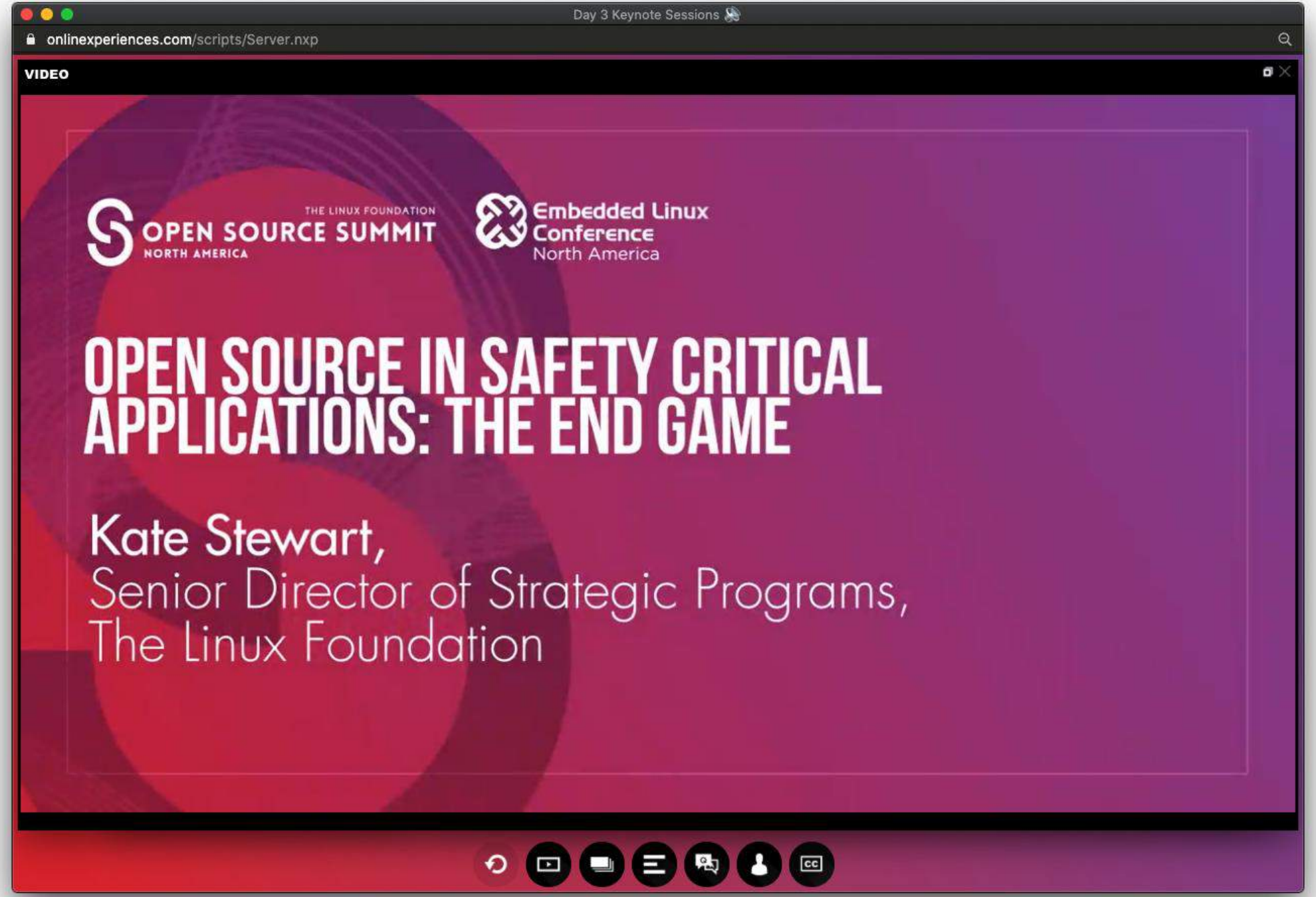

Day 3 Keynote Sessions
onlinexperiences.com/scripts/Server.nxp
VIDEO
THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA
Embedded Linux
Conference
North America
OPEN SOURCE IN SAFETY CRITICAL APPLICATIONS: THE END GAME
Kate Stewart,
Senior Director of Strategic Programs,
The Linux Foundation
CC

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION OPEN SOURCE SUMMIT NORTH AMERICA

Embedded Linux Conference North America

VIDEO

SLIDES

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

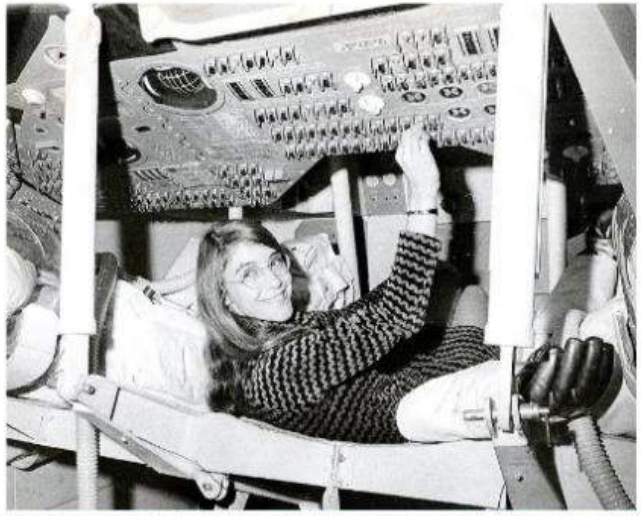
VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES



source: https://en.wikipedia.org/wiki/Margaret_Hamilton_(software_engineer)#/media/File:Margaret_Hamilton_in_action.jpg

2

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Apollo On-Board Flight Software

- The challenge was unique: build man-rated software; meaning astronauts' lives were at stake. It had to WORK—the first time
- Not only did the software, itself, have to be ultra-reliable, but it would need to be able to detect an error and recover from it in real time
- Learning by "doing" and "being". Hardware engineers came with rules; we didn't. Problems had to be solved that had never been solved before. At times, we made it up
- Most developers were fearless and young; yet, dedication and commitment a given
- Managers (mostly from hardware backgrounds) for whom software was a mystery, gave us total freedom and trust

source: https://www.lcse2018.org/getImage/orig/8E50th.10w.0.pdf
video: https://www.youtube.com/watch?v=ZbVOF0Uk58U

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Open Source is the Foundation for Innovation

"**99%** of codebases audited in 2019 contained **open source components**. Open source made up **70%** of the audited codebases." - 2020 Black Duck Report

" We've observed **double and triple digit growth** in open source component ecosystems for a decade, and there is no slowdown in sight." 2019 SonaType Report

THE LINUX FOUNDATION

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Source: https://www.space.com/spacex-reuse-crew-dragon-falcon-9-rockets.html (Image: © Bill Ingalls/NASA)

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

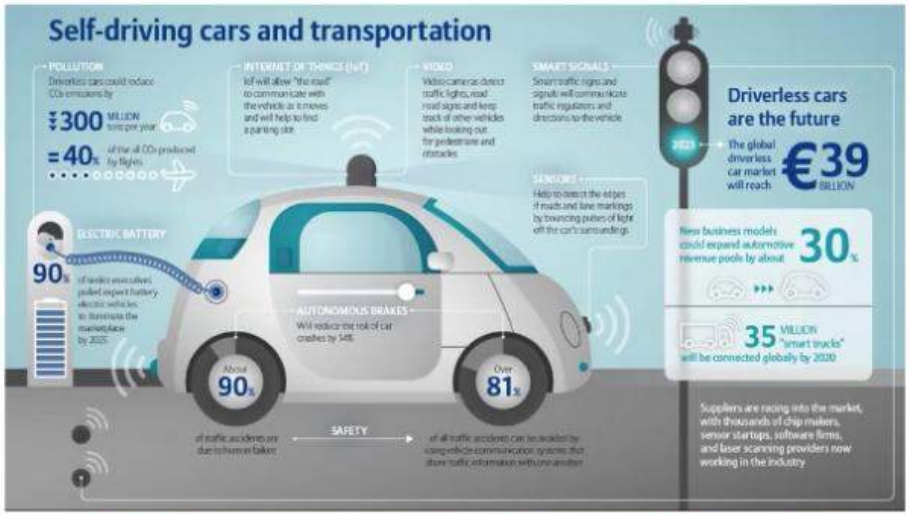
VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES



Source: https://www.datasciencecentral.com/profiles/blogs/ai-in-transportation-top-3-real-world-cases

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

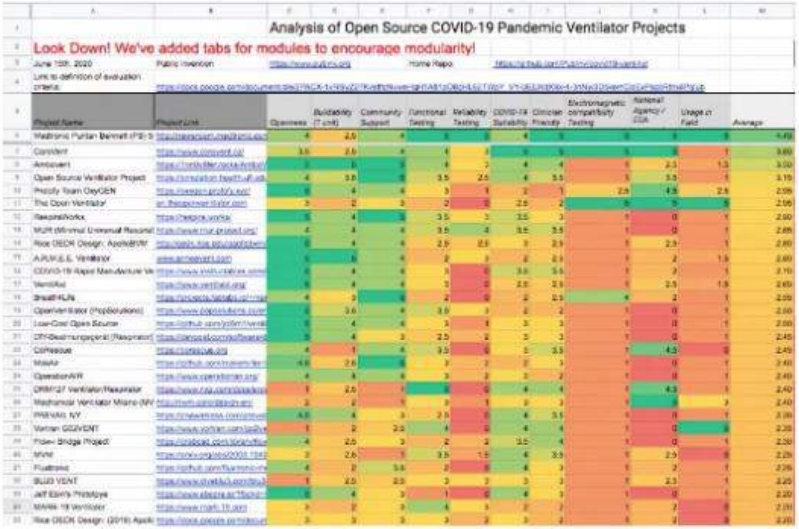
VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES



Analysis of Open Source COVID-19 Pandemic Ventilator Projects

Look Down! We've added tabs for modules to encourage modularity!

Source: https://docs.google.com/spreadsheets/d/1inYw5H4RiL0AC_J9vPWzJxXCdlkMLPBRdPgEVKF8DZw/edit#gid=0

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Open source is already being used in safety critical applications

THE LINUX FOUNDATION

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Safety Certification of Open Source Projects?

Some of the Linux Foundation projects that working towards being able to demonstrate functional safety

Zephyr™ seL4 ACRN Xen Project CIVIL INFRASTRUCTURE PLATFORM AUTOMOTIVE GRADE LINUX ELISA ENABLING LINUX IN SAFETY APPLICATIONS

smaller footprint ⟷ larger footprint

THE LINUX FOUNDATION

9

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

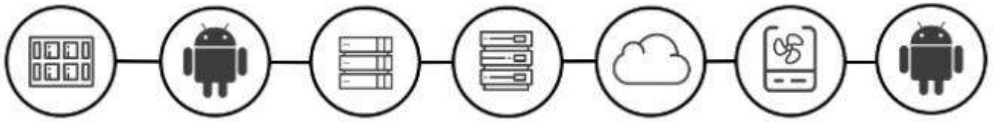
Embedded Linux Conference
North America

VIDEO

SLIDES

Linux Has Grown Into the Most Important Open Source Project in the World

100%	82%	2nd	90%	90%	69%	#1
Supercomputer Market	Smartphone Market Share	To Windows in Enterprise	Mainframe Customers	Public Cloud Workload	Embedded Systems Market	Internet Client



Every market Linux has entered it eventually dominates

THE LINUX FOUNDATION

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

ELISA

ENABLING LINUX IN SAFETY APPLICATIONS

THE LINUX FOUNDATION

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Enabling Linux in Safety-Critical Applications

To assess whether your system is safe, you need to understand your system sufficiently.

➔ If your system's safety depends on **Linux**, you need to **understand** Linux sufficiently for **your system's context and use**

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Safety-Critical Process Approach to Linux

The difference between Linux development for safety-critical and use in general applications **is the way you use it**.

- *Understand* your system and *understand* Linux interactions
- Make sure your system uses Linux based on the *selected* properties of Linux where *you can assure* quality exists already.

ELISA

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Compliance to Objectives of Safety Standards by Development Process Assessment:

- ➔ Linux has been **continuously developed for 29+ years**
- ➔ **Continuous process Improvement is in place.**
  - ✓ When technical or procedural issues in the kernel development are identified and pressing, the community addresses them.
- ➔ Evidence for the **requisite process quality** and **process improvement quality exists** already.
- ➔ This **evidence can indicate** that all objectives of a safety integrity level 2 for **selected parts and properties are met**.

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

ELISA Mission Statement

Define and maintain a common set of elements, processes and tools that can be incorporated into specific Linux-based, safety-critical systems amenable to safety certification.

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Path forward for "Closing the Gaps"

Kernel Development Community

Kernel Development Process Working Group

Identify safe reference process requirements and assess Linux Process Collateral and introduce features to fill the gaps

Safety Architecture Working Group

Identify Linux Software Architecture elements for FFI Analysis and Safety Mechanisms

Safety Standards

- IEC 61508 Generic Standard
  - IEC 62304 Medical devices
  - IEC 61511 Industrial Processes
  - ISO 26262 Automotive
  - …
- DO178B/C Aeronautics
- UL 1998
- ...

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

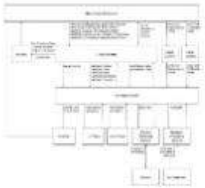
SLIDES

Proving out the Path

Medical Devices Working Group

Automotive Working Group

. . .



NDA

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Understanding the Limits

The collaboration:

- *cannot engineer* your system to be safe
- *cannot ensure* that you know how to apply the described process and methods
- *cannot create* an out-of-tree Linux kernel for safety-critical applications (Remember the continuous process improvement argument!)
- *cannot relieve* you from your responsibilities, legal obligations and liabilities.

But it will provide a **path forward** and peers to **collaborate** with!

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

What Will Success Look Like?

Assets for safety certification of Linux-based systems

- consisting of a complete process, selected kernel features and tools, and previous process assessments
- shown feasible with a reference system(s)
- usable by properly educated system integrators
- maintained over industrial-grade product lifetimes
- well-known and accepted by safety community, certification authorities and standardization bodies in multiple industries
- positively recognised and impacting the Linux kernel community
- hardware collateral from multiple supporting vendors

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

More Information about ELISA?

Next workshop: virtual in 2020Q3 (more info on devel mail list in July)

Web site: https://elisa.tech

Mail lists: https://lists.elisa.tech/g/devel

Sources: https://github.com/elisa-tech/workgroups

ELISA

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Zephyr™

THE LINUX FOUNDATION

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Zephyr Project

Zephyr

- **Open source** real time operating system
- Built with **safety and security** in mind
- Vibrant **Community** Participation
- **Cross-architecture** with broad SoC and development board support.
- **Vendor Neutral** governance
- **Permissively** licensed - Apache 2.0
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**
- **Product** development ready using LTS includes security updates
- **Certification** ready with Auditable

THE LINUX FOUNDATION PROJECTS

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Zephyr

Zephyr OS: Development

- **Quality** is a **mandatory expectation** for software across the industry.
- Assumptions:
  - Software Quality is enforced across Zephyr project members
  - Compliance to internal quality processes is expected.
- **Software Quality** is not an additional requirement caused by functional safety standards.
- Functional safety considers Quality as an **existing pre-condition**.

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

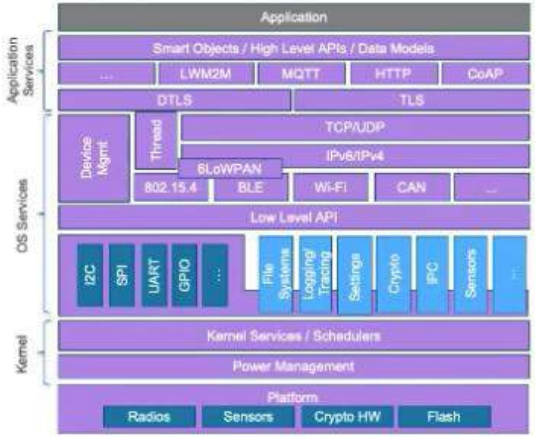
Embedded Linux Conference
North America

VIDEO

SLIDES

Architecture

Zephyr



- Highly Configurable, Highly Modular
- Cooperative and Preemptive Threading
- Memory and Resources are typically statically allocated
- Integrated device driver interface
- Memory Protection: Stack overflow protection, Kernel object and device driver permission tracking, Thread isolation
- Bluetooth® Low Energy (BLE 5.1) with both controller and host, BLE Mesh
- 802.15.4 OpenThread
- Native, fully featured and optimized networking stack

Fully featured OS allows developers to focus on the application

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

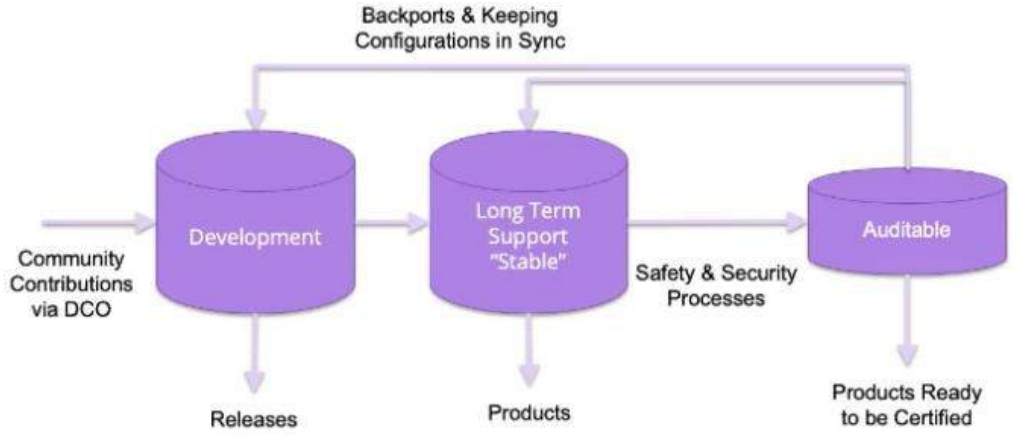
Embedded Linux Conference
North America

VIDEO

SLIDES

Zephyr

Code Repositories



25

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Zephyr

Zephyr OS: Auditable

An auditable code base will be established from a subset of the **Zephyr OS LTS**.

- Code bases will be kept in sync.
- More rigorous processes (necessary for certification) will be applied to the auditable code base.

Processes to achieve selected certification to be:

- Determined by **Safety** Committee and **Security** Committee
- Coordinated with **Technical Steering** Committee

Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

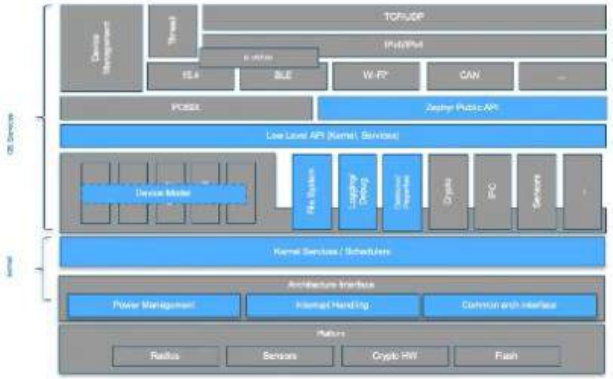
Zephyr OS: Initial Certification Focus - 61508

Zephyr

In scope
Out of scope

Scope will be **extended** to include **additional components** as determined by the safety committee

Some of the modules under consideration for the next iteration include: Crypto, IPC, Flash, etc.



Day 3 Keynote Sessions

onlinexperiences.com/scripts/Server.nxp

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Zephyr

Zephyr Project Roadmap

LTS 1
- User-space and Memory Protection Support
- Logging and Shell infrastructure
- Timer and Tick-less overhaul
- BSD Socket based networking

- MISRA-C Compliance
- Commercial Compiler Support and IDE Integration
- Multi Core / SMP
- Bluetooth® Split Link Layer
- Advanced Power Management

- E2E Cloud Integration
- Sound/Audio Capabilities
- Next Gen Bluetooth Technologies
- Quality Standards Compliance
- Certifiable Code Base

Accelerated Path
- Functional Safety Certification
- Quality Standards Compliance

LTS 2
- Functional Safety Certification
- Security Certification

2019 2020 2021

SLIDES

Zephyr

More Information about Zephyr?

Github:
- https://github.com/zephyrproject-rtos/zephyr

Orientation:
- https://www.zephyrproject.org/community/how-to-contribute
- https://www.zephyrproject.org/doc/contribute/contribute_guidelines.htm

Mail Lists:
- https://lists.zephyrproject.org/g/main

Slack:
- https://zephyrproject.slack.com

VIDEO

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference
North America

VIDEO

SLIDES

Summary

- Functional safety can **coexist** with open source projects, but we need to become **efficient at scale**.
- Quality needs to be driven at the open source **project level**
  - Need to showcase quality processes and plans for process improvements publicly
- Manage **developer** and **certification authority** expectations
  - Work within a well defined certification scope and focus on interfaces to system.
  - Understand the system where you want to use certified open source and get early buy in on design from certification authorities.

THE LINUX FOUNDATION

30

Questions?

For more information on these Linux Foundation projects see:

- https://www.zephyrproject.org/
- https://elisa.tech/

Or contact:
stewart@linux.com

Thank you!