Safety
Critical
Advisory
Panel

Standardizing Technologies for Safety Critical Systems

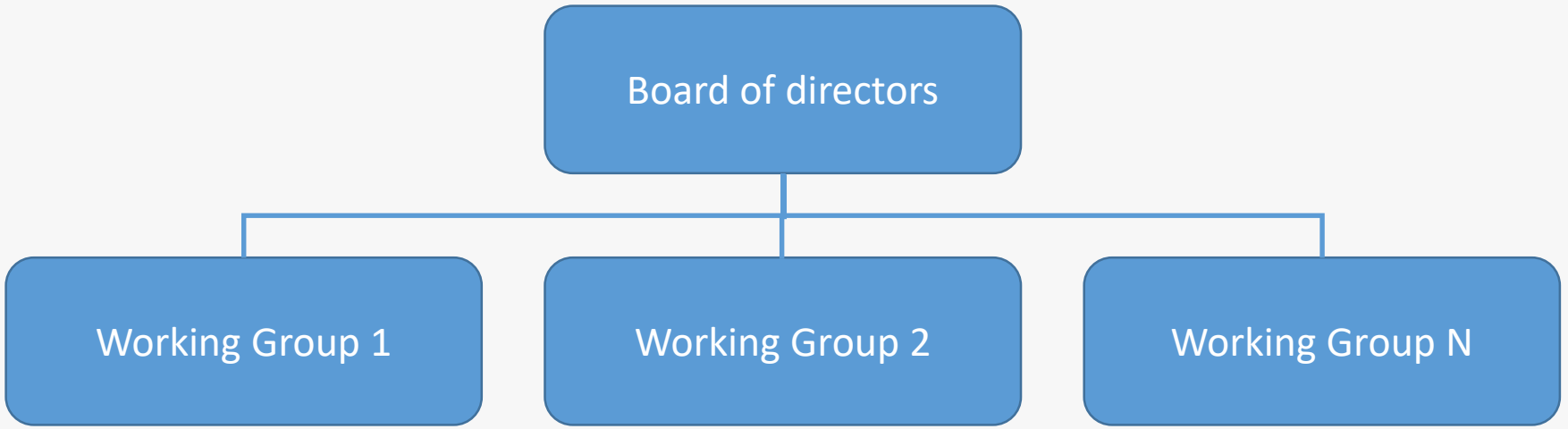
Illya Rudkin

SCAP Editor

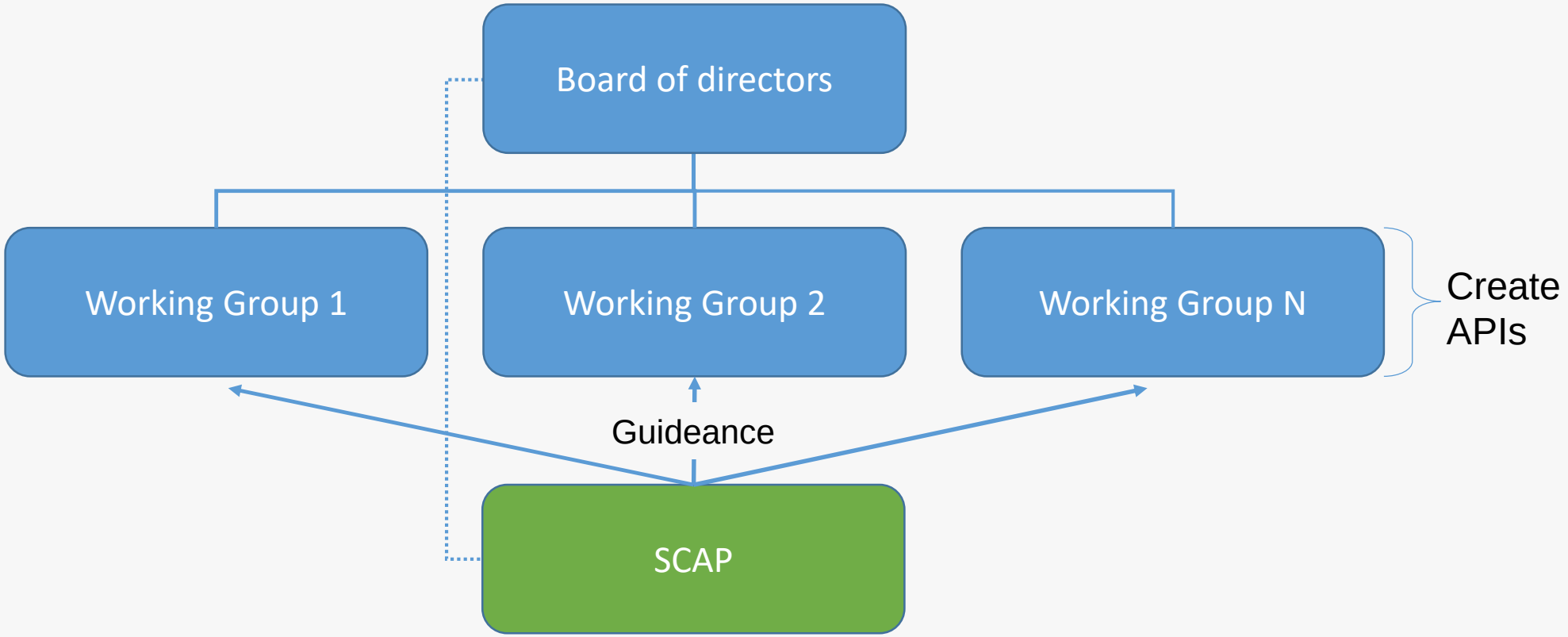
Principal Engineer Safety Critical Software

codeplay
THE HETEROGENEOUS SYSTEMS EXPERTS

- Formed in the year 2000
- Structure for key industry players
  - Approximately 120 members
- Creation of royalty free open standards
- Cross-platform technology + safety critical
- Not for profit, member-funded consortium
- Gfx, parallel compute, vision processing, and more


Board of directors
Working Group 1
Working Group 2
Working Group N

KHRONOS™ GROUP

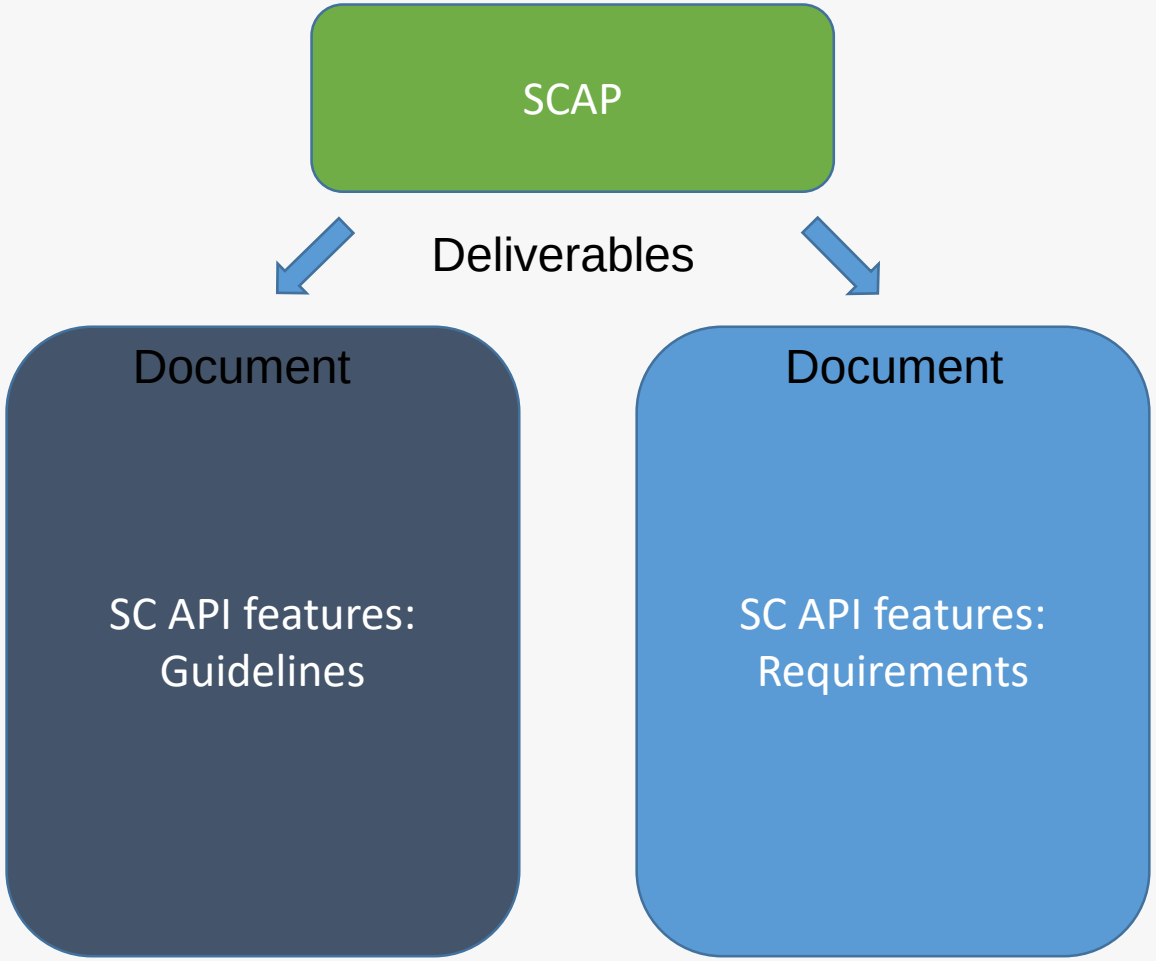


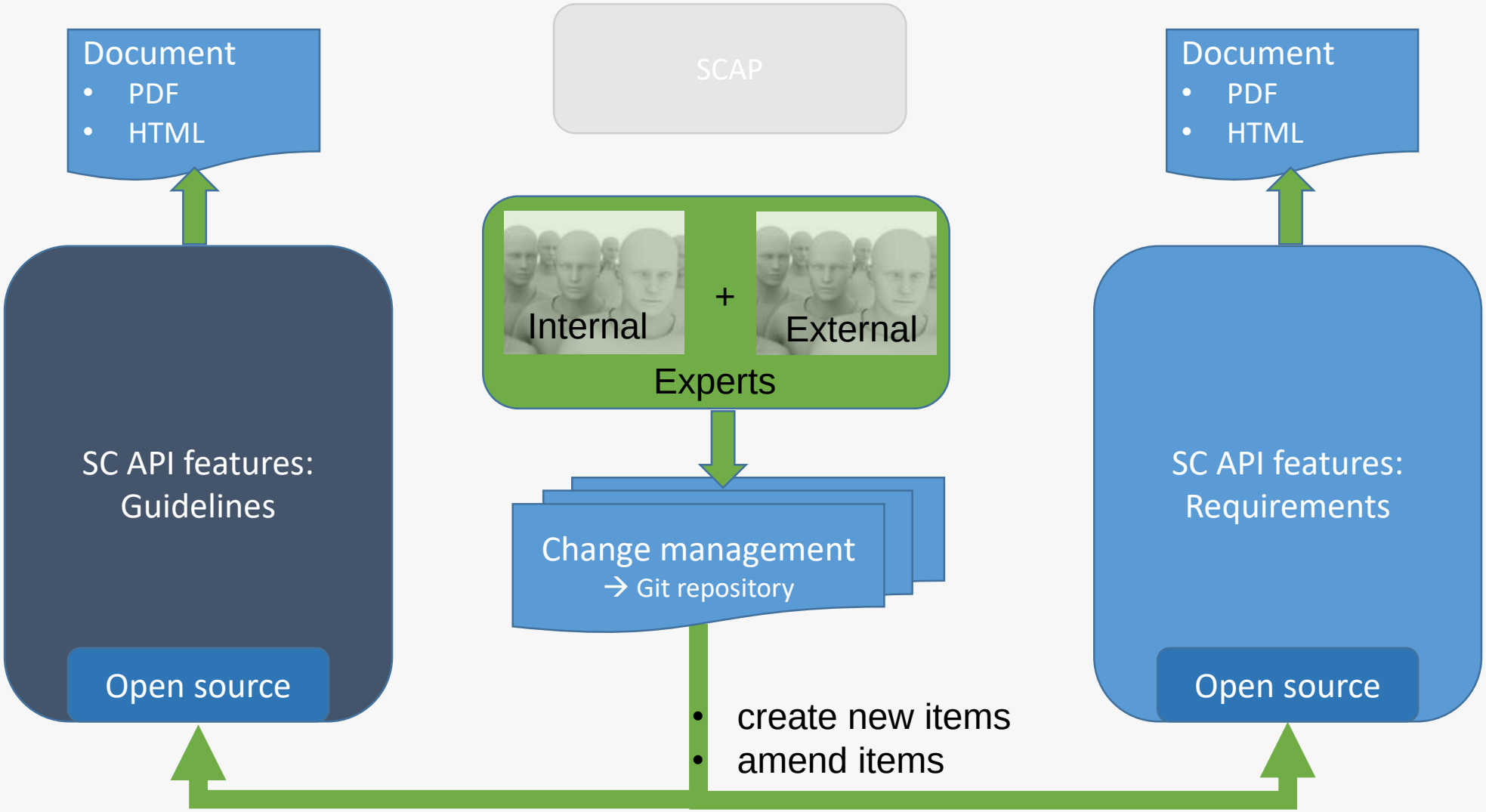
SCAP

Formed in 2016

Safety Critical Advisory Panel to create guidelines for the design of safety critical graphics, compute and vision processing APIs. The Safety Critical Advisory Panel will be open to both Khronos members and invited experts from the industry. Markets such as Advanced Driver Assistance Systems (ADAS), autonomous vehicles, robotics and avionics increasingly need advanced acceleration APIs that are designed to provide reliable operation and enable system safety certification. The guidelines will be openly published and adopted as part of Khronos' proven API design process.

Experienced practitioners in the field of safety critical system design are invited to apply for Advisory Panel membership, at no cost, with more details at the Khronos Safety Critical working group page.


SCAP
Deliverables
Document
SC API features:
Guidelines
Document
SC API features:
Requirements


Document
• PDF
• HTML
SCAP
Document
• PDF
• HTML
Internal
+
External
Experts
SC API features:
Guidelines
Change management
→ Git repository
SC API features:
Requirements
Open source
Open source
• create new items
• amend items

SCAP

Khronos experts from:
- Semiconductor
- Image processing
- Parallel data compute processing
- ….

Experts

Khronos invited experts from:
- Medical
- Automotive
- ….

Open Standard Safety Critical APIs

Encourages familiarity, innovation and SC ratified

Can lead to low entry cost, efficiency, flexibility, reduce time

SC API features: Requirements

An example

3.2.3. Asynchronous Calls

Asynchronous calls are those which are initiated by the program but may not execute or use their parameter data until a later time. Safety Critical APIs shall be clearly define when any parameter data is used, especially data which is passed via reference or pointer. When pointers are used for output parameters to Asynchronous functions the API shall clearly define when the data is copied to the output parameter. If the output data is populated after an asynchronous event the API shall define a means by which the program can check to validate the data has been written to the output. If a pointer is used for an input to the function the API shall define when the data is used and when that buffer may be reused by the application.

The API shall also define when the parameters can be changed and reused by the program. When API internal data structures are used by a program the life of the variable shall be defined; including when the internal data structure can be reused, if the data must be in the data structure prior to a specific call, and if the data is changed in a way that the application can view the change.

All asynchronous functions shall provide a means to allow the application to determine completion of the function.

Safety critical standard	**Relevant**	**Notes**
DO-178C/ED-12C		
ISO 26262		
IEC 62304		

SC API features: Guidelines

An example

3.2.1. List of SC RTOS and their unique features

This section lists some of the unique features some operating systems support and how those features can result in unintended behavior. This list is not exhaustive or complete, it is meant as a guide and place to share issues which were caused by the unique features of operating systems.

Table 3.2.1: List of RTOS

RTOS Name	Vendor	Unique Features
DeOS	DDC-I	Time Partitioning
Integrity	Green Hills Software	Time Partitioning
Integrity-178	Green Hills Software	ARINC 653 Time Partitioning
Lynx	LynxOS	
Lynx	LynxOS 178	ARINC 653 Time Partitioning
Nucleaus	Mentor Graphics	
QNX	QNX	
ThreadX	Express Logic	
VxWorks	Wind River	
VxWorks 653	Wind River	ARINC 653 Time Partitioning

SC API features:
Requirements

Some Subjects

Requirement	Description
1	Memory management
2	Deterministic behavior
3	Asynchronous Calls
4	Notification of Change of State
5	Garbage Collection Methods
6	Fully Testable
7	Undefined Behavior

SC API features:
Guidelines

Some Subjects

Guideline	Description
1	List of SC RTOS and their unique features
2	Memory management
3	Conformance testing
4	The SC API
5	Explicit timeout values
6	MISRA compliance
7	Real Time
8	Scheduling
9	Debug Functionality

SC API features: Guidelines

Workshop task

SC API features: Requirements

In groups itemize, discuss and produce the specifics of an API you have had experience with in a safety context where it conflicted with a safety concern.

Context:

- Which domain / which safety standard was being followed?
- Which API ?
- What was the hazard identified ?
- Give the level of safety required ? e.g. ISO 262626 assigned risk level of ASIL D (highest risk level)
- Did you mitigate the hazard identified ?
- How did you mitigate the issue ?

Can also consider:

- Were there specifics about the implementation behind the API which the API could not handle ?
- Was it related to a cyber-security concern ?

Leadership Products Enabling Advanced Applications on Complex Processor Systems

Company

High performance software solutions for custom heterogeneous systems

Enabling the toughest processor systems with open standards based tools and middleware

Established 2002 in Scotland, UK

Markets

Vision Processing
Machine Learning
Data Compute

High Performance Compute (HPC)
Automotive (ISO 26262)
IoT, Smartphones & Tablets
Medical & Industrial

Products

ComputeCpp™

C++ platform with SYCL enabling vision and machine learning applications e.g. TensorFlow™

ComputeAorta™

The heart of Codeplay's compute technology, enabling OpenCL™, SPIR™, HSA™ and Vulkan™

Partners

AMD
ARM
BROADCOM
Imagination
QUALCOMM
Movidius
Many Global Companies