Automotive

ISO 26262 Certificates for Tools
Approach and Examples

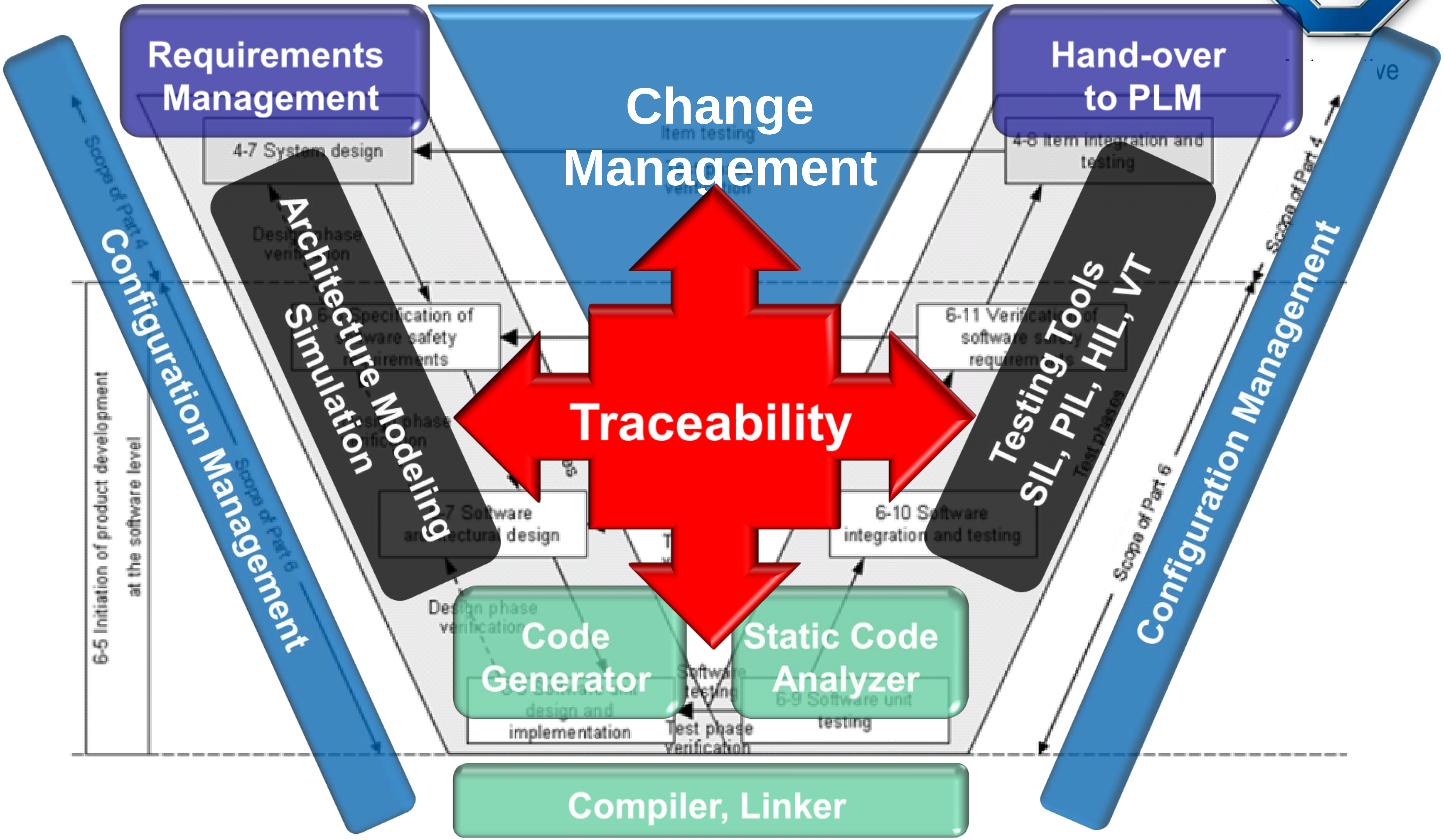
Agenda

Automotive

- Introduction
- Using tools in the safety lifecycle
- Classification of tools
  - The tool impact level (TI)
  - The tool error detection level (TD)
- Qualification of tools
- Summary: Output of tool evaluation

USING TOOLS IN THE SAFETY LIFECYCLE

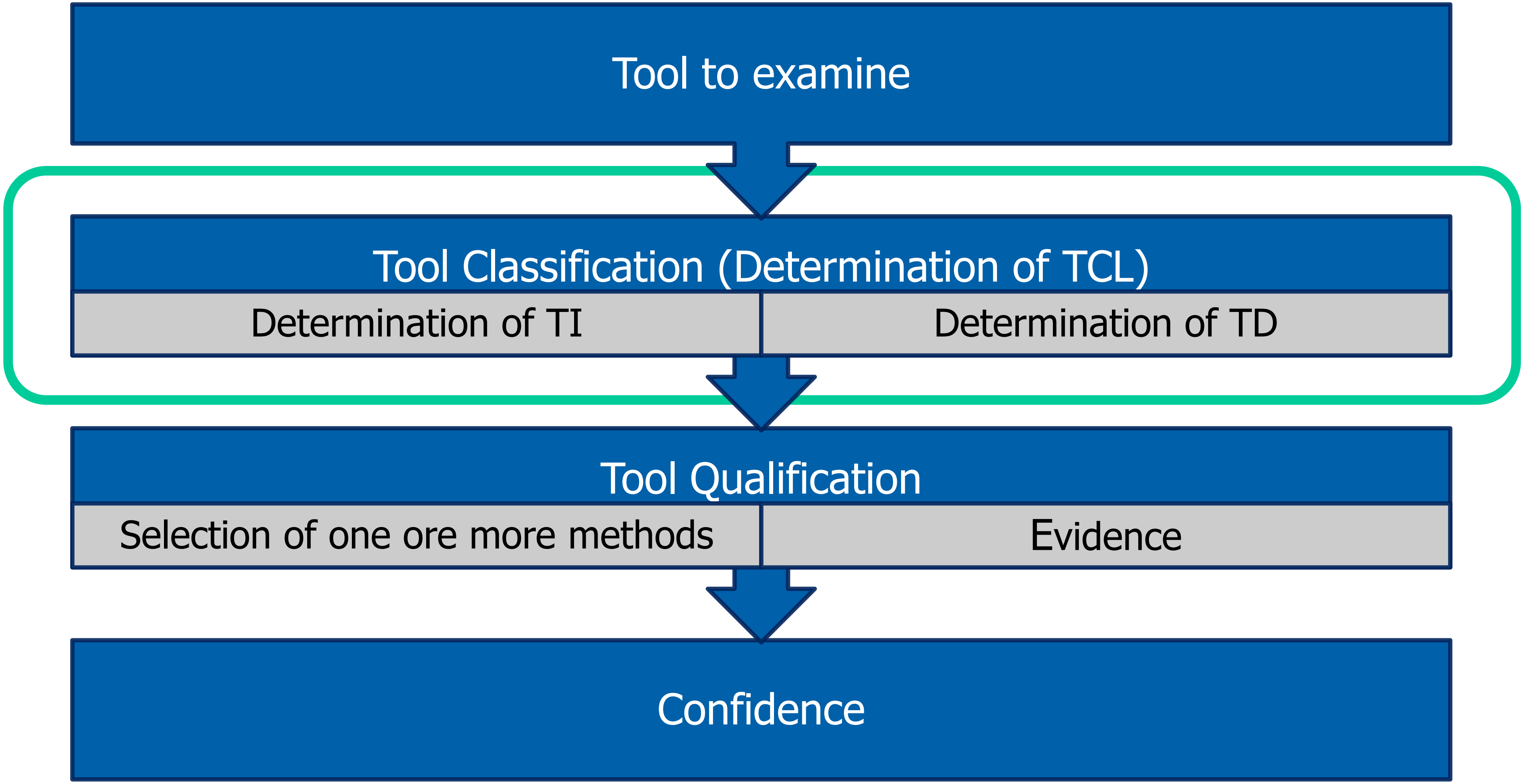
Scope of a qualified toolchain


Requirements Management
Change Management
Hand-over to PLM
Architecture Modeling
Simulation
Traceability
Testing Tools
SIL, PIL, HIL, VT
Configuration Management
Configuration Management
Code Generator
Static Code Analyzer
Compiler, Linker
4-7 System design
4-8 Item integration and testing
Item testing
verification
Design phase verification
6-6 Specification of software safety requirements
6-11 Verification of software safety requirements
Design phase verification
6-7 Software architectural design
6-10 Software integration and testing
Design phase verification
6-8 Software unit design and implementation
6-9 Software unit testing
Software testing
Test phase verification
Test phases
6-5 Initiation of product development at the software level
Scope of Part 4
Scope of Part 6
Scope of Part 4
Scope of Part 6

CLASSIFICATION OF TOOLS

Confidence in the use of SW-Tools

Automotive



Tool to examine

Tool Classification (Determination of TCL)

Determination of TI

Determination of TD

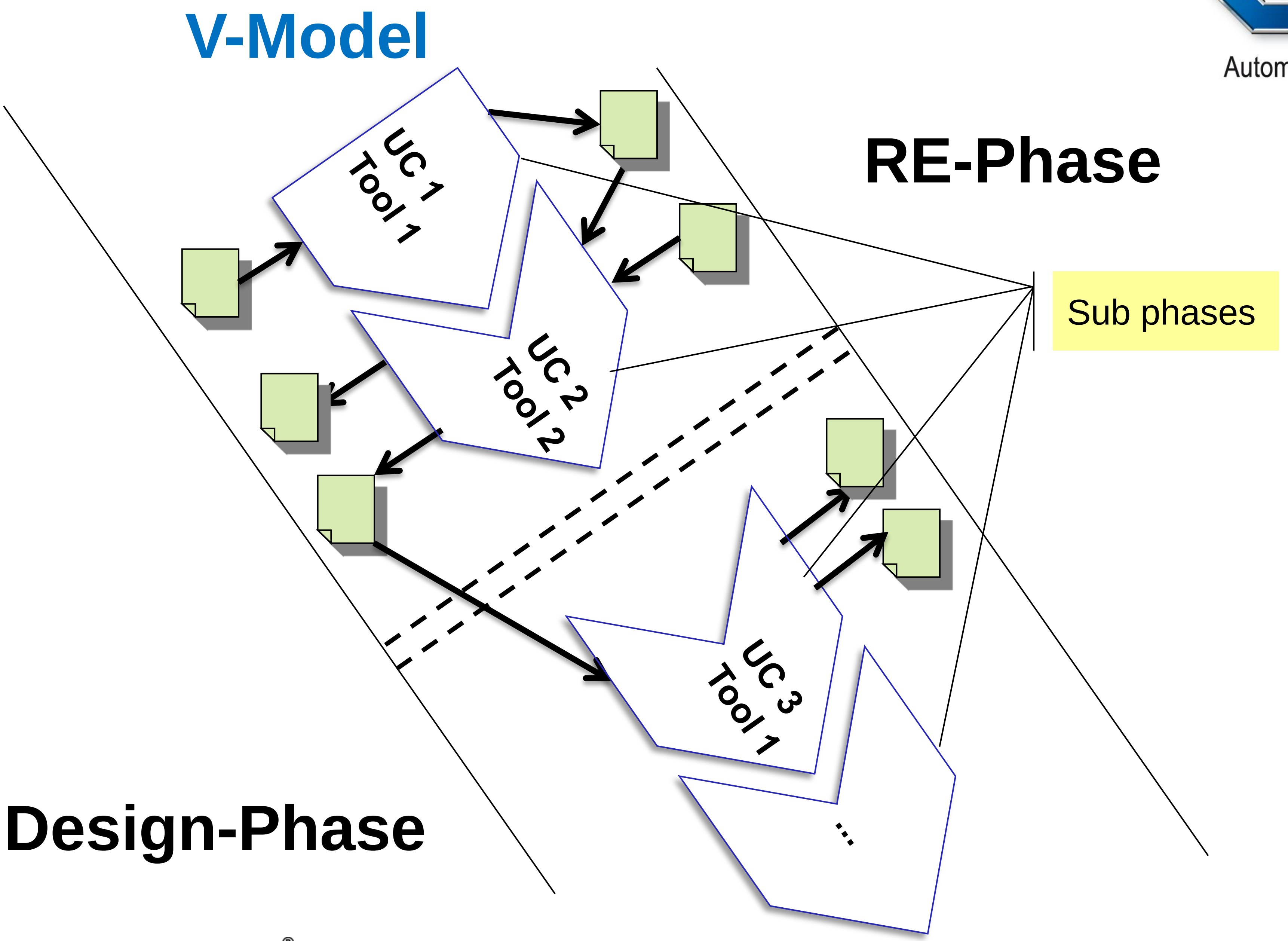
Tool Qualification

Selection of one ore more methods

Evidence

Confidence

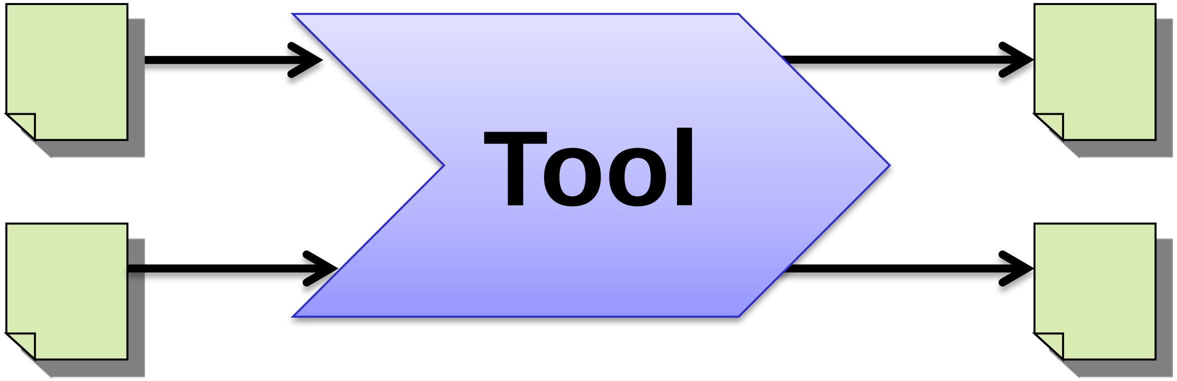
Proposal: Identification of Use Cases



Analysis of Use Cases

Automotive

- Consider inputs and outputs of Use Case
- Derive possible failures
- For each failure:
  - Analyze the effect of failures (violation of safety goal): TI
  - Analyze mitigations in the process: TD
  - Use methods known from FMEA
- Rate TCL for Tool in this UC based on result



Tool impact level depending on the use case

Automotive

Tool Impact = 1

- Tools which cannot introduce any error to my product
- Tools which cannot mask a product error
- Tools which cannot introduce any deviations into my safety lifecycle

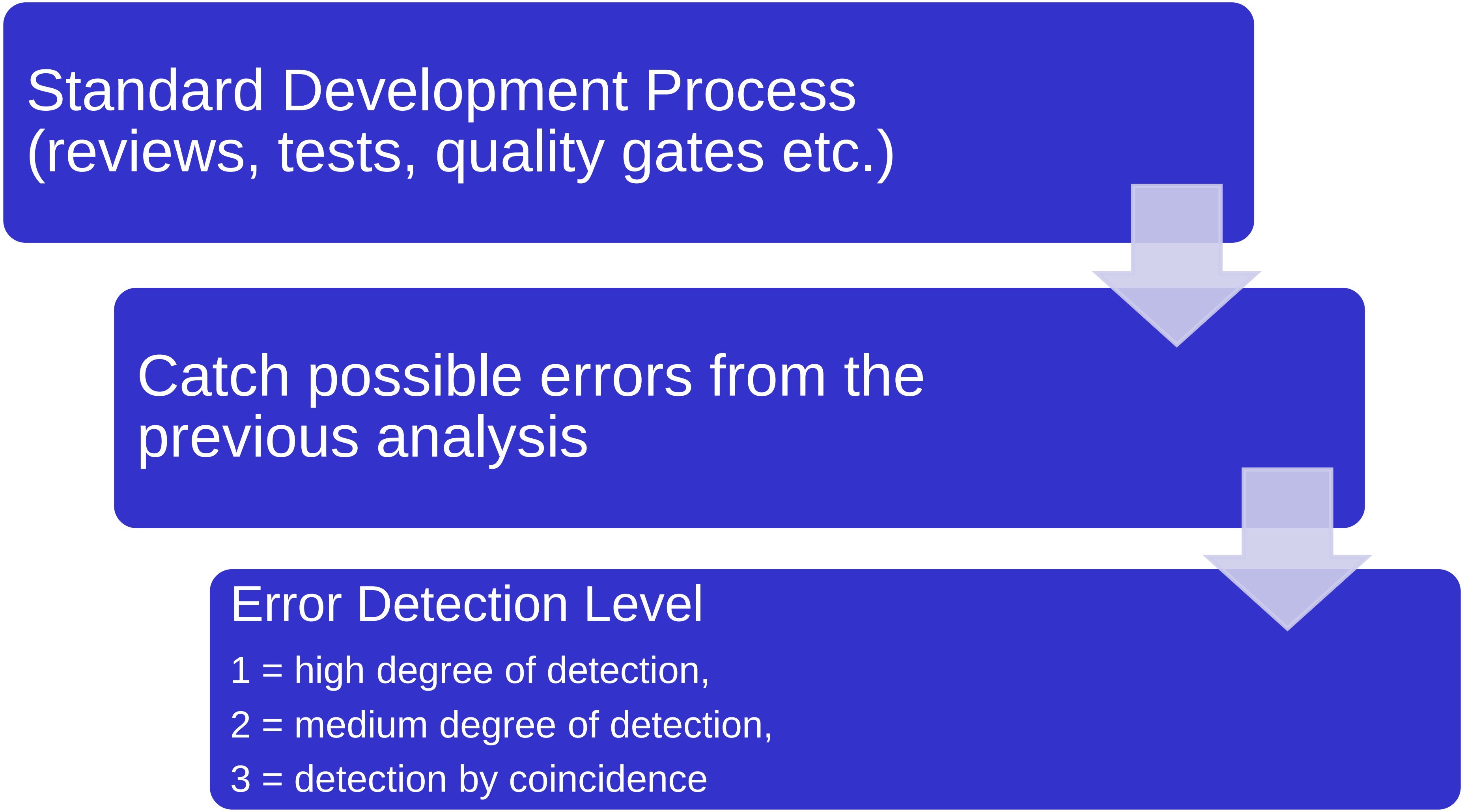
Tool Impact = 2

- All tools which can lead to errors in my product
- All tools which used in testing/validating the product
- All tools relied on in the safety lifecycle

Interm. Result of the Tool Classification

Tool	Use Case	Possible Deviations	Tool Impact
Tool 1	Use Case 1.1	Error 1.1.1	TI 2
		Error 1.1.2	
	Use Case 1.2	Error 1.2.1	
Tool 2	Use Case 2.1	No error	TI 2
	Use Case 2.2	Error 2.2.1	
	Use Case 2.3	Error 2.3.1	
		Error 2.3.2	
		Error 2.3.3	
Tool 3	Use Case 3.1	Error 3.1.1	TI 1
Tool 4	Use Case 4.1	Error 4.1.1	TI 1
…	…	…	…

Determining the Error Detection Level



Standard Development Process (reviews, tests, quality gates etc.)

Catch possible errors from the previous analysis

Error Detection Level

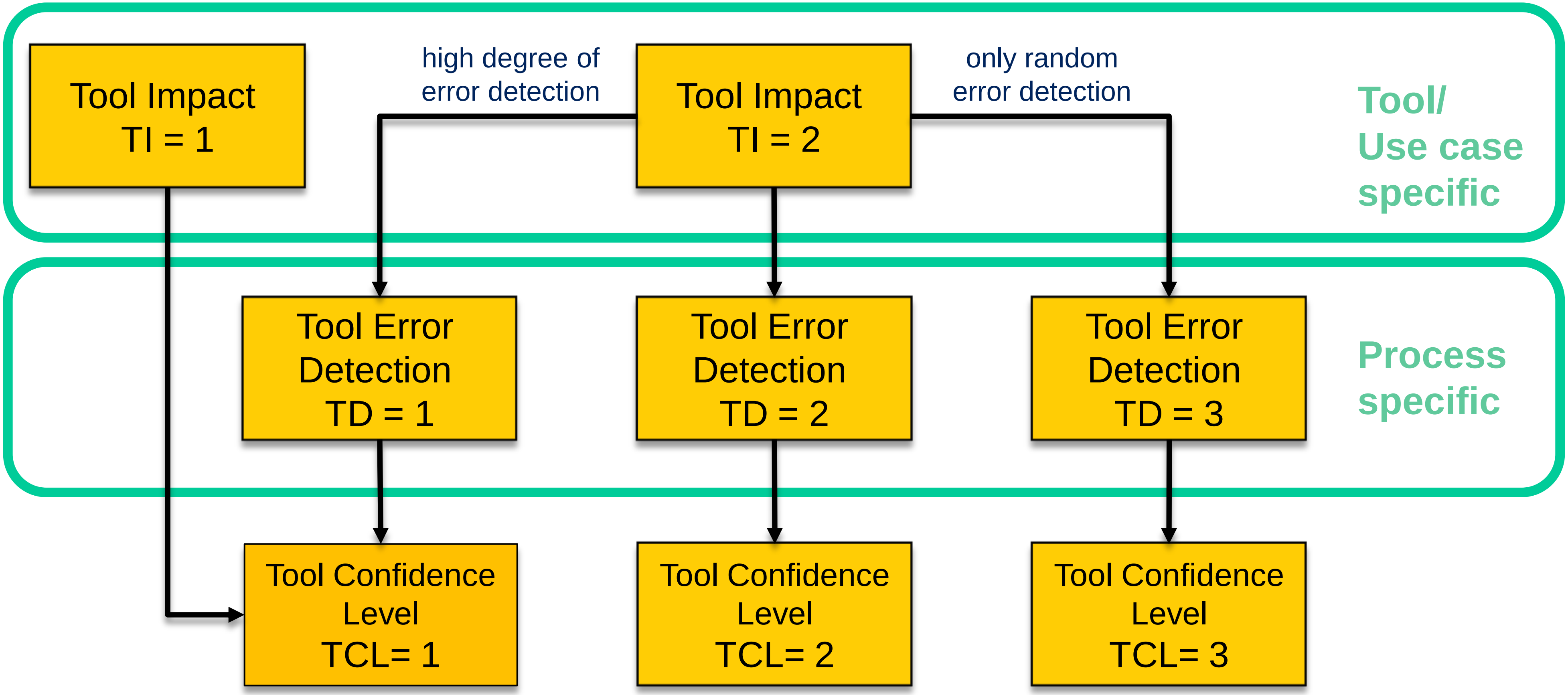
1 = high degree of detection,

2 = medium degree of detection,

3 = detection by coincidence

Tool Classification

Automotive

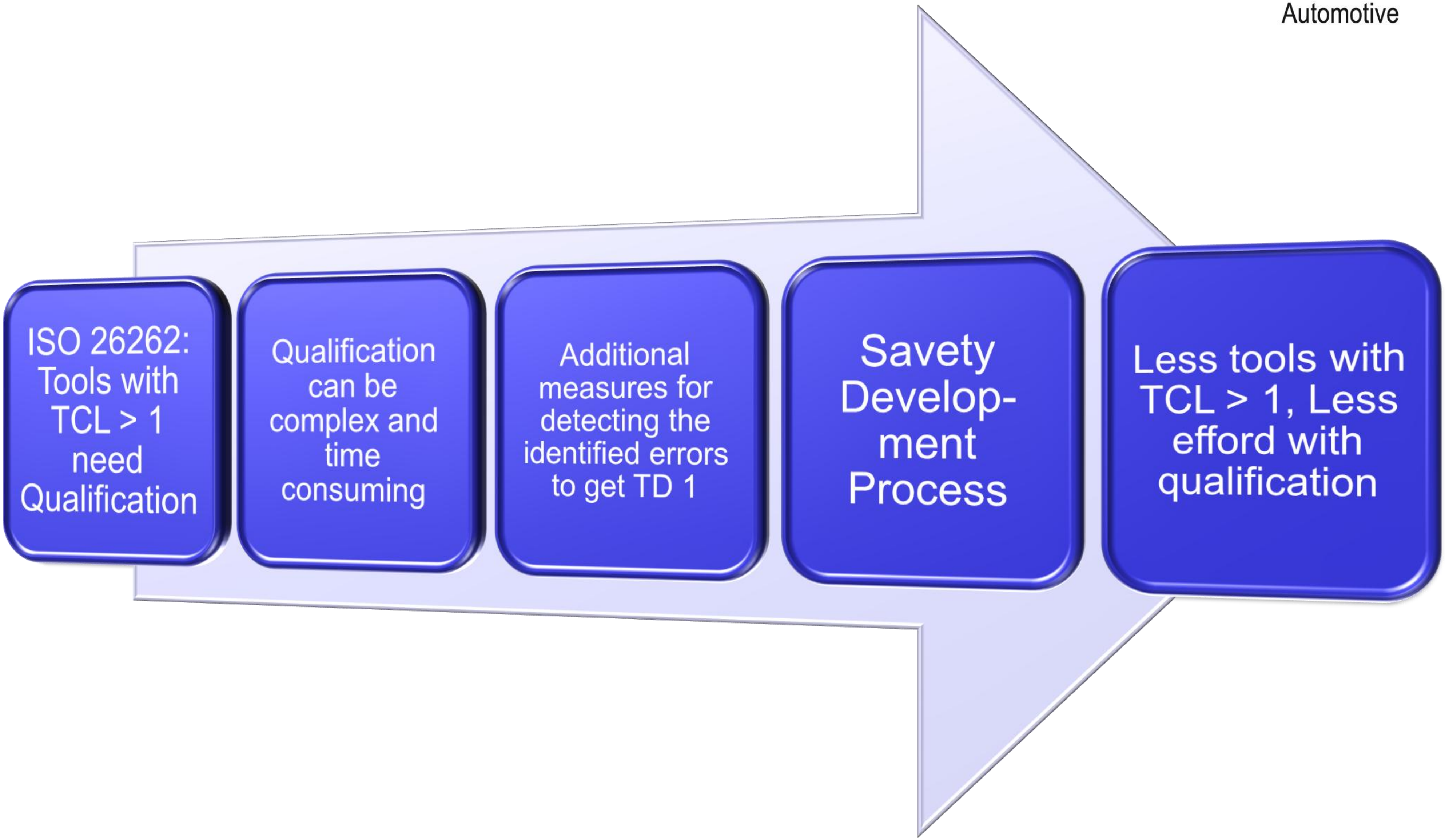


Result of Tool Classification

Automotive

Tool	Use Case	Possible Deviations	Tool Impact TI	Error Detection TD	Confidence Level TCL
Tool 1	Use Case 1.1	Error 1.1.1	TI 2	TD 1	TCL 1
		Error 1.1.2			
	Use Case 1.2	Error 1.2.1			
Tool 2	Use Case 2.1	No error	TI 2	TD 2	TCL 2
	Use Case 2.2	Error 2.2.1			
	Use Case 2.3	Error 2.3.1			
		Error 2.3.2			
		Error 2.3.3			
Tool 3	Use Case 3.1	Error 3.1.1	TI 2	TD 3	TCL 3
Tool 4	Use Case 4.1	Error 4.1.1	TI 1	TD 3	TCL 1
…	…	…	…	…	…

Proposal: Lower the TCL



ISO 26262: Tools with TCL > 1 need Qualification

Qualification can be complex and time consuming

Additional measures for detecting the identified errors to get TD 1

Savety Develop-ment Process

Less tools with TCL > 1, Less efford with qualification

Result of Tool Classification

Automotive

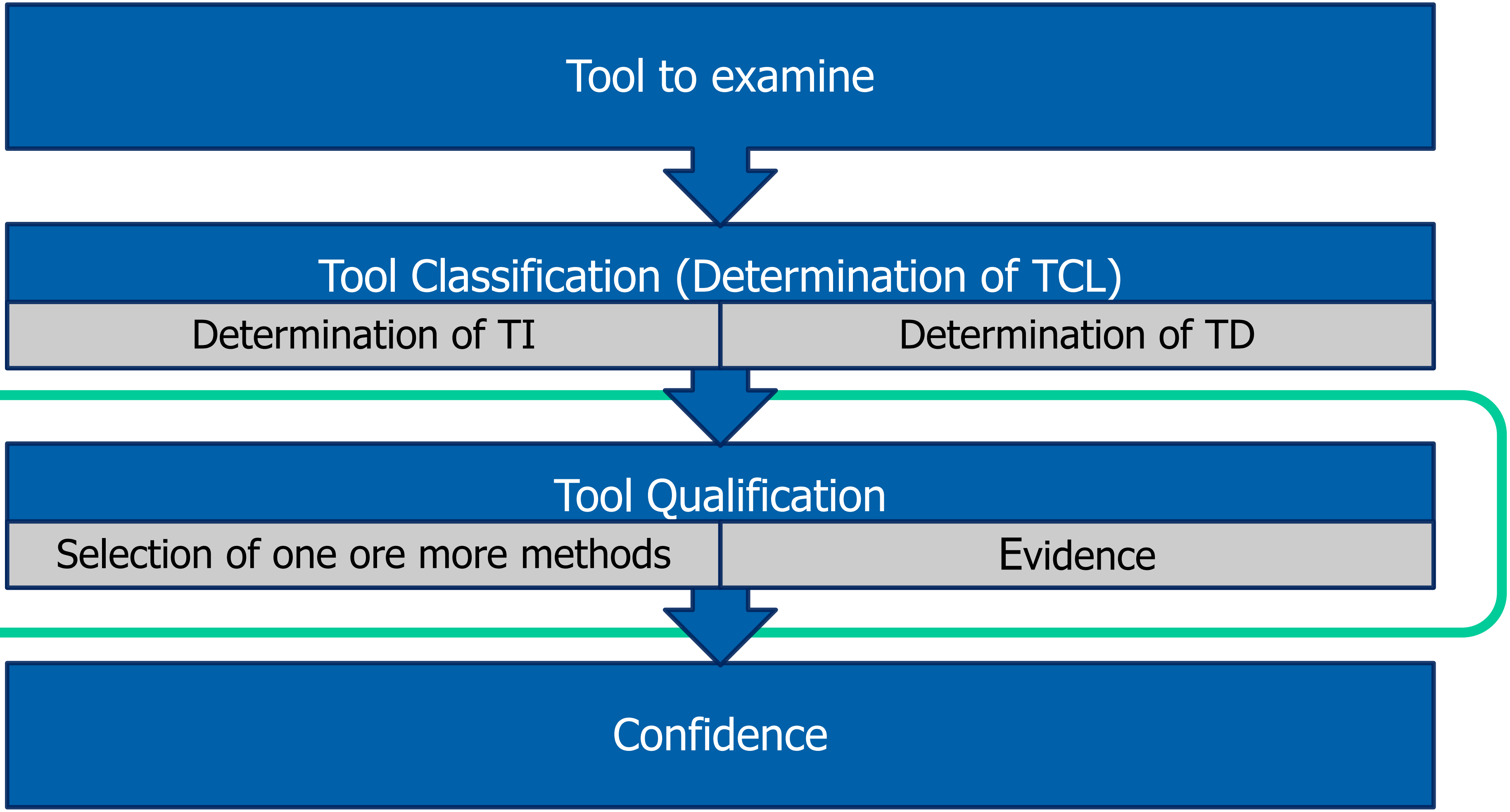
Tool	Use Case	Possible Deviations	Tool Impact TI	Error Detection TD	Confidence Level TCL
Tool 1	Use Case 1.1	Error 1.1.1	TI 2	TD 1	TCL 1
		Error 1.1.2			
	Use Case 1.2	Error 1.2.1			
Tool 2	Use Case 2.1	No error	TI 2	TD 2	TCL 2
	Use Case 2.2	Error 2.2.1			
	Use Case 2.3	Error 2.3.1			
		Error 2.3.2			
		Error 2.3.3			
Tool 3	Use Case 3.1	Error 3.1.1	TI 2	TD 1	TCL 1
Tool 4	Use Case 4.1	Error 4.1.1	TI 1	TD 3	TCL 1
…	…	…	…	…	…

Automotive

QUALIFCATION OF TOOLS

Confidence in the use of SW-Tools

Automotive



Tool to examine

Tool Classification (Determination of TCL)

Determination of TI

Determination of TD

Tool Qualification

Selection of one ore more methods

Evidence

Confidence

Selection of appropriate qualification methods

	Methods for TCL 3	ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance with a safety standard[a]	+	+	++	++

[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.

EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508 or RTCA DO-178

	Methods for TCL 2	ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	++	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	++	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	+	++
1d	Development in accordance with a safety standard[a]	+	+	+	++

[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.

EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508 or RTCA DO-178

Selection of qualification measures

1. Increased confidence from use

2. Evaluation of the tool development process

3. Validation of the software tool

4. Development in accordance with a safety standard

Qualification of SW Tools

Automotive

1. Increased confidence from use
   - Same purpose, same use cases, comparable environment and functional constraints
   - Sufficient and adequate data (duration/frequency)
   - Specification of the tool is unchanged
   - Systematic accumulation of known errors

2. Evaluation of the tool development process
3. Validation of the software tool
4. Development in accordance with a safety standard

Qualification of SW Tools

1. Increased confidence from use

2. Evaluation of the tool development process
   - Assessment of the development process applied for the tool (appropriate national or international standard)

3. Validation of the software tool
4. Development in accordance with a safety standard

Qualification of SW Tools

1. Increased confidence from use
2. Evaluation of the tool development process

3. Validation of the software tool
   - To demonstrate that the tool complies with its specified requirements
   - Analysis of errors
   - Examination of the reaction of the software tool to anomalous operating conditions

4. Development in accordance with a safety standard

Qualification of SW Tools

1. Increased confidence from use
2. Evaluation of the tool development process
3. Validation of the software tool

4. Development in accordance with a safety standard
   - No safety standard is fully applicable to the development of software tools.
   - a relevant subset of requirements of the safety standard can be selected

Selection of qualification measures

1. Increased confidence from use
   - Tools often change
   - Use cases are different

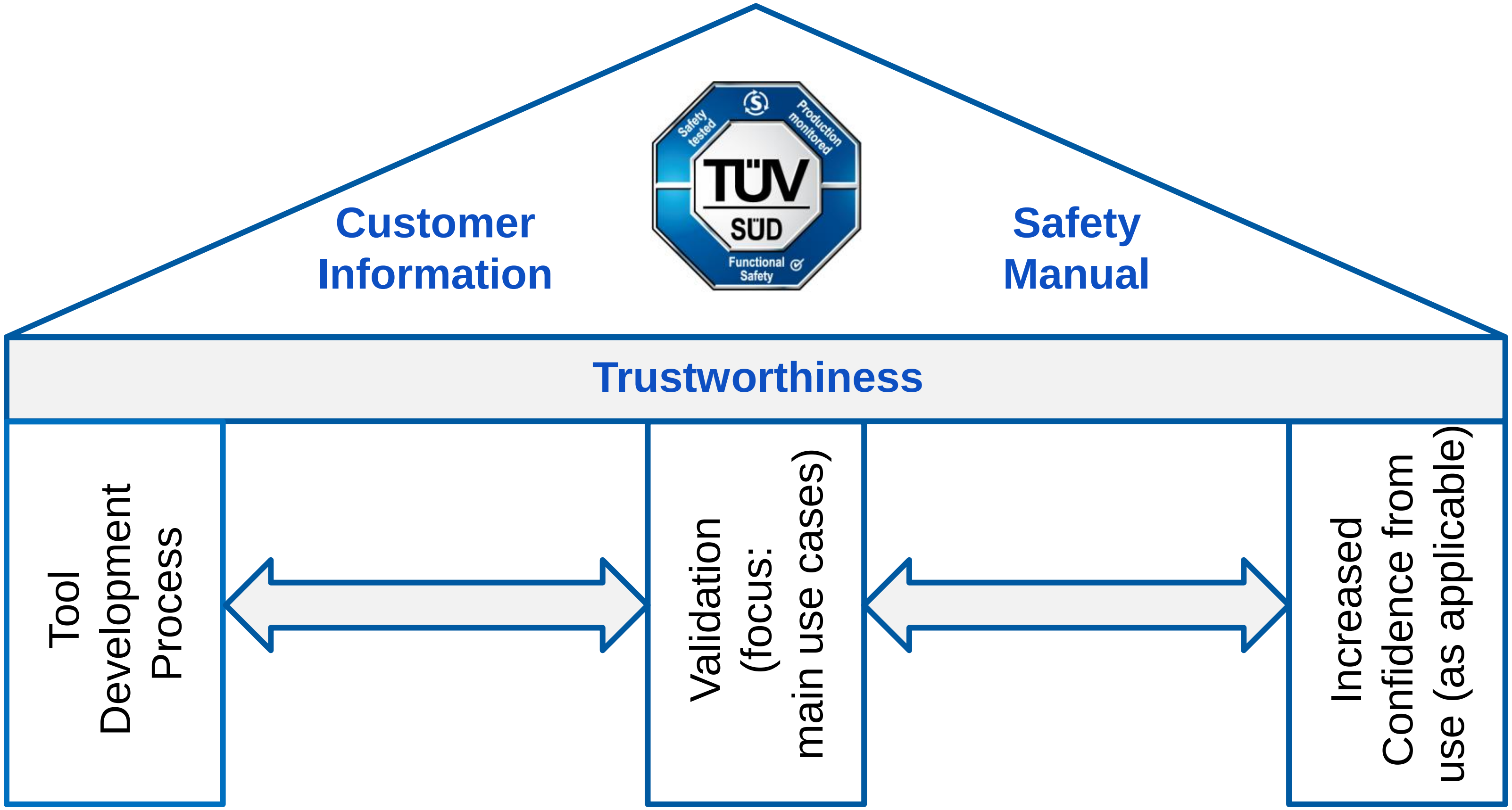
2. Evaluation of the tool development process
   - Requires audit of tool vendor (re-audit for new versions)

3. Validation of the software tool
   - Requires validation suite matching the use cases

4. Development in accordance with a safety standard
   - No tool (for the automotive domain) is developed in full compliance with ISO 26262 (yet)

Alternative: Certified Tools

TÜV SÜD Automotive

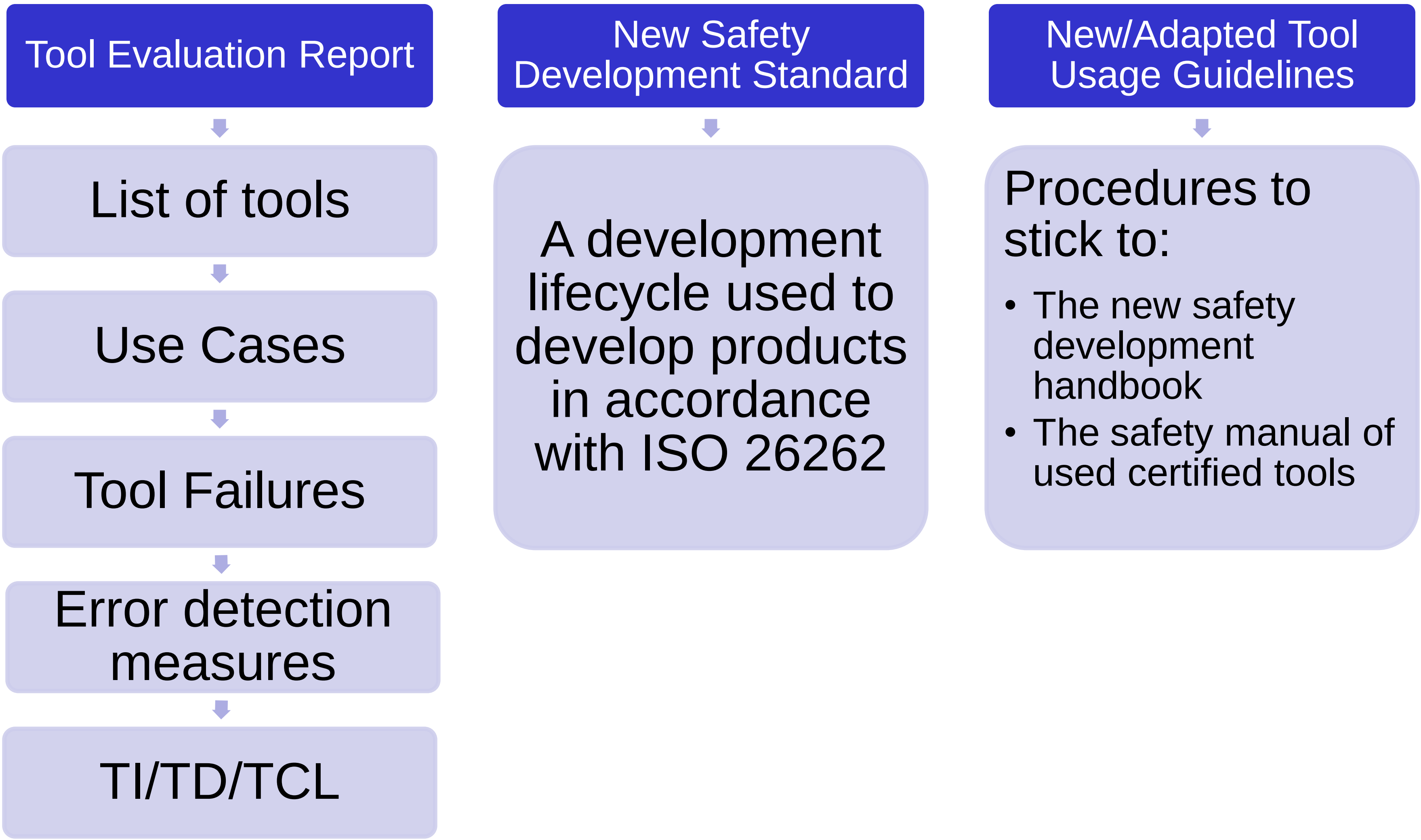


Usage of a certified tools

Automotive

- Tool certificate is valid for the certified versions
- Tool user has to stick to the user manual (Evidence by tool usage guideline or development process description)
- Use cases not listed in the user manual need seperate handling (TI – TD – TCL)

Result of Tool Evaluation



Tool Evaluation Report

List of tools

Use Cases

Tool Failures

Error detection measures

TI/TD/TCL

New Safety Development Standard

A development lifecycle used to develop products in accordance with ISO 26262

New/Adapted Tool Usage Guidelines

Procedures to stick to:

- The new safety development handbook
- The safety manual of used certified tools

Your Competent Partner

TÜV SÜD

Automotive

Tel. 089/32950-861
Fax 089/32950-870
e-mail: elektronik@tuev-sued.de

Automotive