



Simulink PLC Coder für sichere IEC 61131 Steuerungen bei MAGIRUS GmbH

Eine Fallstudie über die Verwendung, die Instrumentierung und die Anpassungen des Simulink PLC Coders für sichere und nicht sichere Steuerungssoftware bei MAGIRUS.

Kai Kriegl

Ulm - Germany

Dienstag, 26. Juni 2018



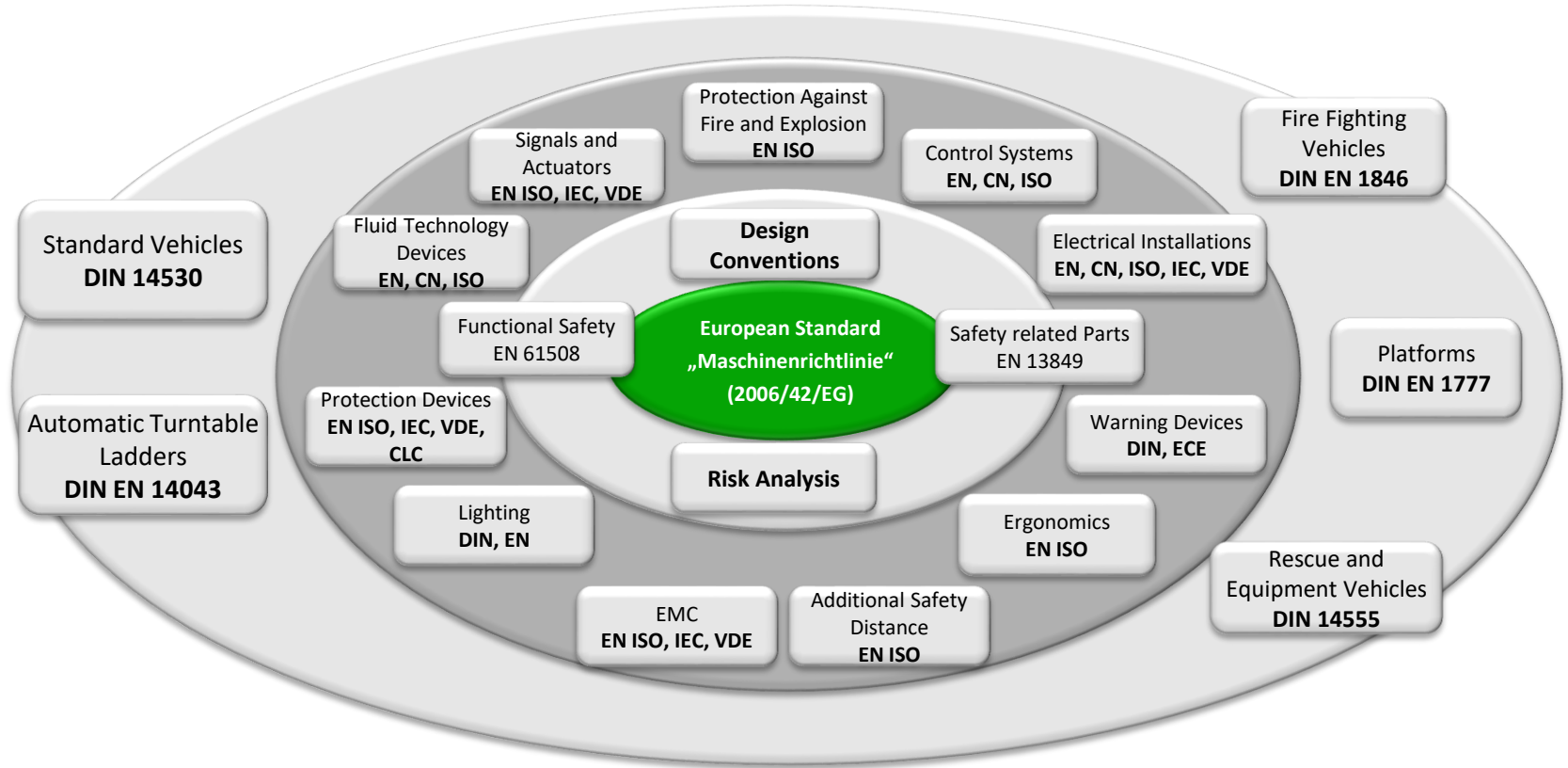
Kurze Einführung

MAGIRUS



Kurze Einführung

Normatives Umfeld



Simulink PLC Coder bei MAGIRUS

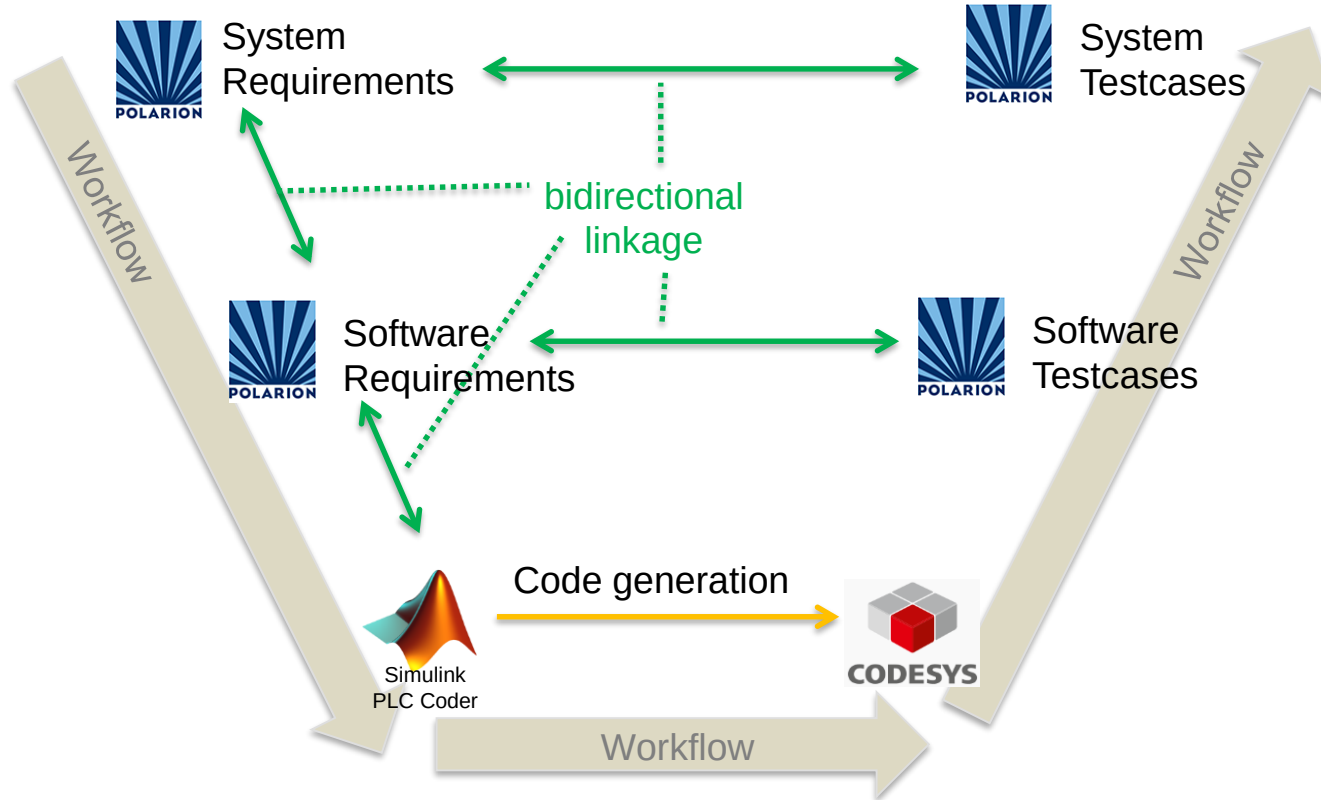
Agenda

- Kurze Einführung
- Toolchain bei MAGIRUS
 - Polarion, MATLAB, CODESYS
 - CoDeSys / DIN EN 61131
- Simulink PLC Coder
 - Simulink PLC Coder Einstellungen
 - Dokumentation im Model
 - Model-Advisor Checks
 - Safety Erweiterungen
- Software-Architektur
 - Schichtenmodell
 - ‚Input-Forcing‘ - ‚Output-Forcing‘
 - Zusammenfassung
- Testkonzept
- Fazit / Ausblick



Toolchain bei MAGIRUS

Polarion, MATLAB, CODESYS



- RTE in SIL2 Zertifizierung
 - EEPROM, I/O Handling Task-Hierarchien, Kommunikation
- IEC 61131 ist europäische Norm über Grundlagen der SPS Programmierung
 - LD Ladder Diagram
 - FBD Function Block diagram
 - IL Instruction List
 - **ST Structured Text**
- SIL2: Sicherheitsanforderungsstufe
 - SIL2 ist vergleich bar zu ASIL B/C

Simulink PLC Coder

Simulink PLC Coder Einstellungen

Target IDE

☒ Show full target list

Target IDE Path

PLCopen XML

3S CoDeSys 2.3

3S CoDeSys 3.3

3S CoDeSys 3.5

3S Automation 3

Target IDE Path

C:\Program Files\3S Software

Code Output Directory

plcsrc

☐ Generate testbench for subsystem

Auto-generated identifier naming rules —

Maximum identifier length: 63

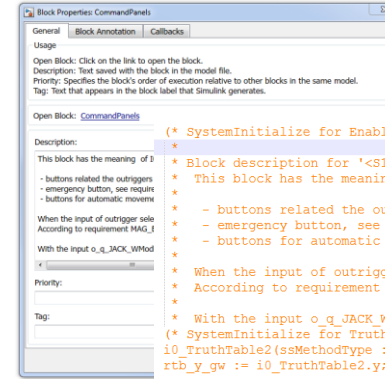
SPS spezifische Erweiterungen im ST-Code

ST-Code für SIL Tests in der Target IDE

Maximale Länge der Variablennamen

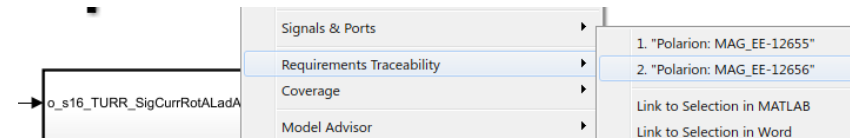
Block descriptions

Die DIN EN61508 verlangt nach einer Dokumentation der Funktionsblöcke auch im ST-Code



Requirements Traceability

Zur besseren Nachverfolgung, welches Requirement wie in MatLab / Simulink umgesetzt ist und wie der dazugehörige ST-Code aussieht, sollen auch die Requirement Links in den ST-Code übernommen werden.



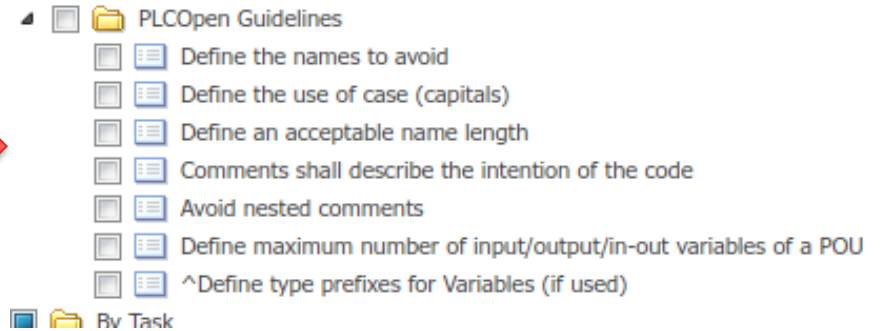
```
(* Outputs for Atomic SubSystem: '<S6>/MAG_EE-12655 // 12656' *)
*
* Block requirements for '<S6>/MAG_EE-12655 // 12656':
* 1. Polaron: MAG_EE-12655
* 2. Polaron: MAG_EE-12656 *)
(* Logic: '<S22>/Logical Operator' incorporates:
* Import: '<Root>/u16_TURR_LRPlgd_C'
* Import: '<Root>/u16_TURR_SwSPlgd_C'
* Logic: '<S22>/Logical Operator1' *)
rtb_RelationalOperator1_cj := (u16_TURR_LRPlgd_C <> 0) AND ( NOT (u16_TURR_SwSPlgd_C <> 0));
```


PLCopen - Technical Committee 5

Safety Software

Technical Specification

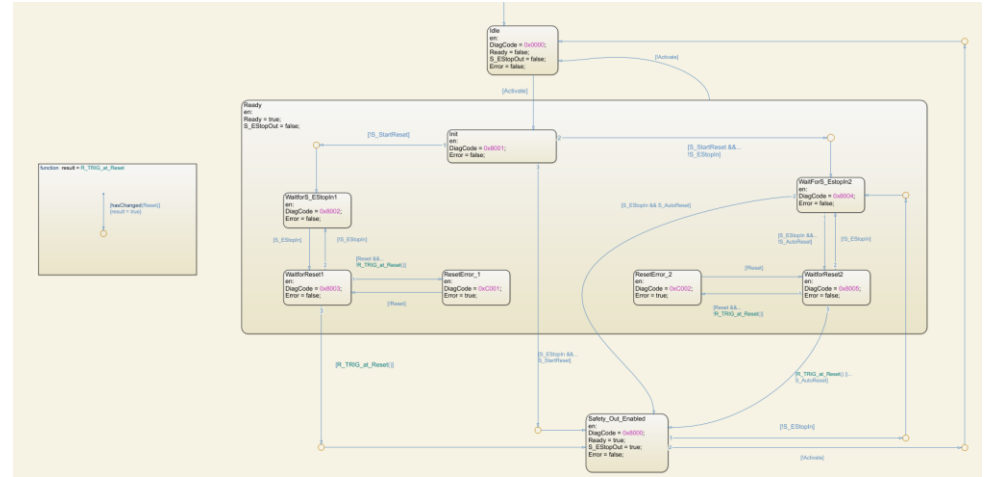
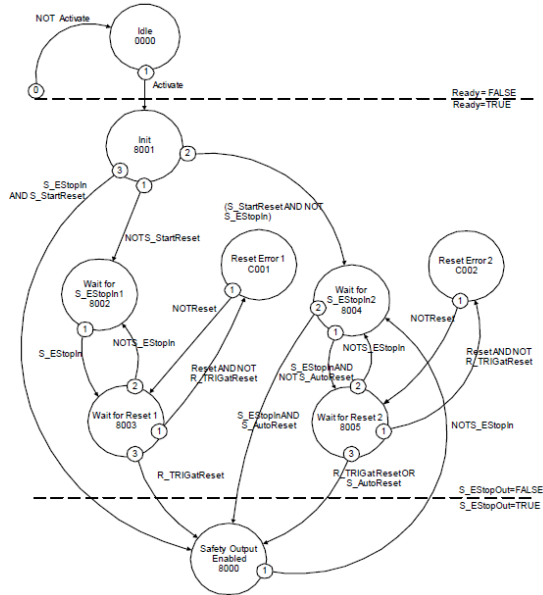
Part 1: Concepts and Function Blocks



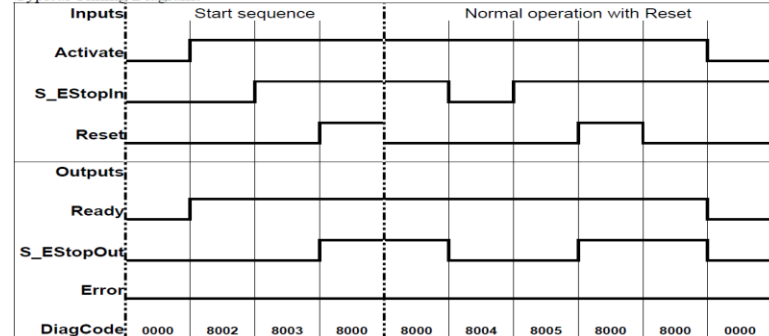
Model Advisor Checks für:

- Variablennamen
- Kommentare
- Verwendung von Schlüsselwörtern

6.4. Emergency Stop

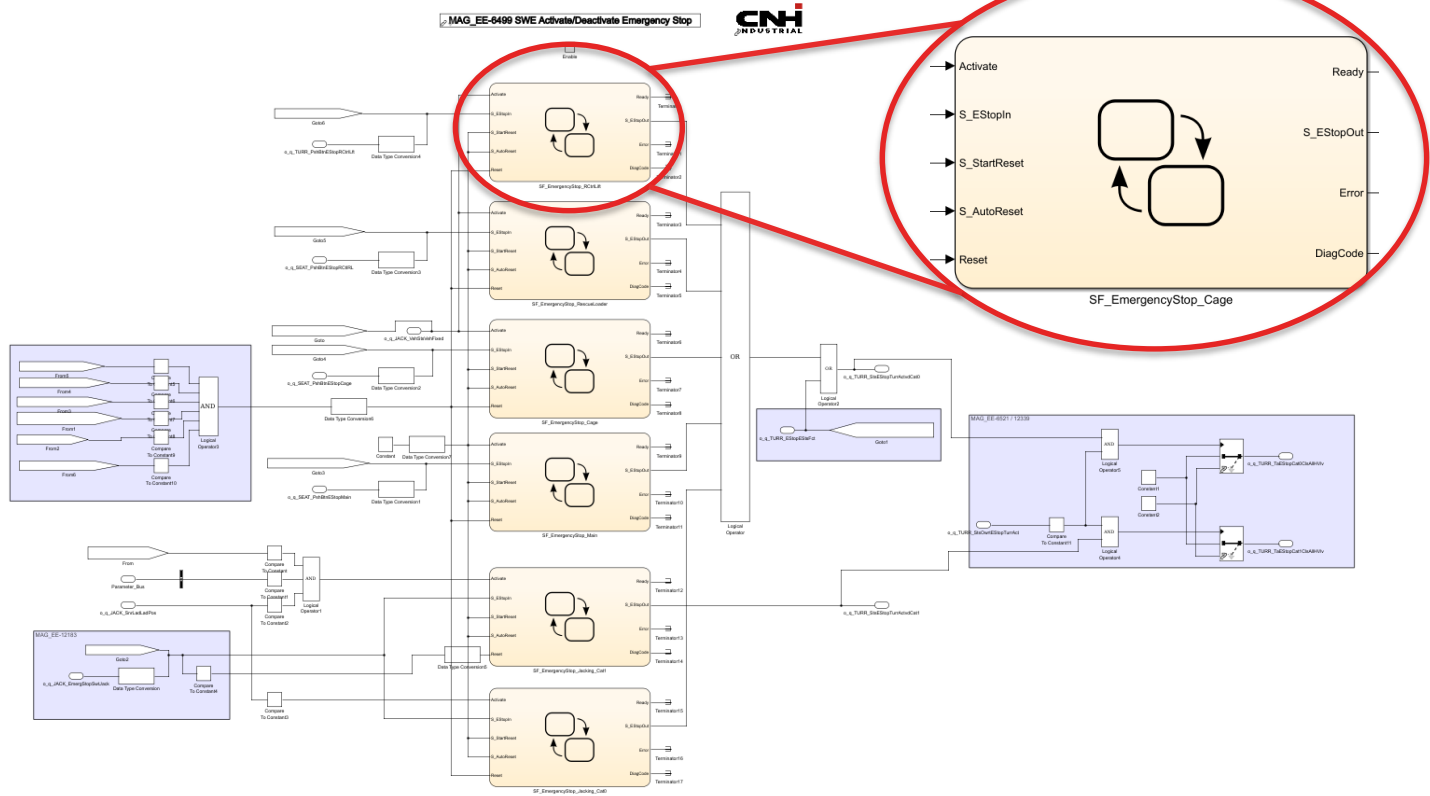


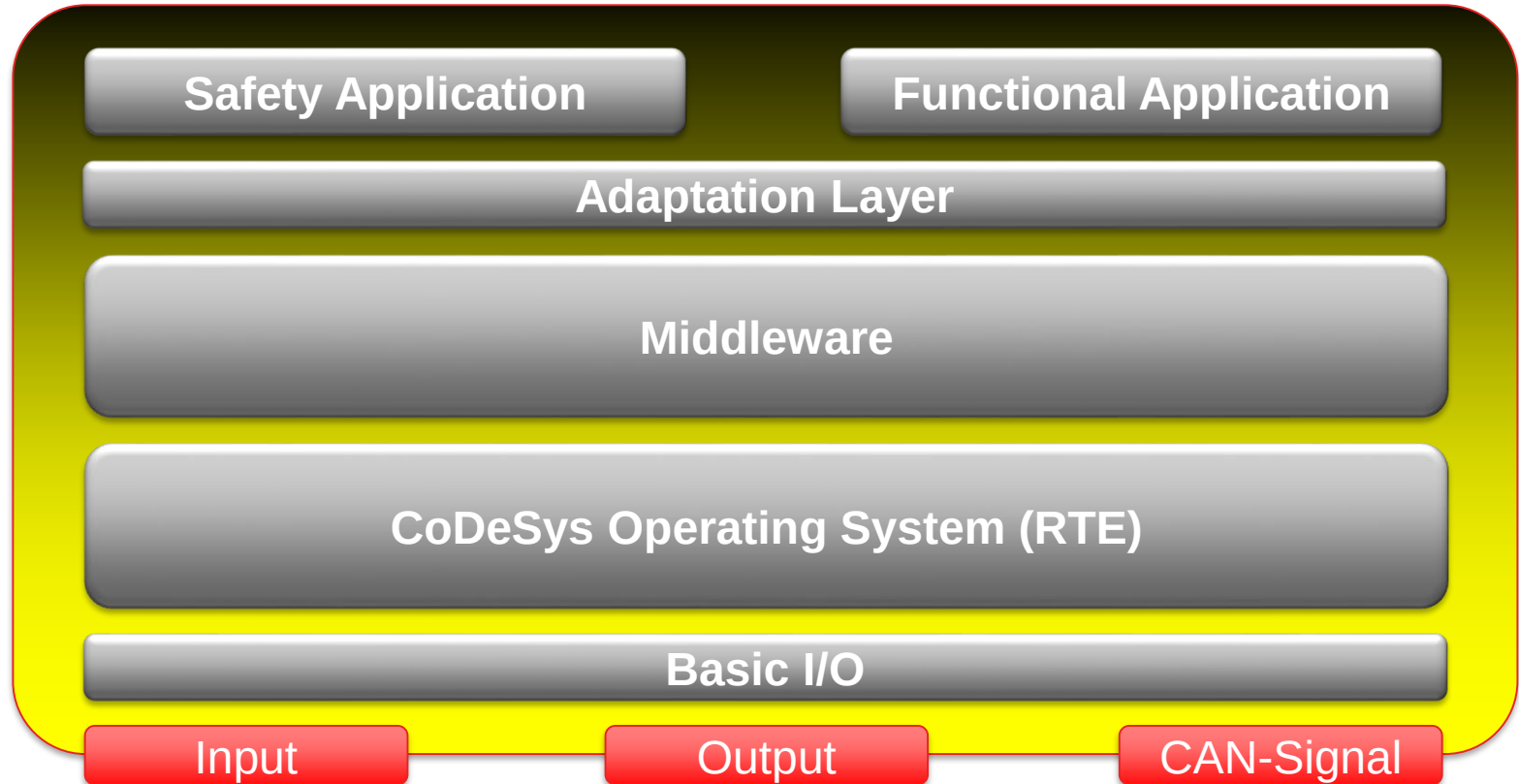
Typical Timing Diagrams



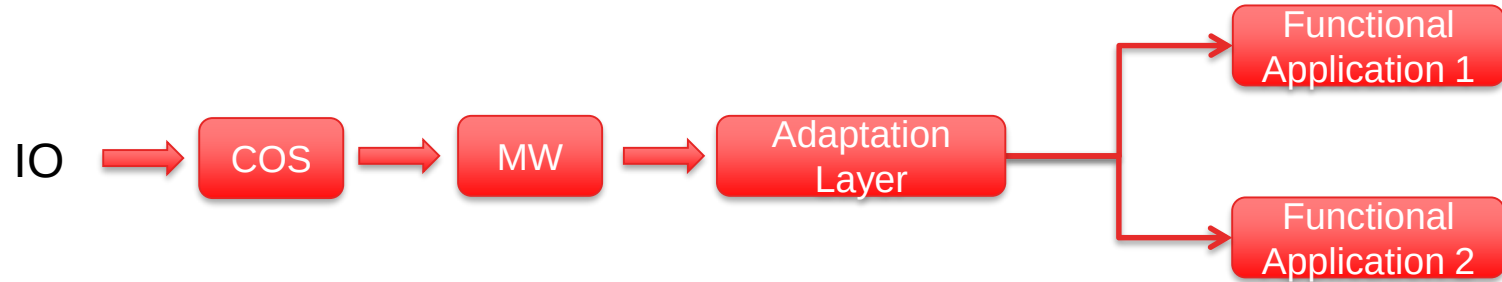
Simulink PLC Coder

Safety Erweiterungen

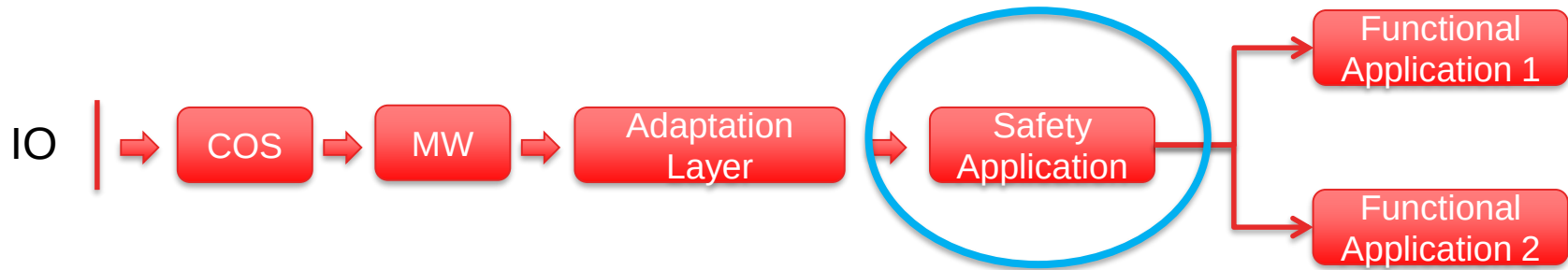




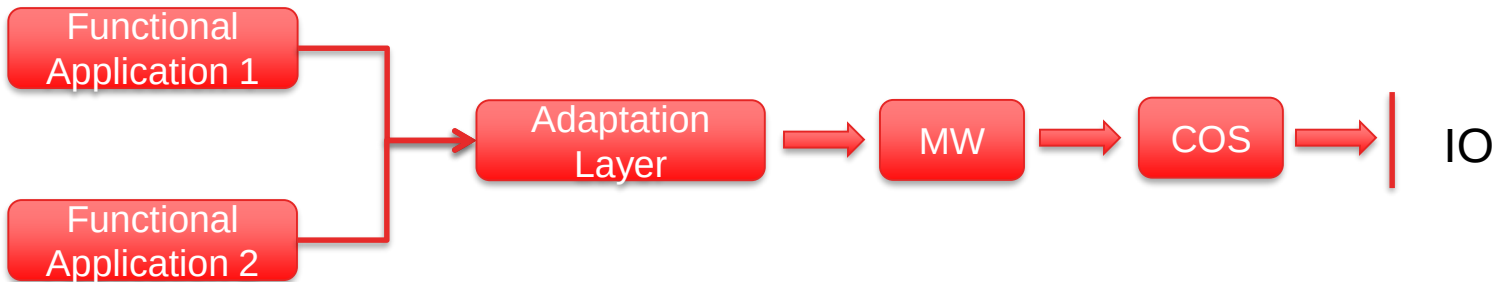
Allgemeine Funktionsweise:



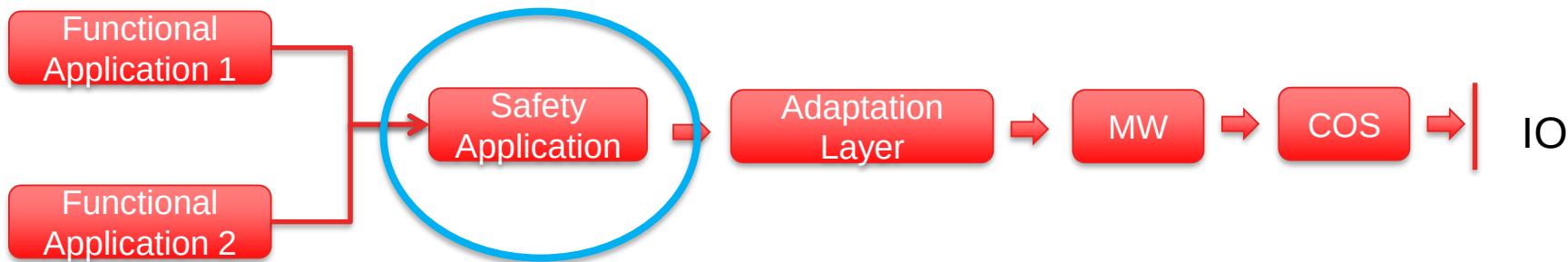
Funktionsweise bei sicheren Eingängen



Allgemeine Funktionsweise:

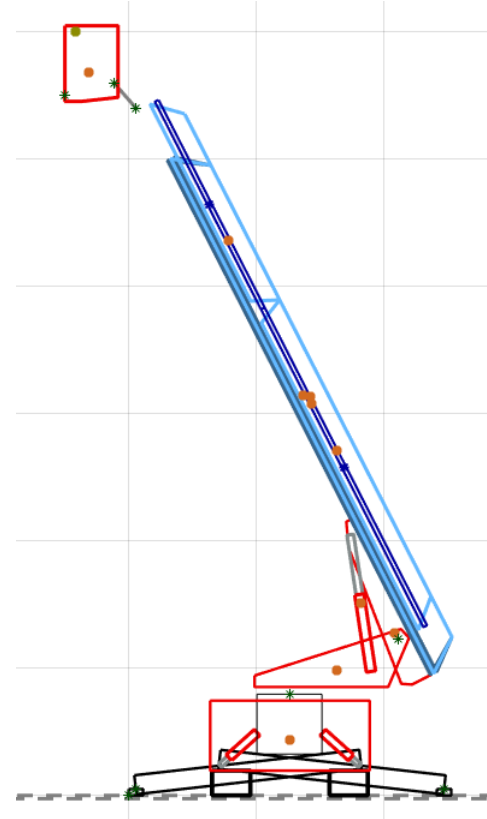


Funktionsweise bei sicheren Ausgängen

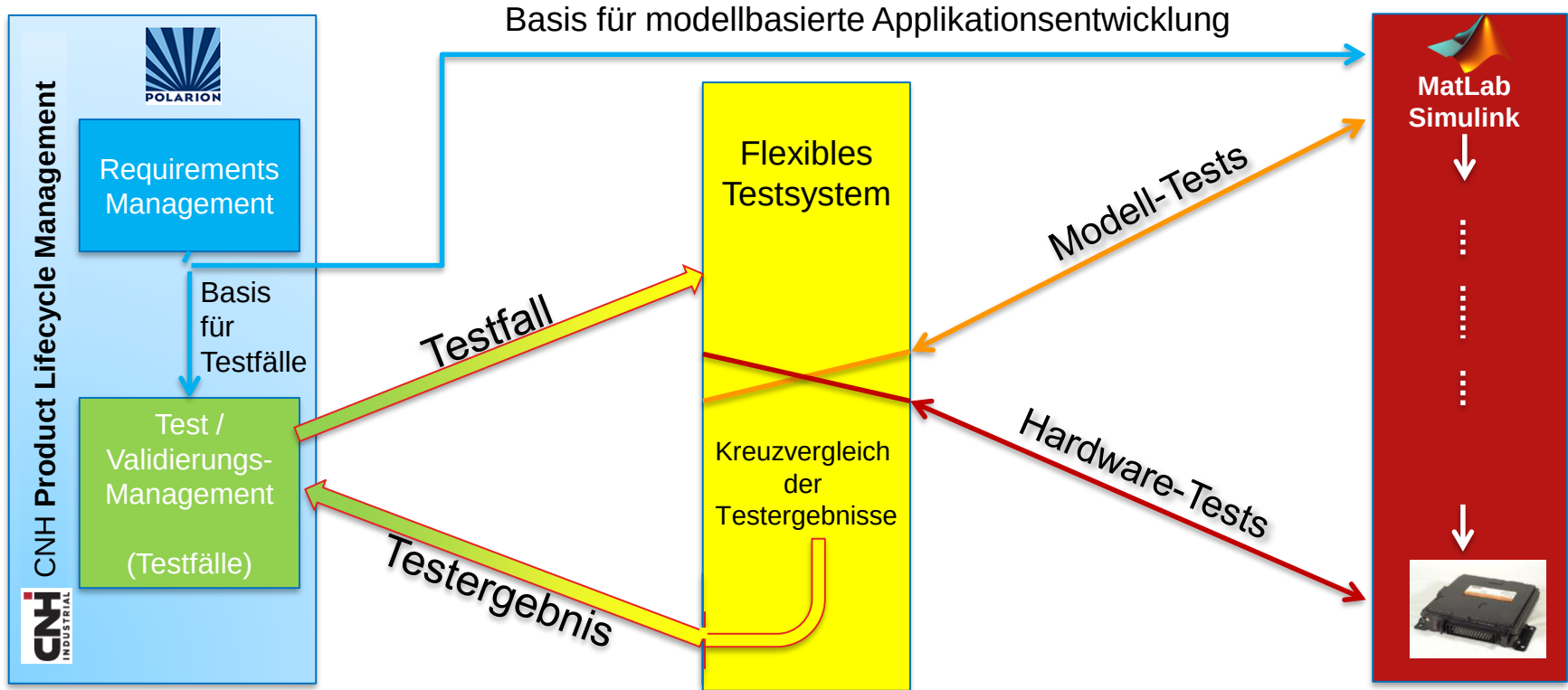


Software - Architektur

Zusammenfassung



Testkonzept



Testkonzept – 2

Vorteile für MAGIRUS:

- Entwicklungsgeschwindigkeit
- Entwicklungsteilung
- Unabhängigkeit vom Steuergerätehersteller
- Klar definierter Entwicklungsprozess

- Fortführung des Entwicklungsprozesses durch stückweise Testen der neuen Module
- MATLAB, Simulink und Simulink PLC Coder als Entwicklungswerkzeug gesetzt
- Kontinuierliche Weiterentwicklung des Simulink PLC Coders



**Vielen Dank
für
Ihre Aufmerksamkeit**