Institutionalize a certified ISO26262 safety process

M. Rohleder, C. Röttgermann, M. Müller
NXP Semiconductors, Germany
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

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

- Tools & Flows (not ISO26262 certified)
  - useful but cannot be used as is
- ISO26262 certification effort by external body
- ISO26262 specific deliverables
  - extensive effort investment
- ISO26262 device certificate
Safety Process Certification

Tools & Flows
ISO 26262 certified

ISO26262 process certification by external body

internal certification

ISO26262 safety case & deliverables to customer

use "as is"

reduced device specific certification effort

invest here

invest in training
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!!!

further elaborated in the following
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

Frontend Release
Generation Process

Modified IP

Prev. BOM

Actual BOM

defines list of IP blocks

setup.tcl

generates

Control script

complete and consistent SoC & IP configuration

DesignSync Database

generates

Configuration

populates into empty workspace

For review by Design Lead

Directory tree of any IP block as defined by the IPDSS

apply release tag

basic checks

release message

release baseline

controls

© Accellera Systems Initiative
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)
  – Tool Impact (TI1/TI2): Possibility that a malfunction can introduce or fail to detect errors
  – Tool error Detection (TD1-3): Confidence in detecting or preventing such errors

⇒ Tool Confidence Level (TCL1-3)
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
Hazard Analysis and Risk Assessment

• **Semiconductors - Safety Element out of Context (SEooC)**

• **Failure Modes, Effects, and Diagnostic Analysis (FMEDA)**
  - Identifies failure rates $\lambda$, failure modes, and diagnostic capabilities for error causes and their impact on the SEooC
  - Quantitative numbers for failure rates need to be provided ($\rightarrow$ data extraction)
  - ISO26262 specifies the diagnostic coverage required for a specific ASIL level

• **Fault Tree Analysis (FTA)**
Hazard Analysis and Risk Assessment

“Dynamic FMEDA” → FMEDA tailored to an actual application and its environment

Target Achievement respective to ISO 26262 and IEC 61508 Ed. 2.0

Single-Point Fault Metric: $\geq 99.84\%$
Latent Fault Metric: $\geq 99.94\%$
SFF: $\geq 99.84\%$

$\lambda_{SPF} + \lambda_{RF} (ISO26262), \lambda_{DU} (IEC61508): 2.18E-10 \text{ h}^{-1}$

$\lambda_{total, ISO26262}: 1.38E-07 \text{ h}^{-1}$
$\lambda_{total, IEC61508}: 1.38E-07 \text{ h}^{-1}$
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 !!!

© Accellera Systems Initiative
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!