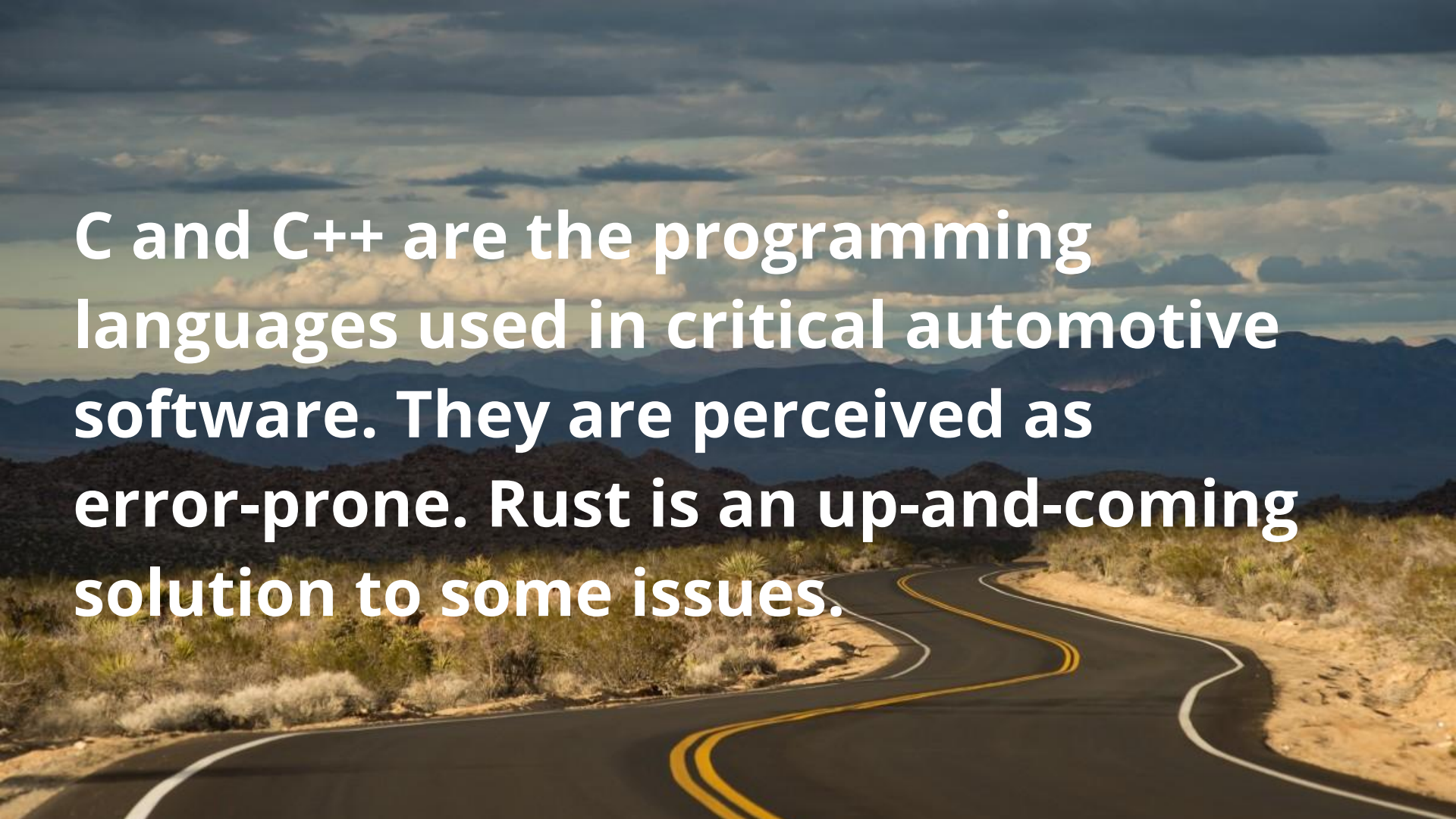
Rust in Automotive: Shifting Left and Shifting into Gear

Pete LeVasseur
Eclipse uProtocol
Safety-Critical Rust Consortium

Free stock photos - PxHere - 1055658

Changing Winds



C and C++ are the programming languages used in critical automotive software. They are perceived as error-prone. Rust is an up-and-coming solution to some issues.

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3215760/nsa-releases-guidance-on-how-to-protect-against-software-memory-safety-issues/

Example headwinds

PRESS RELEASE | Nov. 10, 2022

NSA Releases Guidance on How to Protect Against Software Memory Safety Issues

FORT MEADE, Md. — The National Security Agency (NSA) published guidance today to help software developers and operators prevent and mitigate software memory safety issues, which account for a large portion of exploitable vulnerabilities.

https://advocacy.consumerreports.org/wp-content/uploads/2023/01/Memory-Safety-Convening-Report.pdf

Example headwinds

Future of Memory Safety

Challenges and Recommendations

YAEL GRAUER
JANUARY 2023

CR Consumer Reports | Security Planner

https://www.vice.com/en/article/a3mgxb/the-internet-has-a-huge-cc-problem-and-developers-dont-want-to-deal-with-it

Example headwinds

Magazine TV News Culture Tech Munchies Music Waypoint Shop Newsletters

Tech

The Internet Has a Huge C/C++ Problem and Developers Don't Want to Deal With It

By Alex Gaynor November 15, 2018, 8:39am

https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf

Example headwinds

Guidelines on Minimum Standards for Developer Verification of Software

Paul E. Black
Barbara Guttman
Vadim Okun

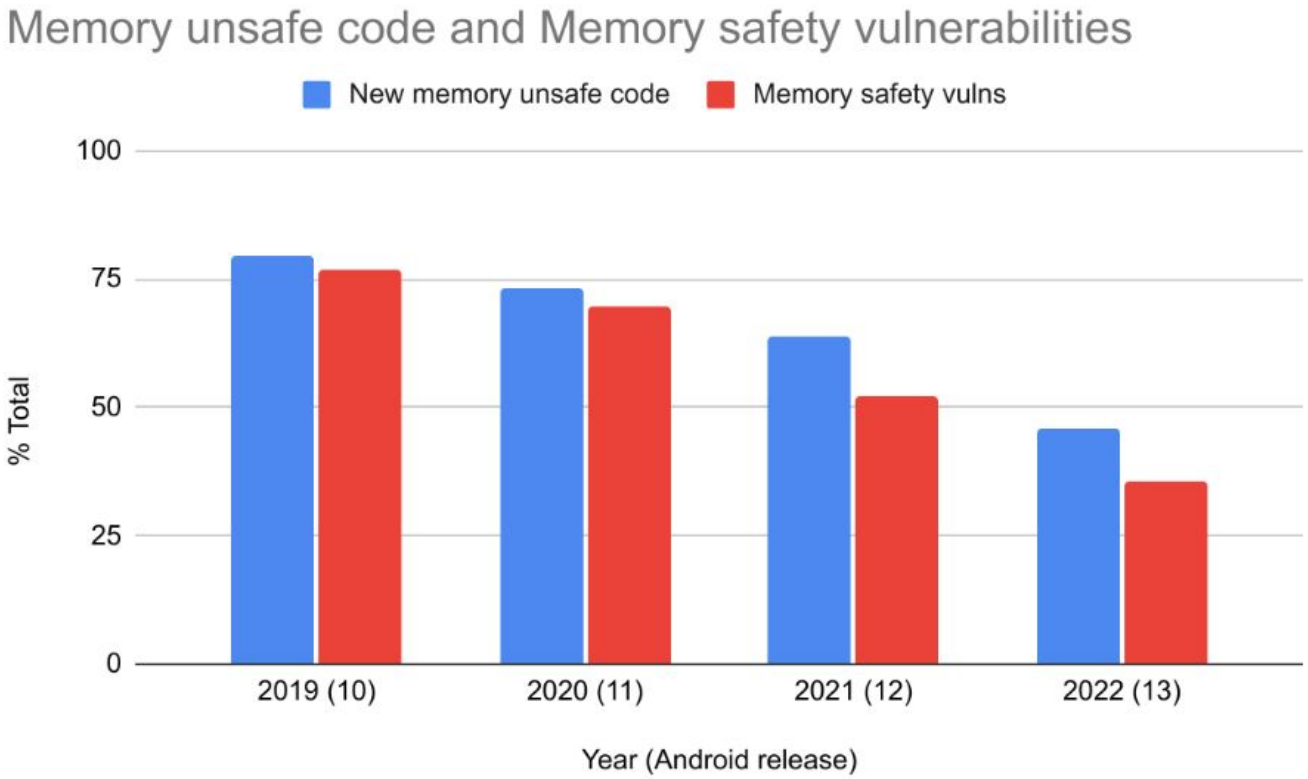
These are only some of the publications from a few years ago. The regulations and pressure have only increased since then.

Meeting the Moment

I see Rust's mission as making it dramatically more accessible to author and maintain foundational software. *By foundational I mean the software that underlies everything else.* - Niko Matsakis

Rust as bumper rails for quality software

Coexistence possible, still see memory-safety benefits



https://security.googleblog.com/2022/12/memory-safe-languages-in-android-13.html

But, can we use Rust in a safety setting?

DOVER, DELAWARE, USA, June 12, 2024 – The Rust Foundation, AdaCore, Arm, Ferrous Systems, HighTec EDV-Systeme GmbH, Lynx Software Technologies, OxidOS, TECHFUND, TrustInSoft, Veecle, and Woven by Toyota are thrilled to jointly announce the Safety-Critical Rust Consortium. The primary objective of this group will be to support the responsible use of the Rust programming language in safety-critical software — systems whose failure can impact human life or cause severe environmental or property harm.

Safety-Critical Rust Consortium Membership is open to Rust Foundation member organizations and other invitees, such as industry, academic, and legal experts.

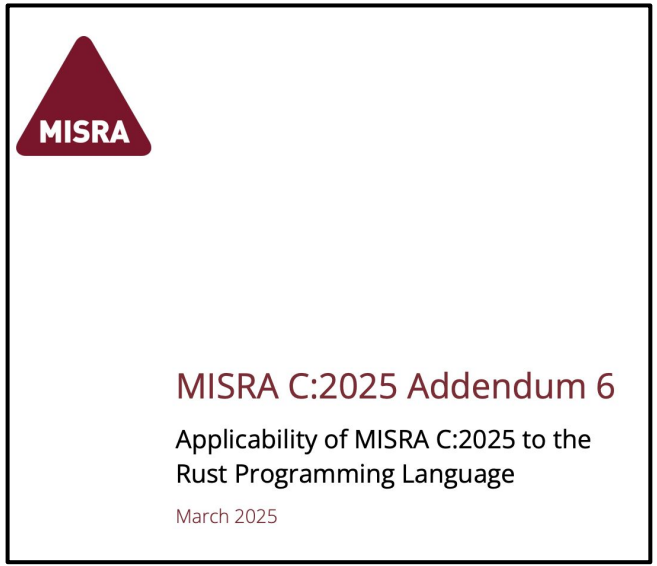
Work under the consortium will begin with the creation of a public charter and goals, and meeting minutes will be published on an ongoing basis. The Safety-Critical Rust Consortium will liaise with the Rust Project through Rust Foundation Project Directors and members of Rust Project teams. The Consortium's scope, which will be fully delineated in the charter, may include the development of guidelines, linters, libraries, static analysis tools, formal methods and language subsets to meet industrial and legal requirements. The Consortium's deliverables will be developed and licensed in a manner compatible with other Rust Project endeavors.

https://rustfoundation.org/media/announcing-the-safety-critical-rust-consortium/

Rust is in Motion in Automotive

Rust Adoption

- Infineon
- Vector
- Aptiv
- Ampere
- Volvo Cars



> 50% of rules are irrelevant to Rust

Ferrocene

- ASIL-D Compiler
- Language specification
- Ferrous Systems
- Now considered de-facto in safety-critical

Rust supports platforms in-use in Automotive

`*-nuttx-elf`

Tier: 3

nto-qnx

Tier: 3

The QNX® Neutrino (nto) Real-time operating system. Known as QNX OS from version 8 onwa

This support has been implemented jointly by Elektrobit Automotive GmbH and QNX.

Target maintainers

- Florian Bartels, `Florian.Bartels@elektrobit.com`, https://github.com/flba-eb
- Tristan Roach, `TRoach@blackberry.com`, https://github.com/gh-tr
- Jonathan Pallant `Jonathan.Pallant@ferrous-systems.com`, https://github.com/jonathan
- Jorge Aparicio `Jorge.Aparicio@ferrous-systems.com`, https://github.com/japaric

`*-wrs-vxworks`

Tier: 3

Targets for the VxWorks operating system.

Target triplets available:

- `x86_64-wrs-vxworks`
- `aarch64-wrs-vxworks`
- `i686-wrs-vxworks`
- `armv7-wrs-vxworks-eabihf`
- `powerpc-wrs-vxworks`
- `powerpc64-wrs-vxworks`
- `powerpc-wrs-vxworks-spe`
- `riscv32-wrs-vxworks`
- `riscv64-wrs-vxworks`

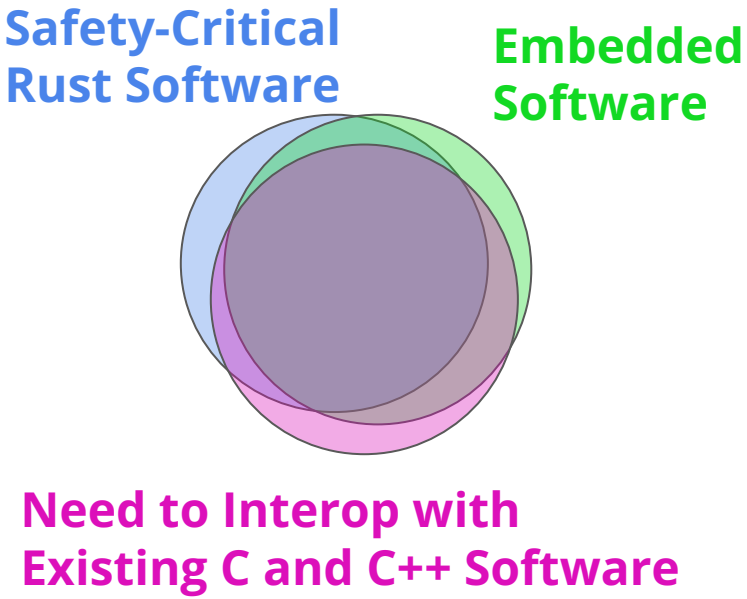
Safety-Critical Rust Consortium

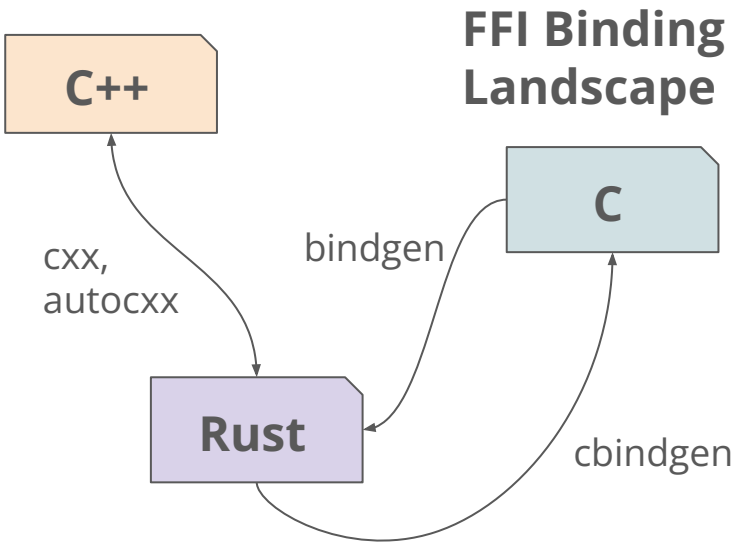
+ Safety - Critical = Safety-Critical Rust Consortium

Subcommittee

- → Tooling
- → Coding Guidelines
- → Liaison

C++/Rust Interop Initiative





Goals

- Improve interop binding tools
- Build richer interop into Rust language and compiler
- Social interop with C++

Eclipse SDV WG

Projects using Rust

KUKSA → Vehicle Services Data Broker

uProtocol → Service Mesh Abstraction

Zenoh → Low-latency middleware

iceoryx → Zero-copy shared-memory transport

Rust SIG

- Knowledge-share for Rust best-practices in Automotive
- Lightweight consensus building around tools and methods

Jumping In

Being a Rust expert is not required. There are needs related to understanding the Automotive industry's safety-critical standards and complying with them.

Interested in pitching in?

SDV
Eclipse Software Defined Vehicle

SDV COMMUNITY MAILING LIST

SDV community is the mailing list for SDV community discussions. Subscribe to the list for all things SDV.

Subscribe

SDV COMMUNITY CALENDAR

Join the SDV Community Calendar to learn more about SDV related plans.

Subscribe

SLACK

Join the conversations on SDV's slack workspace and see what the community members are up to.

Join Workspace

ECLIPSE NEWSLETTER

The Eclipse Foundation Community Newsletter is your destination for original articles about projects and key technologies.

Subscribe

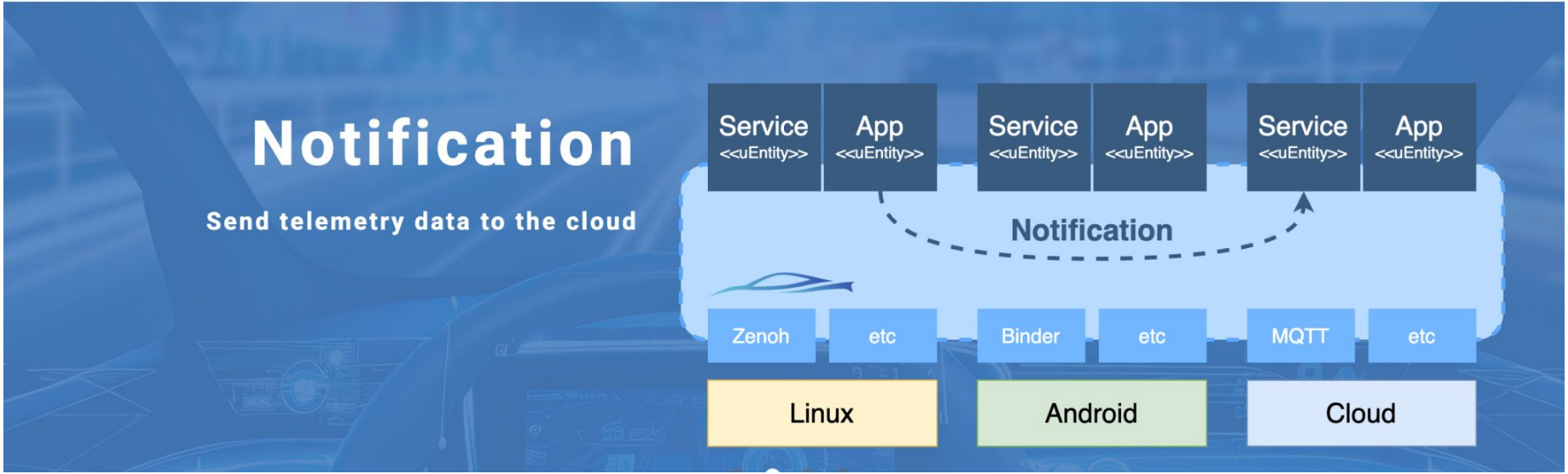
https://sdv.eclipse.org/get-engaged/

Interested in pitching in?

uProtocol

CONNECTING AUTOMOTIVE APPS AND SERVICES, EVERYWHERE

ABOUT DOCS & MEDIA GETTING STARTED



https://uprotocol.org/

Interested in pitching in?

https://arewesafetycriticalyet.org/

Safety-Critical Rust Consortium

Are We Safety Critical Yet?

It depends 🤔, we have a few certified compilers, a few certification products in-progress and a few use cases.

Find out!

Coding Guidelines

Tooling

Liaison

https://github.com/rustfoundation/safety-critical-rust-consortium

Thank You!

Pete LeVasseur

Safety-Critical Rust Consortium

uProtocol
CONNECTING AUTOMOTIVE APPS AND SERVICES, EVERYWHERE