# Institutionalize a certified ISO26262 safety process

M.Rohleder, C.Röttgermann, M.Müller

NXP Semiconductors, Germany



accellera SYSTEMS INITIATIVE

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

# Agenda

- A first milestone: MPC5643L
- Device versus Process Certification (institutionalize)
- Safety Management
- CM and CC process and definitions
- Confidence in use of software tools
- Hazard Analysis and Risk Assessment
- Safety Requirements
- Verification
- Conclusion and Outlook

# A first milestone: MPC5643L

The manufacturer may use the mark:

CERTIFIED exida ISO 26262 ASIL D

**Reports:**
Freescale 11/08-067-C R009 V1 R0
Results of the ISO 26262 Functional Safety Assessment

**Validity:**
This assessment is valid for Microcontroller MPC5643L

This assessment is valid until August 31, 2015.

V1 R1 September, 2012

exida CERTIFICATION

Certificate / Certificat
Zertifikat / 合格証

FREESCALE 1108067 P0026 C001

*exida* Certification S.A. hereby confirms that the:

**MICROCONTROLLER MPC5643L**

**FREESCALE Halbleiter Deutschland GmbH**
**Munich, Germany**

Has been assessed per the relevant requirements regarding µC development and verification & validation of:

**ISO 26262 : 2011 Parts 2, 4, 5, 7, 8, 9 and 10 (to the extent applicable)**

and meets requirements providing:

**Systematic Integrity: ASIL D**

**Safety related function:**
The µC supports the execution of safety-related software by a dual-core lock-step architecture with memory protection and centralized fault collection and control unit.

**Application restrictions:**
The microcontroller shall be used per the Safety Application Guide requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

Worlds first microcontroller to achieve formal ISO26262 certification

- Performed by Exida, an independent accredited certification body
- Certificate issued a few months after release of the ISO26262 standard
- Valid for all ASILs, up to ASIL D

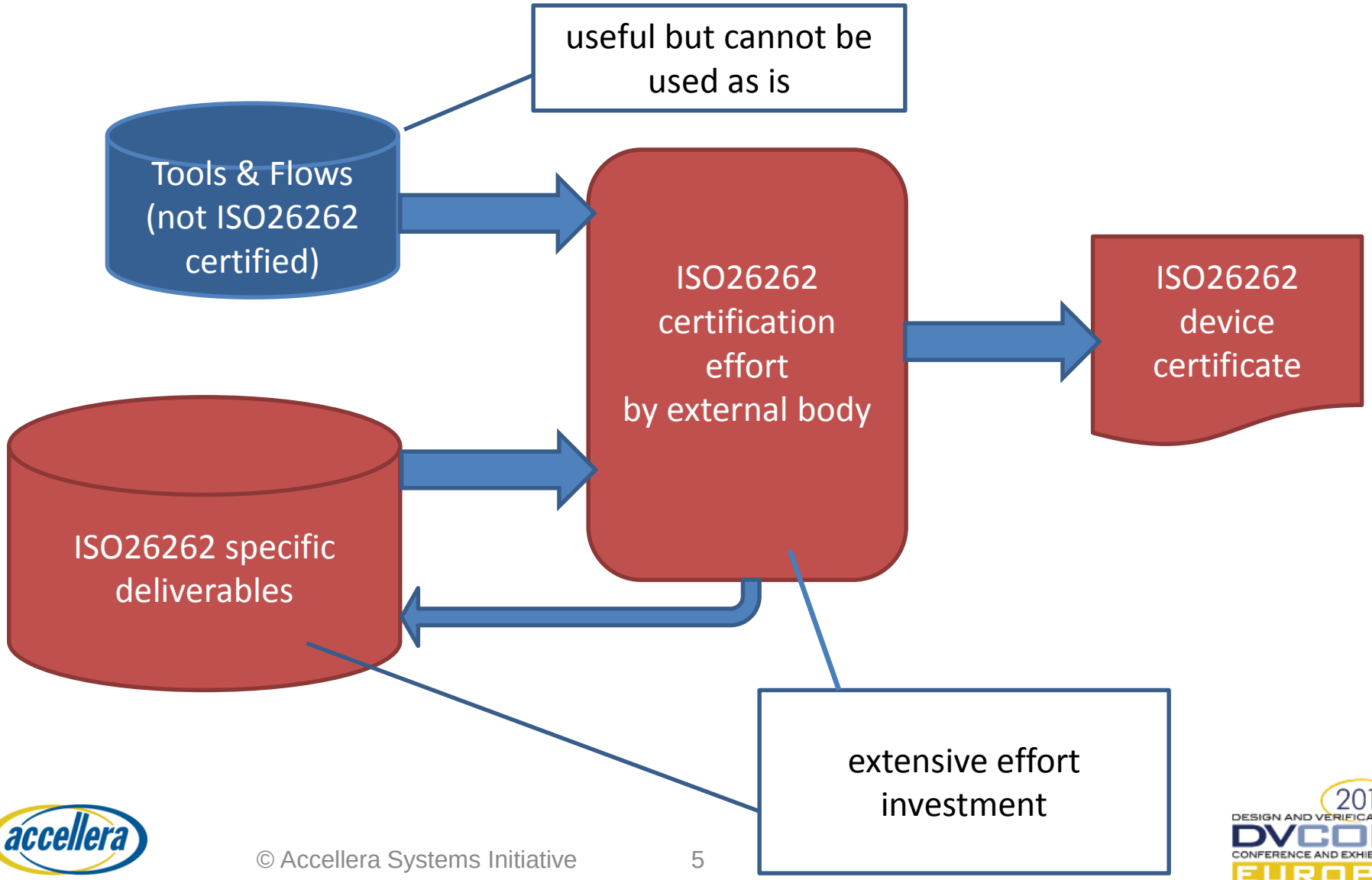
More Details:
http://www.nxp.com/safeassure

# Institutionalization

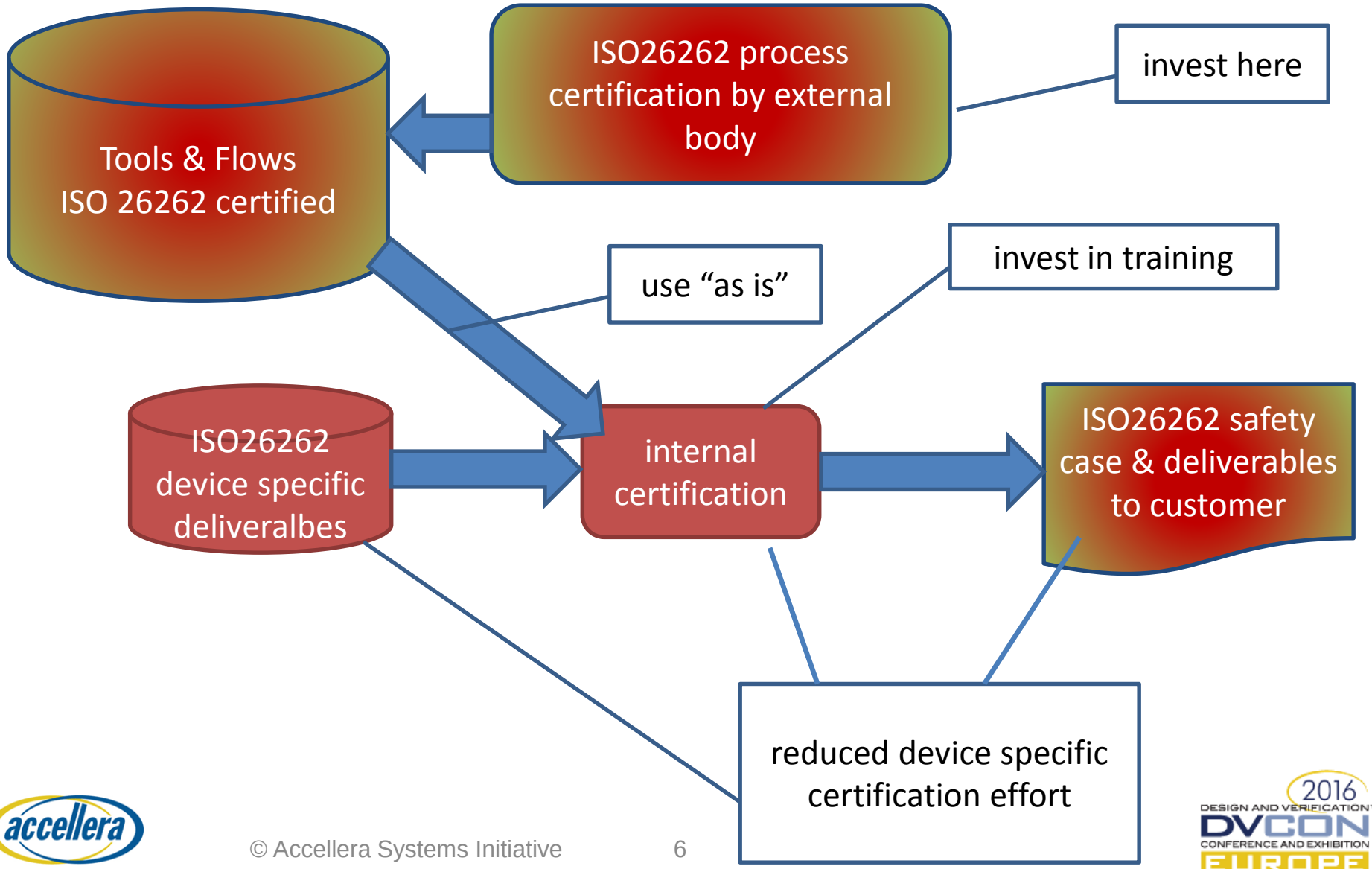
Do we need to certify *every* device ?

Can we afford this ?

# Device certification



# Safety Process Certification



# Key aspects for moving from device to process certification

- Safety Management
- CM and CC process and definitions
- Confidence in use of SW tools
- Hazard Analysis and Risk Assessment
- Safety Requirements

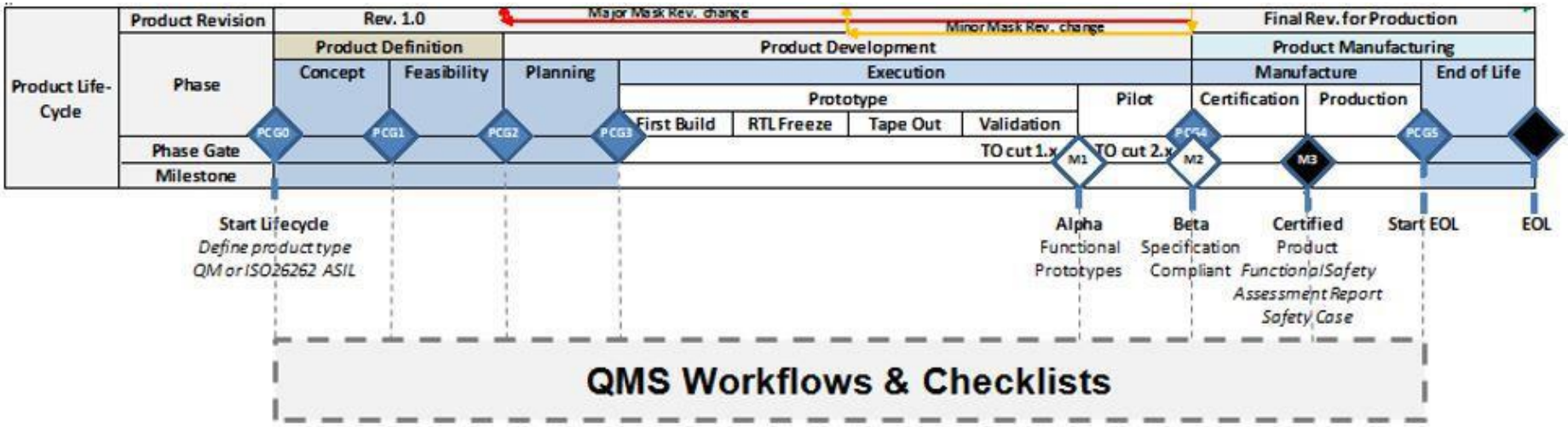
**!!!Put in place tools!!!**

# Safety Management

- Safety Plan
  - template specifying the complete set of safety activities
  - defines the mapping of safety related activities and information to the standard development flow
- Safety Case
  - specifies all work products and corresponding information
- Development Interface Agreement (DIA)
  - required for distributed development of SoCs/IP blocks

# Safety Management

- Introducing safety related activities into the *standard development process* for SoCs and IP blocks
  - specifies phases, quality gates and associated checklists
  - ISO26262: confirmation reviews (w/ independence level)
  - supported by an internal tool (QMS)

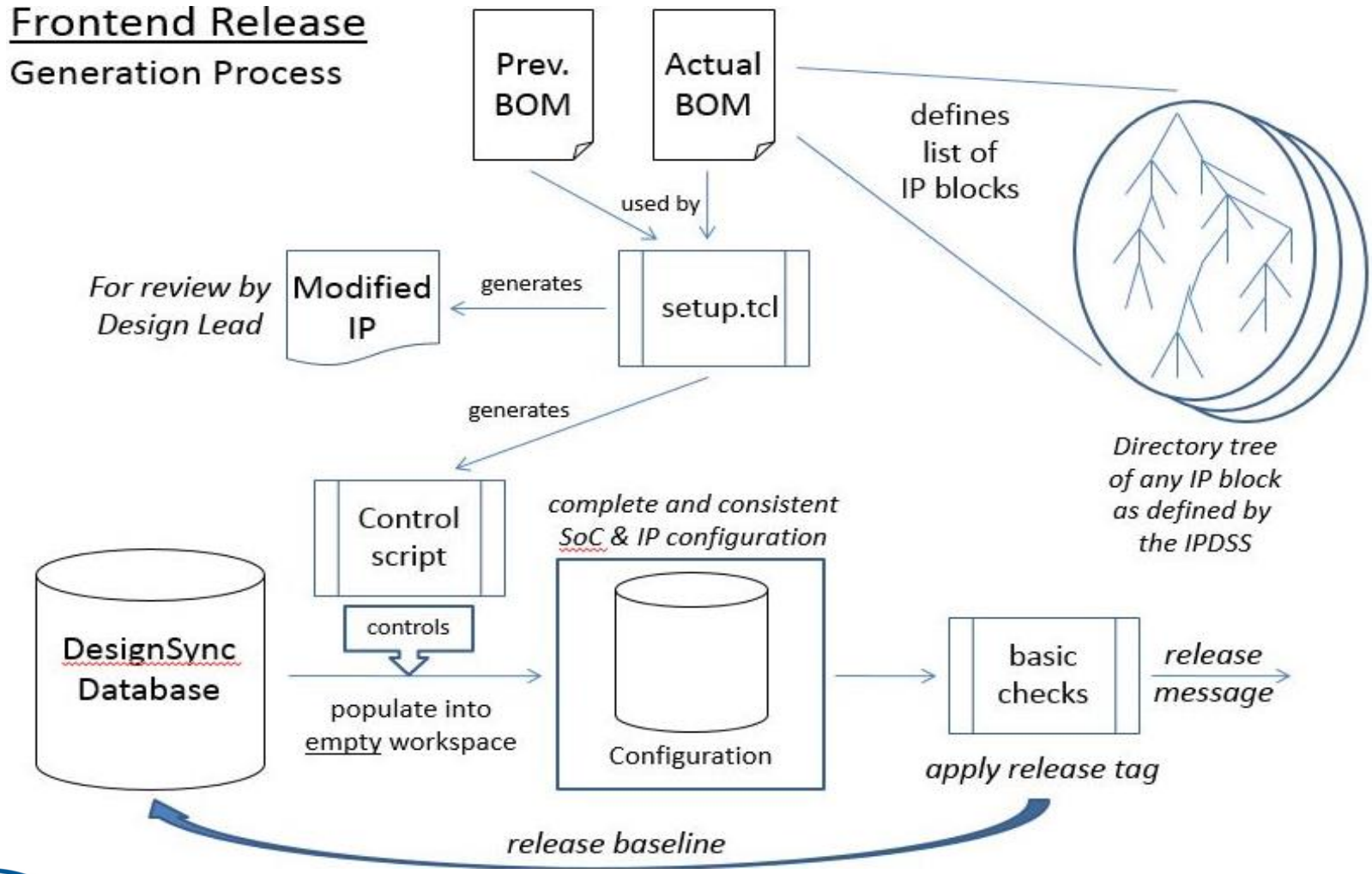


# CM & CC process and definitions

- Configuration Management (CM)
  - identification of CM items: IP, SoC databases, tools, documents
  - release procedure(s): lifecycle (LC) based, quality goals, reproducible
  - configuration item verification, data retention and archival
- Change Control (CC)
  - access control, analysis of change requests and their impact
  - change control process and procedures
  - notification of changes, defect tracking

**Scope**: *every work product* - defines roles & responsibilities, how to achieve compliance

# CM & CC Example



# Confidence in Use of Software Tools

ISO26262 requires for every tool used to determine the level of *confidence in use of a software tool*

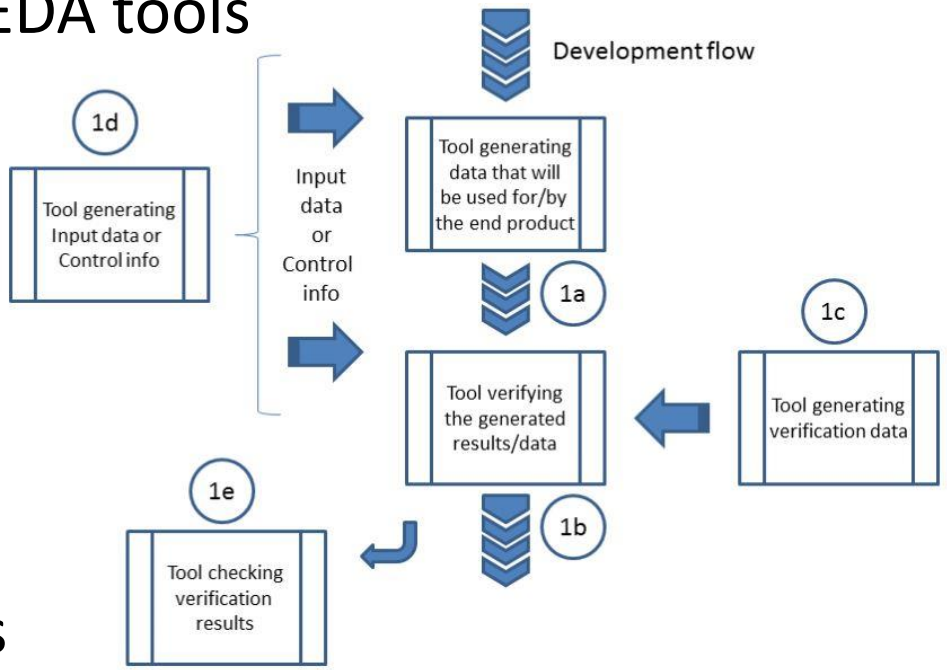
- Need to rely on the correct function of a software tool
- Minimize the risk for systematic faults in the developed product due to malfunctions of a software tool (generation/verification)
  - **T**ool **I**mpact (TI1/TI2):
    Possibility that a malfunction can introduce or fail to detect errors
  - **T**ool error **D**etection (TD1-3):
    Confidence in detecting
    or preventing such errors

➔ **T**ool **C**onfidence **L**evel (TCL1-3)

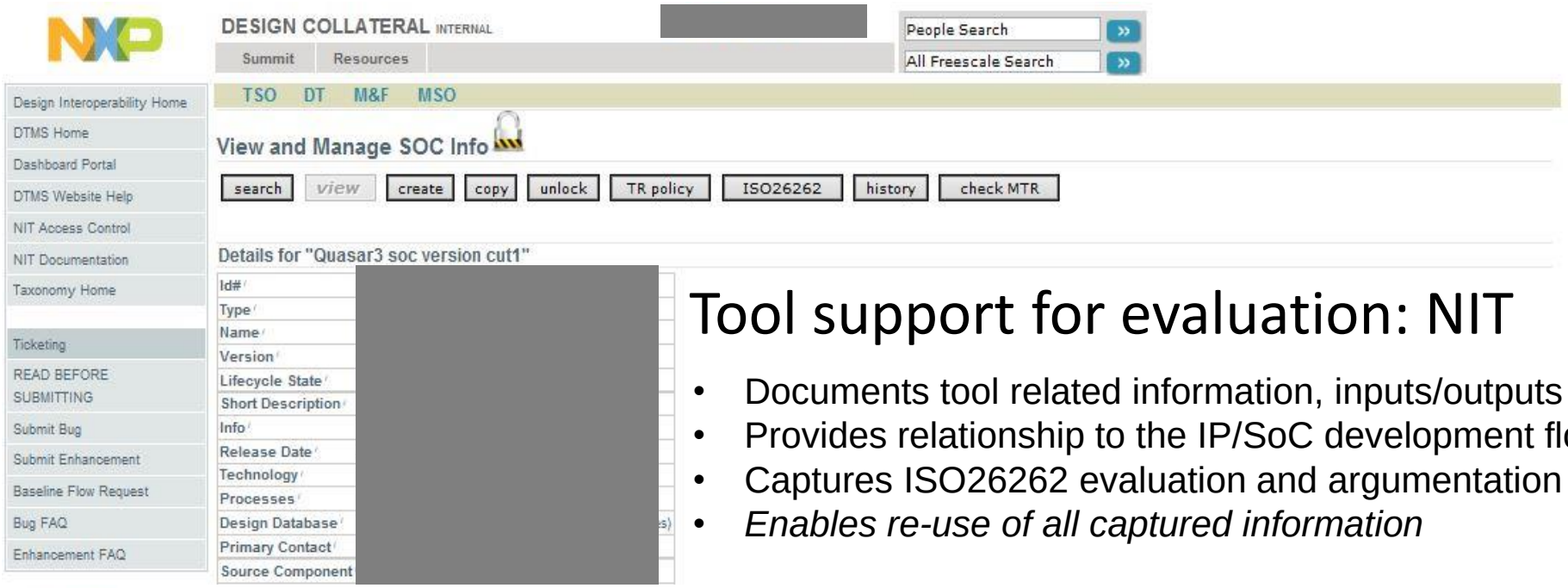
| Tool Confidence Level | | Tool error Detection | | |
|---|---|---|---|---|
| | | TD1 | TD2 | TD3 |
| Tool Impact | TI1 | *TCL1* | *TCL1* | *TCL1* |
| | TI2 | *TCL1* | *TCL2* | *TCL3* |

# Confidence in Use of Software Tools

- Identified the need for some more formal classification criteria for TI and TD w.r.t. EDA tools
- Tailored to specifics of EDA
  - frequent releases, bug fixes
  - deep, connected flows
  - tight interaction w/ vendors
- Must take into account scripts and/or generators for inputs and result checks
- Identified assessment elements that can be reused



# Confidence in Use of Software Tools




## Tool support for evaluation: NIT

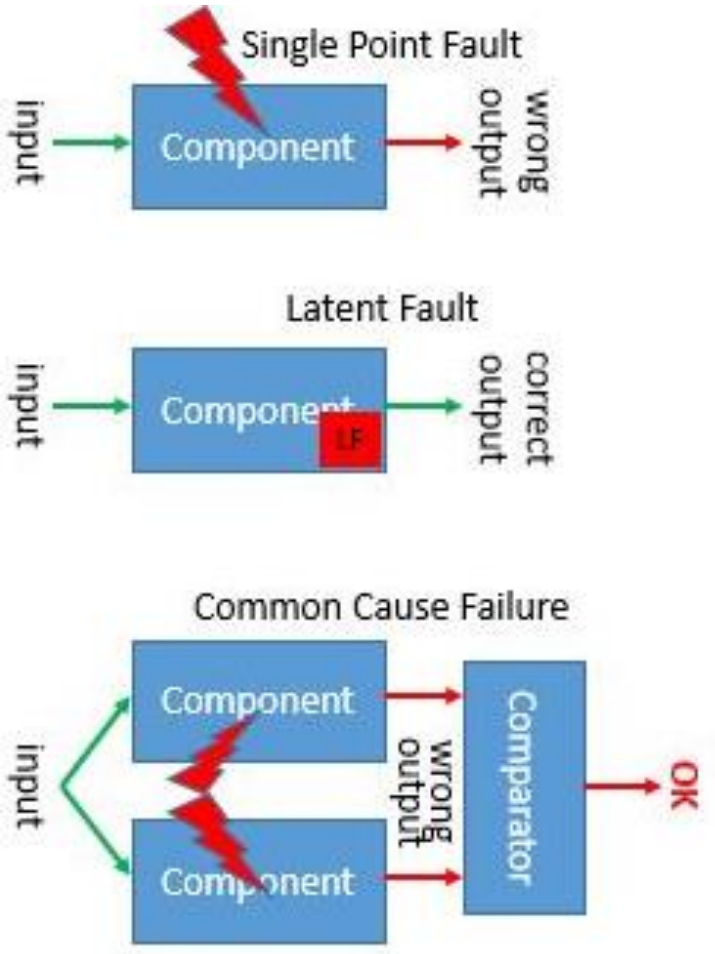
- Documents tool related information, inputs/outputs
- Provides relationship to the IP/SoC development flow
- Captures ISO26262 evaluation and argumentation
- *Enables re-use of all captured information*

Flow/Tools

| Flow | Flow Atom | Base Tool Name | Tool Label | Version | Package | ISO26262 | Source | Comments |
|---|---|---|---|---|---|---|---|---|
| RTL to Manufacturing | CDC Checking | lec | Conformal LEC | 14.20-p100 | cadence-confrml-/14.20.100 | completed | *this component* | from Tool Repository setup |
| RTL to Manufacturing | Gate Equivalence Checks | lec | Conformal LEC | 14.20-p100 | cadence-confrml-/14.20.100 | approved | *this component* | from Tool Repository setup |
| RTL to Manufacturing | Logical Synthesis | rtl_compiler | RTL Compiler (rc) | 14.10-s022_1 | cadence-rc-/14.12.000 | completed | *this component* | from backend Tool Repository setup |

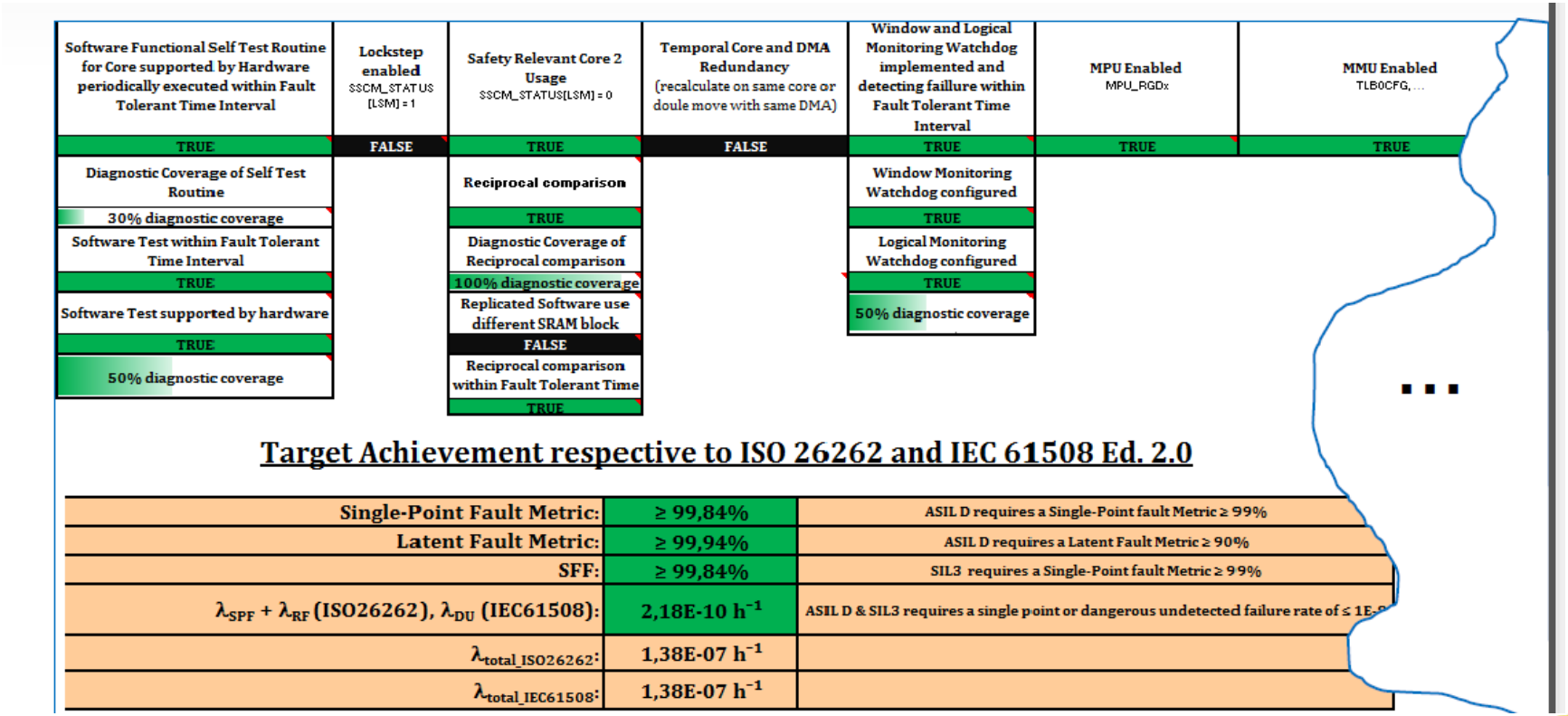
# Hazard Analysis and Risk Assessment

- Semiconductors - **S**afety **E**lement **o**ut **o**f **C**ontext (SEooC)
- **F**ailure **M**odes, **E**ffects, and **D**iagnostic **A**nalysis (FMEDA)
  - Identifies failure rates λ, failure modes, and diagnostic capabilities for error causes and their impact on the SEooC
  - Quantitative numbers for failure rates need to be provided (→ *data extraction*)
  - ISO26262 specifies the diagnostic coverage required for a specific ASIL level
- **F**ault **T**ree **A**nalysis (FTA)



# Hazard Analysis and Risk Assessment

"Dynamic FMEDA" → FMEDA tailored to an actual application and its environment

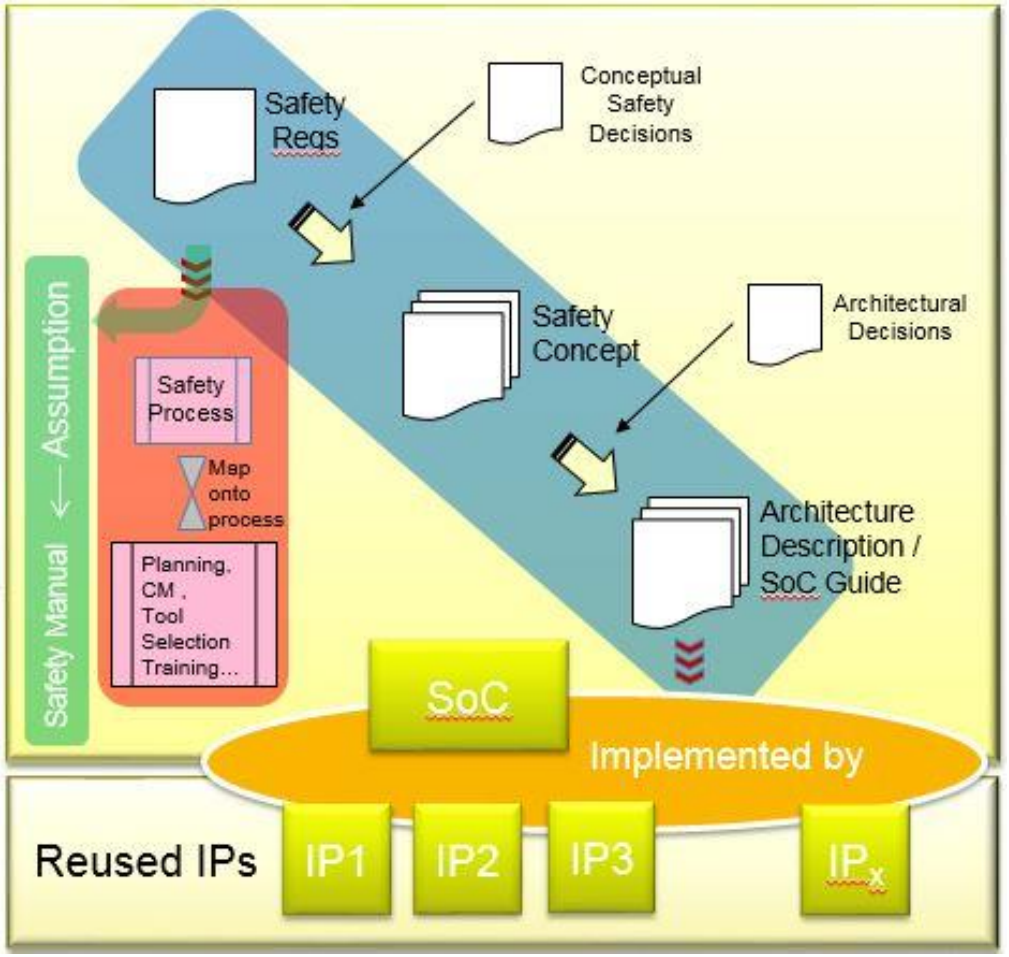


# Safety Requirements

ISO26262 specifies safety requirements that can be mapped to:

- Development *Process*
- Usage assumptions: *Safety Manual* (SM)
- Requirements for the SEooC *implementation*
  - SoC and architecture
  - individual IP blocks

**Refinement is required !!!**



# Verification : Requirements

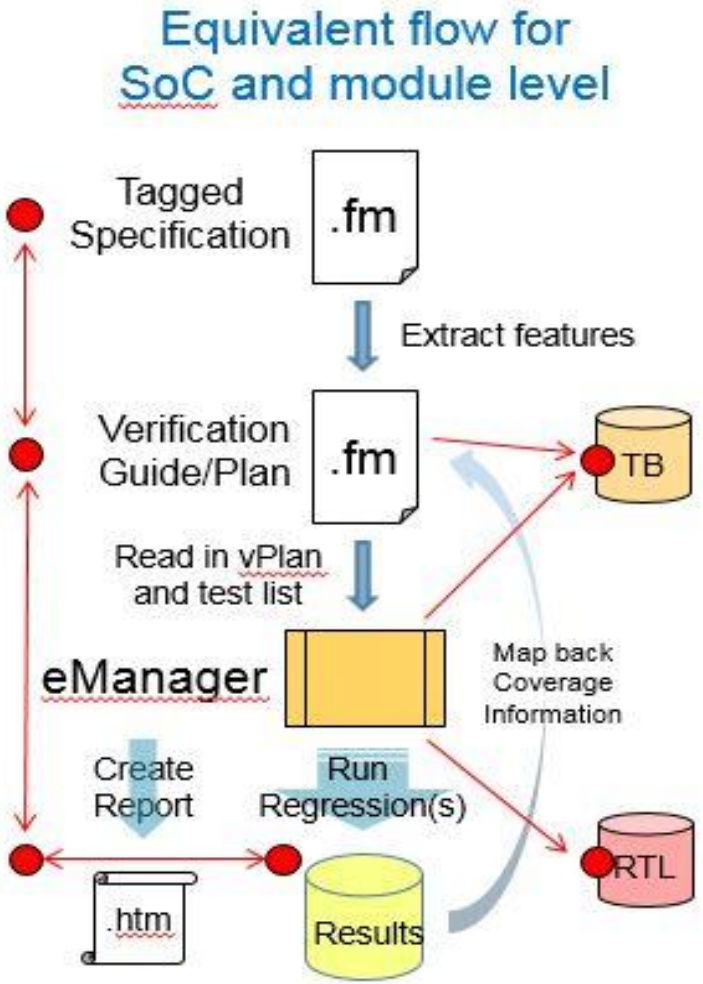
Verification of safety requirements involves several aspects:

- safety requirement *refinement*
  → capability to trace up <-> down
- mapping of safety requirements
  - onto a set of IP block specific *features*
  - on a *combination* or an *interaction* between IP blocks (SoC, architecture)
- Must ensure complete coverage
  - Complete traceability *down to verification results*

# Verification : Features

Mapping of *safety specific* requirements onto features

- Permits full reuse of existing flows for feature verification
- Provides a *common and consistent* verification of all features (w/ or w/o safety relationship)
- Enables reuse of verification items across different SoCs, even for different safety architectures



# Summary and Outlook

- Certifying *every individual SoC* can be very expensive
  - SEooC limits re-use of certification
  - be prepared to deliver what customer needs to certify it's system

- *Institutionalize a safety aware development process* can cover many aspects of the ISO2626
  - move to process certification by making use of similar aspects of your SoC projects
  - drive integration into existing processes and flows
  - drive usage of tools
  - certify integration
  - be careful and continuously adjust and improve

Thank you for your attention!