Certified tools for Functional Safety

IAR SYSTEMS

Hyun-Do Lee

Agenda

- The need for certified tools
- Functional safety projects
- Simplified validation
- Support and updates
- Validated product versions
- Summary

The need for certified tools

- Increased number of embedded systems with functional safety requirements
- Standards require support tools to be qualified
- The amount of work for qualification of tools can be high, if the tools are not pre-qualified

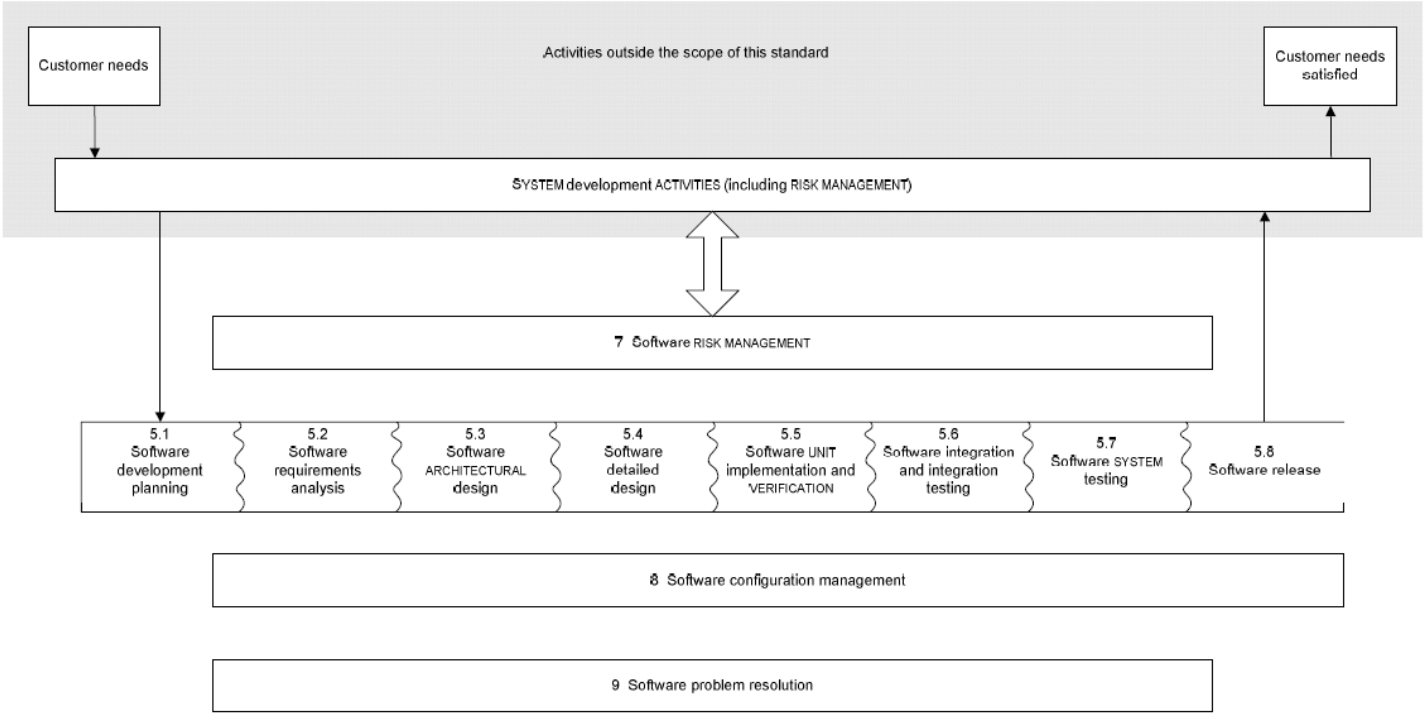
IEC 61508
- The international umbrella standard for functional safety
- Used within all kinds of industries with requirements on reliability and safety
    - Process industries, the oil and gas industry, nuclear power plants, machinery, railway control systems, etc.

ISO 26262
- Used for automotive safety-related systems

EN 50128
- Used for railway applications

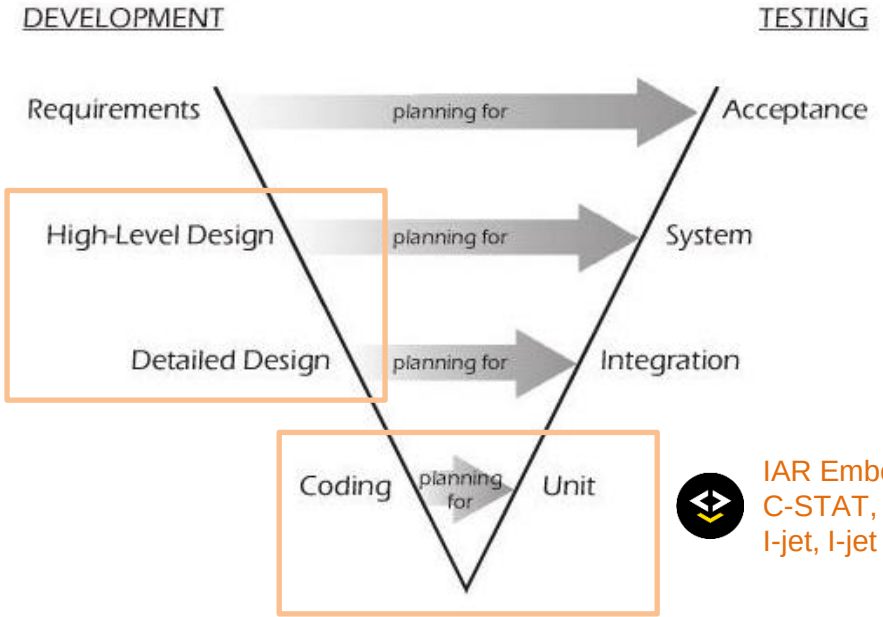
IEC 62304
- medical device software – software life cycle processes

The need for certified tools - SW Validation

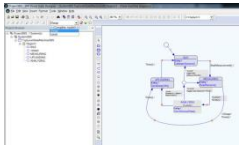


Over view of software development processes and activities, *IEC 62304*

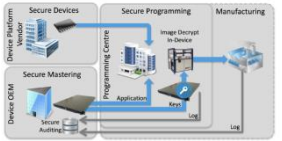
The need for certified tools - V Model



IAR Visual State



Embedded Trust
- Security



IAR Embedded Workbench
C-STAT, C-RUN
I-jet, I-jet Trace

Systematic Software testing - Rick D. Craig and Stefan P. Jaskiel

Solutions for safety-critical applications

Certified toolchain

- A special functional safety edition of IAR Embedded Workbench

Simplified validation

- Functional Safety certificate from TÜV SÜD
- Safety report from TÜV SÜD
- Safety guide

Guaranteed support through the product life cycle

- Prioritized support
- Validated service packs
- Regular reports of known problems

Available for:	Validated according to:
ARM	IEC 61508
Renesas RX	ISO 26262
Renesas RL78	EN 50128 (ARM and RH850)
Renesas RH850	IEC 62304

Certifications

IAR Embedded Workbench for ARM V8.22.3

IAR Embedded Workbench for RX V3.10.5

IAR Embedded Workbench for RL78 V3.10.2

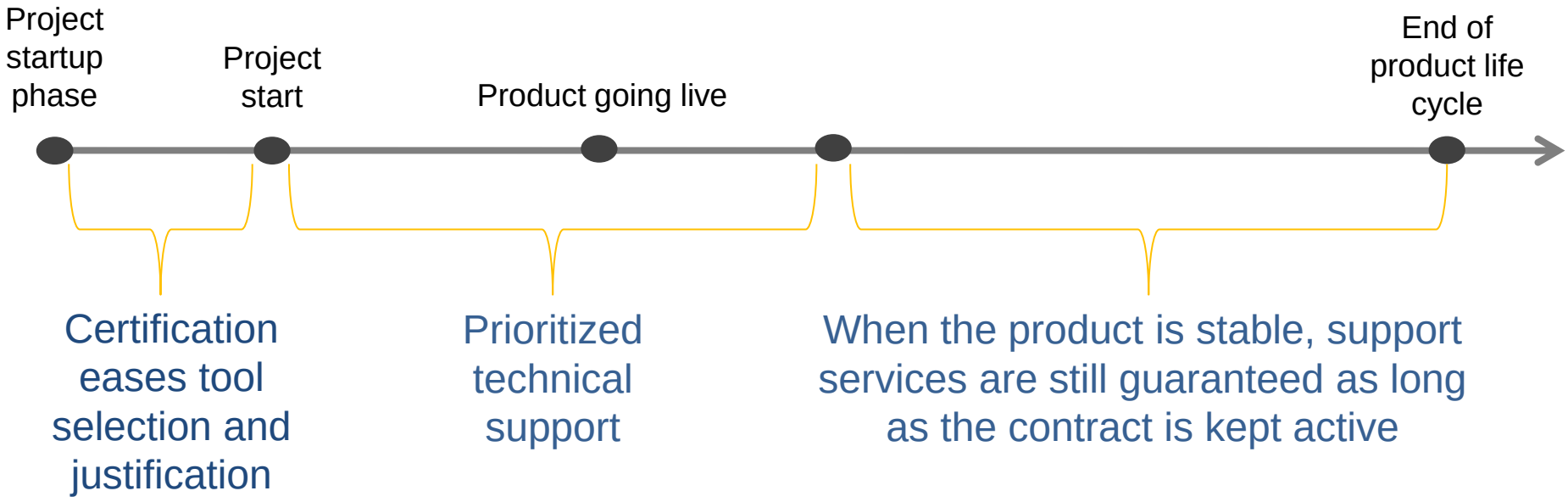
IAR Embedded Workbench for RH850 V1.40.3

Certified for safety-related software development for each Safety Integrity Level (SIL) according to IEC 61508 and each Automotive Safety Integrity Level (ASIL) of ISO 26262 without further tool qualification

The tools for ARM and RH850 are also certified for EN 50128, a European railway standard derived from IEC 61508 and IEC 62304 for Medical device.

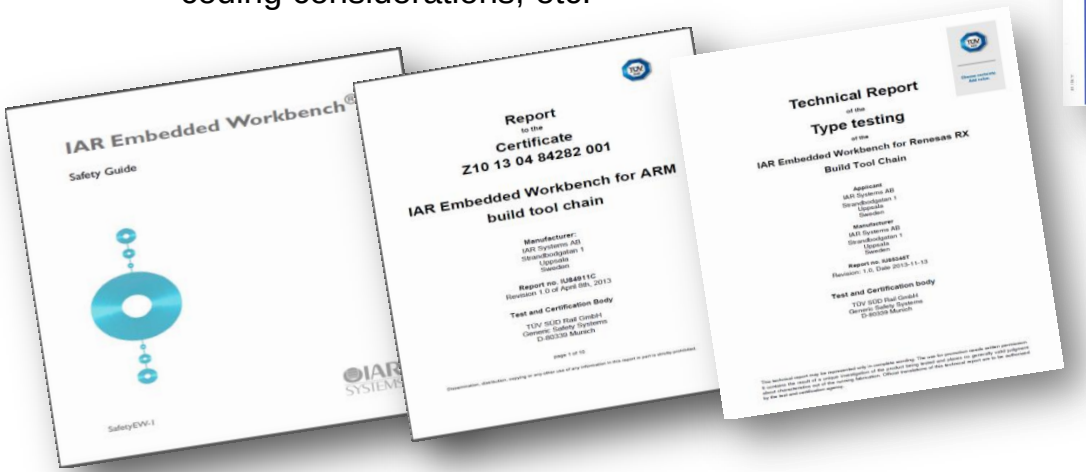
The certification validates the quality of IAR Systems' entire development processes, as well as the delivered software.

Functional Safety projects



Simplified validation

- Functional safety certificate from TÜV SÜD
- Safety report from TÜV SÜD
- Safety Guide
  - Complement to the IAR Embedded Workbench user guides
  - Highlights issues to be considered when using the build toolchain for projects with functional-safety requirements
  - Includes system considerations, implementation and coding considerations, etc.



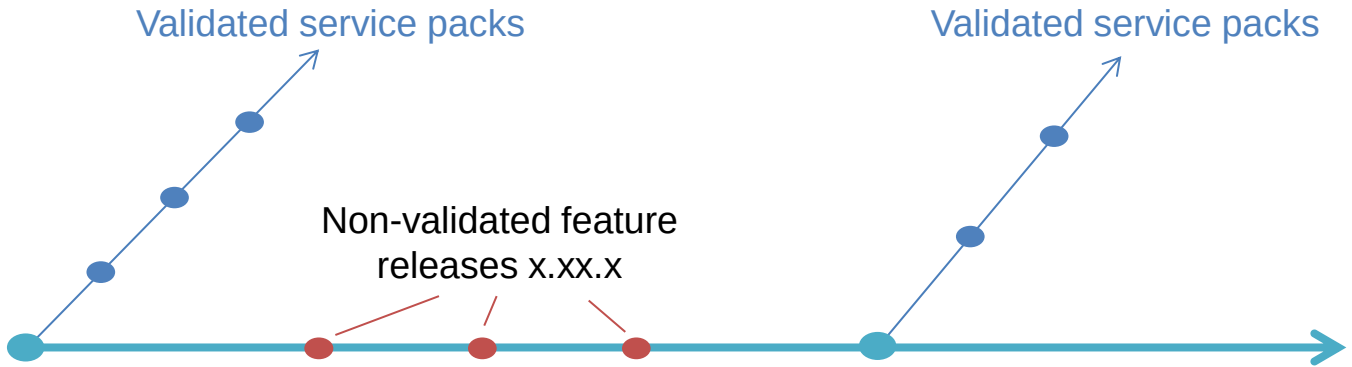
Support and updates

Functional Safety Support and Update Agreement (SUA)

- Guaranteed support for the sold version for the longevity of the contract
- Prioritized technical support
- Validated service packs
- Regular reports of known deviations and problems
- Included for the first year

Extensive technical support
when and where you need it provided by support offices worldwide

Validated product versions



- For a certified product, a new certified version is released approximately every 12-18 months
- A certified version is considered a ”frozen” version, on which bug fixes are applied in terms of validated service packs
- No new product features are added to a certified version or the corresponding service packs

Summary

Summary

- Complete development toolchain for ARM, RX, RL78 and RH850
- Certified according to IEC 61508, ISO 26262 and IEC 62304, and for ARM and RH850 also EN 50128
- Comprensive documentation including certificate, safety guide and report from TÜV SÜD
- Extensive support agreement

www.iar.com/safety

Thank you for your attention!