Project Overview

Advancing Open Source Safety-Critical Systems

Philipp Ahmann, Robert Bosch GmbH

ELISA

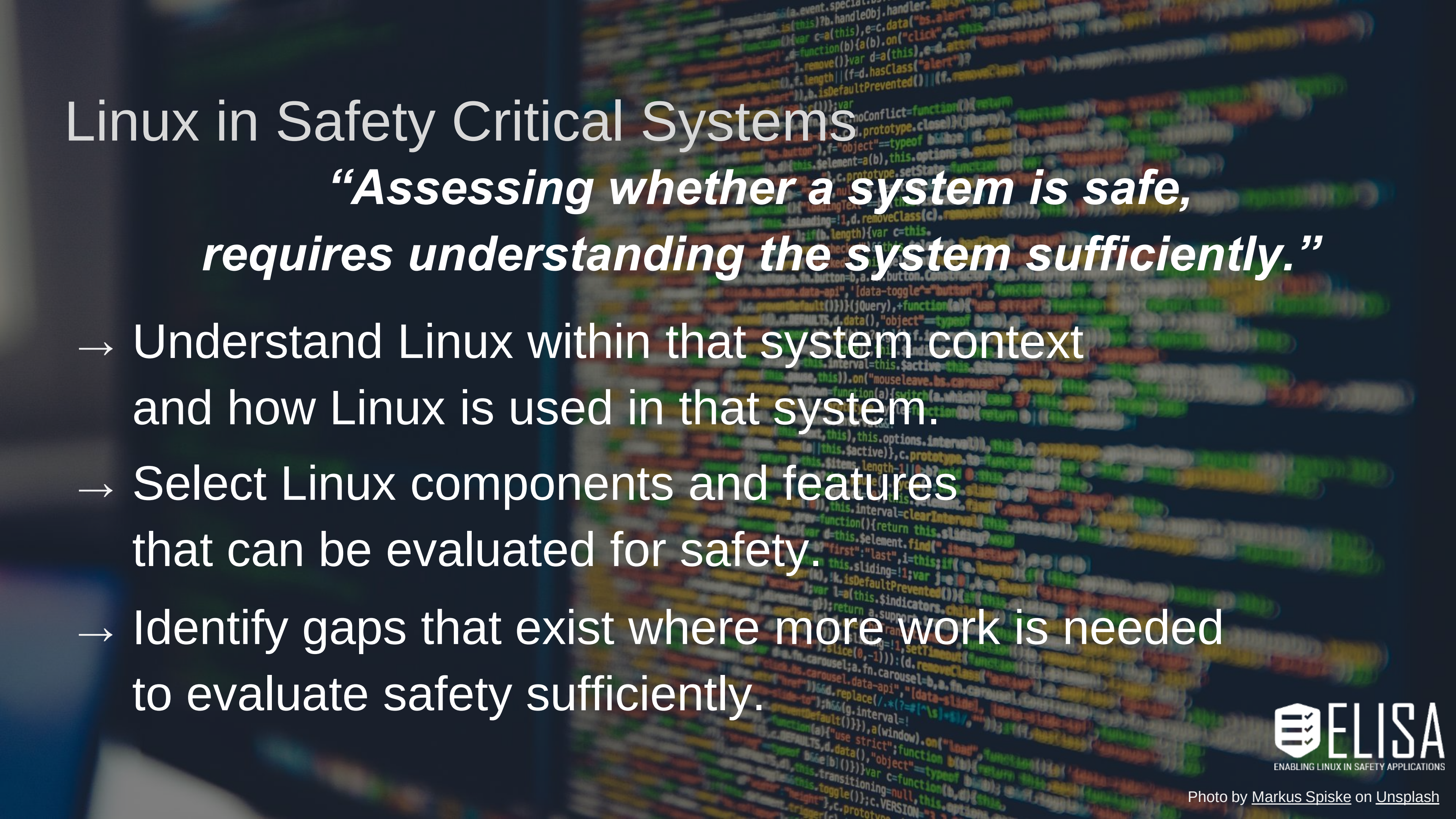
ENABLING LINUX IN SAFETY APPLICATIONS

Aerospace · Automotive · Linux Features

Medical Devices · OS Engineering Process

Safety Architecture · Systems · Tools

Linux in Safety Critical Systems



"Assessing whether a system is safe, requires understanding the system sufficiently."

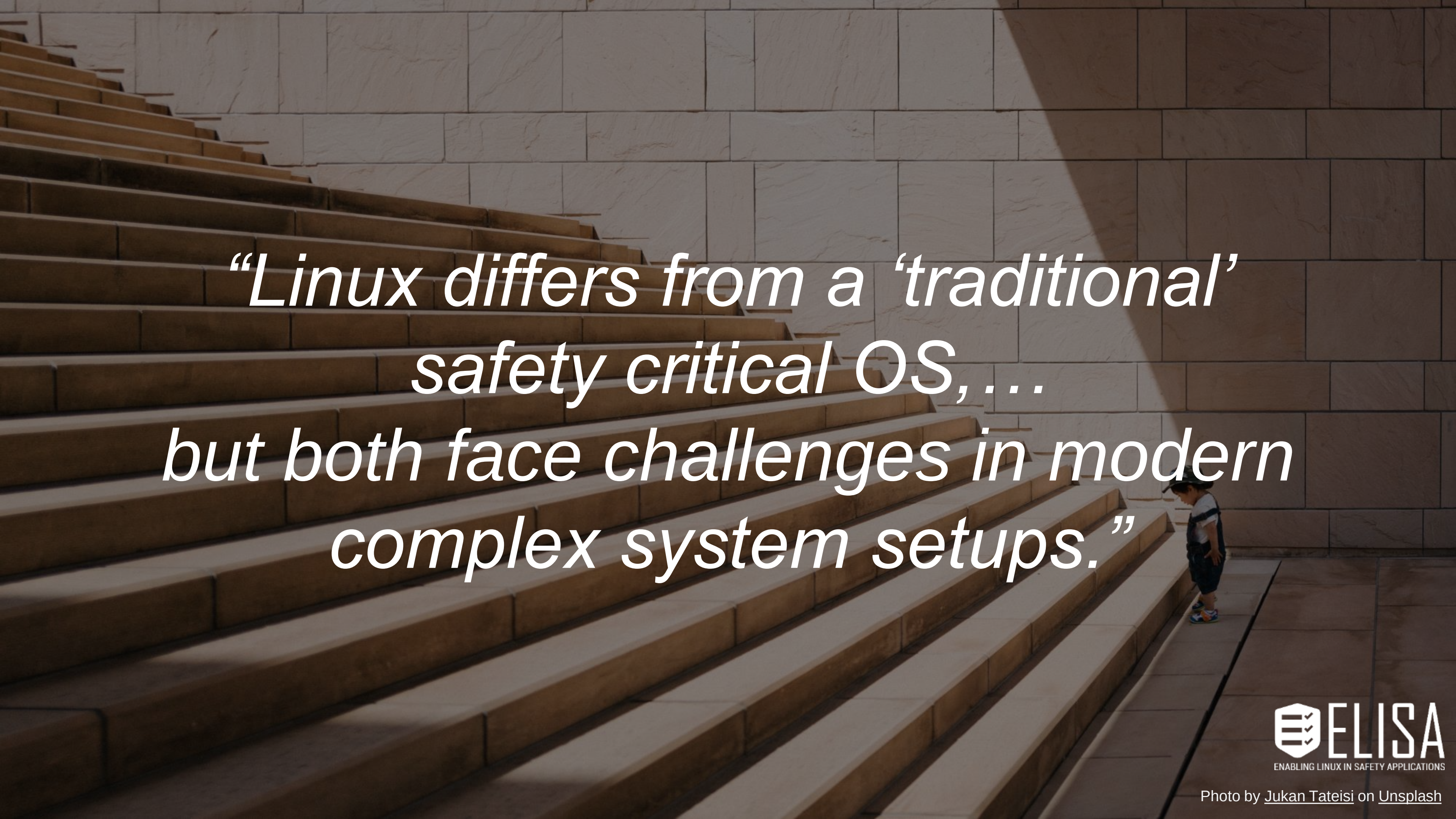
→ Understand Linux within that system context and how Linux is used in that system.

→ Select Linux components and features that can be evaluated for safety.

→ Identify gaps that exist where more work is needed to evaluate safety sufficiently.

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

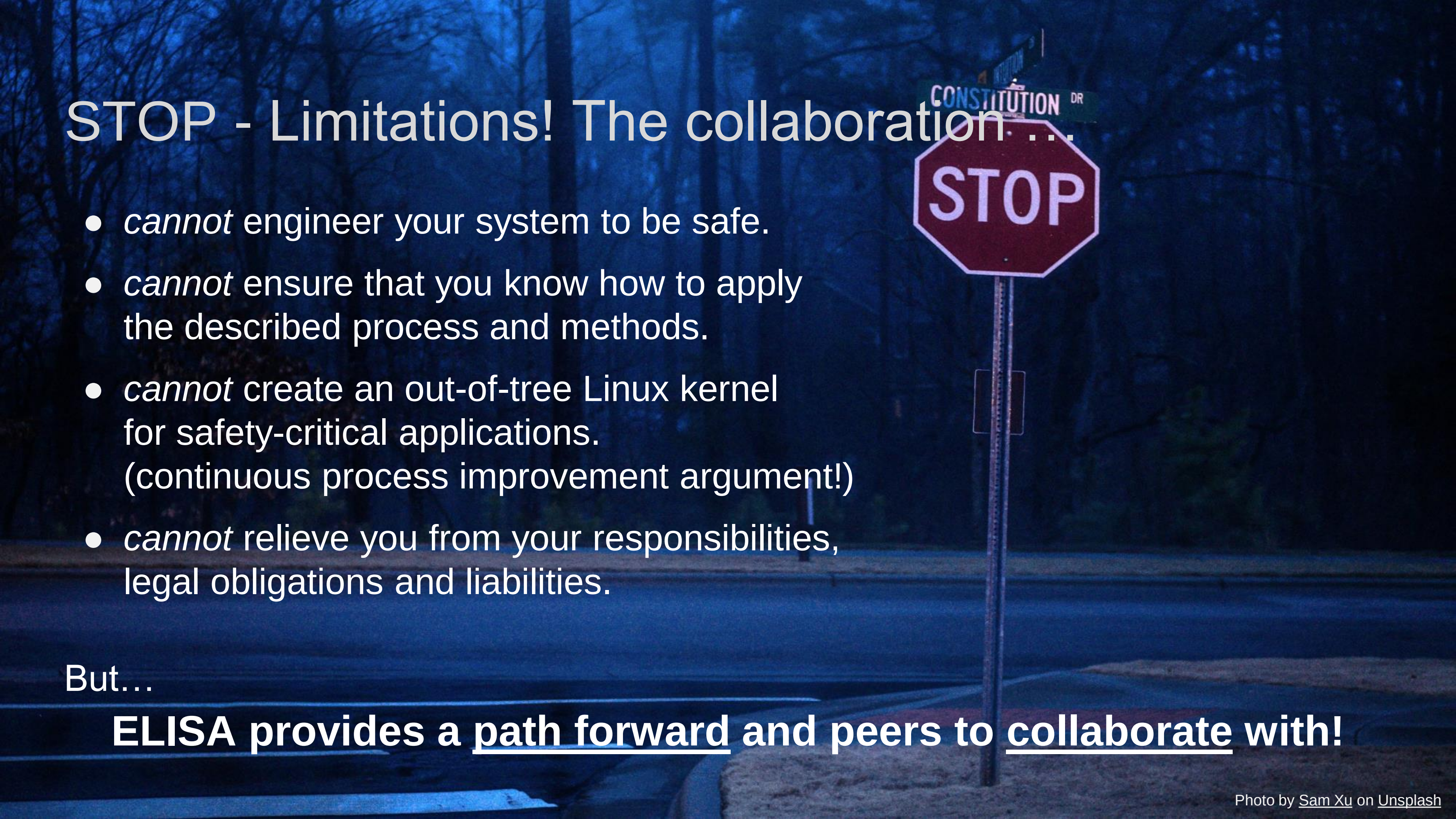
Photo by Markus Spiske on Unsplash



“Linux differs from a ‘traditional’ safety critical OS,… but both face challenges in modern complex system setups.”

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Photo by Jukan Tateisi on Unsplash



STOP - Limitations! 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.
  (continuous process improvement argument!)
- *cannot* relieve you from your responsibilities, legal obligations and liabilities.

But…

ELISA provides a path forward and peers to collaborate with!

Photo by Sam Xu on Unsplash

Premier Members

BOEING

Red Hat

General Members

AISIN

arm

斑马智行
Powered by AliOS

BOSCH

Codethink

Elektrobit

地 平 线
Horizon Robotics

HUAWEI

LINUTRONIX
LINUX FOR INDUSTRY

SAIC
上汽集团
SAIC MOTOR

SUSE

SUZUKI

WNDRVR

Associate Members

AUTOMOTIVE
GRADE LINUX

OTH
OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Industry Support

CIVIL
INFRASTRUCTURE
PLATFORM

OSADL
Open Source Automation Development Lab eG

UL

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Photo by Sam Xu on Unsplash

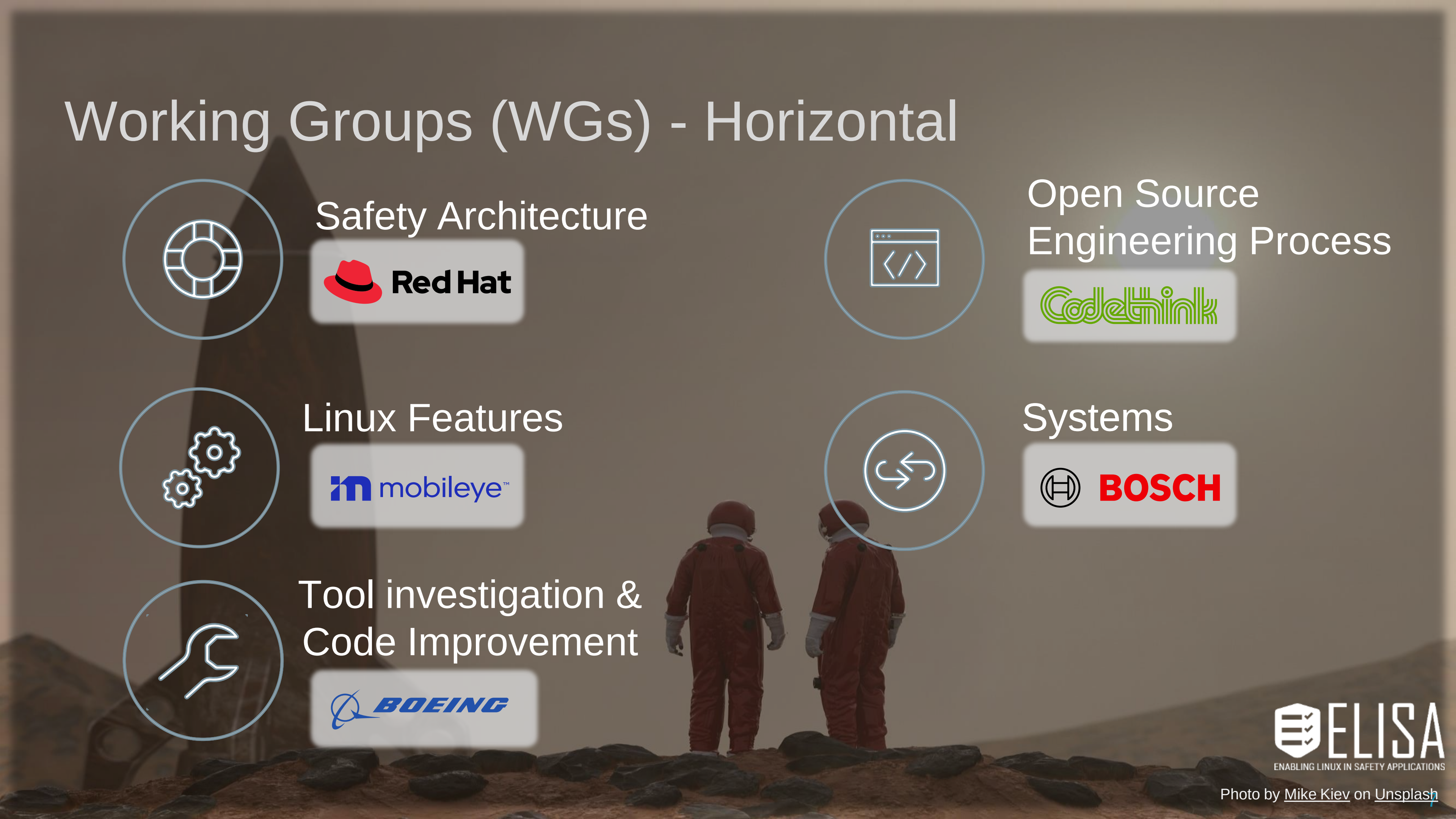
“The mission of the project is
to define and maintain a common
set of elements, processes and tools
that can be incorporated into
Linux-based, safety-critical systems
amenable to safety certification.”

from the technical charter

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Photo by Mike Kiev on Unsplash

Working Groups (WGs) - Horizontal



Safety Architecture

Red Hat

Linux Features

mobileye

Tool investigation & Code Improvement

BOEING

Open Source Engineering Process

Codethink

Systems

BOSCH

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Photo by Mike Kiev on Unsplash

Working Groups (WGs) - Vertic

Aerospace

BOEING

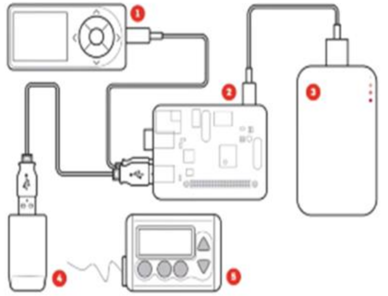
Automotive

BOSCH

Medical Devices

THE LINUX FOUNDATION

Codethink



OpenAPS elements

1. Continuous glucose monitor
2. Computer
3. Battery
4. Radio stick
5. Insulin pump

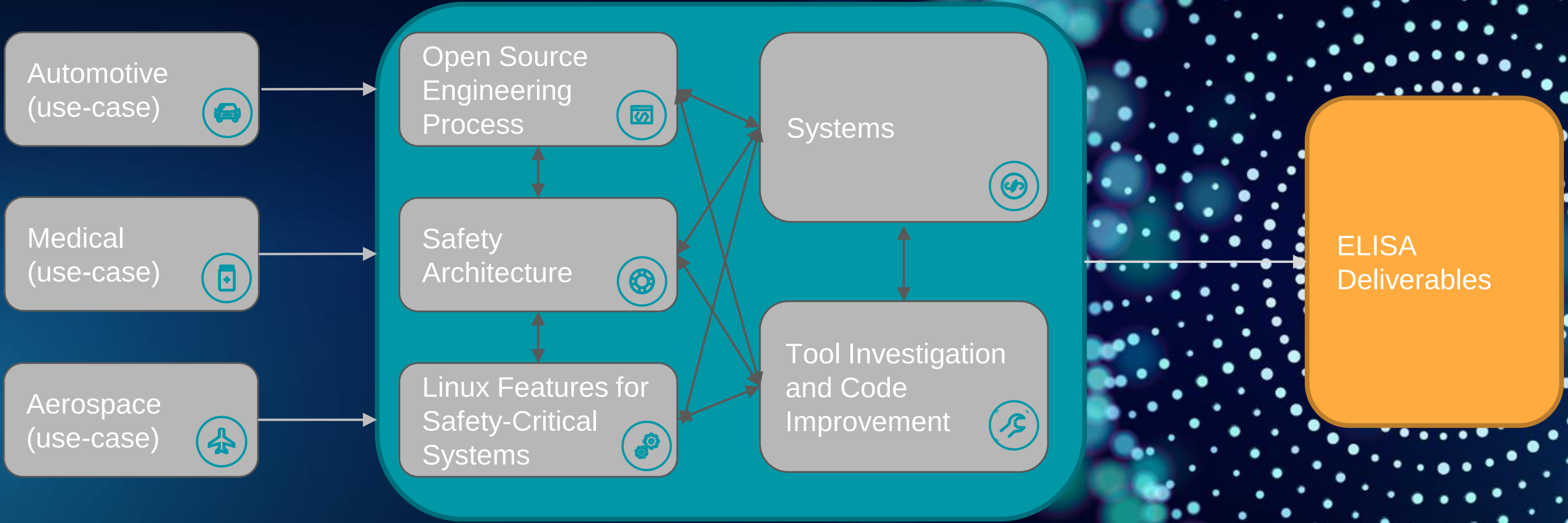
@DanaMLewis

Dana Lewis‘ OpenAPS project: https://youtu.be/kgu-AYSnyZ8

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Photo by Mike Kiev on Unsplash

Artifacts & Activities


Automotive (use-case)
Medical (use-case)
Aerospace (use-case)
Open Source Engineering Process
Safety Architecture
Linux Features for Safety-Critical Systems
Systems
Tool Investigation and Code Improvement
ELISA Deliverables

ELISA Working Groups - Deliverables

meta-elisa

- Elements / Software

Reproducible system

STPA

- Processes

Codechecker

Workload tracing

- Tools

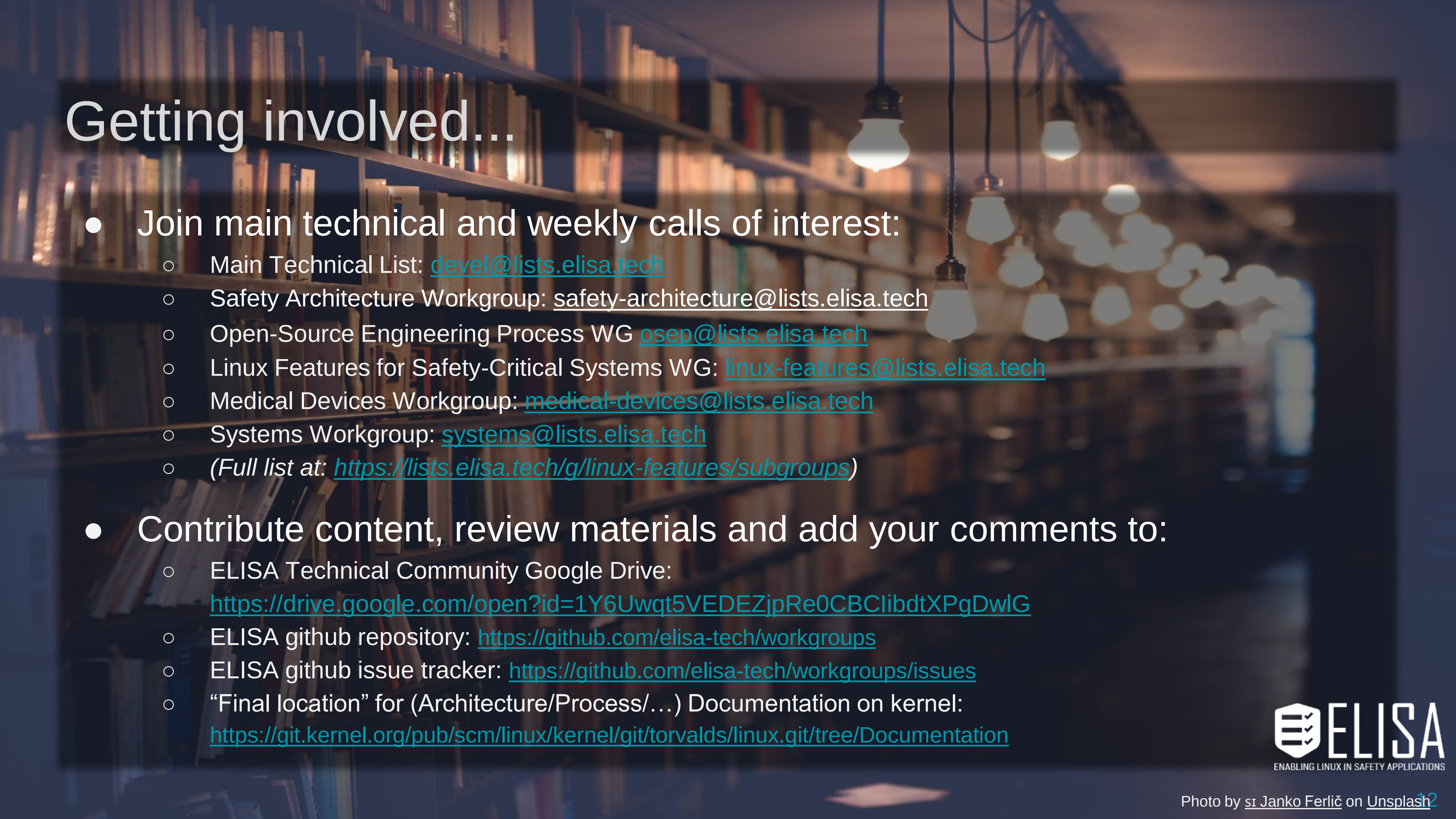
Call-Tree

RT Linux

- Documentation

GitHub / Gdrive / Blog / Whitepaper

Photo by Mitchell Luo on Unsplash



Getting involved...

- Join main technical and weekly calls of interest:
  - Main Technical List: devel@lists.elisa.tech
  - Safety Architecture Workgroup: safety-architecture@lists.elisa.tech
  - Open-Source Engineering Process WG osep@lists.elisa.tech
  - Linux Features for Safety-Critical Systems WG: linux-features@lists.elisa.tech
  - Medical Devices Workgroup: medical-devices@lists.elisa.tech
  - Systems Workgroup: systems@lists.elisa.tech
  - *(Full list at: https://lists.elisa.tech/g/linux-features/subgroups)*
- Contribute content, review materials and add your comments to:
  - ELISA Technical Community Google Drive: https://drive.google.com/open?id=1Y6Uwqt5VEDEZjpRe0CBCIibdtXPgDwlG
  - ELISA github repository: https://github.com/elisa-tech/workgroups
  - ELISA github issue tracker: https://github.com/elisa-tech/workgroups/issues
  - “Final location” for (Architecture/Process/…) Documentation on kernel: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/tree/Documentation

Photo by Janko Ferlič on Unsplash

THANK YOU!