ORS VEDS Technisches Sicherheitskonzept

\_merged\_0

\_merged\_1

**Inhaltsverzeichnis**

*Please update the table of contents.*

# Einleitung

## Dokumentenstatus

​​

## Dokumentenzweck

## Dokumentenfreigabe

​​

​​

## Requirement Management Tool

​​

# Technisches Sicherheitskonzept VEDS

​​

## Sicherheitsarchitektur des VEDS

### Aufgabenverteilung im Sicherheitskonzept des VEDS

VEDS/VEDS-11768**VEDS-11768, Information,**Finalized**,**Inapplicable **- Aufgabenverteilung im Sicherheitskonzept**

In dem Bild [12.1-2- VEDS Sicherheitsarchitektur](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11550) erkennt man, dass zwei Steuergeräte sicherheitsbezogene Aufgaben für den Antrieb übernehmen; die DMU und die ICU.  
In beiden ECUs gibt es zum eigentlichen Funktions-Controller (DMU-APPC und ICU-MC) zusätzlich die Safety-Controller DMU-SC sowie ICU-SC. In den folgenden Kapiteln werden die jeweiligen Aufgaben der Safety-Controller im Sicherheitskonzept beschrieben.

​​

#### Aufgaben der DMU im Sicherheitskonzept

VEDS/VEDS-11554**VEDS-11554, Information,**Finalized**,**Inapplicable **- Aufgaben des DMU-SC im Sicherheitskonzept**

Der DMU-SC ist für die Einhaltung der im Antriebssystem geltenden Sicherheitsziele verantwortlich. Dazu wertet der DMU-SC parallel und unabhängig vom DMU-APPC alle Signale aus, die für die Bestimmung des Fahrwunsches, des Bremswunsches und des Fahrzeugzustands notwendig sind. Der DMU-SC gibt die Drehmomenterzeugung im Umrichter über ein sicherheitsgerichtetes Signal frei. Der DMU-SC überwacht das realisierte Moment und prüft in Abhängigkeit des Fahrzustands und der aufgrund Fahrwunsch, Bremswunsch und Fahrtrichtungswunsch zulässigen Momente, ob ein Sicherheitsziel gefährdet ist. Bei Verletzung eines Sicherheitszieles stellt der DMU-SC den sicheren Zustand her.

​​

#### Aufgaben der ICU im Sicherheitskonzept

VEDS/VEDS-11551**VEDS-11551, Information,**Finalized**,**Inapplicable **- Aufgaben des ICU-SC im Sicherheitskonzept**

Der ICU-SC unterstützt das Sicherheitskonzept, indem er das von dem Antriebsmotor erzeugte Drehmoment redundant und unabhängig von der Funktion des MC erfasst und sicher an den DMU-SC überträgt. Der ICU-SC überwacht alle für die Sicherheit relevanten Komponenten und lässt den Normalen Betrieb (MC steuert den Antriebsmotor über die Leistungselektronik an) nur zu, wenn die Integrität der sicherheitsrelevanten Komponenten sichergestellt ist.  
Der ICU-SC liest das Sicherheitsfreigabesignal vom DMU-SC ein und lässt keinen Betrieb zu wenn das Signal nicht entsprechend der Spezifikation detektiert wird.  
Bei Detektion, dass das Sicherheitsfreigabesignal entzogen wurde, leitet der ICU-SC eine Abschaltsequenz ein, die den Sicheren Zustand "Drehmomentfreiheit" herstellt. Zusätzlich wird nach Erreichen des Stillstands der Umrichter entladen, so dass im Zustand "Fail Safe" auch keine elektrische Gefährdung im Umrichter mehr besteht.

​​

## Zeitliche Anforderungen für das VEDS Sicherheitskonzept

### FHTI Drehmomentfreiheit des Antriebsstrangs

​​

​​

### FHTI Fahrerinformation Anfahren nicht möglich

​​

### FHTI PSU vom 24V-Bordnetz trennen

​​

## Anforderungen an die CAN-Kommunikation

### Sendebotschaften

VEDS/VEDS-12064**VEDS-12064, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Sendebotschaften mit Black Channel Concept absichern**

Das sendende Steuergerät von Botschaften mit sicherheitsrelevanten Inhalten muss diese über das Black Channel Concept absichern.

VEDS/VEDS-12065**VEDS-12065, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Counter für sichere Sendebotschaften**

Die Software jedes Senders einer sicheren Sendebotschaft muss für diese Botschaft einen eigenen unabhängigen Counter implementieren.

VEDS/VEDS-12066**VEDS-12066, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Checksumme für sichere Sendebotschaften**

Die Software jedes Senders einer sicheren Sendebotschaft muss die Checksumme über den Dateninhalt inklusive Counter und ggf. Teile des Identifiers berechnen.

VEDS/VEDS-12079**VEDS-12079, Information,**Finalized**,**Inapplicable **- Spezifikation Black Channel Concept**

Die Berechnungsvorschriften des Black Channel Concepts sind von CAN Netz zu CAN Netz unterschiedlich. Die Durchführungsvorschrift findet sich in der jeweiligen Spezifikation des jeweiligen CAN-Netzes.   
​​

### Empfangsbotschaften

VEDS/VEDS-12062**VEDS-12062, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Empfangsbotschaften mit Black Channel überprüfen**

Das empfangende Steuergerät muss über Black Channel Concept abgesicherte Empfangsbotschaften mit sicherheitsrelevanten Inhalten vor Verwendung auf korrekte Checksumme und plausible Counter überprüfen.

VEDS/VEDS-12067**VEDS-12067, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Verwerfen von Abgesicherten Botschaften mit Verletzungen des Black Channel Concept**

Die Software des empfangenden Steuergeräts darf die Inhalte von Nachrichten mit Fehlern in Checksumme oder Counter nicht verwenden.  
​​

VEDS/VEDS-12063**VEDS-12063, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Zyklische Empfangsbotschaften auf Timeout überprüfen**

Das empfangende Steuergerät muss zyklische Empfangsbotschaften auf Einhaltung der Zykluszeit überprüfen.

VEDS/VEDS-12081**VEDS-12081, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Verwerfen von Inhalten zyklischer Botschaften**

Die Software des empfangenden Steuergeräts darf die Inhalte einer Nachricht nach Ablauf deren Timeoutzeit nicht weiter verwenden.

VEDS/VEDS-12080**VEDS-12080, Information,**Finalized**,**Inapplicable **- Spezifikation Timeoutzeiten**

Die Timeout-Zeiten der einzelnen Botschaften sind in der Spezifikation des jeweilligen CAN-Netzes enthalten.  
​​

# Technisches Sicherheitskonzept DMU

​​

​​

**abgeleitete HWSRs:**

​​

## Sicherheitsmechanismen in der DMU

### Sichere Zustände der DMU

#### Sicherheitsfreigabe entziehen

​​

​​

**abgeleitete HWSRs:**

**abgeleitete SWSRs:**

​​

##### Anforderungen zur Vermeidung von Latentfehlern des Sicherheitsschalters

​​

**abgeleitete SWSRs:**

​​

​​

#### Fahrerinformation Anfahren nicht möglich

​​

​​

​​

**abgeleitete HWSRs:**

​​

**abgeleitete SWSRs:**

​​

### Ermittlung der Überwachungsgrößen für die Sicherheitsmechanismen (Safety Fault Use Case SFUC)

​​

#### Fahrzeugbewegungszustand

​​

​​

**abgeleitete SWSRs:**

​​

#### Sollmomentgrenzen

​​

##### Fahrwunschermittlung

​​

​​

**abgeleitete SWSRs:**

​​

##### Bremswunschermittlung

​​

​​

​​

##### Limitierungswunschermittlung

​​

​​

​​

##### Fahrtrichtungswunschermittlung

​​

​​

​​

##### Sollmomentgrenzenermittlung

​​

​​

​​

​​

#### Istdrehmoment

​​

​​

**abgeleitete SWSRs:**

​​

### SFUC Überwachungen

#### SFUC Logik

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC01

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC02

​​

​​

**abgeleitete SWSR:**

​​

​​

#### SFUC03

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC04

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC05

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC06

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC07

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC08

​​

​​

**abgeleitete SWSR:**

​​

#### SFUC09

​​

​​

**abgeleitete SWSR:**

​​

#### SFUC10

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC11

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC12

​​

​​

**abgeleitete SWSR:**

​​

#### SFUC13

​​

​​

**abgeleitete SWSRs:**

​​

#### SFUC14

​​

​​

**abgeleitete SWSRs:**

​​

## Sicherheitsintegrität der DMU

​​

### Controllerintegrität

​​

​​

​​

**abgeleitete HWSRs:**

​​

**abgeleitete SWSRs / Safety-Lib-Konfiguration:**

​​

# Technisches Sicherheitskonzept ICU

​​

## CAN-Kommunikation

**abgeleitete HWSRs:**

VEDS/VEDS-10870**VEDS-10870, Sol.-constr. Requirement,**In progress**,**ASIL=C **- CAN SC**

Der Safety Controller muss zwei CAN Schnittstellen bedienen.

VEDS/VEDS-11027**VEDS-11027, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Anzahl CAN Schnittstellen**

Die M302 Hardware muss zwei CAN-Schnittstellen zur Verfügung stellen.

### Sendebotschafen

VEDS/VEDS-12070**VEDS-12070, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Absichern der A1\_DIS\_SC**

Der ICU-SC muss die Botschaft A1\_DIS\_SC mit dem Black Channel Concept absichern.  
Die Berechnungsvorschrift ist dem Dokument "ROD VEDS CAN Interface Electric CAN.docx" zu entnehmen.

### Empfangsbotschaften

VEDS/VEDS-12071**VEDS-12071, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Timeout von Empfangsbotschaften**

Die ICU-SC Software muss die Botschaft A1\_DMU\_APPC auf Timeout überwachen.  
​​

## Zustände der ICU

VEDS/VEDS-11586**VEDS-11586, Information,**Finalized**,**Inapplicable **- Sichere Zustände der ICU**

Der ICU-SC ist in der Lage den Fahrmotor unabhängig vom ICU-MC drehmomentfrei zu machen. Der ICU-SC ist ebenfalls in der Lage, die elektrische Sicherheit innerhalb des Umrichters DIS herzustellen und zu überwachen, solange sich der Fahrmotor nicht dreht. Für die Funktionale Sicherheit und das Erreichen des sicheren Zustands "Drehmomentfreiheit am Antriebsstrang" kann der ICU-SC direkt die Leistungselektronik des Umrichters und ein DC-Schütz ansteuern.  
Als funktional Sicherer Zustand wird hier angenommen, dass alle Abschaltelemente des ICU-SC so angesteuert werden oder worden sind, dass der Fahrmotor drehmomentfrei ist.

VEDS/VEDS-11813**VEDS-11813, Information,**Finalized**,**Inapplicable **- Zustandsübergangsdiagramm ICU-SC**

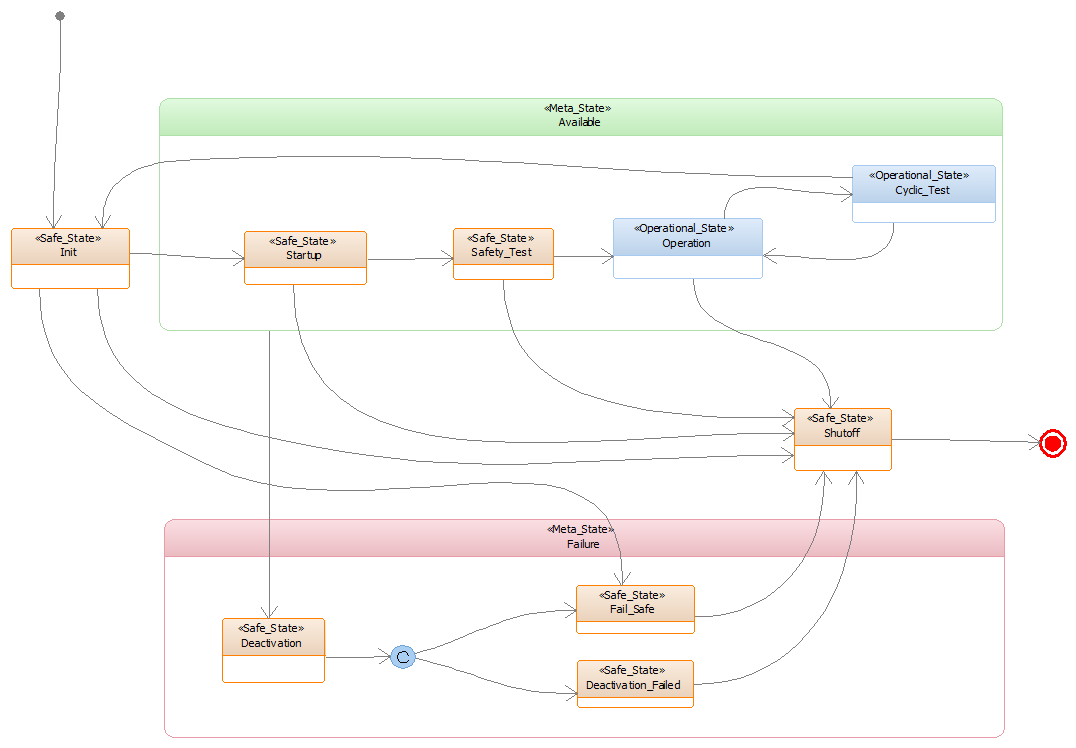
[](http://hdhapppolarion/polarion/wi-attachment/VEDS/VEDS-11813/2-SC_Statechart.png?revision=51256)

Figure 1 Zustandsübergangsdiagramm SC

​​

VEDS/VEDS-11896**VEDS-11896, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Zustände des SC**

Der ICU SC muss auf dem CAN die folgenden internen Zustände melden:  
Sichere Zustände:

* INIT
* STARTUP
* SAFETY\_TEST
* DEACTIVATION
* FAIL\_SAFE
* DEACTIVATION\_FAILED
* SHUTOFF

Zustände im Betrieb:

* OPERATION
* CYCLIC\_TEST

Diese Zustände zeigen den anderen beteiligten Steuergeräten den Zustand des ICU-SC an.  
​​

VEDS/VEDS-11894**VEDS-11894, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sicherer Zustand INIT**

Im Zustand INIT lädt der ICU-SC die Software und nimmt seine eigene Peripherie in Betrieb.  
Die externen Controllerbausteine IWDT und Resolverchip PGA werden konfiguriert und in Betrieb genommen.  
Der ICU-SC startet in diesem Zustand alle Überwachungen:

* [2VEDS-11180- Einlesen KL15 an Analogeingang](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11180)
* [3VEDS-11603- Überwachung des Sicherheitsfreigabesignals](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11603)
* [4VEDS-11778- Synchrone Erfassung der Motorströme](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11778)
* [5VEDS-11780- Resolverlage synchron zum INHIBIT Signal](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11780)
* [6VEDS-11598- Drehmomenterfassung des Fahrmotors](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11598)
* [7VEDS-11991- Ermittlung der Drehzahl des Fahrmotors](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11991)
* [8VEDS-11795- Plausibilisierung des DC Schütz Hauptkontakts](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11795)
* [9VEDS-11819- Überwachung der Versorgungsspannungen für Resolver und Strommessung](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11819)
* [10VEDS-11897- Überwachung der Spannung am Hauptkontakt des Schützes](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11897)

In diesem ersten Zustand sind alle Freigaben nicht gewährt und das DC-Schütz wird nicht angesteuert.

VEDS/VEDS-11895**VEDS-11895, Sol.-constr. Requirement,**Finalized**,**Inapplicable **- Sicherer Zustand STARTUP**

Im Zustand STARTUP schließt der ICU-SC das DC-Schütz. Hierzu kann kurzzeitig der Bremswiderstand eingeschaltet werden um Spannung im Zwischenkreiskondensator abzubauen.  
Die Startup-Sequenz wird nur gestartet, wenn im System keine Integritätsverletzungen vorliegen, die Drehzahl des Fahrmotors Stillstand entspricht und das Klemme 15 Signal HIGH ist.  
  
  
Die Freigabe für den Fahrmotor wird in diesem Zustand nicht gewährt.  
​​

VEDS/VEDS-11906**VEDS-11906, Sol.-constr. Requirement,**Finalized**,**Inapplicable **- Sicherer Zustand SAFETY\_TEST**

Im Zustand SAFETY\_TEST prüft der ICU-SC die Abschaltpfade. Der Einfluss auf die Freigabe für den Bremswiderstand wird geprüft. Danach wird das Schalten des DC-Schützes sowie alle Signale zur Plausibilisierung des DC-Schützes getestet.  
Der SAFETY\_TEST folgt direkt auf die STARTUP Sequenz und kann nicht unterbrochen werden.  
Während des Zustands SAFETY\_TEST dürfen keine Integritätsverletzungen vorliegen, die Drehzahl des Fahrmotors muss Stillstand entsprechen und das Klemme 15 Signal muss HIGH sein.  
  
Die Freigabe für den Fahrmotor bleibt während des SAFETY\_TEST nicht gewährt.  
​​

VEDS/VEDS-12127**VEDS-12127, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Betriebszustand OPERATION**

Im Zustand OPERATION sind alle Überwachungen aktiv und keine Integritätsverletzungen detektiert. Die Freigaben sind gewährt so dass der ICU-MC den Fahrmotor und den Bremswiderstand ansteuern kann

VEDS/VEDS-12128**VEDS-12128, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Betriebszustand CYCLIC\_TEST**

Im Zustand CYCLIC\_TEST sind alle Überwachungen aktiv und keine Integritätsverletzungen detektiert. Die Freigaben sind nicht gewährt. Die ICU-SC Software testet in diesem Zustand ob das DC-Schütz geöffnet werden kann.  
​​

VEDS/VEDS-11904**VEDS-11904, Sol.-constr. Requirement,**Finalized**,**Inapplicable **- Sicherer Zustand DEACTIVATION**

Im Zustand DEACTIVATION wird die sicherheitsgerichtete Abschaltung des Antriebsstrangs mit Ziel der Drehmomentfreiheit hergestellt. Im Zustand DEACTIVATION wird der Zwischenkreis des DIS entladen, wenn das Fahrzeug zum Stillstand gekommen ist, um eine elektrische Gefährdung im Umrichter auszuschließen.  
  
Die Freigabe für Bremswiderstand ist entzogen solange sich das Fahrzeug noch bewegt und das DC-Schütz wird geöffnet. Je nach Drehzahl des Fahrmotors bleibt die Freigabe für die Motorpulse gewährt und es kann auch noch Spannung im Zwischenkreis vorliegen.

VEDS/VEDS-12125**VEDS-12125, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sicherer Zustand FAIL\_SAFE**

Wenn die funktionale Sicherheit und die elektrische Sicherheit hergestellt werden konnte nachdem eine Shutoff Sequenz durchlaufen wurde, wird der Zustand FAIL\_SAFE eingenommen.

VEDS/VEDS-12126**VEDS-12126, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sicherer Zustand DEACTIVATION\_FAILED**

Wenn eine Shutoff Sequenz durchlaufen wurde und mindestens eine Aktion nicht erfolgreich durchgeführt werden konnte, die ggf. die Funktionale oder Elektrische Sicherheit gefährdet, wird der Zustand DEACTIVATION\_FAILED eingenommen.  
​​

VEDS/VEDS-11905**VEDS-11905, Sol.-constr. Requirement,**Finalized**,**Inapplicable **- Sicherer Zustand SHUTOFF**

Im Zustand SHUTOFF wird die Abschaltung des Umrichters durchgeführt. Wenn das Fahrzeug zum Stillstand gekommen ist und das Klemme 15 Signal LOW ist, wird der Zustand SHUTOFF eingenommen. Um eine elektrische Gefährdung im Umrichter auszuschließen wird vor Abschaltung der Versorgungsspannung der Zwischenkreis entladen.  
  
Die Freigabe für die Motorpulse ist entzogen und das DC-Schütz wird geöffnet. Der Zwischenkreis wird über den Bremswiderstand entladen.  
​​

VEDS/VEDS-12096**VEDS-12096, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Zustände des ICU-SC**

Der ICU-SC muss den Zustandsautomat und folgende Zustände wie beschrieben umsetzen:

* [11VEDS-11894- Sicherer Zustand INIT](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11894)
* [12VEDS-11895- Sicherer Zustand STARTUP](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11895)
* [13VEDS-11906- Sicherer Zustand SAFETY\_TEST](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11906)
* [14VEDS-12127- Betriebszustand OPERATION](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12127)
* [15VEDS-12128- Betriebszustand CYCLIC\_TEST](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12128)
* [16VEDS-11904- Sicherer Zustand DEACTIVATION](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11904)
* [17VEDS-12125- Sicherer Zustand FAIL\_SAFE](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12125)
* [18VEDS-12126- Sicherer Zustand DEACTIVATION\_FAILED](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12126)
* [19VEDS-11905- Sicherer Zustand SHUTOFF](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11905)
* [20VEDS-11813- Zustandsübergangsdiagramm ICU-SC](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11813)
* [21VEDS-11825- Sequenzdiagramm Abschaltsequenz](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11825)
* [22VEDS-11827- Sequenzdiagramm Shutoffsequenz](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11827)
* [23VEDS-11883- Sequenzdiagramm Startup und Safety Test](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11883)
* [24VEDS-11886- Sequenzdiagramm zyklischer Schütz Test](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11886)

### Drehmomentfreiheit am Antriebsstrang herstellen

VEDS/VEDS-11587**VEDS-11587, Information,**Finalized**,**Inapplicable **- Abschaltung aller Energiesenken**

Das Sicherheitsziel "Drehmomentfreiheit am Antriebsstrang herstellen" wird vom ICU-SC unabhängig von der aktuellen Drehzahl und dem aktuell anliegenden Moment (antreibend oder bremsend) hergestellt. Während des Antreibens ist der Fahrmotor die Energiesenke für die Elektrische Energie, während bei einer elektrischen Bremsung als Energiesenken für die Elektrische Energie die Fahrzeugbatterie, die Nebenverbraucher und der Bremswiderstand des Umrichters in Frage kommen. Um den Energiefluss zu unterbrechen, werden durch den ICU-SC alle Energiesenken abgeschaltet. Um alle Energiesenken abzuschalten, wird das DC-Schütz geöffnet und der Bremswiderstand abgeschaltet. Somit kann weder elektrische Energie in weiteres Moment an der Antriebswelle gewandelt werden, noch mechanische Energie durch eine drehende Maschine in elektrische Energie umgesetzt werden.  
Abhängig von der Drehzahl bei der Abschaltung werden die Leistungshalbleiter des Fahrmotors abgeschaltet, um ein stromloses Öffnen des DC-Schützes zu ermöglichen. Das ist der Fall bei niedrigen Drehzahlen, wenn die induzierte Spannung im Stator des Fahrmotors kleiner als die Batteriespannung ist. Bei einer Abschaltung bei höheren Drehzahlen wird der Fahrmotor in den Zwischenkreis zurückspeisen, wenn er nicht angesteuert wird. Daher wird in diesem Betriebszustand die Ansteuerung der Halbleiter des Motors nicht unterbrochen bevor das DC-Schütz geöffnet hat. Dadurch kann der Strom durch das DC-Schütz beim Öffnen in vielen Fällen minimiert werden. Da keine Elektrische Energie mehr gewandelt werden kann, wird der Fahrmotor in der Folge drehmomentfrei. Hinweis: Bei hohen Drehzahlen verbleibt durch Verluste in der Maschine ein geringes generatorisches Moment an der Welle.

VEDS/VEDS-11588**VEDS-11588, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Abschaltung der Energiesenke Fahrmotor**

Der ICU-SC muss die Energiesenke Fahrmotor sicher abschalten.

VEDS/VEDS-11589**VEDS-11589, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Abschaltung der Energiesenke Batteriespeicher**

Der ICU-SC muss die Energiesenke Batteriespeicher sicher abschalten.

VEDS/VEDS-11590**VEDS-11590, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Abschaltung der Energiesenke Bremswiderstand**

Der ICU-SC muss die Energiesenke Bremswiderstand sicher abschalten.

VEDS/VEDS-11986**VEDS-11986, Information,**Finalized**,**Inapplicable **- Abschaltung Bremswiderstand**

Um den Bremswiderstand abzuschalten, entzieht der ICU-SC die Freigabe für den Leistungshalbleiter des Bremschoppers. Es fließt kein Strom im Bremswiderstand. Der Fahrmotor wird abgeregelt solange die Regelung des Motorcontrollers noch funktioniert. Bei abgeschalteten oder defekten Leistungshalbleitern und hoher Drehzahl des Fahrmotors wird der Zwischenkreis soweit aufgeladen, dass keine Energie mehr vom Fahrmotor in den Zwischenkreis gespeist wird. Ein ungesteuertes bremsendes Moment wird somit vermieden.

**abgeleitete SWSRs:**

VEDS/VEDS-11592**VEDS-11592, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Entziehen der Freigabe der Leistungshalbleiter des Fahrmotors**

Die ICU-SC Software muss im Falle einer Abschaltsequenz die Freigabe der Leistungshalbleiter für die drei Phasen des Fahrmotors entziehen, wenn die aktuelle Drehzahl des Fahrmotors kleiner ist als die Rückspeisegrenze bei der aktuellen Zwischenkreisspannung.

VEDS/VEDS-11593**VEDS-11593, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Abschaltung des DC-Schützes**

Die ICU-SC Software muss im Falle einer Abschaltsequenz den DC-Schütz abschalten.  
​​

VEDS/VEDS-11591**VEDS-11591, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Entziehen der Freigabe des Leistungshalbleiters des Bremschoppers**

Die ICU-SC Software muss im Falle einer Abschaltsequenz die Freigabe des Leistungshalbleiters des Bremschoppers entziehen.

**abgeleitete HWSRs:**

VEDS/VEDS-10978**VEDS-10978, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Ansteuerung DC-Relais durch SC**

Der SC muss das DC-Relais ansteuern

VEDS/VEDS-11039**VEDS-11039, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Ansteuerung DC-Relais durch SC**

Das DC-Relais muss vom Sicherheitsrechner angesteuert werden

VEDS/VEDS-11252**VEDS-11252, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Ansteuerung des Bremswiderstand durch den SC sicher abschalten**

Der SC muss das Ansteuersignal des MC an den BR unterbrechen und den BR sicher abschalten können.  
Die Abschaltung des Ansteuersignals vom MC an den BR muss durch den SC in einer speziellen Hardwareschaltung (z.B. Gatterlogik) erfolgen.  
  
Hinweis: Die Abschaltung des BR ist sicherheitsrelevant im Rahmen der FuSi (Drehmomentfreiheit herstellen durch abschalten der Energiesenken)

VEDS/VEDS-11187**VEDS-11187, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Freigabe Bremswiderstand durch SC**

Der SC muss das Ansteuersignal des MC an den BR durch das Signal "SafetyEnableBR" unterbrechen und den BR sicher abschalten können.

VEDS/VEDS-11186**VEDS-11186, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Freigabe Motor-Ansteuerpulse durch SC**

Der SC muss die Motor-Ansteuerpulse des MC mit dem Signal "EnableMotorPulses" abschalten können.

VEDS/VEDS-11251**VEDS-11251, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Motor-Ansteuerpulse durch den SC unterbrechen**

Der SC muss die Motor-Ansteuerpulse des MC abschalten können.  
  
Hinweis:  
Während Startup und Systemtest sperrt der SC die Motor-Pulse des MC solange, bis getestet ist, dass das DC-Schütz funktioniert. Dies stellt keine Sicherheitsfunktion dar (nur QM).

### Erfassung des Sicherheitsfreigabesignals

VEDS/VEDS-11602**VEDS-11602, Information,**Finalized**,**Inapplicable **- Sicherheitsfreigabesignal**

Das Sicherheitsfreigabesignal dient im Sicherheitskonzept als dedizierter Abschaltpfad, mit dem die DMU den sicheren Zustand "Drehmomentfreiheit im Antriebsstrang herstellen" anfordern kann. Wenn das Sicherheitsfreigabesignal vom ICU-SC nicht (mehr) detektiert wird, leitet die Software die Abschaltsequenz ein. Die Reaktion erfolgt unmittelbar ohne Toleranzzeit in der Software. Das Signal wird als gültig erkannt, wenn ein bestimmter Signalpegel (24V) als auch eine bestimmte Frequenz (50 Hz) und Tastverhältnis (50%) eingehalten werden. In allen anderen Fällen wird das Signal als nicht korrekt eingestuft und in der Folge die Erzeugung von Drehmomenten durch den Umrichter sicher verhindert.

VEDS/VEDS-11603**VEDS-11603, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Überwachung des Sicherheitsfreigabesignals**

Der ICU-SC muss das Sicherheitsfreigabesignal überwachen und bei nicht korrekt anliegendem Signal die Abschaltsequenz durchführen.  
​​

VEDS/VEDS-11611**VEDS-11611, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachung der Schaltfrequenz des Sicherheitsfreigabesignals**

Die ICU-SC Software muss die Flanken des Sicherheitsfreigabsignals überwachen. Das Signal ist gültig, wenn mindestens 3 mal in Folge aufeinanderfolgende Flanken detektiert werden, die innerhalb von minimal 8,5 ms bis maximal nach 12 ms nach der vorherigen erfolgen.

VEDS/VEDS-11612**VEDS-11612, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Unerwartete Flanke detektiert**

Wenn die ICU-SC Software eine Flanke des Sicherheitsfreigabesignals detektiert, die weniger als 8,5 ms nach der vorherigen Flanke erfolgt (zu hohe Frequenz, falsches Tastverhältnis, gestörtes Signal), wird das Sicherheitsfreigabesignal als ungültig eingestuft.

VEDS/VEDS-11613**VEDS-11613, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Keine Flanke detektiert**

Wenn die ICU-SC Software nach mehr als 12 ms nach der vorangegangenen Flanke keine folgende Flanke detektiert (zu niedrige Frequenz, falsches Tastverhältnis, ausbleibendes Signal), wird das Sicherheitsfreigabesignal als ungültig eingestuft.  
​​

**abgeleitete HWSRs:**

VEDS/VEDS-11141**VEDS-11141, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Schaltung Externe Sicherheitsfreigabe (STO)**

Die M302 muss eine Schaltung zur Auswertung der Externen Sicherheitsfreigabe (Safety Torque Off - STO) bereitstellen und die Signalinformation an den SC bereitstellen.

VEDS/VEDS-11243**VEDS-11243, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Beeinflussung Signal**

Das Stromsignal der Externen Sicherheitsfreigabe darf auf der M302 nicht auf Masse geführt werden  
  
Hinweis:  
Auf der DMU existiert eine Masseschalter, der den Stromfluss unterbrechen können muss

​​

### Abschaltsequenz

VEDS/VEDS-11988**VEDS-11988, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Abschaltsequenz**

Der ICU-SC muss die Abschaltsequenz durchlaufen wenn das Sicherheitsfreigabesignal entzogen wird oder eine sonstige erkannte Integritätsverletzung dies erfordert.

VEDS/VEDS-11989**VEDS-11989, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Reaktionszeit**

Die ICU-SC Software muss bei ungültigem Sicherheitsfreigabesignal und bei erkannter Integritätsverletzung unverzüglich mit der Abschaltsequenz beginnen.  
​​

VEDS/VEDS-11825**VEDS-11825, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sequenzdiagramm Abschaltsequenz**

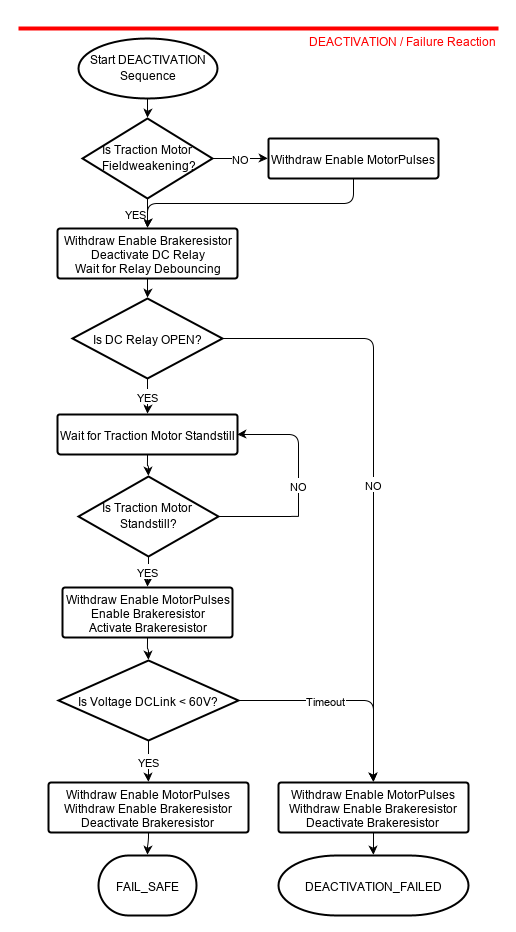
Die ICU-SC Software muss die Abschaltsequenz nach folgendem Schema umsetzen.  
[](http://hdhapppolarion/polarion/wi-attachment/VEDS/VEDS-11825/1-diagram_20190729-1334.53450.mxg.png?revision=48611)

Figure 2 Deactivation Sequence

### Shutoffsequenz

VEDS/VEDS-11828**VEDS-11828, Information,**Finalized**,**Inapplicable **- Shutoff**

Wenn das Klemme 15 Signal nach dem Debouncing (Entprellen) vom SC als LOW detektiert wird, die Abschaltung über das CAN Signal ShutoffClearance gewährt wird und sich das Fahrzeug im Stillstand und einem der Zustände INIT, STARTUP, SAFETY\_TEST, OPERATION, FAIL\_SAFE oder DEACTIVATION\_FAILED befindet, wird der Zustand Shutdown betreten, in dem das System außer Betrieb genommen wird und die Umrichterplatine ICU inklusive aller Umrichterkomponenten abschaltet. Nachdem der Sichere Zustand hergestellt ist und der Zwischenkreis entladen wurde, schickt der SC an den IWDT das Kommando "Go to STANDBY". Der IWDT bringt im Zustand STANDBY den SC in den Reset. Der MC wird zusätzlich über das SS1 Signal des IWDTs über die Abschaltung informiert. Der IWDT schaltet alle Versorgungsspannungen ab. Dadurch wird auch die Spannungsversorgung des MC abgeschaltet.   
​​

VEDS/VEDS-12072**VEDS-12072, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Shutoffsequenz**

Die ICU-SC Software muss die Shutoffsequenz nach der folgenden Sequenz umsetzen:  
[25VEDS-11827- Sequenzdiagramm Shutoffsequenz](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11827)

VEDS/VEDS-11827**VEDS-11827, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sequenzdiagramm Shutoffsequenz**

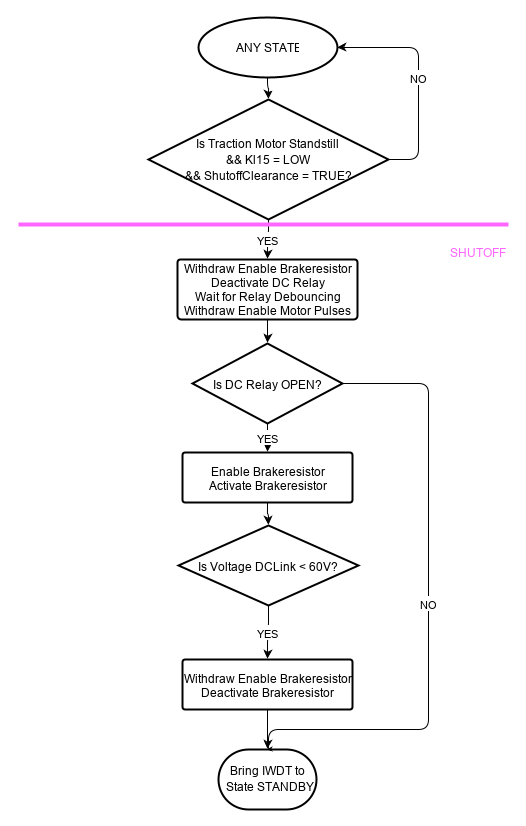
Die ICU-SC Software muss die Shutoffsequenz nach folgendem Sequenzdiagramm umsetzen.  
[](http://hdhapppolarion/polarion/module-attachment/VEDS/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept/diagram_20190729-1619.01090.mxg.png?revision=62965)

Figure 3 Shutoff Sequence

**abgeleitete HWSRs:**

VEDS/VEDS-11180**VEDS-11180, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Einlesen KL15 an Analogeingang**

Der SC muss das Klemme 15 Signal an einem Analogeingang einlesen.  
  
***Hinweis:***  
 *Ein Analogeingang ist erforderlich, um den Signalpegel zu plausibilisieren.*

​​

## Überwachungen in der ICU

VEDS/VEDS-11594**VEDS-11594, Information,**Finalized**,**Inapplicable **- Überwachungen durch den ICU-SC**

Der ICU-SC überwacht folgende Signale laufend während des Sicherheitstests, des Betriebs und der Abschaltung bis zum Shutoff:

* Drehmoment des Fahrmotors
* Hilfskontakte des DC-Schütz
* Strom und Spannung am DC-Schütz.
* Drehzahl des Fahrmotor

### Ermittlung des Drehmoments in der ICU

VEDS/VEDS-11597**VEDS-11597, Information,**Finalized**,**Inapplicable **- Erfassung der Drehmomentwerte des Fahrmotors**

Der ICU-SC kann die Stromwerte der LEM-Wandler im Umrichter unabhängig vom MC erfassen und auswerten. Während des Betriebs des MC wird ein Signal (INHIBIT Signal) des MC an den Resolver-Chip vom ICU-SC als Trigger genutzt um die Stommesswerte synchron zum MC Regeltask zu erfassen. Dies ist notwendig, da die Stromverläufe bei laufender Regelung näherungsweise dreieckförmig verlaufen. Wenn eine negative Flanke auf dem Inhibit Signal des MC detektiert wird, werden zunächst die Ströme 1 und 2 gleichzeitig und direkt im Anschluss der Strom 3 gesampelt. Der SC bildet aus den drei Strömen die Stromsumme, die näherungsweise Null betragen muss. Aus den drei Strömen wird mithilfe des zeitlich gleichzeitig erfassten Lagewinkelsignals des Resolvers die transformierten Ströme in dq-Koordinaten berechnet. Mit diesem Stromwertepaar (Id Iq) wird in den abgelegten Induktivitäts-Kennfeldern des Fahrmotors die Induktivitäten (Ld und Lq) interpoliert. Das aktuell realisierte Moment an der Maschinenwelle wird mit diesen Induktivitäten und dem Stromwertpaar berechnet.  
Wenn über längere Zeit keine Flanke des Inhibitsignals detektiert wird, wird der Drehmomentwert asynchron aus den drei Maschinenströmen und der gleichzeitig erfassten Lage des Resolvers berechnet.  
​​

VEDS/VEDS-11598**VEDS-11598, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Drehmomenterfassung des Fahrmotors**

Der ICU-SC muss aus den drei Strömen I1 I2 und I3 und dem Resolverlagesignal das Maschinenmoment berechnen.  
​​

#### Messwerterfassung

VEDS/VEDS-11778**VEDS-11778, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Synchrone Erfassung der Motorströme**

Der ICU-SC muss bei vorliegendem INHIBIT Signal des MC die Motorströme und die Resolverlage synchron zur fallenden Flanke erfassen.

VEDS/VEDS-11779**VEDS-11779, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Strommessung synchron zum INHIBIT Signal**

Die ICU-SC Software muss die fallende Flanke des INHIBIT Signals als Trigger für die Wandlung und Erfassung der 3 Motorströme I1, I2 und I3 konfigurieren.

VEDS/VEDS-11780**VEDS-11780, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Resolverlage synchron zum INHIBIT Signal**

Die ICU-SC Software muss die fallende Flanke des INHIBIT Signals als Trigger für die Abfrage des aktuellen Lagewinkels des Resolverchips konfigurieren.

VEDS/VEDS-11776**VEDS-11776, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Speicherung der synchron zu INHIBIT erfassten Werte**

Die ICU-SC Software muss so konfiguriert sein, dass die gewandelten Werte der 3 Ströme und der Resolverlage in einen Speicherbereich geschrieben werden von dem sie im schnellsten Task ausgelesen werden können.

VEDS/VEDS-11599**VEDS-11599, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erfassung des Resolverlagesignals**

Die ICU-SC Software muss synchron zur fallenden Flanke des INHIBIT Signals die 3 Maschinenströme und das Resolver Lagesignal erfassen und für die weitere Verarbeitung zur Verfügung stellen.  
​​

**abgeleitete HWSRs:**

VEDS/VEDS-10890**VEDS-10890, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Strommessung von vier Halbbrücken**

Die M302 muss die Ströme der vier Halbbrücken messen.

VEDS/VEDS-10891**VEDS-10891, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Separate Messschaltungen Strommessungen MC und SC**

Die Pegel der Stromwandler müssen an den Messbereich der Controller MC und SC über eine jeweils separate Schaltung angepasst werden.  
Hinweis:  
Bei der Auslegung der Schaltung ist auf ein möglichst geringen FIT-Rate zu achten.

VEDS/VEDS-11138**VEDS-11138, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Erfassen Triggersignals des MC an des Resolverchip**

Der SC muss das Triggersignal zum Auslesen der Lageinformation "INHB" vom MC an den Resolverchip erfassen, um dessen Flanke zur Synchronisierung auf den MC nutzen zu können.

VEDS/VEDS-11128**VEDS-11128, Sol.-constr. Requirement,**In progress**,**ASIL=C **- SC Kommunikation mit Resolverchip via SPI**

Der SC muss mit dem Resolverchip via SPI kommunizieren. Dabei ist der SC Master.  
Die SPI-Kommunikation ist mit vier Leitungen aufzubauen (SDI, SDI, SCLK, CS)

​​

#### Messwertüberprüfung

VEDS/VEDS-11777**VEDS-11777, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Gelesene Werte auf Aktualität prüfen**

Die ICU-SC Software muss prüfen, ob die Werte von I1, I2, I3 und der Resolverlage neu sind und nicht schon einmal ausgelesen wurden.  
Bereits verarbeitete Rohwerte dürfen nicht nochmals verwendet werden. Dies kann entweder durch Löschen, Eintragen einer Kennung etc. erfolgen.

VEDS/VEDS-11792**VEDS-11792, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Asynchrone Messwerterfassung**

Die ICU-SC Software muss bei ausbleibenden neuen Werten aufgrund fehlender Flanke des INHIBIT Signals die Ströme I1, I2, I3 und den Resolverlagewinkel asynchron im schnellsten Task erfassen.  
​​

VEDS/VEDS-11793**VEDS-11793, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Plausibilisierung der Motorströme**

Die ICU-SC Software muss im schnellsten Task überprüfen, ob die Ströme I1, I2 und I3 gültig sind.  
Wenn ein Rohwandelwert einen Randwert darstellt, wird er als ungültig bewertet. Wenn alle 3 Rohwerte gültig sind, muss die Stromsumme berechnet werden. Wenn die Stromsumme den hierfür relevanten Grenzwert überschreitet, werden alle Ströme als ungültig eingestuft.

VEDS/VEDS-11791**VEDS-11791, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Plausibilisierung der Resolverlage**

Die ICU-SC Software muss im schnellsten Task überprüfen, ob der Resolverchip einen Fehler meldet.  
Wenn eine Fehlerkennung vorliegt, so wird der aktuell vorliegende Resolverlagewert als ungültig bewertet.

VEDS/VEDS-11595**VEDS-11595, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Berechnung der transformierten Ströme**

Die ICU-SC Software muss im schnellsten Task aus den 3 Strömen I1, I2 und I3 und der Resolverlage und einem Resolver Offset im Parametersatz die transformierten Ströme im dq-Koordinatensystem berechnen.  
Wenn nur 2 gültige Stromwerte vorliegen, so sollen die transformierten Strömen aus den 2 gültigen Strömen und der Resolverlage berechnet werden; der ungültige Strom wird dann ignoriert. Wenn kein gültiger Resolverlagewert oder weniger als 2 gültige Ströme vorliegen, werden die berechneten transformierten Ströme auf ungültig gesetzt.  
​​

VEDS/VEDS-11596**VEDS-11596, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Bestimmung des Drehmomentwertes**

Die ICU-SC Software muss im schnellsten Task das Drehmoment bestimmen.  
Die Induktivitäten (Ld und Lq) werden aus den transformierten Strömen (Id und Iq) anhand der parametrierten Induktivitäts- Kennfeldern interpoliert. Das Drehmoment wird anhand der interpolierten Induktivitäten und dem Stromwertepaar berechnet. Wenn keine gültigen transformierten Ströme vorliegen, soll der Drehmomentwert auf ungültig gesetzt werden.

VEDS/VEDS-11815**VEDS-11815, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Mittelung und Übertragung des Drehmomentwertes**

Die ICU-SC Software muss die im schnellsten Task ermittelten Drehmomentwerte über die Dauer der CAN-Zykluszeit gemittelt auf dem CAN-Bus zur Verfügung stellen.  
Wenn während der CAN-Zykluszeit keine oder nur ungültige Drehmomentwerte ermittelt werden, soll eine Ungültigkeitskennung auf dem CAN übertragen werden. Einzelne ungültige Drehmomentwerte sollen bei der Mittelung ignoriert werden.  
​​

VEDS/VEDS-11814**VEDS-11814, Information,**Finalized**,**Inapplicable **- Mittelung des Drehmoments**

Die Mittelung des Drehmoments soll die Auswirkung von Ausreißern minimieren. Die Mittelung dient ebenfalls der Filterung des durch Wandlung und Messschaltung verursachten Rauschens.  
​​

### Überwachung des Zustand DC Schütz

VEDS/VEDS-11794**VEDS-11794, Information,**Finalized**,**Inapplicable **- Überwachung des DC Schütz**

Das DC Schütz stellt im Sicherheitskonzept das wichtigste Element dar, um sicher Drehmomentfreiheit herstellen zu können. Der Schaltzustand des Hauptkontakts ist hierbei sicherheitsrelevant. Die Funktion des Schützes kann über einen zwangsgeführten Hilfskontakt als Wechsler oder zwei zwangsgeführte Hilfskontakte überwacht werden. Diese zwangsgeführten Hilfskontakte werden durch die Ankerstellung des Hauptkontakts betätigt. Hierbei ist ein Hilfskontakt NO geöffnet, wenn der Hauptkontakt geöffnet hat. Der Hilfskontakt NC ist geschlossen, wenn der Hauptkontakt geöffnet ist. Wird der Hauptkontakt geschlossen, betätigt der Anker beide Hilfskontakte, so dass der NO Hilfskontakt dann geschlossen ist und der NC Hilfskontakt dann geöffnet wird. Der jeweils geschlossene Hilfskontakt überträgt ein alternierendes Signal, das vom ICU-SC erzeugt wird. Durch die Überwachung des Signalpegels und der Frequenz kann die Integrität des Signals durch den SC garantiert werden.

VEDS/VEDS-11892**VEDS-11892, Information,**Finalized**,**Inapplicable **- Prinzipschaltbild DC-Schütz**

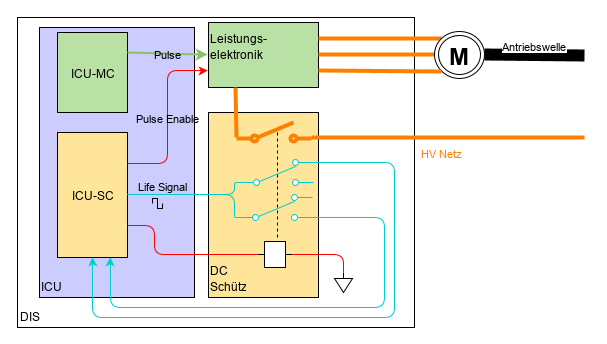
[](http://hdhapppolarion/polarion/wi-attachment/VEDS/VEDS-11892/1-diagram_20190805-1501.44573.mxg.png?revision=56708)

Figure 4 Prinzipschaltbild DC-Schütz

​​

**abgeleitete HWSRs:**

VEDS/VEDS-12083**VEDS-12083, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Ausführung Hauptkontakt**

Die Hardware des DC-Schütz muss einen Hauptkontakt bereitstellen, der im energiefreien Zustand den Kontakt öffnet (Monostabil, Normally Open).

VEDS/VEDS-12084**VEDS-12084, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Ausführung Hilfskontakte**

Die Hardware des DC-Schütz muss Hilfskontakte bereitstellen, die durch die Bewegung des Hauptkontakts geschaltet werden und monostabil sind (zwangsgeführt, normally closed bzw. normally opened)

VEDS/VEDS-12086**VEDS-12086, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Entgegengesetzte Hilfskontakte**

Die Hardware des DC-Schütz muss das Alternierende Signal je nach Stellung des Hauptkontakt auf die eine oder die andere Überwachungsleitung legen. Die Ausführung als Wechsler oder als parallel betätigte NO und NC Kontakte ist freigestellt.  
​​

#### Plausibilisierung des Schaltzustandes des DC-Schütz

VEDS/VEDS-11795**VEDS-11795, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Plausibilisierung des DC Schütz Hauptkontakts**

Der ICU-SC muss während des Sicherheitstests, des Betriebs und der Abschaltung laufend den Zustand des Hauptkontaktes überwachen und zum gewünschten Schaltzustand plausibilisieren.

VEDS/VEDS-11796**VEDS-11796, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erzeugen eines alternierenden Signals zur Überwachung der Hilfskontakte**

Die ICU-SC Software muss ein alternierendes Signal erzeugen, das auf beide Hilfskontakte gegeben wird.

VEDS/VEDS-11797**VEDS-11797, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Einlesen der Signale von den beiden Hilfskontakten**

Die ICU-SC Software muss von beiden Hilfskontakten den digitalen Signalzustand einlesen.

VEDS/VEDS-11798**VEDS-11798, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Bestimmen des Schaltzustands der beiden Hilfskontakte**

Die ICU-SC Software muss anhand des digitalen Einlesesignals jedes Hilfskontakts bestimmen, ob der Kontakt geöffnet, geschlossen oder unplausibel ist.

VEDS/VEDS-12085**VEDS-12085, Information,**Finalized**,**Inapplicable **- Bewertung Schaltzustand Hilfskontakt**

* Ein geschlossener Kontakt wird erkannt wenn mindestens die letzten drei Signalwechsel und Pegel des alternierenden Signals phasenrichtig bestimmt werden konnten.
* Ein geöffneter Kontakt wird erkannt, wenn das Signal konstant auf HIGH Pegel bleibt.
* In allen anderen Fällen muss die ICU-SC Software den Status des Hilfskontakts als unplausibel einstufen.

VEDS/VEDS-12102**VEDS-12102, Sol.-constr. Requirement,**Finalized**,**Inapplicable **- Bestimmen des Schaltzustands des DC Schütz über Hilfskontakte**

Die ICU-SC Software muss anhand der Schaltzustände der beiden Hilfskontakte den Zustand des Hauptkontaktes bestimmen.  
Wenn der NO Hilfskontakt als geschlossen detektiert wird und der NC Hilfskontakt als offen detektiert wird, muss der Hauptkontakt als geschlossen bestimmt werden.  
Wenn der NO Hilfskontakt als geöffnet detektiert und der NC Hilfskontakt als geschlossen detektiert wird, muss der Hauptkontakt als geöffnet bestimmt werden.  
Bei jeder anderen Kombination muss der Schaltzustand des DC Schütz Hauptkontakt als unbestimmt detektiert werden.  
​​

VEDS/VEDS-11803**VEDS-11803, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erfassung des Schützspulenstroms**

Die ICU-SC Software muss den Strom in die Schützspule messen.

VEDS/VEDS-12103**VEDS-12103, Sol.-constr. Requirement,**Finalized**,**Inapplicable **- Bewertung des Spulenstroms**

Wenn der gemessene Strom den hierfür relevanten Grenzwert überschreitet, muss von einem angesteuerten Schütz ausgegangen werden.  
Wenn der Strom nahe 0 gemessen wird, muss von einem nicht angesteuerten Schütz ausgegangen werden.  
​​

VEDS/VEDS-11799**VEDS-11799, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erfassung der Spulenspannung des DC Schütz**

Die ICU-SC Software muss die Spannung am Ausgang der Spulenansteuerung messen.

VEDS/VEDS-11800**VEDS-11800, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Plausibilisierung der Schützansteuerung**

Die ICU-SC Software muss die Spulenansteuerung plausibilisieren.  
Wenn kein Schützstrom gemessen wird und die Spannung an der Spule 0 Volt beträgt, muss ein nicht angesteuertes Schütz detektiert werden.  
Wenn ein Schützstrom gemessen wird und die Spannung am Ausgang der Spulenansteuerung den hierfür geltenden Grenzwert übersteigt, muss ein angesteuertes Schütz detektiert werden.  
Wenn ein Schützstrom gemessen wird und die Spannung am Ausgang kleiner als der hierfür geltende Grenzwert ist, muss von einem Kurzschluss in der Schützansteuerung ausgegangen werden.  
Wenn kein Schützstrom gemessen wird und die Spannung am Ausgang den hierfür geltenden Grenzwert übersteigt, muss ein defektes oder nicht angeschlossenes Schütz detektiert werden.

**abgeleitete HWSRs:**

VEDS/VEDS-11185**VEDS-11185, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Ausgabe Signal zur Überwachung der Hilfskontakte DC-Relais**

Der SC muss ein Signal zur Überwachung der Hilfskontakte des DC-Relais ausgeben. Abhängig von der Schaltung auf der M302 kann dies sowohl ein PWM-Signal als auch ein Dauerpegel sein.

VEDS/VEDS-11183**VEDS-11183, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Einfache Überwachung des DC-Relais durch SC**

Der SC muss an einem Eingang das durch eine Hardwareschaltung aufbereitete Überwachungssignal wieder einlesen.

VEDS/VEDS-11184**VEDS-11184, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Erweiterte Überwachung des DC-Relais durch SC**

Um auch einen Wechselkontakt des Hilfskontaktes des DC-Relais einlesen zu können soll der SC an zwei Eingängen das jeweils durch eine Hardwareschaltung aufbereitete Überwachungssignal wieder einlesen.  
  
weitere Anforderungen zum DC-Relais siehe Kapitel [26DC-Relais (Freischaltschütz)](http://hdhapppolarion/polarion/#/project/VEDS/workitem?id=VEDS-11034)

VEDS/VEDS-11031**VEDS-11031, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Auswertung zwei Signale Hilfskontakte DC-Relais**

Die M302 muss die Stellung der Hilfskontakte über zwei getrennte Eingänge einlesen (Wechselschalter am Relais).

VEDS/VEDS-12087**VEDS-12087, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Spannungsmessung HS-Treiber für DC-Relais**

Die M302 muss dem SC das vom HS-Treiber bereitgestellte Spannungssignal an einem Analogeingang bereitstellen.

VEDS/VEDS-12088**VEDS-12088, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Strommessung HS-Treiber für DC-Relais**

Die M302 msus dem SC das vom HS-Treiber bereitgestellte Stromsignal an einem Analogeingang bereitstellen.  
​​

​​

#### Überwachung des DC-Schütz Hauptkontakts

VEDS/VEDS-11897**VEDS-11897, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Überwachung der Spannung am Hauptkontakt des Schützes**

Der ICU-SC muss die Spannung über dem Hauptkontakt des DC-Schütz während des Betriebs überwachen.  
Die ICU-SC Software muss die von der Software vorgegebene Schützansteuerung mit der Stellung der Hilfskontakte und dem Plausibilisierungsergebnis der Schützansteuerung plausibilisieren. Die Bewertung soll laufend stattfinden. Wenn unplausible Zustände detektiert werden, die länger anhalten als die Schaltdauer des Schützes ist, so soll von einer Integritätsverletzung des DC-Schützes ausgegangen werden und die entsprechende Fehlerreaktion ausgelöst werden. Der ICU-SC muss vor dem Schließen des DC-Schütz Hauptkontakts sicherstellen, dass die beiden Spannungen nicht mehr als 35 Volt voneinander abweichen, um die Hauptkontakte des Schütz vor großen Einschaltströmen (Inrush currents) zu schützen, die die Kontakte verschweißen könnten. Während des Betriebs bei geschlossenem Schütz dürfen die gemessenen Spannungen dauerhaft nicht mehr als 20 Volt voneinander abweichen. Andernfalls wird eine Integritätsverletzung des DC-Schützes angenommen und eine Sicherheitsabschaltung durchgeführt.

VEDS/VEDS-11898**VEDS-11898, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erfassung der DC-Link Spannung**

Der ICU-SC Software muss zyklisch die DC-Link Spannung ermitteln und auf dem CAN-Bus zur Verfügung stellen.

VEDS/VEDS-11899**VEDS-11899, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erfassen der HV-Terminal Spannung**

Die ICU-SC Software muss zyklisch die HV-Terminal Spannung ermitteln und auf dem CAN-Bus zur Verfügung stellen.

VEDS/VEDS-11900**VEDS-11900, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Schließen des DC-Schütz**

Die ICU-SC Software darf den DC-Schütz in den Zuständen STARTUP, SAFETY\_TEST und CYCLIC\_TEST nur schließen, wenn die beiden Spannungen DC-Link Voltage und HV-Terminal Voltage nicht mehr als 35 Volt voneinander abweichen.  
​​

VEDS/VEDS-11901**VEDS-11901, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachen der Kontaktspannung bei geschlossenem DC-Schütz**

Die ICU-SC Software muss bei geschlossenem Schütz in den Zuständen STARTUP, SAFETY\_TEST, OPERATION und CYCLIC\_TEST zyklisch die Differenz der beiden Spannungen DC-Link Voltage und HV-Terminal Voltage ermitteln.  
Wenn die Spannungen dauerhaft mehr als 20V voneinander abweichen, muss von einer Integritätsverletzung ausgegangen werden.  
​​

**abgeleitete HWSRs:**

VEDS/VEDS-10940**VEDS-10940, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Wandler SC**

Die M302 muss die Zwischenkreisspannung sowie die HV-Terminal Spannung dem SC aufbereitetet (Pegelanpassung) bereitstellen.

VEDS/VEDS-10941**VEDS-10941, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Messung Spannung Zwischenkreis und HV-Terminal**

Die M302 muss die Möglichkeit bieten, die Zwischenkreisspannung und die Spannung HV-Terminal zu messen.

VEDS/VEDS-11118**VEDS-11118, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Messung Zwischenkreisspannung im SC**

Der SC muss die Spannung des Zwischenkreises unabhängig vom MC messen.

VEDS/VEDS-11120**VEDS-11120, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Messung Spannung HV-Terminal im SC**

Der SC muss die Spannung von HV-Terminal unabhängig vom MC messen.

​​

### Erfassung der Drehzahl des Fahrmotors

VEDS/VEDS-11991**VEDS-11991, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Ermittlung der Drehzahl des Fahrmotors**

Der ICU-SC muss in allen Zuständen (außer während der Initialisierung) die Drehzahl des Fahrmotors ermitteln und sicher über den CAN-Bus zur Verfügung stellen.

VEDS/VEDS-11992**VEDS-11992, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Ermittlung der Drehzahl des Fahrmotors über SPI**

Die ICU-SC Software muss zyklisch beim Resolverchip die Drehzahl des Resolvers abfragen und daraus die Drehzahl des Fahrmotors berechnen.  
Die Drehzahl kann entweder direkt aus dem PGA411 Register ausgelesen werden oder aus den zyklisch erfassten Lagewerten des Resolvers durch Differenzieren gebildet werden.

VEDS/VEDS-11993**VEDS-11993, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Mittelung des Drehzahlwerts**

Die ICU-SC Software muss den Drehzahlwert des Fahrmotors öfter sampeln als die Zykluszeit der CAN-Nachricht in der er übertragen wird. Die Drehzahl soll gemittelt werden bevor sie übertragen wird.

VEDS/VEDS-12105**VEDS-12105, Information,**Finalized**,**Inapplicable **- Drehzahlermittlung**

Die Filterzeitkonstante soll kleiner sein als die Zykluszeit der CAN-Nachricht. Ungültige Momentanwerte der Drehzahl sollen vom Filter ignoriert werden.  
Wenn im Task keine Drehzahl ermittelt werden kann, so soll eine Diagnosemeldung abgesetzt werden und als Drehzahlwert Nicht Verfügbar eingetragen werden. Die internen Statusmaschinen sollen immer mit dem aktuellsten Drehzahlwert arbeiten. Solange zwischen zwei CAN Nachrichten mindestens eine Drehzahl ermittelt werden kann soll diese Drehzahl gesendet werden. Wenn Zwischen zwei CAN Nachrichten keine aktuelle Drehzahl ermittelt werden konnte, soll die Nicht Verfügbar Kennung gesendet werden.

​​

## Sicherheitsintegrität der ICU

VEDS/VEDS-11604**VEDS-11604, Information,**Finalized**,**Inapplicable **- Sicherheitsintegrität der ICU**

Die Sicherheitsintegrität des ICU-SC wird durch die Zusammenarbeit des ICU-SC und des IWDT Baustein TLF35584 sowie Funktionen in der Software innerhalb des SC hergestellt. Durch die externe Hardware Beschaltung wird sichergestellt, dass der sichere Zustand auch eingenommen wird, wenn der ICU-SC nicht arbeitet, nicht mit Spannung versorgt ist, sich im Reset befindet oder programmiert wird. Der ICU-SC ist ein reiner Sicherheitsbaustein ohne funktionale Aufgaben. Daher befindet er sich bezüglich des Einflusses seiner Fehler im Latentfehlerpfad.

VEDS/VEDS-12097**VEDS-12097, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Single-Point-Fault Metrik**

Die Single-Point-Fault Metrik des ICU-SC muss >= 90% betragen.  
​​

VEDS/VEDS-12380**VEDS-12380, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Überwachung und Absicherung des SC**

Der ICU-SC muss seine Controllerfunktionen und seine Software auf Integrität überwachen.

### Überwachung von Controllerfunktionen

VEDS/VEDS-11996**VEDS-11996, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachung Speicherbereiche**

Die ICU-SC Software muss die verwendeten Speicherbereiche und Daten überwachen und Fehler erkennen.

VEDS/VEDS-11998**VEDS-11998, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachung der Controller Hardware**

Die ICU-SC Software muss die verwendeten Peripheriebausteine auf korrekte Funktion überwachen.  
​​

### Absicherung von Software und Datensatz

VEDS/VEDS-12100**VEDS-12100, Information,**Finalized**,**Inapplicable **- Absicherung der Daten**

Um Fehler bei der Übertragung, dem Laden oder dem Verarbeiten der Daten des Programmcodes und des verwendeten Datensatzes erkennen zu können, müssen sowohl der Programmcode als auch der Datensatz durch eigene CRC-Checksummen abgesichert werden. Vor der Abarbeitung des Programmcodes muss dieser auf Checksummenfehler geprüft werden. Der Datensatz ist nur gültig wenn er zu der Version des Programmcodes passt und die Checksummenprüfung fehlerfrei verläuft.

VEDS/VEDS-12101**VEDS-12101, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Absichern des Datensatzes**

Die ICU-SC Software muss den Datensatz durch eine CRC Überprüfung auf Fehler überwachen.

VEDS/VEDS-12098**VEDS-12098, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Absichern des Programmcodes**

Die ICU-SC Software muss den Programmcode durch eine CRC Überprüfung auf Fehler überwachen.  
  
​​

### Überwachung der Versorgungsspannungen

VEDS/VEDS-11818**VEDS-11818, Information,**Finalized**,**Inapplicable **- Überwachung der Versorgungsspannungen**

Der IWDT erzeugt und überwacht die Versorgungsspannungen des ICU-SC und des Treiberbausteins für die CAN-Kommunikation. Diese Spannungen haben Relevanz für die Überwachung der Sicherheitsziele im ICU. Eine Systemreaktion findet durch den IWDT statt. Gleichzeitig gibt es aber auch Spannungen für den Resolverbaustein und die Versorgung der Strommessung, die für eine korrekte Ermittlung des Drehmoments relevant sind. Diese Spannungen werden nicht vom IWDT erzeugt und überwacht. Diese Spannungen werden vom ICU-SC eingelesen und mit Grenzwerten verglichen. Bei zu großer Abweichung kann eine sichere Drehmomentbestimmung nicht mehr gewährleistet werden und führt somit zu einer Verletzung der Sicherheitsintegrität.

VEDS/VEDS-11605**VEDS-11605, Information,**Finalized**,**Inapplicable **- Überwachung der Versorgungsspannungen des ICU-SC**

Bei Unterspannung wird der SC durch den IWDT resetted und bei Überspannung wird der SC durch den IWDT resetted und die Versorgungsspannung abgeschaltet.

VEDS/VEDS-11819**VEDS-11819, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Überwachung der Versorgungsspannungen für Resolver und Strommessung**

Der ICU-SC muss die Versorgungsspannungen überwachen, die für eine korrekte Erfassung der Ströme und der Resolverlage notwendig sind.

VEDS/VEDS-11820**VEDS-11820, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachung der Spannungen +-24V für Strommessung**

Die ICU-SC Software muss die Versorgungsspannung +24V und -24V überwachen.  
Bei Überschreiten oder Unterschreiten der hierfür geltenden Grenzwerte, muss die ICU-SC Software eine Sicherheitsintegritätsverletzung annehmen.

VEDS/VEDS-11817**VEDS-11817, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachung der Spannung +15V für Momentenbestimmung und Schaltzustandbestimmung DC Schütz**

Die ICU-SC Software muss die Versorgungsspannung +15V überwachen.  
Bei Überschreiten oder Unterschreiten der hierfür geltenden Grenzwerte, muss die ICU-SC Software eine Sicherheitsintegritätsverletzung annehmen.  
​​

VEDS/VEDS-12476**VEDS-12476, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Überwachung der Spannung +3,3V für die digitalen Schnittstellen des Resolverchips**

Die ICU-SC Software muss die Versorgungsspannung +3,3V überwachen.  
Bevor die Spannung nicht stabil anliegt soll der Resolverchip beim Aufstarten nicht aus dem Reset geholt werden. Während des Betriebs muss die Spannung überwacht werden um die Integrität der digitalen Signale NRESET, RESFAULT, FAULT und RESO\_INHI\_SC zu gewährleisten. Bei Überschreiten oder Unterschreiten der hierfür geltenden Grenzwerte muss die ICU\_SC Software eine Sicherheitsintegritätsverletzung annehmen.  
​​

VEDS/VEDS-11821**VEDS-11821, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Erfassung der Spannung +0,9Voffset für Strommessung**

Die ICU-SC Software muss die Offsetspannung +0,9Voffset erfassen und überwachen.  
Bei Überschreiten oder Unterschreiten der hierfür geltenden Grenzwerte, muss die ICU-SC Software eine Sicherheitsintegritätsverletzung annehmen.

**abgeleitete HWSRs:**

​​

VEDS/VEDS-12094**VEDS-12094, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Spannungsmessung +24V Versorgungsspannung**

Die M302 muss dem SC die Spannung +24V an einem Analogeingang bereitstellen.

VEDS/VEDS-12095**VEDS-12095, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Spannungsmessung -24V Versorgungsspannung**

Die M302 muss dem SC die Spanung -24V an einem Analogeingang bereitstellen.

VEDS/VEDS-12091**VEDS-12091, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Spannungsmessung +15V Versorgungsspannung**

Die M302 muss dem SC die Spannung +15V an einem Analogeingang bereitstellen

VEDS/VEDS-12092**VEDS-12092, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Spannungsmessung +0,9V Referenzspannung**

Die M302 muss dem SC die Spannung +0,9VOffset an einem Analogeingang bereitstellen.

VEDS/VEDS-12477**VEDS-12477, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Spannungsmessung +3,3V Versorgungsspannung**

Die M302 muss dem SC die Spannung +3,3V an einem Analogeingang bereitstellen.  
​​

​​

### Überwachung der Funktion des ICU-SC

VEDS/VEDS-11787**VEDS-11787, Information,**Finalized**,**Inapplicable **- Integritätsüberwachungen**

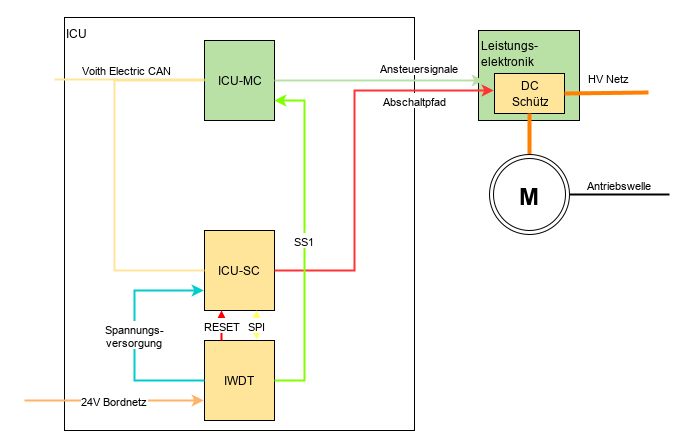
Die Funktionalität des ICU-SC wird über den IWDT Baustein TLF35584 überwacht. Der IWDT Baustein besitzt die Möglichkeit bei einem erkannten Fehler des ICU-SC diesen zu resetten. Als Überwachungen stehen im Baustein ein Window Watchdog, ein Error Signal der SMU (Safety Management Unit) und ein Functional Watchdog zur Verfügung. Diese drei Funktionen erfordern ein zeitlich und funktional genau spezifiziertes Verhalten des ICU-SC, das es dem IWDT ermöglicht, Software oder Laufzeitfehler des ICU-SC zu erkennen.  
[](http://hdhapppolarion/polarion/wi-attachment/VEDS/VEDS-11787/1-diagram_20200217-1427.17017.mxg.png?revision=76513)

Figure 5 Sicherheitsarchitektur ICU

​​

VEDS/VEDS-11786**VEDS-11786, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Fehler in der Abarbeitung der SC Software müssen erkannt werden**

Der ICU-SC muss den IWDT so konfigurieren, dass der IWDT Laufzeitfehler des ICU-SC erkennen kann.

VEDS/VEDS-11614**VEDS-11614, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Functional Watchdog**

Die ICU-SC Software muss den Functional Watchdog des IWDT konfigurieren und während des Betriebs korrekt triggern.

VEDS/VEDS-11615**VEDS-11615, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Window Watchdog**

Die ICU-SC Software muss den Window Watchdog nach der Initialisierung über die SPI Schnittstelle desaktivieren.

VEDS/VEDS-11816**VEDS-11816, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- ERR-Signal**

Die ICU-SC Software muss die SMU so konfigurieren, dass am FSP Ausgang das ERR Signal für den IWDT mit der korrekten Frequenz erzeugt wird.  
​​

**abgeleitete HWSRs:**

VEDS/VEDS-11182**VEDS-11182, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Watchdog (IWDT) Typ**

Am SC muss der IWDT vom Typ Infineon TLF35584 verwendet werden.

VEDS/VEDS-11178**VEDS-11178, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Reset durch IWDT**

Des SC muss durch das "Reset output - ROT"-Signal des Watchdogs (IWDT) zurückgesetzt werden können.  
Hinweis:  
Der SC muss dadurch automatisch den "sicheren Zustand" herstellen

VEDS/VEDS-11181**VEDS-11181, Sol.-constr. Requirement,**In progress**,**ASIL=C **- SPI-Kommunikation zum IWDT**

Der SC muss mit dem IWDT per SPI kommunizieren. Der SC ist Master und steuert Chip Select und Clock an.

VEDS/VEDS-11258**VEDS-11258, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Error Signal von SC an IWDT**

Der SC muss an das Signal "Error Signal Input - ERR" ein Pulsendes Signal geben. Die Frequenz beträgt 10 .. 45 kHz.  
  
Hinweis: Die Error Überwachung soll im A-Muster zunächst nicht verwendet und durch Konfiguration im IWDT ausparametriert werden.

​​

### Überwachung des Resolverchips

VEDS/VEDS-12076**VEDS-12076, Information,**Finalized**,**Inapplicable **- Diagnose des Resolverchips PGA411**

Der Resolverchip besitzt als digitalen Ausgang eine Leitung, die erkannte Fehler anzeigt. Diese Leitung wird sowohl vom ICU-SC als auch vom ICU-MC eingelesen. Über die SPI-Schnittstelle kann der ICU-SC die konkreten Fehler aus den entsprechenden Register auslesen. Der ICU-SC kann den PGA411 über eine digitale Leitung resetten um ggf. Fehler zu löschen. Die Fehler des Resolvers können vom ICU-SC über Status CAN Nachrichten auf dem Intercontroller CAN weitergemeldet werden.

VEDS/VEDS-12077**VEDS-12077, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Reaktion auf Resolver Fault**

Der ICU-SC muss zur Plausibilisierung des Lage und Drehzahlwertes vom Resolverchip PGA411 die Resolver Fault Leitung mindestens so häufig einlesen wie Drehmomente berechnet werden. Drehzahlen und Lagesignale, die während eines angezeigten Fehlers des Resolvers eingelesen werden, dürfen nicht als gültige Signale weiterverwendet werden.

VEDS/VEDS-12074**VEDS-12074, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Einlesen des Resolver Fault**

Die ICU-SC Software muss das Signal Fault vom Resolverchip PGA411 im schnellsten Task einlesen.

VEDS/VEDS-12078**VEDS-12078, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Fehlerreaktion bei detektiertem Fehler**

Die ICU-SC Software muss die Fehler des Resolverchips PGA411 quitieren und gegebenenfalls den Resolverchip wieder konfigurieren. Wenn der Fehler persistent ist, muss von einer Integritätsverletzung ausgegangen werden.  
​​

**abgeleitete HWSRs:**

VEDS/VEDS-10856**VEDS-10856, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Typ Resolverchip**

Die Erzeugung des Erregersignals und Auswertung des Lagesignals erfolgt mittels des Resolver-Chips PGA411-Q1 von Texas Instruments.

VEDS/VEDS-11137**VEDS-11137, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Reset-Leitungen zum Resolver-Chip**

Der SC muss die beiden Signale "RESET" und "FAULTRES" bedienen.

VEDS/VEDS-11136**VEDS-11136, Sol.-constr. Requirement,**In progress**,**ASIL=C **- Fehlersignale Resolverchip an SC**

Der SC muss das "FAULT"-Signal des Resolver-Chips einlesen

​​

### Safety Test

VEDS/VEDS-11881**VEDS-11881, Information,**Finalized**,**Inapplicable **- Safety Test**

Zu Beginn jedes Betriebszyklus wird im Rahmen des Hochfahrens des Systems vom ICU-SC ein Safety Test durchgeführt. Dieser Safety Test dient dazu, vor der Freigabe des Fahrbetriebs die sicherheitsrelevanten Anteile des Systems auf korrekte Funktion und latente Fehler zu testen. Wenn ein Test nicht erfolgreich durchlaufen wird, so wird der Betrieb nicht freigegeben.

VEDS/VEDS-11882**VEDS-11882, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Safety Test am Beginn eines Betriebszyklus**

Der ICU-SC muss zu Beginn jedes Betriebszyklus die Freigabe des Bremswiderstands, das Aktivieren des Bremswiderstands und die Funktion des DC-Schütz nach der folgenden Startup und Safety Test Sequenz testen, bevor der Fahrbetrieb freigegeben werden darf:  
[27VEDS-11883- Sequenzdiagramm Startup und Safety Test](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11883)

VEDS/VEDS-11883**VEDS-11883, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sequenzdiagramm Startup und Safety Test**

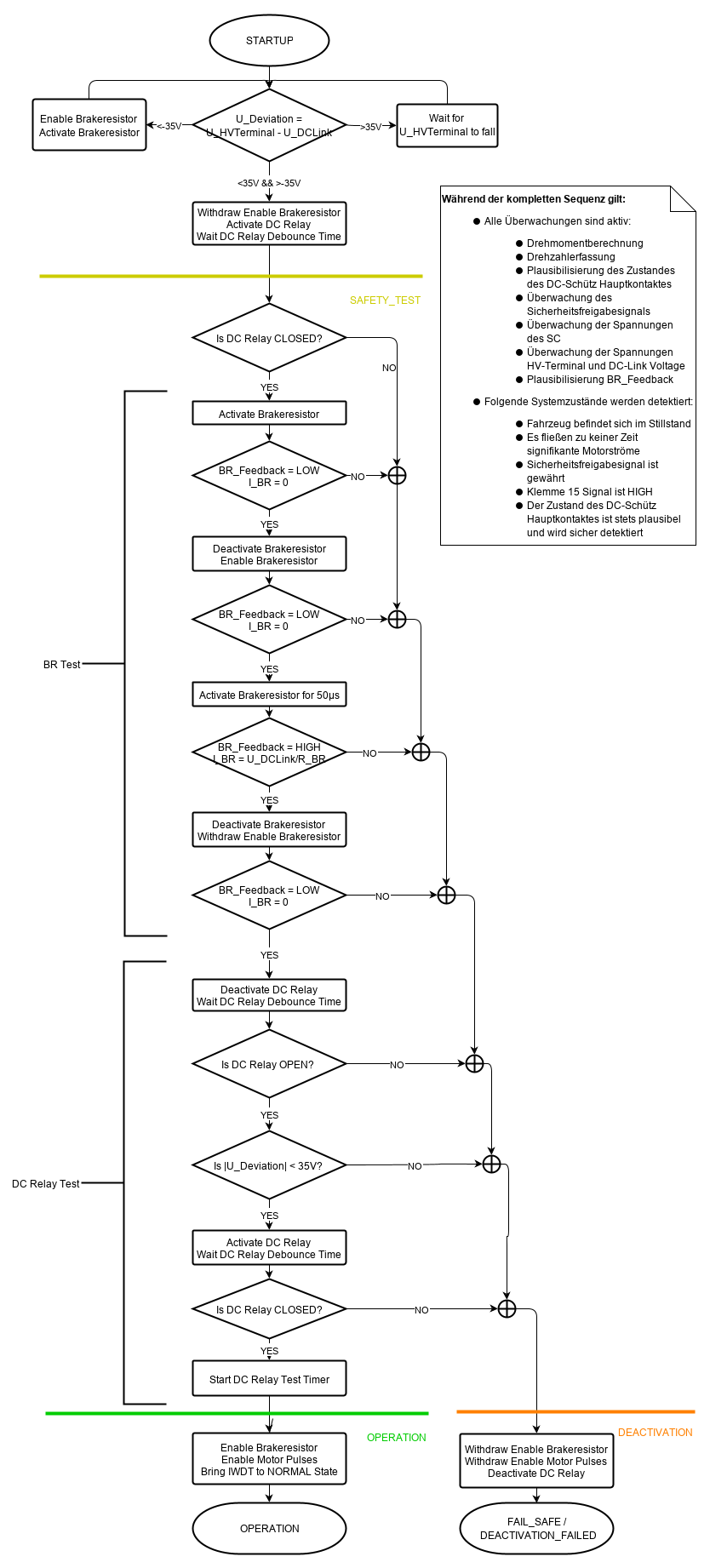
Die ICU-SC Software muss die Startup und Safety Test Sequenz umsetzen.  
[](http://hdhapppolarion/polarion/wi-attachment/VEDS/VEDS-11883/1-diagram_20190731-0915.29257.mxg.png?revision=62965)

Figure 6 Safetytest Sequence

​​

VEDS/VEDS-11887**VEDS-11887, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- SC Zustand nach Init**

Die ICU-SC Software muss sicherstellen, dass während der Initialisierung und an deren Ende alle Sicherheitsfreigaben nicht gewährt sind und das DC Relais nicht angesteuert wird.

VEDS/VEDS-11884**VEDS-11884, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Safety-Test BR-Freigabe**

Die ICU-SC Software muss die Funktion der Freigabe Bremswiderstand testen indem die Ansteuerung gemäß der dargestellten Sequenz durchlaufen und überprüft wird.  
Bei einem Ergebnis, das nicht dem erwarteten Verhalten entspricht, wird der Safety-Test als gescheitert bewertet und der FAIL\_SAFE Zustand eingenommen.

VEDS/VEDS-11987**VEDS-11987, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Safety-Test DC-Schütz Ansteuerung**

Die ICU-SC Software muss nach jeder Schalthandlung eine Toleranzzeit abwarten um bei prellenden Kontakten unplausible Zwischenzustände zu vermeiden.  
​​

### Zyklischer Schütz Test

VEDS/VEDS-11885**VEDS-11885, Information,**Finalized**,**Inapplicable **- Zyklischer Schütz Test**

Um den Entdeckungsgrad latenter Fehler im DC Schütz zu erhöhen, wird ein zyklischer Schütz Test vorgesehen, der nach einer Wartezeit während einer Ruhephase im Betrieb getriggert werden soll. Um den Fahrbetrieb nicht zu beeinträchtigen und das Schütz nicht durch die Schaltvorgänge zu belasten, wird der Test nur im Stillstand ohne Momentenanforderung durchgeführt. Hierzu wird vom DMU APPC ein Signal auf dem Electric CAN bereitgestellt, das einen Haltemodus anzeigt. Haltemodus bedeutet hier ein Halt, der nicht verkehrsbedingt ist. Das ist zum Beispiel ein Halt an einer Bushaltestelle. Argumente für die DMU sind hierbei der Fahrzeugstillstand und gleichzeitig z. B. geöffnete Türen oder das Einlegen der Haltestellenbremse oder der Parkbremse.

VEDS/VEDS-12073**VEDS-12073, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Zyklischer Schütz Test**

Der ICU-SC muss zyklisch den Schütz Test wie folgt durchführen:  
[28VEDS-11886- Sequenzdiagramm zyklischer Schütz Test](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11886)

VEDS/VEDS-11984**VEDS-11984, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Integritätsfehler beim Cyclic Test**

Wenn vom ICU-SC während des zyklischen Tests eine Integritätsverletzung festgestellt wird, muss er die Abschaltsequenz durchführen und in den Zustand DEACTIVATION wechseln.

VEDS/VEDS-11985**VEDS-11985, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Spannungsabweichung beim Cyclic Test**

Wenn während der Öffnungsphase des DC-Schütz die Spannung über den Kontakten soweit ansteigt, dass ein Schließen aufgrund des Inrush-Current zu einer Schädigung führen könnte, so soll der Kontakt geöffnet bleiben und der Zustand des SC in den Zustand INIT wechseln. Hierbei muss der SC nicht zurückgesetzt und neu konfiguriert werden.   
​​

VEDS/VEDS-11886**VEDS-11886, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Sequenzdiagramm zyklischer Schütz Test**

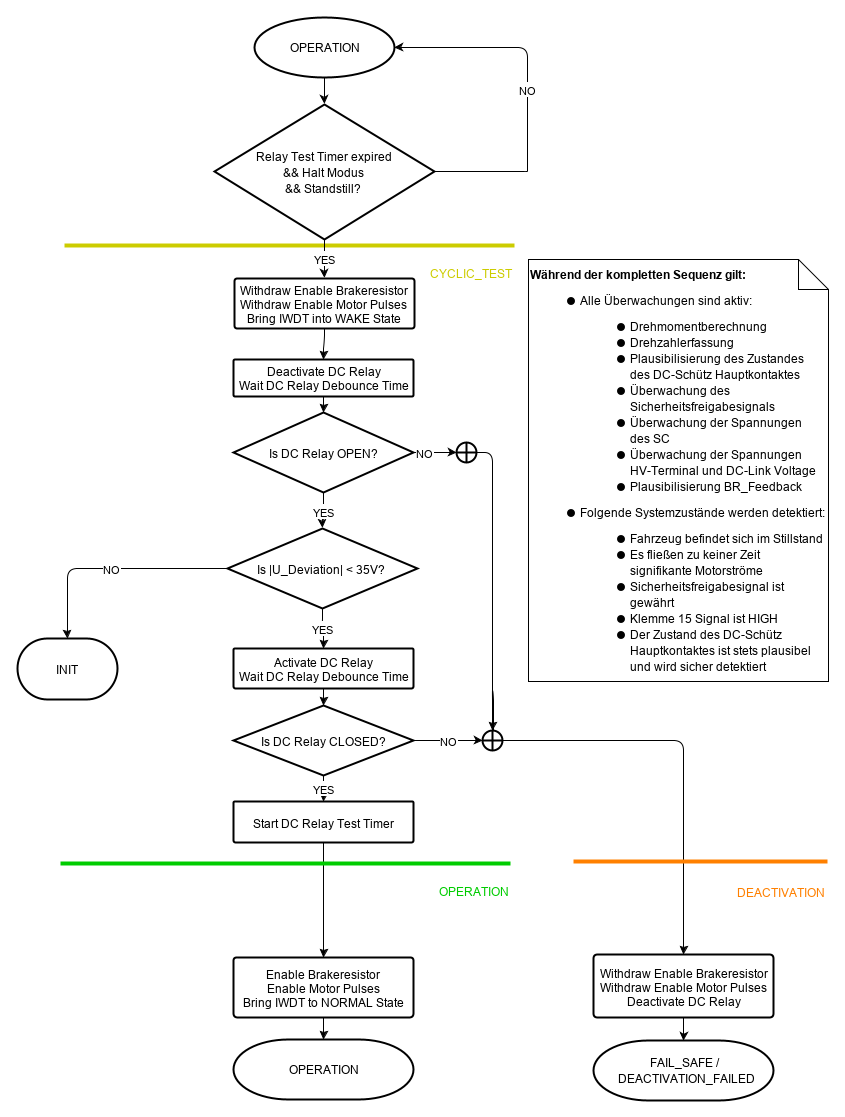
Die ICU-SC Software muss den zyklischen Schütztest nach folgendem Sequenzdiagramm durchführen  
[](http://hdhapppolarion/polarion/wi-attachment/VEDS/VEDS-11886/1-diagram_20190731-1232.39690.mxg.png?revision=62978)

Figure 7 Cyclic-Test Sequence

​​

### Reaktion auf Integritätsverletzungen

VEDS/VEDS-11789**VEDS-11789, Tech. Safety Requirement,**Finalized**,**ASIL=C **- Reaktion Integritätsverletzungen**

Wenn vom ICU-SC mindestens eine sicherheitsgerichtete Funktion nicht mehr sicher ausgeführt werden kann, muss der ICU-SC den jeweiligen sicheren Zustand einleiten.

VEDS/VEDS-11790**VEDS-11790, Sol.-constr. Requirement,**Finalized**,**ASIL=C **- Integritätsverletzungen**

Die ICU-SC Software muss bei folgenden Ereignissen eine Integritätsverletzung annehmen:

* Dauerhafte Unterschreitung oder Überschreitung der überwachten Spannungen  
  [29VEDS-11820- Überwachung der Spannungen +-24V für Strommessung](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11820)   
  [30VEDS-11817- Überwachung der Spannung +15V für Momentenbestimmung und Schaltzustandbestimmung DC Schütz](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11817)  
  [31VEDS-11821- Erfassung der Spannung +0,9Voffset für Strommessung](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11821)   
  [32VEDS-12476- Überwachung der Spannung +3,3V für die digitalen Schnittstellen des Resolverchips](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12476)
* Dauerhaft keine plausiblen Lagesignale des Fahrmotors  
  [33VEDS-12078- Fehlerreaktion bei detektiertem Fehler](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12078)
* gescheiterter zyklischer DC-Schütz Test  
  [34VEDS-11984- Integritätsfehler beim Cyclic Test](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11984)
* Drehmomentberechnung nicht möglich  
  [35VEDS-11815- Mittelung und Übertragung des Drehmomentwertes](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11815)
* DC Schütz Schaltzustand nicht zweifelsfrei ermittelbar  
  [36VEDS-12102- Bestimmen des Schaltzustands des DC Schütz über Hilfskontakte](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-12102)
* DC Schütz Schaltzustand entspricht nicht dem kommandierten Zustand  
  [37VEDS-11800- Plausibilisierung der Schützansteuerung](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11800)
* Spannungsdifferenz bei geschlossenem DC-Schütz Hauptkontakt ist unplausibel hoch  
  [38VEDS-11901- Überwachen der Kontaktspannung bei geschlossenem DC-Schütz](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11901)
* Unplausible Stromsumme  
  [39VEDS-11793- Plausibilisierung der Motorströme](http://hdhapppolarion/polarion/#/project/VEDS/wiki/11%20Own%20Requirements%20Specifications/ORS%20VEDS%20Technisches%20Sicherheitskonzept?selection=VEDS-11793)

# Technisches Sicherheitskonzept EACU

​​

​​

# ANNEX - Mitgeltende Unterlagen

​​

​​

# ANNEX - Abbildungsverzeichnis

*Please update the table of figures.*

# ANNEX - Tabellenverzeichnis

*Please update the table of figures.*

# ANNEX - Glossare

​​

# Informationen zu diesem Live-Dokument

## Legende

|  |  |
| --- | --- |
| \_merged\_2Live Doc Legend | |
| FSEIN | System |
| FSE Title | Voith Electrical Drive System |
| FSE Kind | System (comprehensive) |
| Live Doc Type | ORS |
| Live Doc Status | Finalized |
| Live Doc Assignee | - |
| Live Doc SV-Revision | 80565 |

## Änderungshistorie

1

​​

​​

## Statistische Berichte

#### \_merged\_3Report 8: Statuses of WorkItems in current LiveDoc

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WorkItems in this LiveDoc (Sum: 403) | | | | | | | | | | | | | | | | | | | |
|  | **Σ**  **402** | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **402** | - |
|  | **Σ**  **1** | - | **1** |  | | | | | | | | | | | | | | | |
| Referenced WorkItems (Sum: 37) | | | | | | | | | | | | | | | | | | | |
|  | **Σ**  **37** | - | - | - | - | **37** | - | - | - | - | - | - | - | - | - | - | - | - | - |

​​