Robotics Service Bus - Bug #1223
Segmentation fault in YARP transport

10/30/2012 10:02 PM - J. Moringen

Status:	Resolved	**Start date:**	10/30/2012
Priority:	Normal	**Due date:**	
Assignee:	J. Moringen	**% Done:**	100%
Category:	YARP Connector	**Estimated time:**	0.00 hour
Target version:	rsb-0.9		

Description

There is a race condition in the initialization or nameserver code of the YARP transport. The problem seems to be that a Boost.asio service is used without a thread which causes it to create an ad-hoc thread. If the service object (or maybe resources used by the service) is destroyed before the thread exists, an invalid pointer derefences can occur.

Associated revisions

Revision cccd586f - 11/03/2012 03:49 AM - J. Moringen

Avoid unsafe use of asio::io_service in src/rsb/transport/yarp/Connector*.cpp

fixes #1223

The problem was that the Nameserver class, when used by the
OutConnector class, could get an asio::io_service without a
thread. This would cause asio to spawn a thread which in turn could
outlive some of the objects it accessed.

The solution consists in adding an ExecutionContext class which
manages the asio::io_service and its thread and is used by the
*Connector and Nameserver classes.

- src/rsb/transport/yarp/Execution.{h,cpp}: new files; contain
  ExecutionContext and ContextProxy classes
- src/rsb/transport/yarp/ConnectorBase.{h,cpp}: new files; contain
  ConnectorBase class which handles access to the ExecutionContext,
  holds the asio socket and performs basic state management
- src/rsb/transport/yarp/Nameserver.{h,cpp}: use a ContextProxy to
  access the asio::io_service
- src/rsb/transport/yarp/InPushConnector.{h,cpp}: added ConnectorBase
  base class; used for state management, socket and scope store and
  access to the asio::io_service
- src/rsb/transport/yarp/OutConnector.{h,cpp}: similar
- src/CMakeLists.txt: added files
  src/rsb/transport/yarp/Execution.{h,cpp} and
  src/rsb/transport/yarp/ConnectorBase.{h,cpp}

History

#1 - 11/02/2012 07:24 PM - J. Moringen

- Status changed from New to In Progress

- Assignee set to J. Moringen

#2 - 11/03/2012 03:50 AM - J. Moringen

- Status changed from In Progress to Resolved

- % Done changed from 0 to 100

Applied in changeset rsb-yarp-cpp|commit:cccd586fb558f856d1688f824d32a8f1e7b827fb.