

# Zukünftige Wege und Anforderungen der Toolqualifizierung

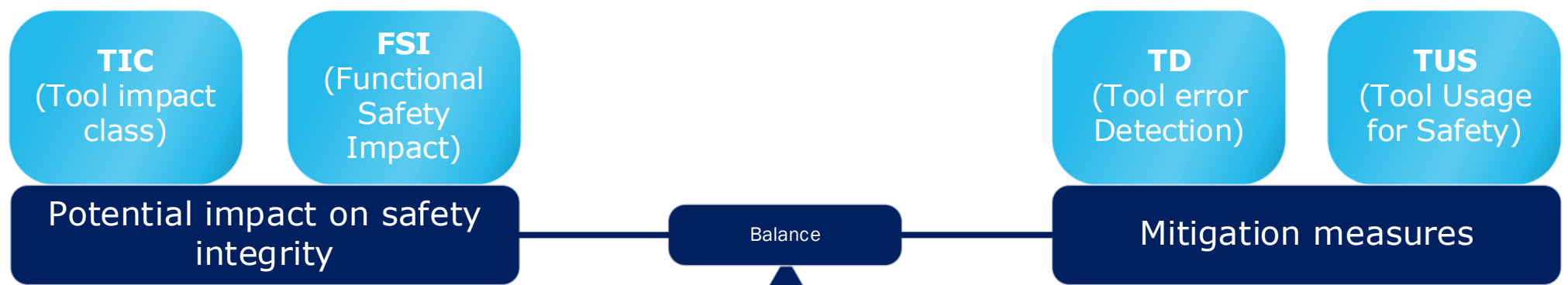
Michael Kieviet

# Software-off-line support tool

- Das “software-off-line support tool” ist ein Softwarewerkzeug, welches bei der Entwicklung einer Sicherheitsfunktion eingesetzt wird. Es ist selbst **kein** Bestandteil der Sicherheitsfunktion und hat somit keinen unmittelbaren Einfluss auf die Sicherheitsfunktion zur Laufzeit.

z.B. Compiler, Test-Tools, Versionsmanagement-Tools, Applikationsparametrierungs-Tools, ...

# Tool Confidence Approach



| TIC | FSI | TUS |     |     |
|-----|-----|-----|-----|-----|
|     |     | TD1 | TD2 | TD3 |
| 2   | 1   | -   | 1   | 1   |
|     | 2   | -   | 1   | 1   |
|     | 3   | 1   | 2   | 2   |
|     | 4   | 1   | 2   | 3   |
| 3   | 1   | -   | 1   | 1   |
|     | 2   |     | 1   | 2   |
|     | 3   | 1   | 2   | 3   |
|     | 4   | 1   | 3   | 4   |



# TIC Tool Impact Class

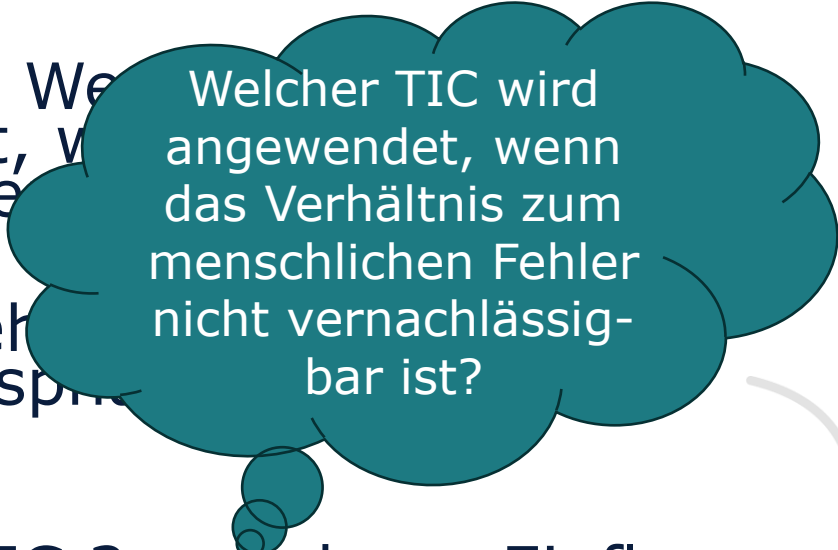
- Einfluss eines Fehlers durch ein "software-off-line support tool" auf die zu entwickelnde Sicherheitsfunktion.

**TIC 3:** Das Ausgabeergebnis (Output) eines Werkzeuges dient zur Realisierung der Sicherheitsfunktion, wird erzeugt oder transformiert. (Beispiel: Compiler)

**TIC 2:** Das Werkzeug wird verwendet, um Fehler in der Sicherheitsfunktion während der Entwicklungsphase zu finden. (Beispiel: Unit-Tester, HiL Test)

**TIC 1:** Das Werkzeug ist weder TIC 3 noch TIC 2 und deren Einfluss ist im Verhältnis zu einem menschlichen Fehler vernachlässigbar.

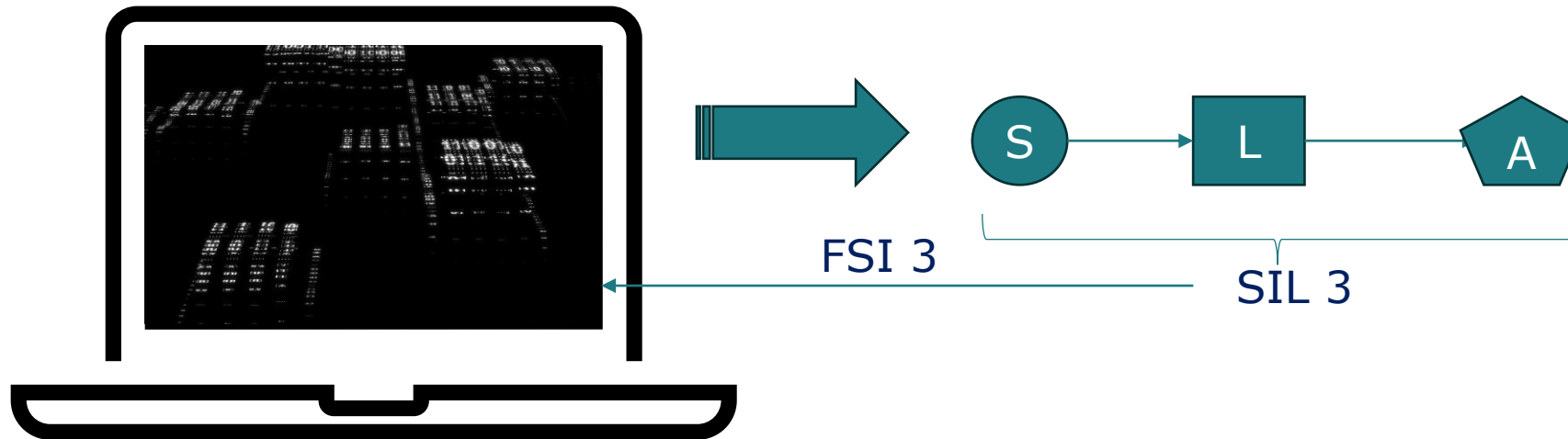
**-> keine Qualifizierung nach IEC 61508 erforderlich!**



Welcher TIC wird angewendet, wenn das Verhältnis zum menschlichen Fehler nicht vernachlässigbar ist?

# FSI Functional Safety Impact

- Ergibt sich aus dem SIL oder dem SC der zu realisierenden Funktionalität, bei der das Werkzeug in der Entwicklung eingesetzt werden soll.



# TD Tool Error Impact Detection / Prevention Level

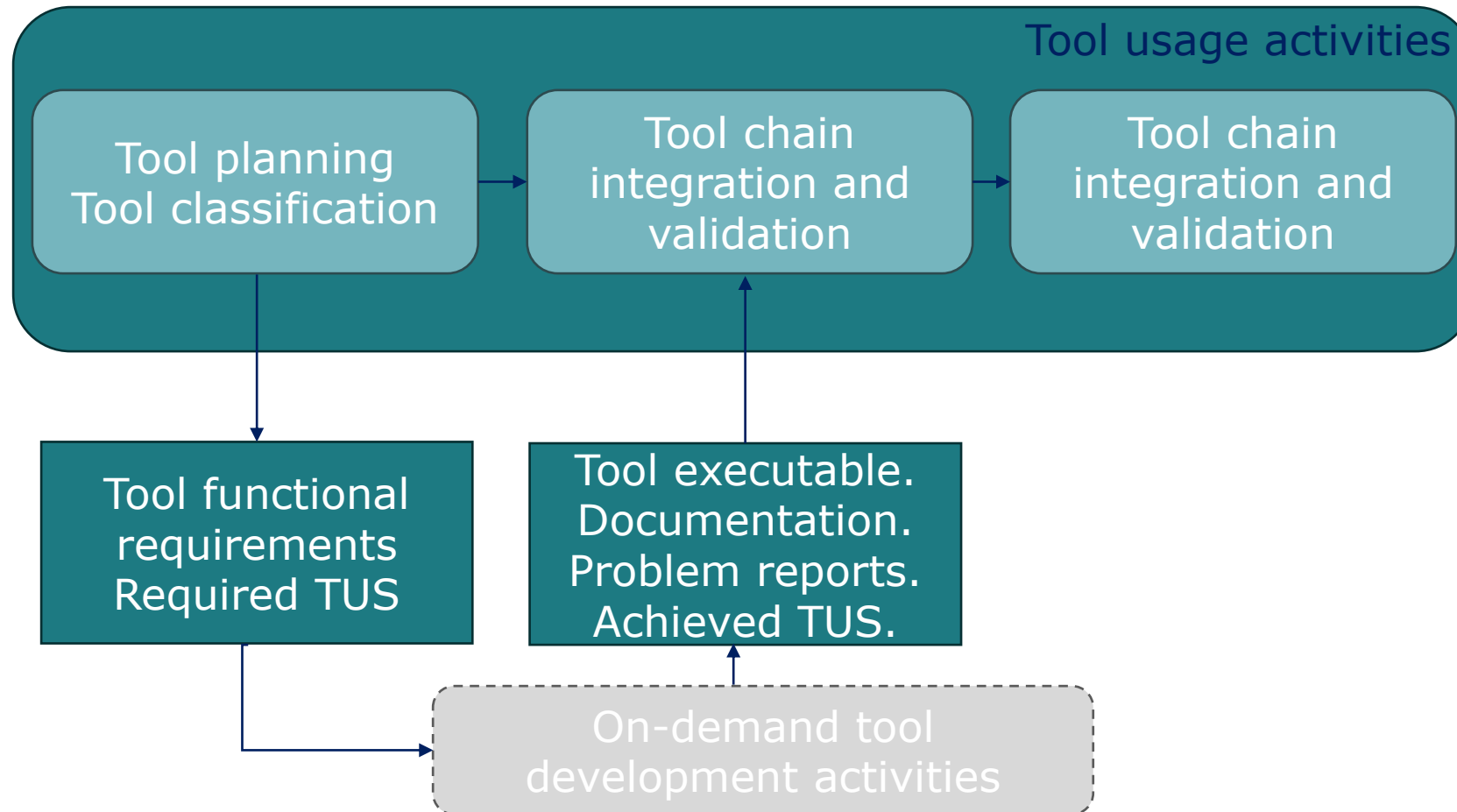
- Einstufung der Effektivität, die zur Fehlererkennung bei der Nutzung des Softwarewerkzeuges herangezogen wird, um Fehlereinflüsse des Softwarewerkzeuges auf die Sicherheitsfunktion zu erkennen oder zu verhindern.

# TUS Tool Usage Level

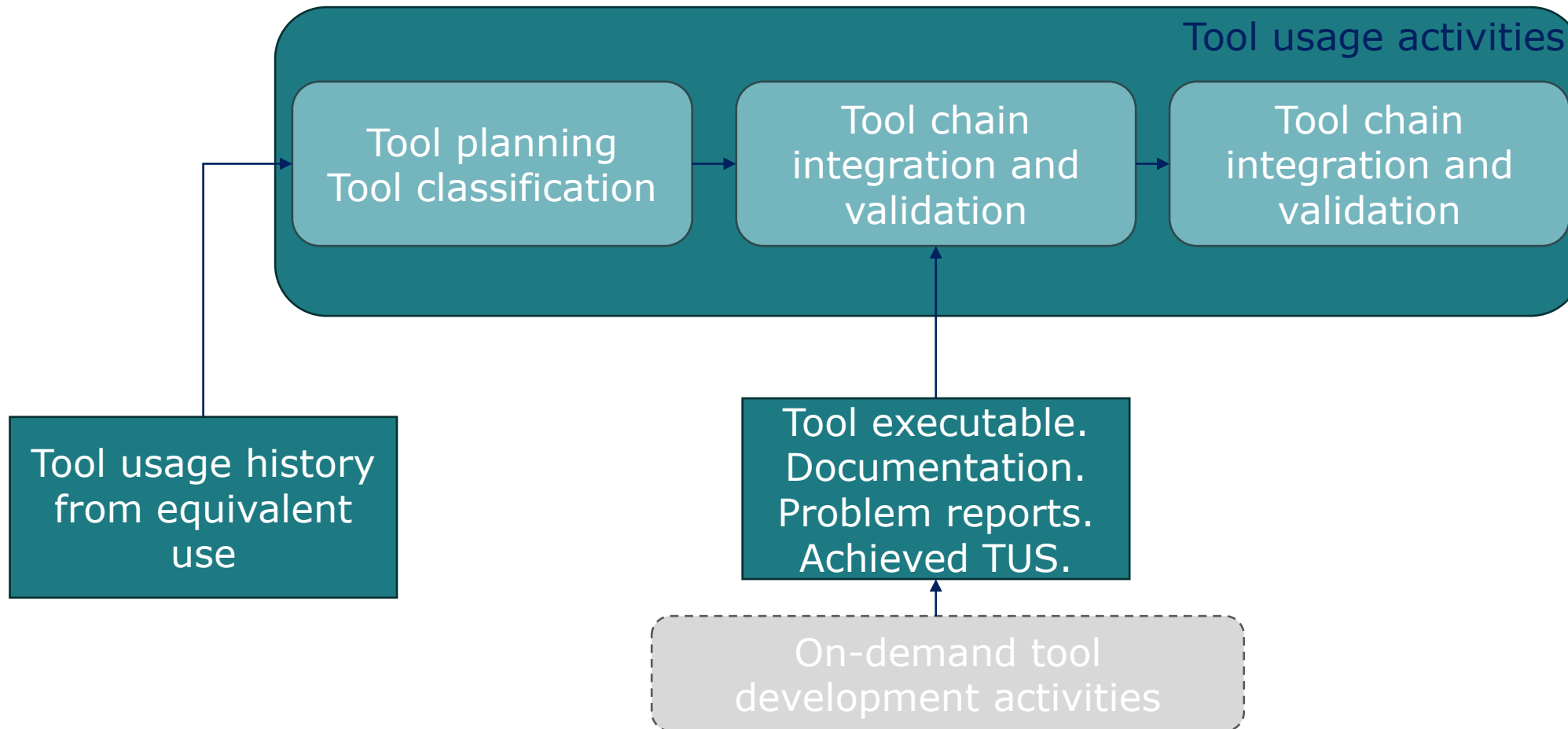
- Maßnahmen, die bei der Entwicklung des Werkzeuges entsprechend des Levels angewendet werden müssen.

| # | Required confidence data                                                                                                                                             | TUS 1 | TUS 2 | TUS 3 | TUS 4 |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-------|-------|
| 1 | Tool usage plan and classification (H.3.1, H.3.2)                                                                                                                    | HR    | HR    | HR    | HR    |
| 2 | Tool user documentation (H.3.3)                                                                                                                                      | HR    | HR    | HR    | HR    |
| 3 | Tool integration and assessment in usage context (H.3.4)                                                                                                             | R     | HR    | HR    | HR    |
| 4 | Tool configuration management in usage context (H.3.5)                                                                                                               | R     | HR    | HR    | HR    |
| 5 | Evidence of tool development for avoidance of systematic faults (H.4.1).<br>-Tool specifications and verification                                                    | PR    | R     | HR    | HR    |
| 6 | Evidence of tool development for avoidance of systematic faults (H.4.1).<br>-Architecture specification and verification<br>-Module design and testing with coverage | PR    | R     | R     | HR    |
| 7 | Evidence of confidence from tool usage history (H.4.2)                                                                                                               | R     | HR    | HR    | HR    |
| 8 | Tool problems management (H.4.3)                                                                                                                                     | R     | HR    | HR    | HR    |

# On demand tools (neu entwickelt)



# COTS (existierend)



Vielen Dank!

