# TH11
# Purchasers and integrators of safety components and products, which information should they ask for?

PSAM16

Thor Myklebust

SINTEF Digital

# Topics

- Introduction
- Background
  - Standards
  - Libraries
  - Integrated circuits
- Which information should they ask for
- Important aspects when having an agile and DevOps approach
- Conclusion

# Introduction

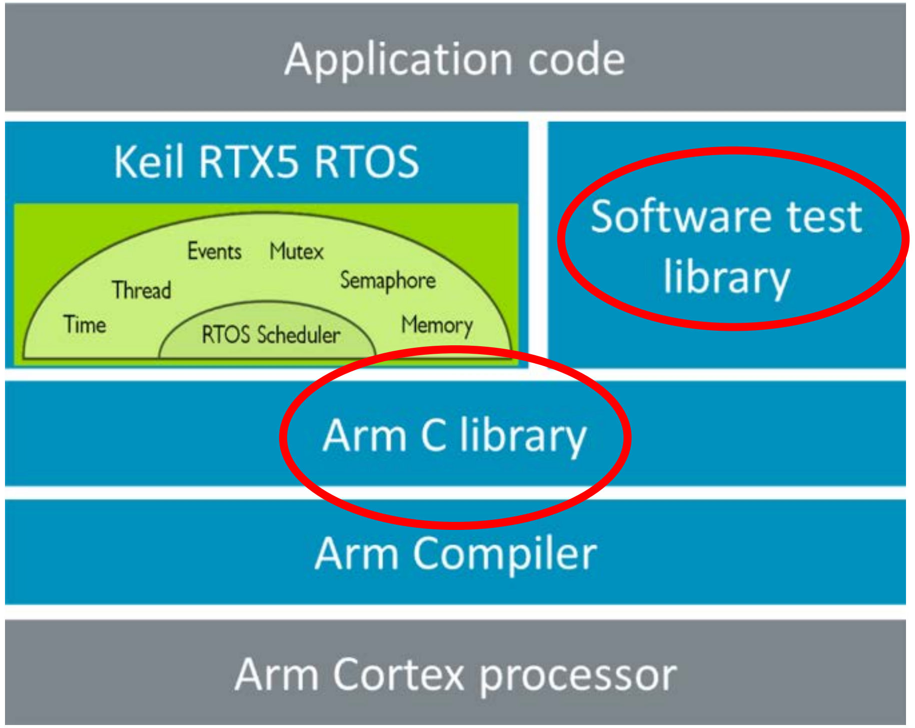
- This paper aims to aid purchasers and integrators with the purchasing process.
- Several manufacturers of safety products and safety systems have to purchase and integrate components and products produced elsewhere and sometimes for another environment or use.
- Examples of components and products that manufacturers integrate are integrated circuits, libraries, openSafety protocols, COTS (Commercial Off-The-Shelf) software and hardware, sensors, and valves.
- Having the knowledge and experience related to these documents implies less work for the manufacturer and earlier approval by certification bodies.
- Without a complete understanding of these documents, the integrators may experience project delays, design challenges, and not having the relevant information available at the right time.

# Relevant standards and documents

| Documents/Standards | IEC 61508<br>Generic safety | ISO 26262<br>Automotive | EN 5012X<br>Railway |
|---|---|---|---|
| Safety manual | Required and described in Part 2 and Part 3. | Not mentioned | Not mentioned |
| Safety case | Not mentioned.<br>Planned to be mentioned in the next edition of the standard | Required | Required |
| Safety-related application conditions (SRAC) | Not mentioned | Not mentioned | SRAC is an important part of the safety case |
| Hazard log (HL) | Not mentioned | Not mentioned | HL is an important part of the safety case |
| Safety assessment report | Not mentioned | Required | Required |
| User manual | Required but not used the term "user manual" | Required but not used the term "user manual" | Required but not used the term "user manual" |

# Libraries

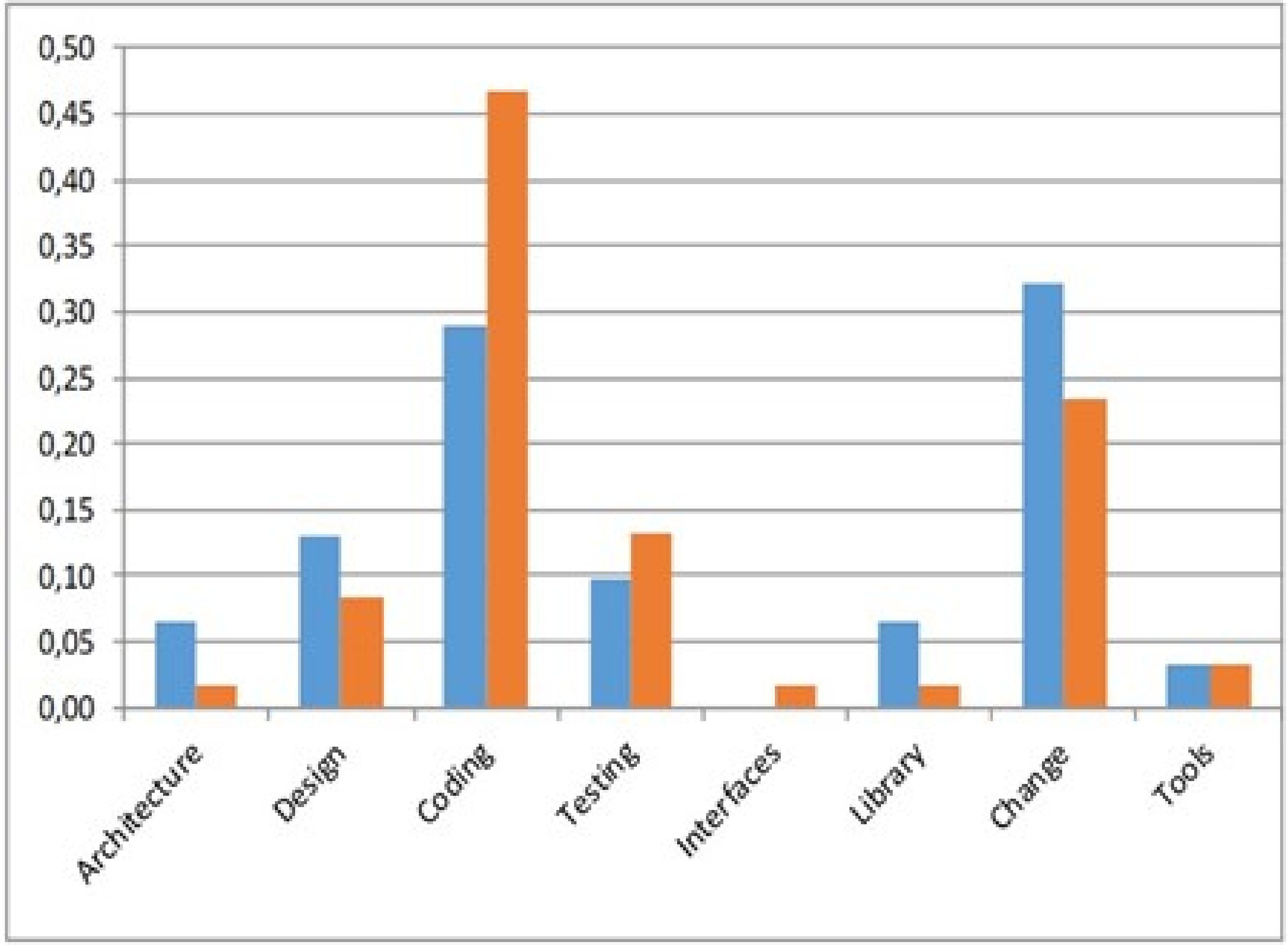
- A software library is a suite of data and programming code that is used to develop software programs and applications.
- It is designed to assist both the programmer and the programming language compiler in building and executing software.



Source: https://community.arm.com/arm-community-blogs/b/embedded-blog/posts/more-safety-and-engineering-efficiency-arms-new-runtime-software-system-to-accelerate-development-of-safety-applications-on-cortex-m-devices

# Libraries

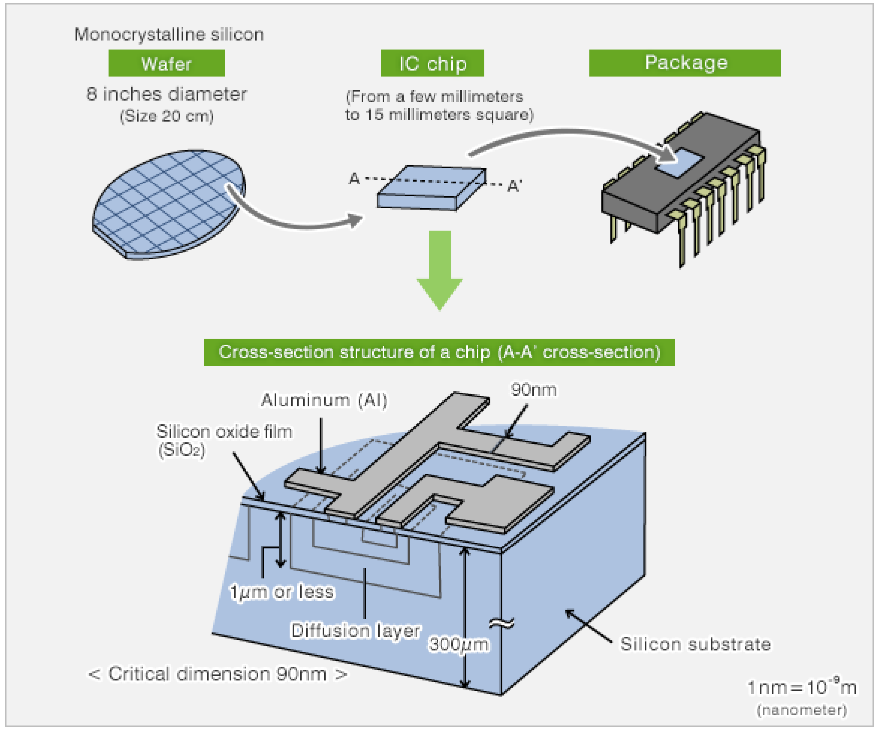
- Knowledge based problem areas identified by software developers
- blue: safety and security
- orange: other



# Integrated circuits

- Safety is an important requirement of the increased use of semiconductors, and ensuring safe vehicles is a massive undertaking.
- Semiconductors are included in safety parts such as automatic driving assistant systems, e.g., automatic lane-keeping system.

A rose by any other name would smell as sweet



# Safety manual

- The safety manual is defined as: "safety manual for compliant items: document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to ensure that the system meets the requirements of IEC 61508 series

Parts of the content list for hardware:

- A functional specification
- Identification of HW and SW
- Constraints
- Failure modes
- Failure rate
- Failure modes detected by diagnostics
- Failure modes of the diagnostics
- etc

# Safety Case

**Idea**

The idea of a safety case is to argue as one would in a court of law –

thus the name safety case.

**Names**

- Safety case
- Assurance case

A safety case are structured based on

- Claim
- Argument: “*How do you know*” - a request for evidence
- Evidence

**Evidence without argument is unexplained**

# Safety assessment Report

- This is the assessment of the safety case or e.g., the certificate report

- The SAR should be checked for
  - assumptions,
  - constraints,
  - intended use and limitations.
  - In some cases, also the independence and competency of the assessor(s) should be evaluated, e.g., when they are not accredited.

# Certificate

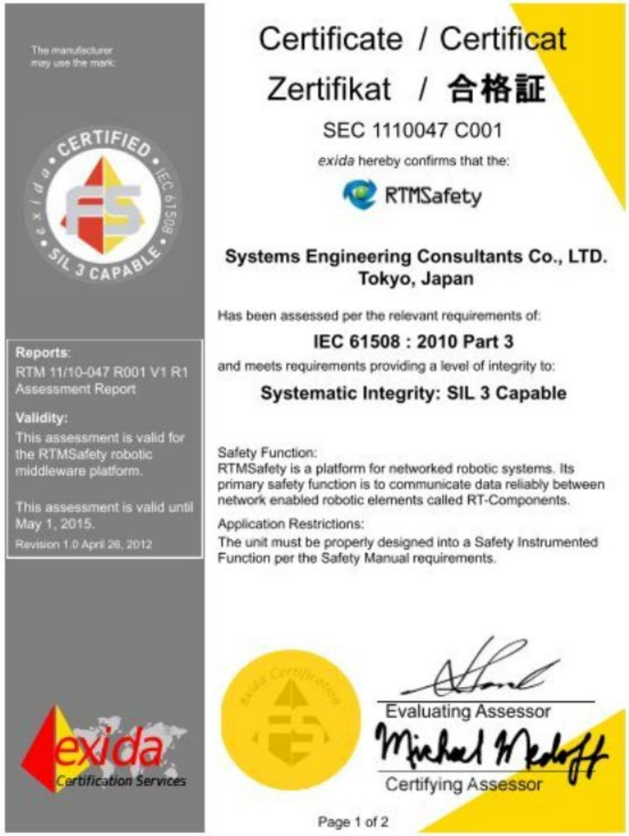
- The certificate report presents the information from the certification that has been performed.
- The certificate normally consists of only one page and states compliance with one or more standards.

ANAB
ANSI National Accreditation Board

NORWEGIAN ACCREDITATION

cofrac

CNAS



The manufacturer may use the mark:

exida • CERTIFIED • IEC 61508 • SIL 3 CAPABLE

**Reports:**
RTM 11/10-047 R001 V1 R1 Assessment Report

**Validity:**
This assessment is valid for the RTMSafety robotic middleware platform.

This assessment is valid until May 1, 2015.

Revision 1.0 April 26, 2012

Certificate / Certificat
Zertifikat / 合格証

SEC 1110047 C001

*exida* hereby confirms that the:

RTMSafety

**Systems Engineering Consultants Co., LTD.**
**Tokyo, Japan**

Has been assessed per the relevant requirements of:

**IEC 61508 : 2010 Part 3**

and meets requirements providing a level of integrity to:

**Systematic Integrity: SIL 3 Capable**

Safety Function:
RTMSafety is a platform for networked robotic systems. Its primary safety function is to communicate data reliably between network enabled robotic elements called RT-Components.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Michael Medoff
Certifying Assessor

exida Certification Services

Page 1 of 2

# Certificate report

A review of 15 certification reports issued by five certification bodies shows a more or less common set of chapters for certificate reports:

- Introduction including scope, assignment, and work method
- Definition of product or system
- References including relevant standards
- Summary of activities performed
- Conclusions

# User manual

- User manuals are important, even though many of them are seldom used. A sign on the wall of a room for a company's developers says it all: "In case of outmost despair – read the manual"
- In modern products and vehicles, it is become common to only deliver the user manual electronically
- The most important issue when reading a system's use manual is to look for clues that the development company has discovered problem late in the process and instead of fixing them in the code they have "fixed" them in the manual.
- Watch out for sentences such as "Do not use function X after having used function Z if the status variable A is less than 6".

# Important aspects when having an agile and DevOps approach

- When using an agile and DevOps approach, living documents (information) are important. Living documents are also named dynamic documents.

- For safety documents it is important to have in mind complete understanding, monitoring, revision and review requirements.

# Important aspects when having an agile and DevOps approach

- There have to be a proactive reaction to unknown risks that will inevitably manifest during operation of autonomous vehicles. And there may be security issues.

- In addition, there will be planned improvements to move quickly to higher levels of autonomy.

# Summary

Based on the discussions above, we can make the following important conclusions:

1. We have developed a template (chapter 3) for an agile safety case for trial operations

2. Working with safety cases will increase the stakeholder's safety awareness.

3. A safety cases can be developed incrementally. The trial Safety Case shall be continually updated to provide a record of the progress of the project

Relevant agile approaches are:

- MVP (Minimum Viable Product)
- incremental development
- agile contracts
- agile software development process
- customer collaboration and
- DevOps.