University of Stuttgart

Institute of Space Systems

Robin Müller
muellerr@irs.uni-stuttgart.de
Institute of Space Systems
Pfaffenwaldring 29, D-70565 Stuttgart, Germany
https://absatsw.irs.uni-stuttgart.de/
https://www.irs.uni-stuttgart.de/

Robin Müller

Investigation of the Rust programming language for Flight Software Development

Current State of the Art for Flight Software Stacks

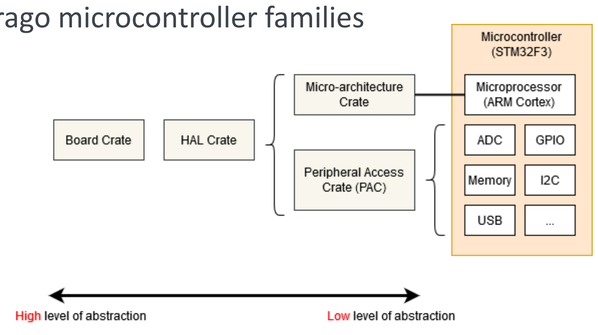
- C and C++ frameworks and libraries are the standard solution, for example NASA cFS or F Prime, or in-house framework FSFW
- Proven and matured technology, but not perfect: Prone to memory-bugs, hard dependency management

Rust – A modern system's programming language

- Compiled language with performance comparable to C and C++
- Safety by Design: The borrow checker prevents memory bugs at compile time
- All the tooling needed to write high-quality software out-of-the-box: Linter, formatter and unit-test harness…
- Easy dependency management

Rust in the Embedded Domain

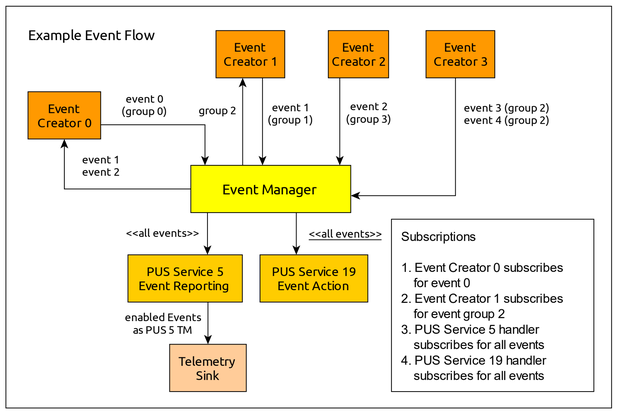
- Strong existing layered ecosystem for working with common microcontrollers
- Good support for interoperability with (vendor provided) C libraries
- Write platform independent drivers with the `embedded-hal` library
- Space domain specific support for radiation-hardened Vorago microcontroller families



Event Management with sat-rs

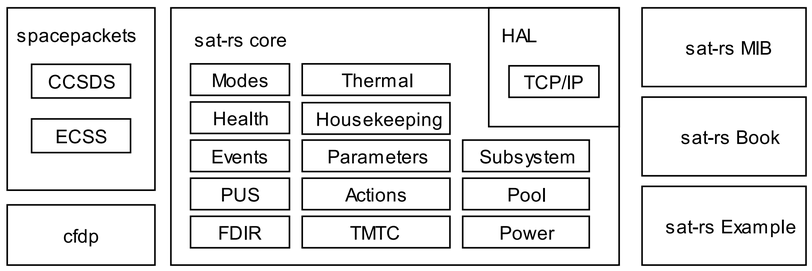
Event system for:

- Obvervability
- Light-weight Inter-Process Communication mechanism
- Fault, Detection, Isolation And Recovery (FDIR) purposes



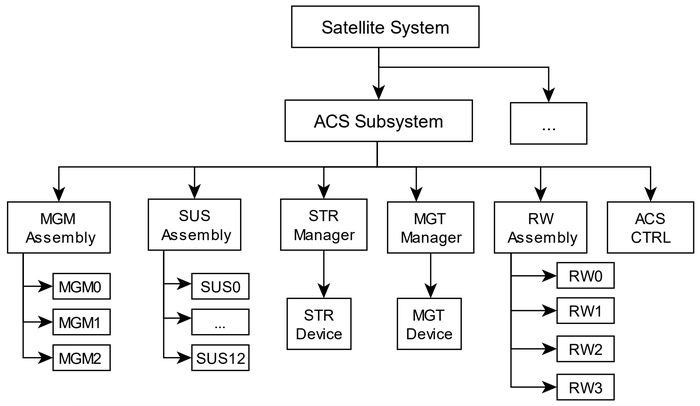
sat-rs – A library collection for writing flight software

- Written specifically for remote systems like satellites and CubeSats
- Written with embedded systems in mind: Run-time allocation is avoided, but still offer good support for systems without a standard run-time
- Standardized and interoperable components extracted to separate libraries, for example for CCSDS and ECSS protocols



Mode Tree Modelling with sat-rs

- Satellite components can be modelled as a tree structure
- Mode commands are propagated down the system tree
- Specify system modes and transition sequences inside table structures



ACS Mode Tree

Mode	MGMs	SUSs	STR	MGT	RWs	ACS CTRL
OFF	OFF	OFF	OFF	OFF	OFF	OFF
SAFE	NORMAL	NORMAL	OFF	OFF	NORMAL	SAFE
IDLE	NORMAL	NORMAL	NORMAL	NORMAL	NORMAL	IDLE

ACS IDLE Sequence

Step	MGMs	SUS	STR	MGT	RWs	ACS CTRL
1	NORMAL	NORMAL	NORMAL	NORMAL	NORMAL	
2						SAFE

sat-rs – A Good Fit for your System as well?

- Existing early flight heritage: Usage for an on-board software simulator and on the ESA OPS-SAT mission
- Example Application which can be run on a host computer and comes with a mini-simulator