DORNERWORKS

WWW.DORNERWORKS.COM

Securing ROS Systems with seL4

Nathan Studer, DornerWorks
Alex Pavey, DornerWorks
Dariusz Milkuski, GVSC
Yale Empie, GVSC
Cristian Balas, GVSC

Agenda

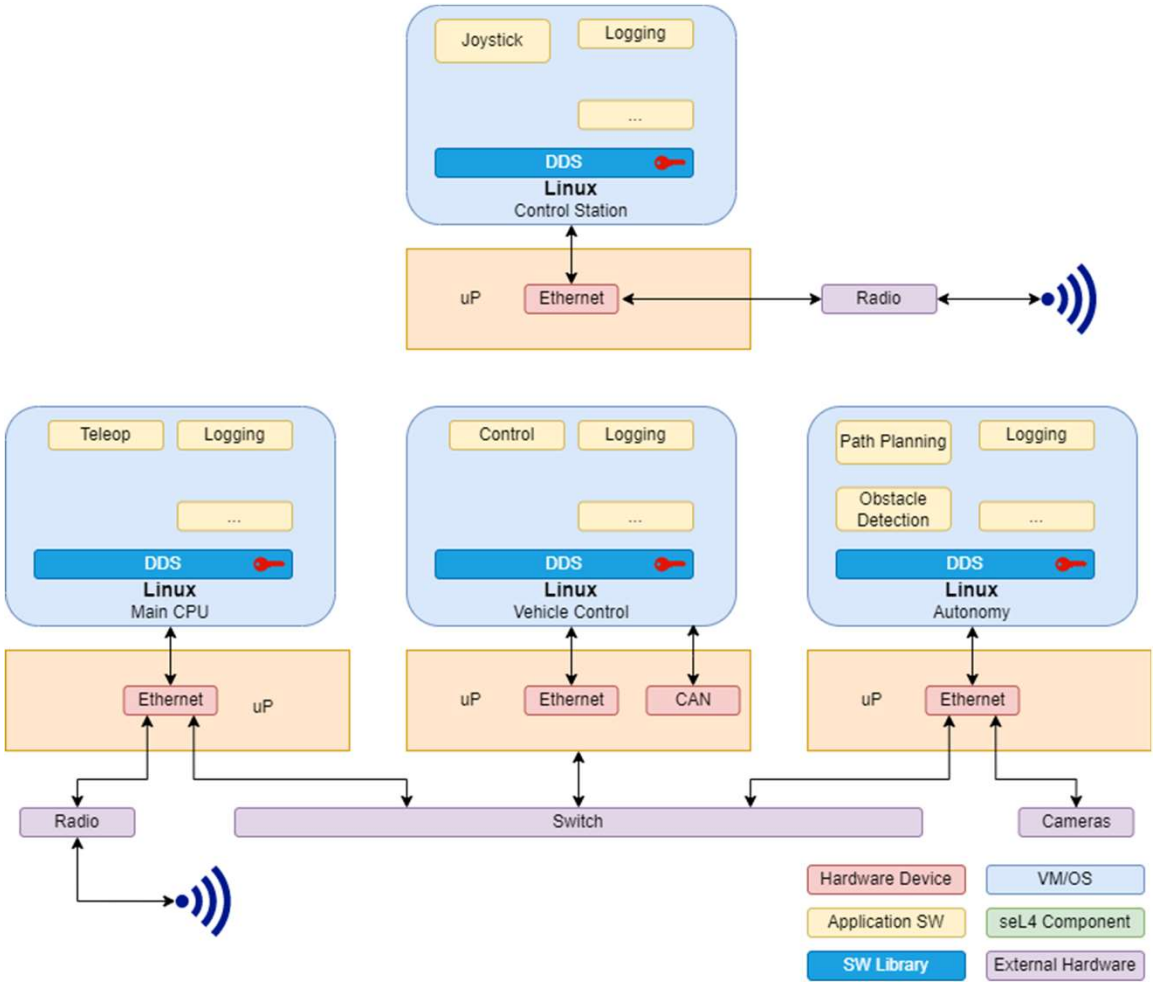
- Background
- Use Case
- ROS Cyber Retrofit in Two Parts
- Results
- Future Work

Problem

- Evil Roomba
- T-1000
- Hijacking

ROS Intro

- Open-Source Meta Operating System
- Message Passing Communication
- Made for code re-use
- Distributed, loosely coupled Framework
- Unix focused



DDS Additional Info

- DDS = Data Distribution Service
- DDS is a standard from the OMG (Object Management Group)
- Middleware protocol
  - Publish-subscribe communications for distributed systems
- DDS-Security Plug-in provides Integrity, Confidentiality, and Access Control using Asymmetric Keys
- Not all DDS libraries implement the whole standard

Project Goals

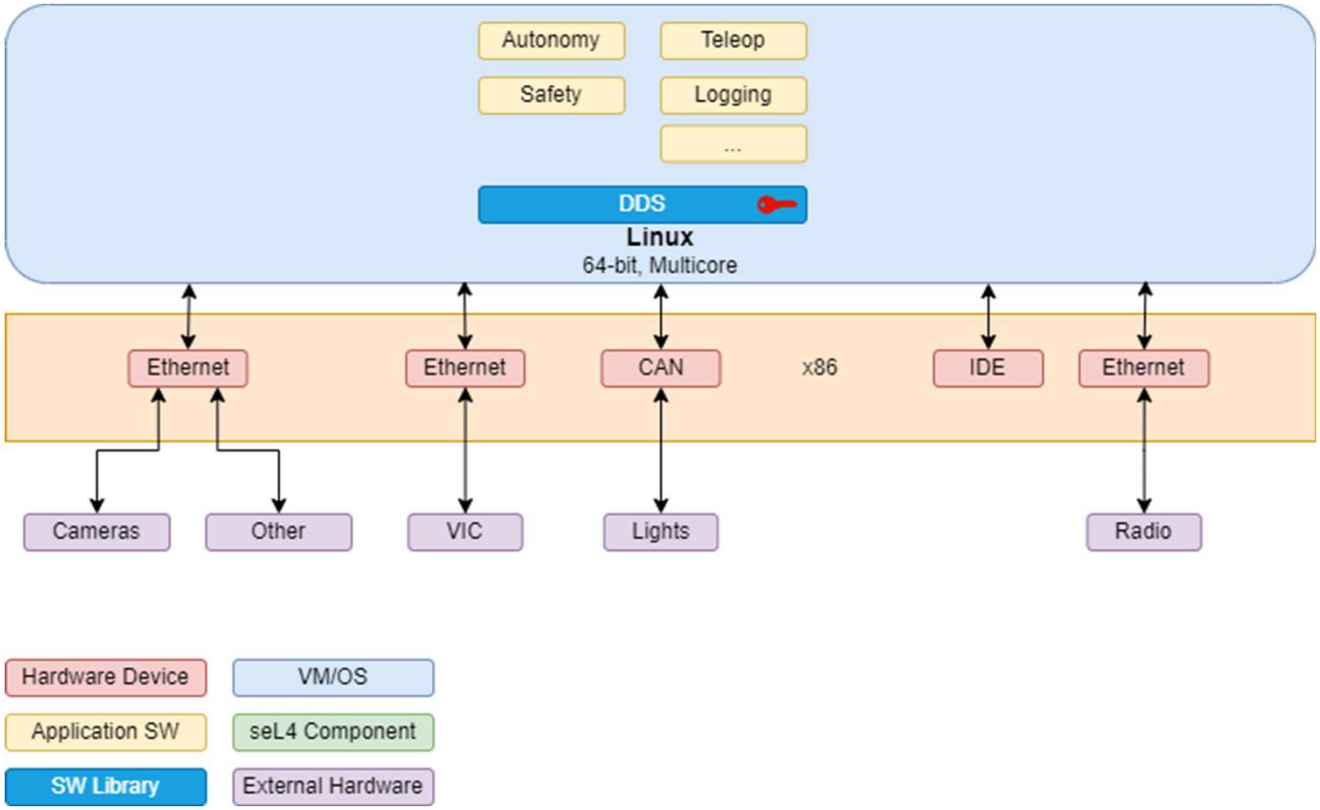
- Further Improve Robotic Security
- Diversify ROS
- Make seL4 more Accessible

System Requirements

- Autonomous Operation using 3rd Party Autonomy Packages
- Teleoperation
- Safety Indicator Lights
- OTA Update
- ROS2 (Not ROS1)

Example Robotic Vehicle Architecture

- x86
- ROS Application
- Safety Functionality
- CAN
- Network
  - Radio
  - Cameras
  - Vehicle Control
  - Etc…

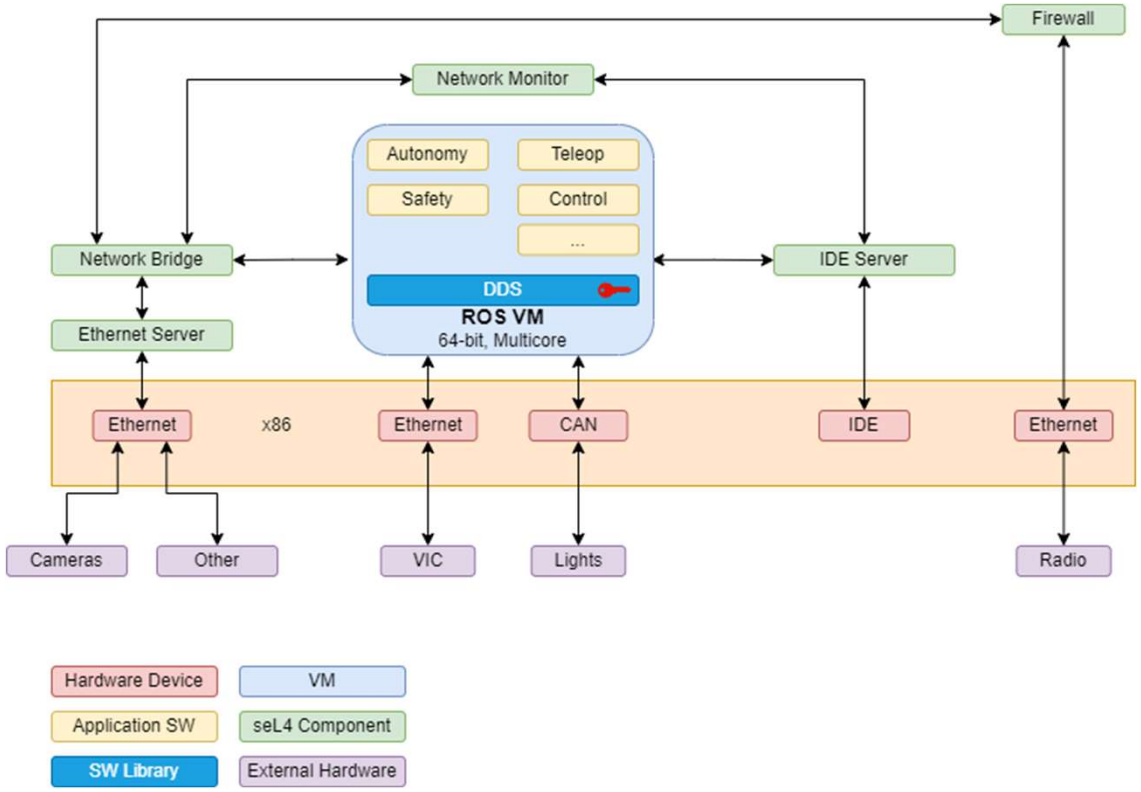


Security Requirements

- Detect Denial of Service
- Detect Intrusion Events
- Detect Invalid Sensor Data
- Prevent Replay Attacks
- Prevent Unauthorized Update
- Prevent Unauthorized Network Access
- Integrity, Confidentiality, and Access Control of ROS Communication
- Isolate and validate Radio
- Return to Home on Compromise

Initial Cyber Retrofit Architecture

- Firewall Radio
- Monitor Network Traffic
- Hide Extra I/O (e.g. i219)



Added Support Functionality

- System
  - Maintenance Mode Switch (Alternative – VM Suspend)
- seL4
  - i210 Driver
  - Large Memory VMs
  - Component VirtIO Net (Direct and LWIP)
  - Network Tap
  - Virt I/O Contention and Performance Fixes
  - Virtualized MSI Interrupt Support

Issues Encountered

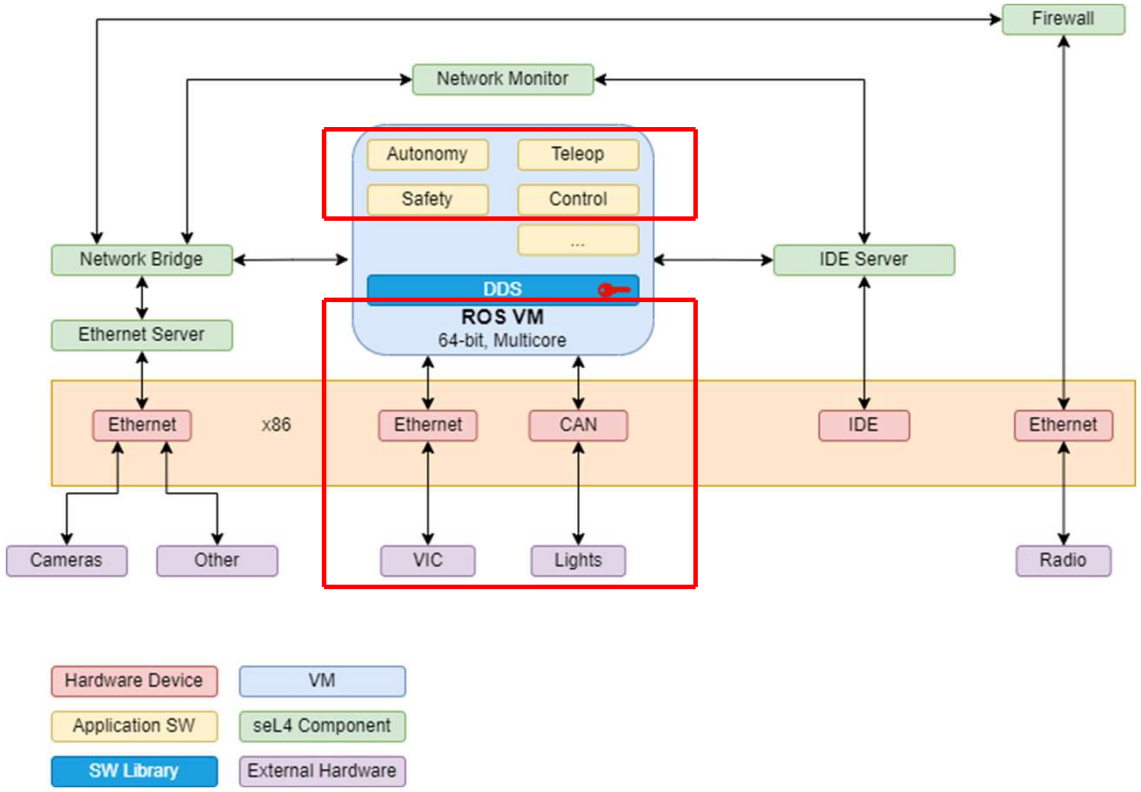
- USB Devices and BIOS Drivers
- VM Boot Sequencing

Cyber Retrofit Results

- Successfully Demonstrated on Vehicle
- Red Team Unsuccessful

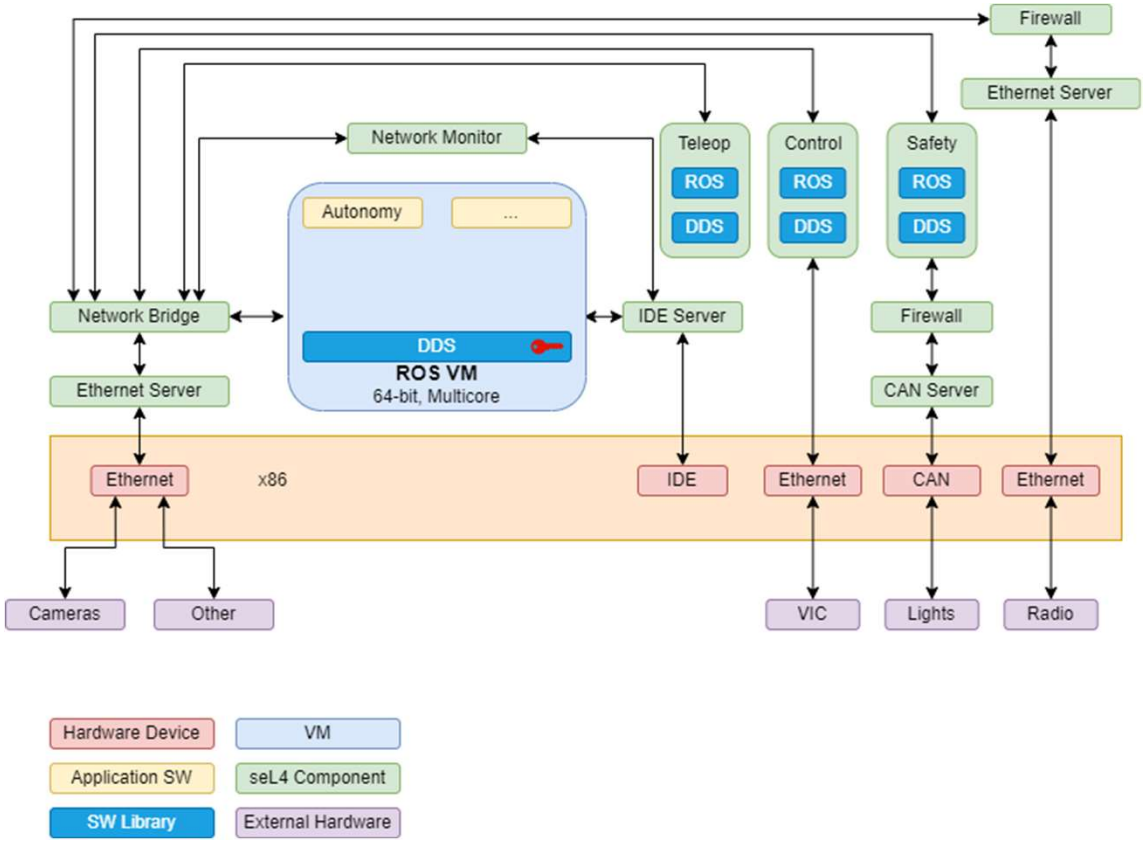
Remaining Security Concerns

- Direct CAN Bus Access
- Critical Functionality in the VM is running alongside the less trusted autonomy stack.
  - Safety Lights
  - Vehicle Control



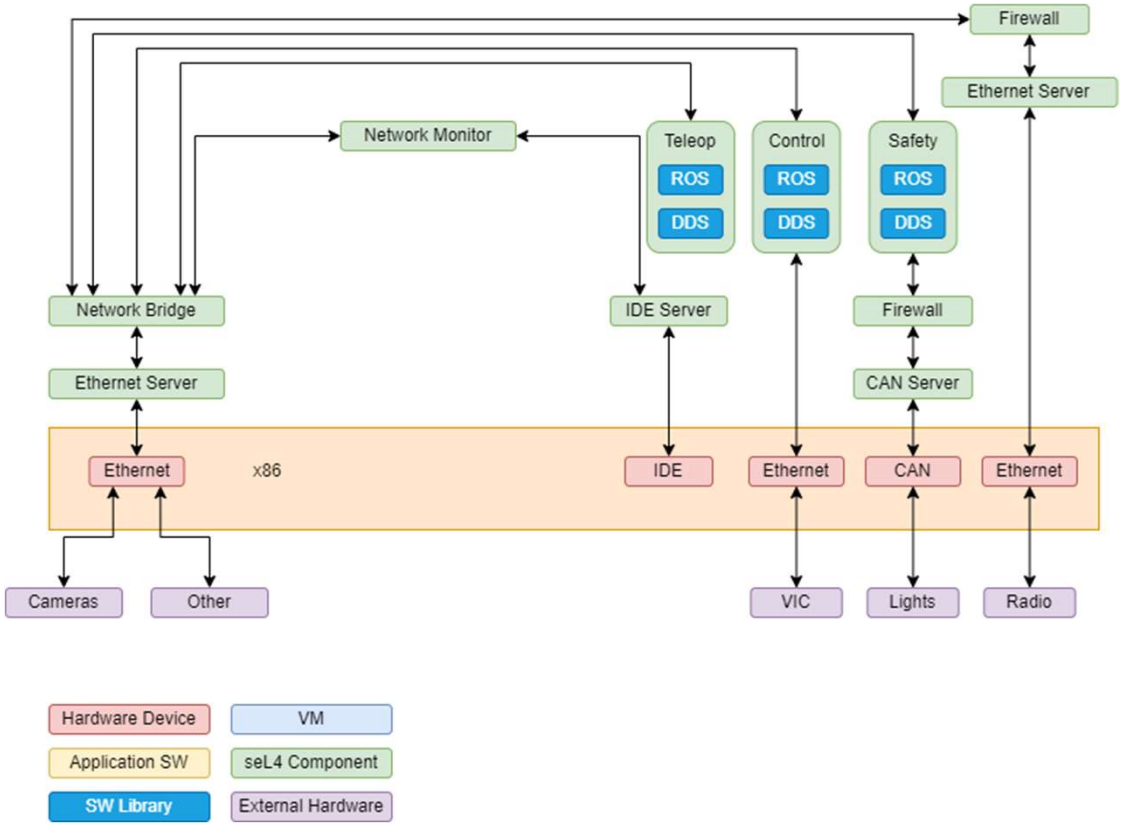
Goal Architecture

- Isolated and Firewalled CAN
- Independent Safety Light and Vehicle Control



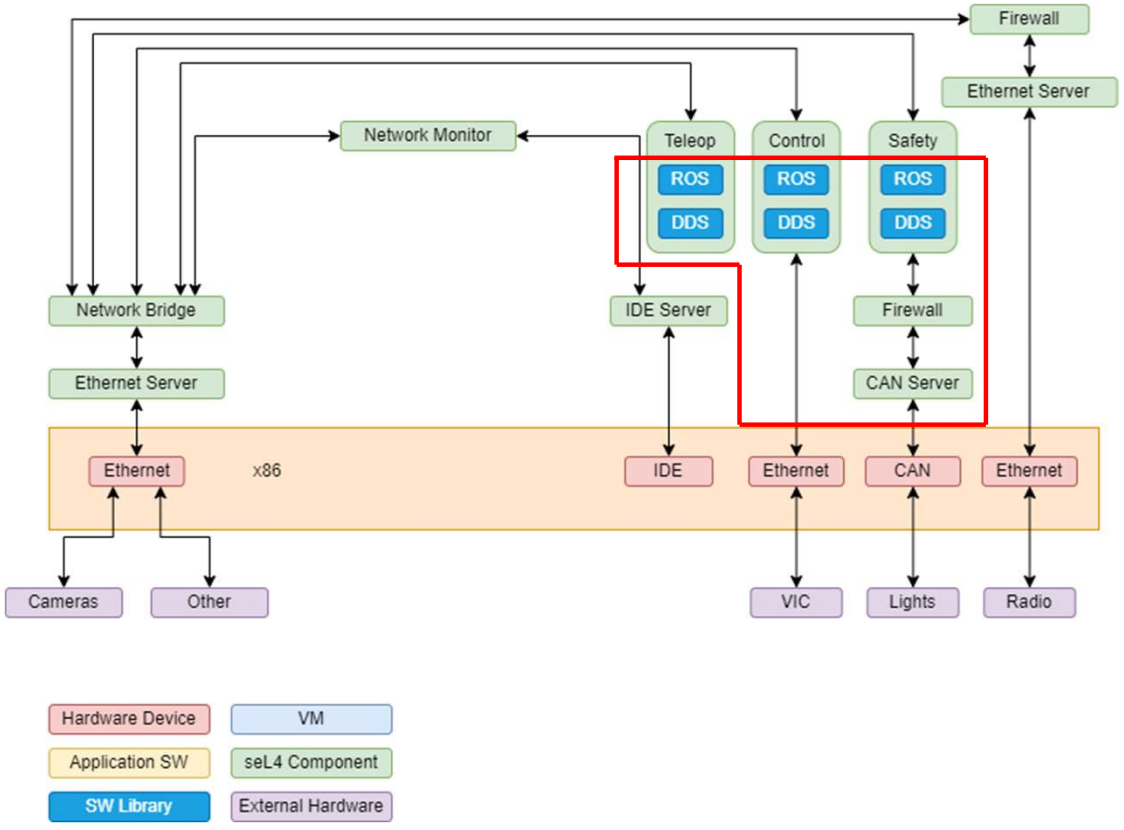
Limp Home Architecture

- Fallback to:
  - Teleop
  - Backtracking
  - Something else



Gaps

- CAN
- ROS
- DDS

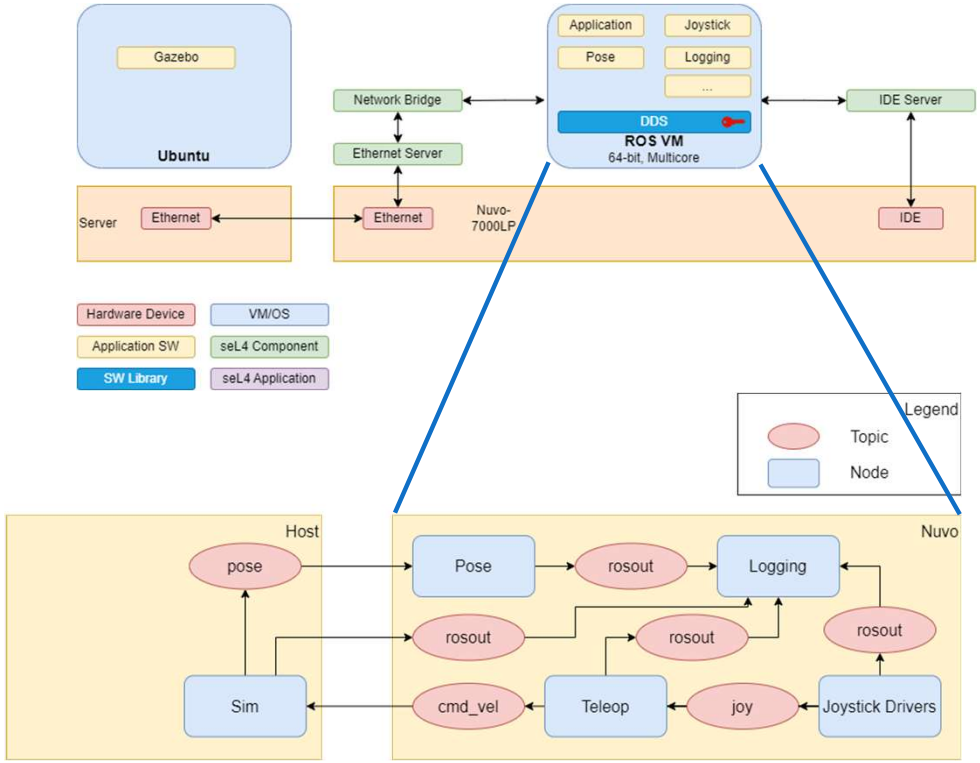


Retrofit Round 2

1. Reference System
2. DDS Port
3. RCL and Micro-ROS Port
4. Native seL4 ROS Nodes
5. Move Reference System Nodes to seL4 Threads

Reference System Info

- ROS Nodes
  - I/O: Joystick
  - Computation: Pose
  - Storage: Logging
  - Teleoperation
- External Connection to Simulator



Compare Contrast seL4 vs ROS

seL4

- Microkernel – significantly less out of box features
- C++ not fully supported
- No publicly available DDS library
- Static, Componentized architecture
- IPC or shared memory for inter-component communication

ROS

- Expects to be run on Linux
- Mostly written in C++
- Requires DDS Middleware
- Dynamic, Node based distributed architecture
- Networking for inter-node communication

Compare Contrast Micro-Ros vs ROS

Micro-ROS

- Targeted for use in Microcontrollers
- Nodes written in C
- Supported on Linux, FreeRTOS, Zephyr, NuttX

ROS

- Typically used on more performant systems
- Nodes written in C++ or python
- Supported on Linux

DDS Candidate Comparison

	eProsima FastDDS	embeddedRTPS	Eclipse CycloneDDS	eProsima Micro-XRCE DDS
Language	C++	C++	C	C
POSIX Threads	Yes	No	Yes	Not required
Transport Interface	Sockets	Raw Mode	Sockets	Sockets, CAN, Serial, Custom
Cross Network Discovery	Yes, using Discovery Server	Untested	Not in version 0.7.0	Yes, using the Agent
RTOS Support	No	FreeRTOS	FreeRTOS	FreeRTOS, Zephyr, NuttX
DDS-Security	Yes	No	Yes	No
Other	• ROS 2 default	• Currently experimental and quite limited	• Foxy uses version 0.7.0	• Client/Agent Architecture • Agent is in C++

DDS Other Candidates

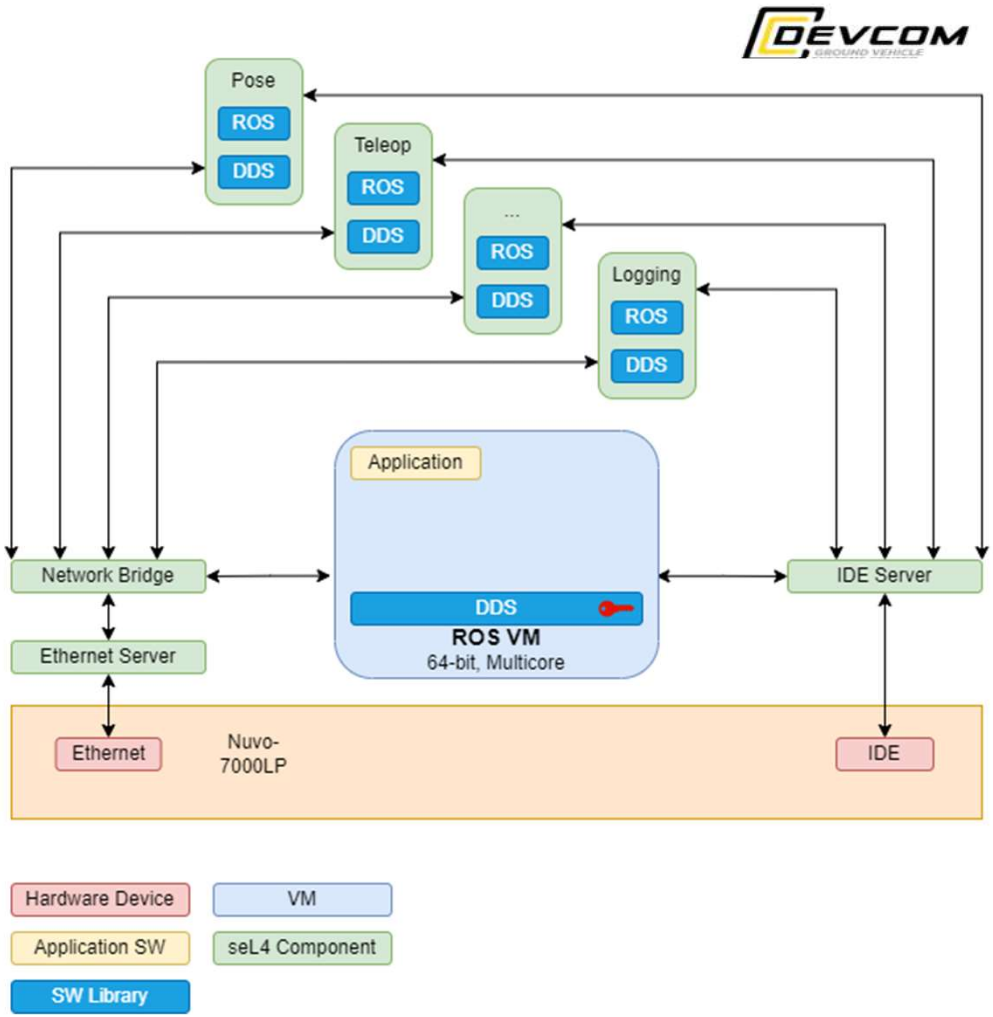
- Twin Oaks CoreDX DDS
  - Not open-source
  - Requires purchase of a license
  - Not currently supported by ROS
- RTI Connext DDS
  - Is currently supported by ROS and is ported to seL4
  - Not open-source
  - License is restrictive, expensive
- Not Evaluated
  - OpenDDS
  - GurumDDS
  - Cerebus DDS
  - Rust DDS
  - Zenoh (DDS Alternative)

Micro-ROS Port Info

- Some C++ but no STL
  - Most just worked
  - Rest easy to convert
- (Micro-)ROS build system
  - Uses Ament CMake with colcon tool
  - seL4 CMake toolchain difficult to extract for use outside of seL4 build system
  - Difficult to integrate with seL4 build system
  - Might be fixed with Microkit

Results

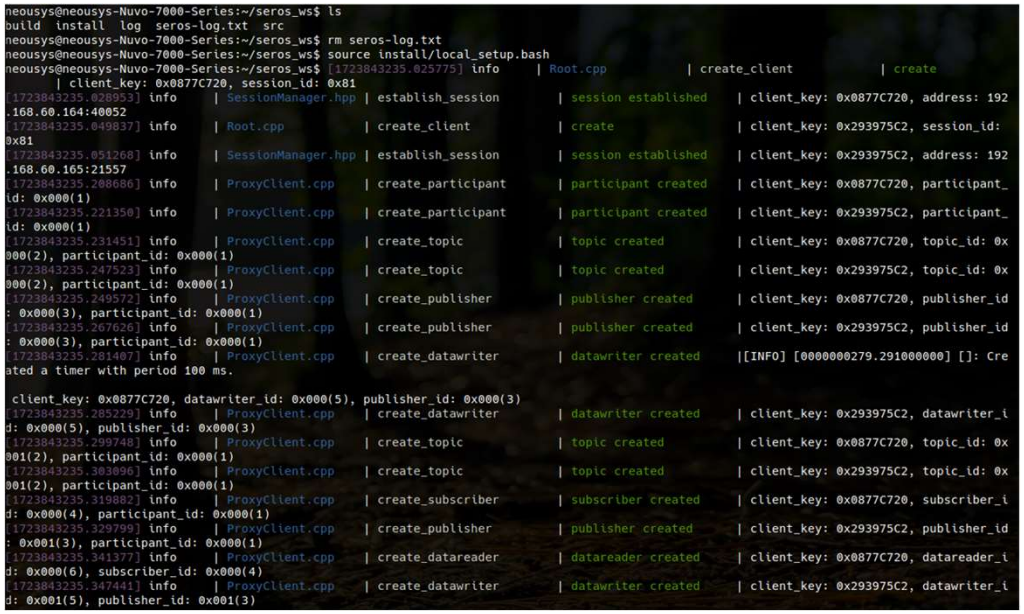
- Ported Micro-XRCE DDS to seL4
- Ported Micro-ROS to seL4
- Migrated several ROS nodes from VM to native seL4 threads

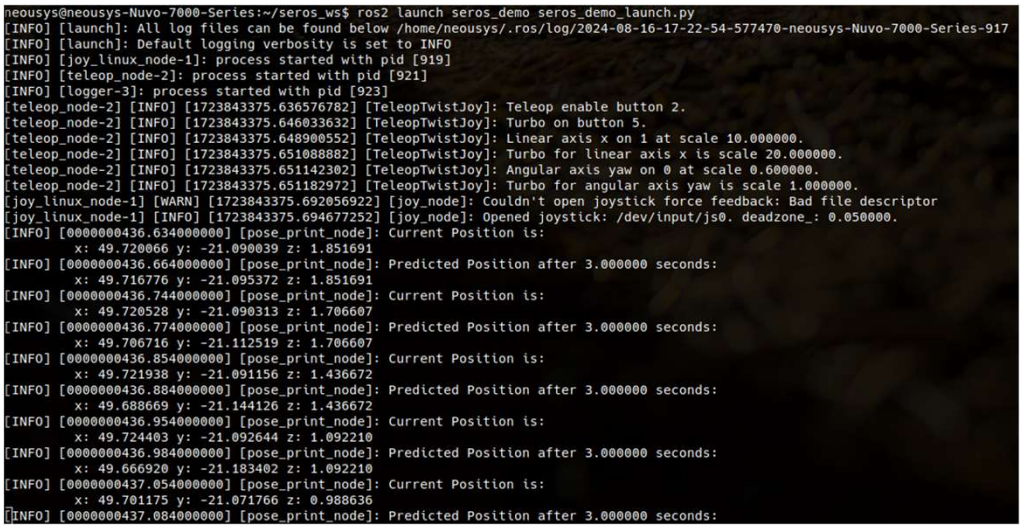


Demo

Simulator environment adapted with help from Dom Larkin of Raytheon BBN.

Demo


neousys@neousys-Nuvo-7000-Series:~/seros_ws$ ls
build install log seros-log.txt src
neousys@neousys-Nuvo-7000-Series:~/seros_ws$ rm seros-log.txt
neousys@neousys-Nuvo-7000-Series:~/seros_ws$ source install/local_setup.bash
neousys@neousys-Nuvo-7000-Series:~/seros_ws$ [1723843235.025775] info | Root.cpp | create_client | create
| client_key: 0x0877C720, session_id: 0x81
[1723843235.028953] info | SessionManager.hpp | establish_session | session established | client_key: 0x0877C720, address: 192
.168.60.164:40052
[1723843235.049837] info | Root.cpp | create_client | create | client_key: 0x293975C2, session_id:
0x81
[1723843235.051268] info | SessionManager.hpp | establish_session | session established | client_key: 0x293975C2, address: 192
.168.60.165:21557
[1723843235.208686] info | ProxyClient.cpp | create_participant | participant created | client_key: 0x0877C720, participant_
id: 0x000(1)
[1723843235.221350] info | ProxyClient.cpp | create_participant | participant created | client_key: 0x293975C2, participant_
id: 0x000(1)
[1723843235.231451] info | ProxyClient.cpp | create_topic | topic created | client_key: 0x0877C720, topic_id: 0x
000(2), participant_id: 0x000(1)
[1723843235.247523] info | ProxyClient.cpp | create_topic | topic created | client_key: 0x293975C2, topic_id: 0x
000(2), participant_id: 0x000(1)
[1723843235.249572] info | ProxyClient.cpp | create_publisher | publisher created | client_key: 0x0877C720, publisher_id
: 0x000(3), participant_id: 0x000(1)
[1723843235.267626] info | ProxyClient.cpp | create_publisher | publisher created | client_key: 0x293975C2, publisher_id
: 0x000(3), participant_id: 0x000(1)
[1723843235.281407] info | ProxyClient.cpp | create_datawriter | datawriter created |[INFO] [0000000279.291000000] []: Cre
ated a timer with period 100 ms.
client_key: 0x0877C720, datawriter_id: 0x000(5), publisher_id: 0x000(3)
[1723843235.285229] info | ProxyClient.cpp | create_datawriter | datawriter created | client_key: 0x293975C2, datawriter_i
d: 0x000(5), publisher_id: 0x000(3)
[1723843235.299748] info | ProxyClient.cpp | create_topic | topic created | client_key: 0x0877C720, topic_id: 0x
001(2), participant_id: 0x000(1)
[1723843235.303896] info | ProxyClient.cpp | create_topic | topic created | client_key: 0x293975C2, topic_id: 0x
001(2), participant_id: 0x000(1)
[1723843235.319882] info | ProxyClient.cpp | create_subscriber | subscriber created | client_key: 0x0877C720, subscriber_i
d: 0x000(4), participant_id: 0x000(1)
[1723843235.329799] info | ProxyClient.cpp | create_publisher | publisher created | client_key: 0x293975C2, publisher_id
: 0x001(3), participant_id: 0x000(1)
[1723843235.341377] info | ProxyClient.cpp | create_datareader | datareader created | client_key: 0x0877C720, datareader_i
d: 0x000(6), subscriber_id: 0x000(4)
[1723843235.347441] info | ProxyClient.cpp | create_datawriter | datawriter created | client_key: 0x293975C2, datawriter_i
d: 0x001(5), publisher_id: 0x001(3)

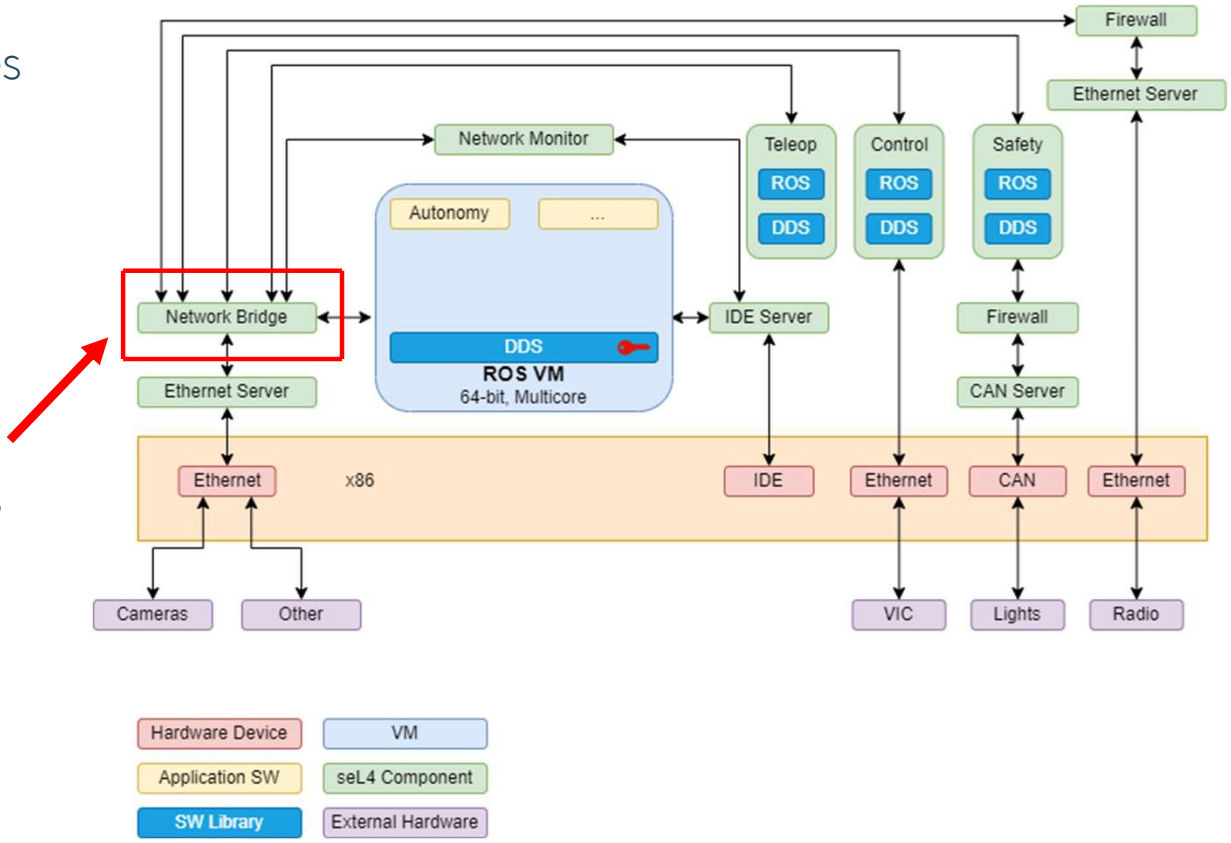

neousys@neousys-Nuvo-7000-Series:~/seros_ws$ ros2 launch seros_demo seros_demo_launch.py
[INFO] [launch]: All log files can be found below /home/neousys/.ros/log/2024-08-16-17-22-54-577470-neousys-Nuvo-7000-Series-917
[INFO] [launch]: Default logging verbosity is set to INFO
[INFO] [joy_linux_node-1]: process started with pid [919]
[INFO] [teleop_node-2]: process started with pid [921]
[INFO] [logger-3]: process started with pid [923]
[teleop_node-2] [INFO] [1723843375.636576782] [TeleopTwistJoy]: Teleop enable button 2.
[teleop_node-2] [INFO] [1723843375.646033632] [TeleopTwistJoy]: Turbo on button 5.
[teleop_node-2] [INFO] [1723843375.648900552] [TeleopTwistJoy]: Linear axis x on 1 at scale 10.000000.
[teleop_node-2] [INFO] [1723843375.651088882] [TeleopTwistJoy]: Turbo for linear axis x is scale 20.000000.
[teleop_node-2] [INFO] [1723843375.651142302] [TeleopTwistJoy]: Angular axis yaw on 0 at scale 0.600000.
[teleop_node-2] [INFO] [1723843375.651182972] [TeleopTwistJoy]: Turbo for angular axis yaw is scale 1.000000.
[joy_linux_node-1] [WARN] [1723843375.692056922] [joy_node]: Couldn't open joystick force feedback: Bad file descriptor
[joy_linux_node-1] [INFO] [1723843375.694677252] [joy_node]: Opened joystick: /dev/input/js0. deadzone_: 0.050000.
[INFO] [0000000436.634000000] [pose_print_node]: Current Position is:
x: 49.720066 y: -21.090039 z: 1.851691
[INFO] [0000000436.664000000] [pose_print_node]: Predicted Position after 3.000000 seconds:
x: 49.716776 y: -21.095372 z: 1.851691
[INFO] [0000000436.744000000] [pose_print_node]: Current Position is:
x: 49.720528 y: -21.090313 z: 1.706607
[INFO] [0000000436.774000000] [pose_print_node]: Predicted Position after 3.000000 seconds:
x: 49.706716 y: -21.112519 z: 1.706607
[INFO] [0000000436.854000000] [pose_print_node]: Current Position is:
x: 49.721938 y: -21.091156 z: 1.436672
[INFO] [0000000436.884000000] [pose_print_node]: Predicted Position after 3.000000 seconds:
x: 49.688669 y: -21.144126 z: 1.436672
[INFO] [0000000436.954000000] [pose_print_node]: Current Position is:
x: 49.724403 y: -21.092644 z: 1.092210
[INFO] [0000000436.984000000] [pose_print_node]: Predicted Position after 3.000000 seconds:
x: 49.666920 y: -21.183402 z: 1.092210
[INFO] [0000000437.054000000] [pose_print_node]: Current Position is:
x: 49.701175 y: -21.071766 z: 0.988636
[INFO] [0000000437.084000000] [pose_print_node]: Predicted Position after 3.000000 seconds:

Remaining Gaps

- DDS Security
- Richer File System Support
- C++ STL Support
- POSIX Threadlike API
- Robot Specific Device Drivers
- Other

Future Work

- Upstream DDS and ROS Libraries
- DDS Improvements
  - Security
  - Performance
  - Scaling
  - etc…
- Micro-ROS to ROS2
- MicroKit (sDDF) Conversion
- Verified Userspace Components
- Additional I/O:
  - Cameras
  - etc…
- Additional Architectures:
  - ARM
  - etc…



Conclusion

- Cyber Retrofit Approach Works
- Able to run basic ROS nodes as seL4 threads
- More work is needed to support additional functionality

Questions?

References

- Murray, V., Lathrop, S., & Mikulski, D. (2024). Towards Deployment of a Zero-Trust Architecture (ZTA) for Automated Vehicles (AV). In Proceedings of the 2024 NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium: Modular Open Systems Approach (MOSA) Technical Session (pp. 13-15). Novi, MI: Southwest Research Institute, Raytheon BBN Technologies, US Army DEVCOM Ground Vehicle Systems Center.
- Mikulski, D. (2014). Soft Security Considerations for Unmanned Systems. In Proceedings of the 2014 NDIA Ground Vehicle Systems Engineering and Technology Symposium: Autonomous Ground Systems (AGS) Technical Session (pp. 12-14). Novi, MI: U.S. Army TARDEC.
- Boulet, M., DelGizzi, R., Lathrop, S., Leahy, B., Montez, J., Rucinski, G., Spinola, M., Thomasmeyer, W., & Towler, J. (2021). Collaborative Migration of an Autonomous Ground Vehicle Software System to ROS 2. In Proceedings of the 2021 NDIA Ground Vehicle Systems Engineering and Technology Symposium: Autonomy, Artificial Intelligence & Robotics (AAIR) Technical Session (pp. 10-12). Novi, MI: MIT Lincoln Laboratory, Stratom, Raytheon BBN, Robotic Research, Neya Systems, National Advanced Mobility Consortium.
- Pereira, S., Mott, C., & Mikulski, D. (2023). Secure Update Process for Robotic and Autonomous Systems. In Proceedings of the 2023 NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium: Autonomy, Artificial Intelligence & Robotics Technical Session (pp. 15-17). Novi, MI: Intelligent Systems Division, Southwest Research Institute, US Army DEVCOM Ground Vehicle Systems Center.
- Mott, C., Mikulski, D., & Pereira, S. (2022). Secure Software Updates for Robotic and Autonomous Systems. In Proceedings of the 2022 NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium: Cybersecurity of Ground Systems Technical Session (pp. 16-18). Novi, MI: Intelligent Systems Division, Southwest Research Institute, US Army DEVCOM Ground Vehicle Systems Center.

WWW.DORNERWORKS.COM