_+0x9d)[0x7fa89b2ad5ed]
/vol/toolkit/nightly/x86_64/successful/lib/librsb.so.0.10(_ZN3rsc9threading26OrderedQueueDispatcherPoolIN5boost10shared_ptrIN3rsb5E
trIN3rsb5EventEEENS4_7HandlerEE22DeliverFunctionAdapter7deliverERNS3_IS7_EERKS6_+0x18)[0x7fa89b2add68]
/vol/toolkit/nightly/x86_64/successful/lib/librsb.so.0.10(_ZN3rsc9threading26OrderedQueueDispatcherPoolIN5boost10shared_ptrIN3rsb5E
trIN3rsb5EventEEENS4_7HandlerEE6workerERKj+0x681)[0x7fa89b2b2a11]
/vol/toolkit/nightly/x86_64/successful/lib/librsb.so.0.10(_ZN5boost6detail11thread_dataINS_8functionIFvvEEEE3runEv+0x1e)[0x7fa89b2ac
x7fa89b2adcbe]
/usr/lib/libboost_thread.so.1.46.1(thread_proxy+0x69)[0x7fa89ca32ce9]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x7e9a)[0x7fa89be5ee9a]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x6d)[0x7fa89b675ccd]
===== Memory map: =====
00400000-0042e000 r-xp 00000000 00:18 1426993312
/homes/cemmeric/Documents/svn/flexirob/modules/lwr-collision/build/build/runCollisionChecking
0062d000-0062e000 r--p 0002d000 00:18 1426993312
/homes/cemmeric/Documents/svn/flexirob/modules/lwr-collision/build/build/runCollisionChecking
0062e000-0062f000 rw-p 0002e000 00:18 1426993312
/homes/cemmeric/Documents/svn/flexirob/modules/lwr-collision/build/build/runCollisionChecking
0064f000-01856000 rw-p 00000000 00:00 0 [heap]
400ac000-400ae000 r-xs 00000000 fc:03 918043 /tmp/glug49Ct (deleted)
41b22000-41ba0000 rw-p 00000000 00:00 0
7fa844000000-7fa844021000 rw-p 00000000 00:00 0
7fa844021000-7fa848000000 ---p 00000000 00:00 0
7fa848000000-7fa848021000 rw-p 00000000 00:00 0
7fa848021000-7fa84c000000 ---p 00000000 00:00 0
7fa84c000000-7fa84c021000 rw-p 00000000 00:00 0
7fa84c021000-7fa850000000 ---p 00000000 00:00 0
7fa850000000-7fa850021000 rw-p 00000000 00:00 0
7fa850021000-7fa854000000 ---p 00000000 00:00 0
7fa854000000-7fa854021000 rw-p 00000000 00:00 0
7fa854021000-7fa858000000 ---p 00000000 00:00 0
7fa8597fb000-7fa8597fc000 ---p 00000000 00:00 0
7fa8597fc000-7fa859ffc000 rw-p 00000000 00:00 0 [stack:2401]
7fa859ffc000-7fa859ffd000 ---p 00000000 00:00 0
7fa859ffd000-7fa85a7fd000 rw-p 00000000 00:00 0 [stack:2400]
7fa85a7fd000-7fa85a7fe000 ---p 00000000 00:00 0
7fa85a7fe000-7fa85affe000 rw-p 00000000 00:00 0 [stack:2399]
7fa85affe000-7fa85afff000 ---p 00000000 00:00 0
7fa85afff000-7fa85b7ff000 rw-p 00000000 00:00 0 [stack:2398]
7fa85b7ff000-7fa85b800000 ---p 00000000 00:00 0
7fa85b800000-7fa85c000000 rw-p 00000000 00:00 0 [stack:2395]
7fa85c000000-7fa85c021000 rw-p 00000000 00:00 0
7fa85c021000-7fa860000000 ---p 00000000 00:00 0
7fa86000f000-7fa86040f000 rw-s 93258000 00:05 14843 /dev/nvidia0
7fa86040f000-7fa8604a1000 r-xp 00000000 00:1b 1109787574
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconverterssandbox.so.0.10
7fa8604a1000-7fa8606a1000 ---p 00092000 00:1b 1109787574
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconverterssandbox.so.0.10
7fa8606a1000-7fa8606a7000 r--p 00092000 00:1b 1109787574
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconverterssandbox.so.0.10
7fa8606a7000-7fa8606a8000 rw-p 00098000 00:1b 1109787574
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconverterssandbox.so.0.10
7fa8606a8000-7fa860717000 r-xp 00000000 00:1b 1109787568
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconvertersstable.so.0.10
7fa860717000-7fa860916000 ---p 0006f000 00:1b 1109787568
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconvertersstable.so.0.10
7fa860916000-7fa86091b000 r--p 0006e000 00:1b 1109787568
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconvertersstable.so.0.10
7fa86091b000-7fa86091c000 rw-p 00073000 00:1b 1109787568
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/rsb0.10/plugins/librsbrstconvertersstable.so.0.10
7fa86091c000-7fa860943000 r-xp 00000000 00:1b 3255559467
/vol/toolkit/nightly/x86_64/2013-10-10_02-00-40/lib/libspread.so.3.0.0Aborted
```

My concern

Of course, this scenario clearly fails because of missing converters (for `rci::JointAngles`): If I add the `rsbrstconvertersrci`

```
[plugins.cpp]
```

```
load = rsbspread:rsbrstconvertersrci:rsbrstconvertersstable:rsbrstconverterssandbox
```

(and resolve all the resulting ambiguity stuff) the component works fine. But shouldn't the component exit with an exception about "missing converters etc." instead of some weird memory error? So, what I complain about/want to report here is the error message/behavior.

Relation to converter ambiguity?

Maybe, this has something to do with the ambiguity issues of `rsb-rst-rci-cca-mfg-converters` (see e.g. #1317)? Although the `rsbrstconvertersrci` plugin is not loaded, there is a registered converter for wire-schema 'string' and rst-type 'rst::.....:JointAngles' but maybe this does not work in this context? Just an idea...

History

#1 - 10/22/2013 08:39 PM - J. Wienke

I think the issue with another converter for the same wire schema is the problem. CCA probably blindly casts into the assumed target type which results in a misinterpretation of the memory.

This is really something I have no idea for how to improve the situation. From the point of a statically typed language without real runtime introspection support you need to do a static cast in the end. CCA could better check that the data type matches the expectation by comparing the string data type in the event. But that is everything we can do so far.

#2 - 10/22/2013 09:23 PM - Anonymous

- Assignee set to *Anonymous*

- Target version set to *cca0.5*

@Johannes: This is exactly what happens.

I will add a type check as Johannes suggests. Thanks for reporting.