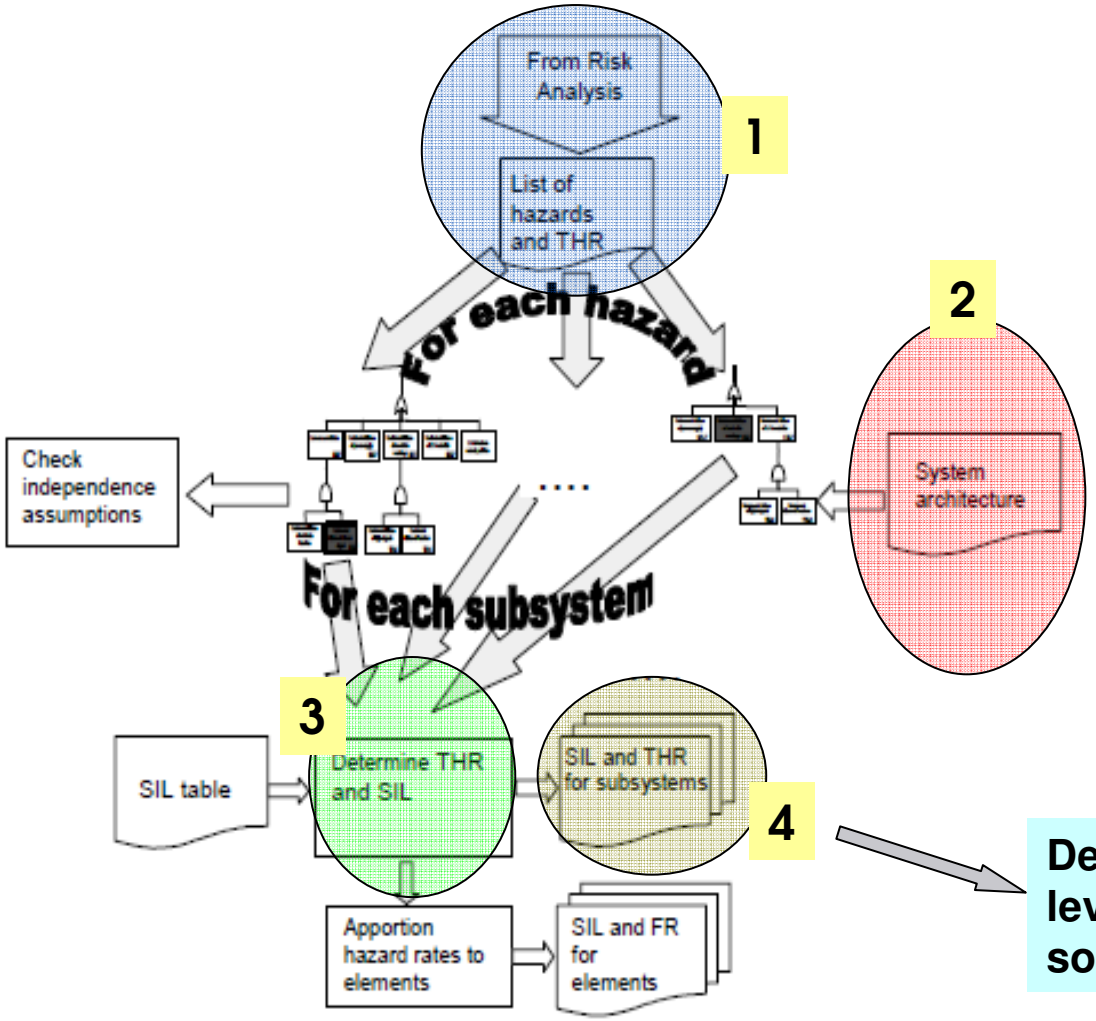
Requirements to be fulfilled according to the CENELEC EN 50128:2011 standardization

Contents

1. state of the art when developing software according to EN 50128
2. Goals of the openETCS according to EN 50128:2011
3. Output of the task „Report on CENELEC standards compliance“
4. openETCS tool chain as a model-based development environment
5. Requirements to be fulfilled by each tools
6. Requirements to be fulfilled by the openETCS tool chain
7. Requirements to activities that can not be automated

1. state of the art when developing software according to EN 50128

The state of the art when developing safety critical software is that you can not develop software without any knowledge about the system (hardware) architecture.



Note:

1. the fault detection depends on system architecture

1. state of the art when developing software according to EN 50128

After the Software SIL is known the software development process can be started

The requirements that have to be fulfilled are then described in the clauses of the EN 50128

Clause 5: Software management and organisation

5.1 Organisation, Roles and Responsibilities
5.2 Personnel
5.3 Lifecycle issues and documentation

Clause 6: Software assurance

6.1 Software testing
6.2 Software verification
6.3 Software validation
6.5 Software quality assurance
6.6 Modification and change control
6.7 Support tools and languages

Clause 7: Generic software developments

7.1 Lifecycle and documentation for generic software
7.2 Software requirements
7.3 Architecture and Design
7.4 Component design
7.5 Component implementation and testing
7.6 Integration
7.7 Overall Software Testing / Final Validation

Clause 8: Development of application data or algorithms

Clause 9: Software deployment and maintenance

9.1 Software deployment
9.2 Software maintenance

1. state of the art when developing software according to EN 50128

- The Clauses 5, 6 and 9 apply to generic software as well as for application data or algorithms.
- The Clause 7 applies only for generic software.
- The Clause 8 provides the specific requirements for application data or algorithms.

In clauses of the EN 50128, requirements are described that have to be fulfilled when developing software according to EN 50128:2011. It is also described, which documents must be created.

To fulfill these requirements, appropriate techniques or measure depending on the safety integrity level of the software must be used

2. Goals of the openETCS according to EN 50128:2011

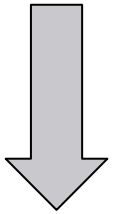
YES	NO
1. The techniques or measures applied in developing software with safety integrity level 4 (SIL4) according to EN 50128:2011 will be applied. 2. All the output documents at each phase of the generic openETCS software life cycle will be produced. 3. Tools for software development, configuration, maintenance, etc. will be developed, so that they can be certified as T3 support Tools according to EN 50128:2011.	1. The generic openETCS software will not be assessed 2. The certification of openETCS tool chain is not part of the project.

3. Output of the task „Report on CENELEC standards compliance“

The Expected Output :

Summary of requirements that must be fulfilled according to the CENELEC EN 50128 standardization

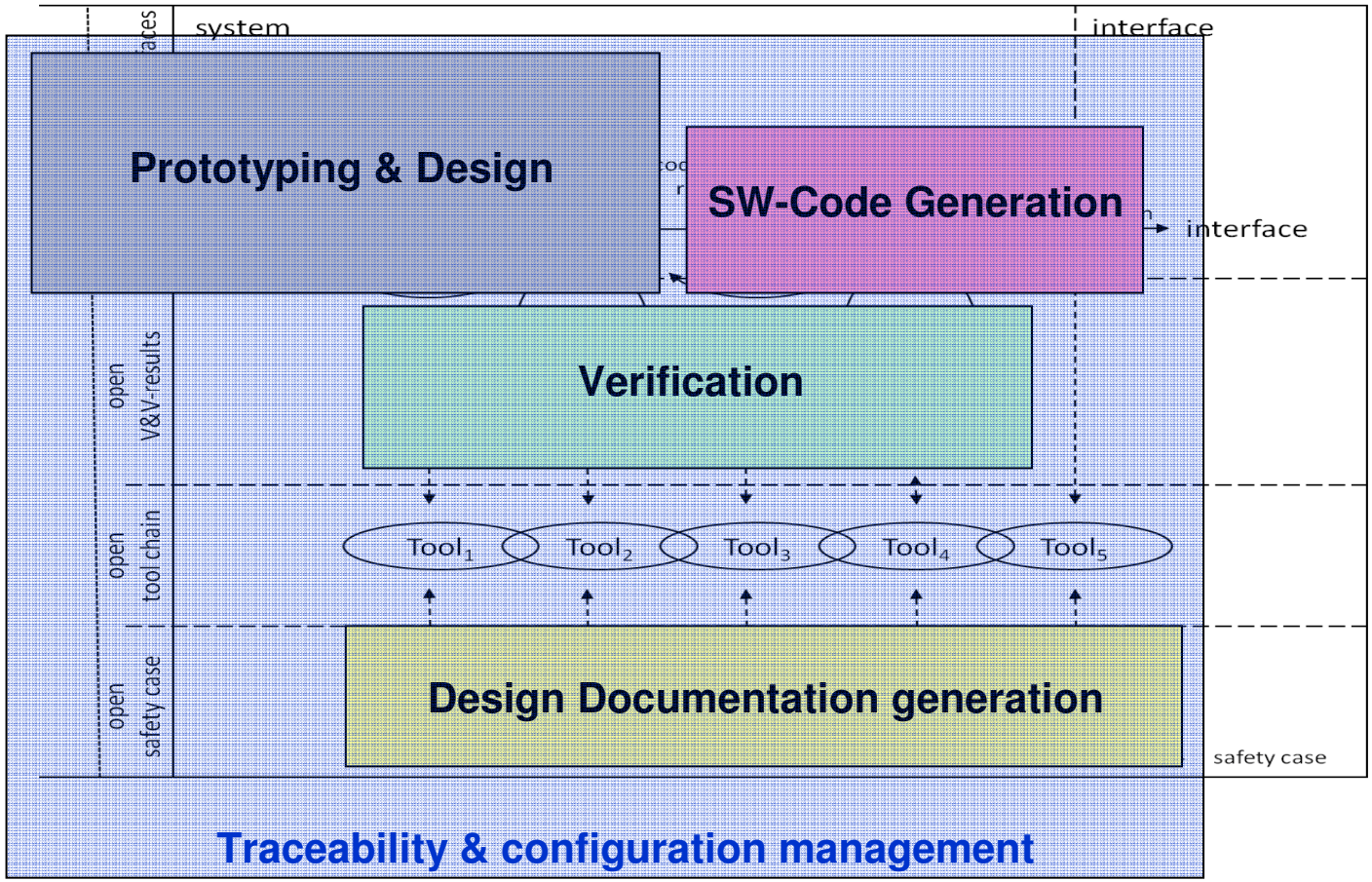
But which products of the openETCS project shall be developed, so that they can be certified according to CENELEC standard EN 50128:2011?



Within the scope of the openETCS project: only the supported Tools and languages

4. openETCS tool chain as a model-based development environment

Automate the software development process using the model-based development approach.



5. Requirements to be fulfilled by each tools

To be T3 compliant according to 50128:2011, each tool shall fulfilled The requirements (6.7.4.1 to 6.7.4.5) or (6.7.4.6 to 6.7.4.11) of EN 50128:2011

NOTE:

1. each tool is intended to be a part of the openETCS tool chain
2. The openETCS is intended to automate the software development process (i.e. the document creation process will be automated)
3. The openETCS is intended to provide techniques or measure for SIL 4 software

6. Requirements to be fulfilled the openETCS tool chain

The openETCS tool chain shall fulfill the following requirements:

1. **The tools within the openETCS tool chain should be able to cooperate.**
   (Tools cooperate if the outputs from one tool have suitable content and format for automatic input to a subsequent tool, thus minimizing the possibility of introducing human error in the reworking of intermediate results.)

2. **It shall be demonstrated that the tool is compatible with the needs of the application.**

3. **The openETCS tool chain shall fulfill** *(when relevant)* **each requirement of clause (6,7 and 8) of the EN 50128:2011**
   (i.e. The listed combinations of techniques and measures for software safety integrity levels 4 according to EN 50128:2011 shall be supported by the openETCS toolchain)

4. **The openETCS tool chain should generate output documentation that is compliant to EN 50128:2011 output documentation.**

7. Requirements to activities that can not be automated

Activities that cannot be automated, have to be clearly controlled and described

Verification activities: how will be verified (produces a verification plan according to EN 50128:2011)

Validation activities: how will be validated (produces a validation plan according to EN 50128:2011)

Quality Assurance activities: how the quality will be assured (produces a Quality Assurance Plan according to EN 50128:2011)

Changes and change management activities:

1. ensure that the software performs as required, preserving the software safety integrity and dependability when modifying the software.
2. ensure that each tool perform as required, preserving the tool class when modifying the tool

(Changes and change management activities have to be performed according to EN 50128:2011)

Thank you for listening

Merlin Pokam	Stephan Jagusch
+49 911 520992 172	+49 911 520992 195
+49 0151 108 215 04	+49 0163 485 872 4
merlin.pokam@AEbt.de	stephan.jagusch@AEbt.de