life.augmented

Functional Safety in Electronic Systems: Principles and Applications

Alessandro Bastoni

Functional Safety Expert

STMicroelectronics

General disclaimer on Exercitations

All material included/used for exercitations has been prepared for teaching purposes.

Accordingly, accuracy of presented examples is not 100%, because simplifications have been done here and there to boost the focus on specific aspects related to the teached topics. Also the detail level can vary in different part of the same example, again because of teaching purposes.

WARNING: applications presented in this document cannot be considered real, accurate use cases. Their mere replication in real projects may lead to mistakes and missing compliance to the safety standards. Use them just for learning activity.

Exercitations

Ex #3 – FTA

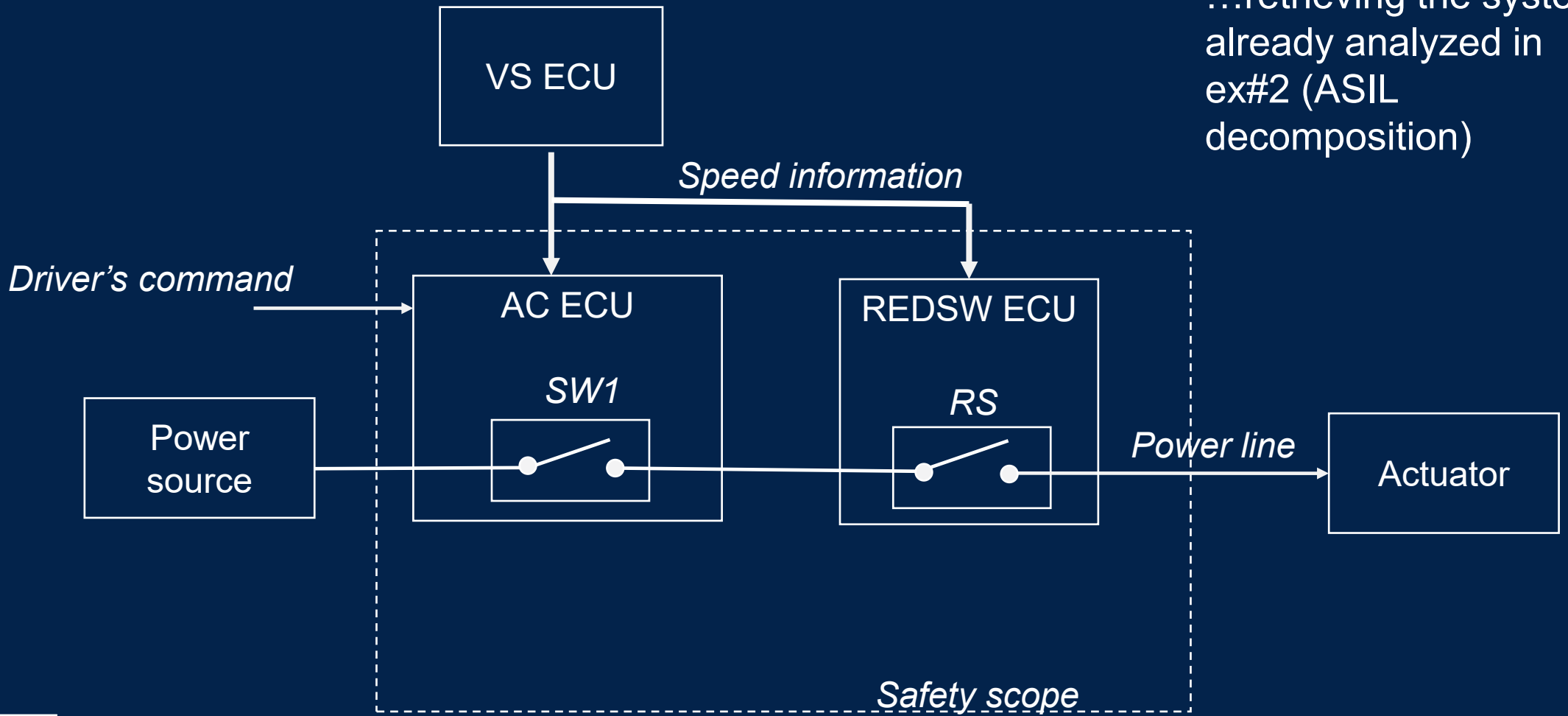
Summary:

Fault tree Analysis example based on the system described in exercitation #2

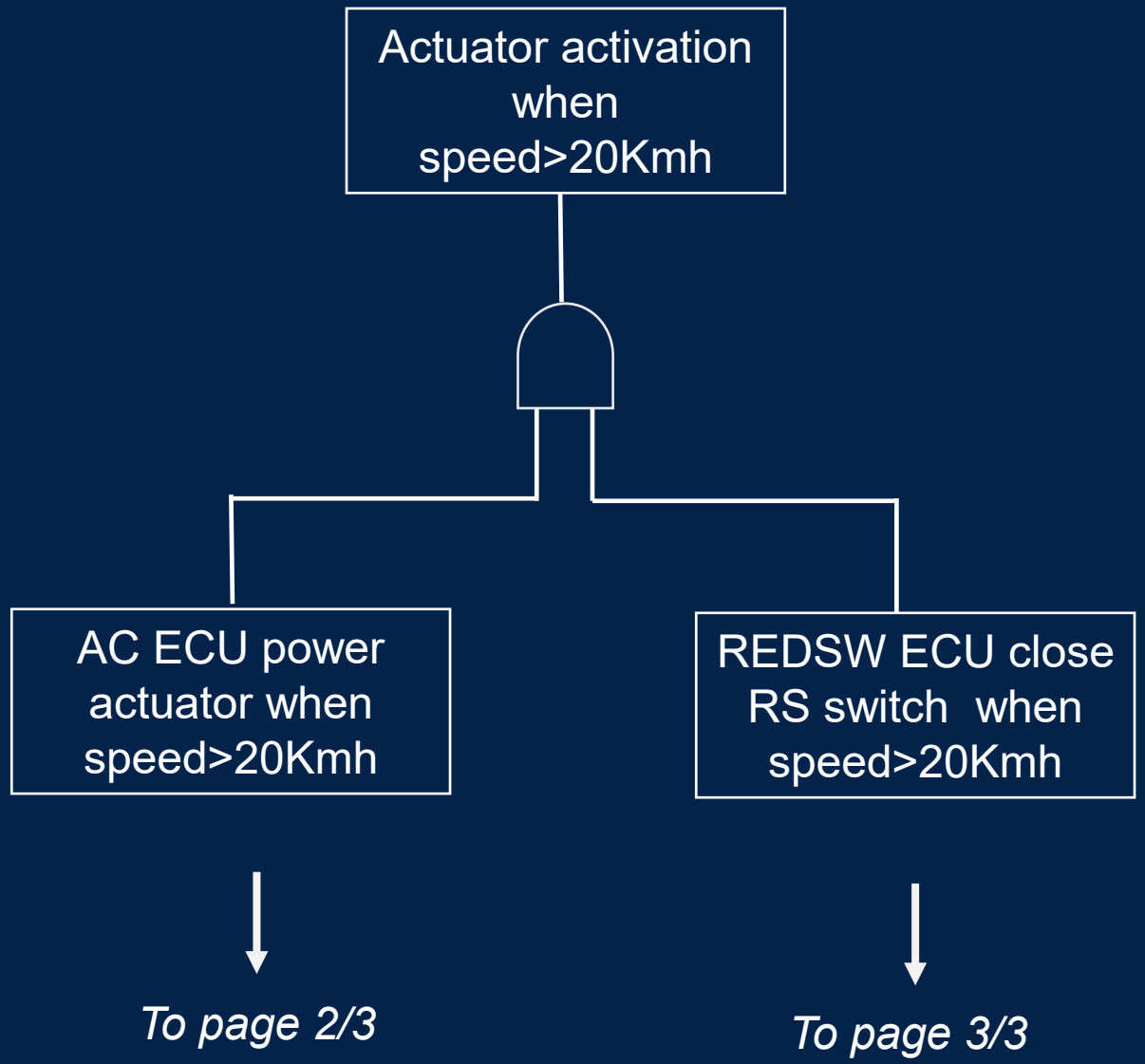
life.augmented

FTA application - example

…retrieving the system already analyzed in ex#2 (ASIL decomposition)

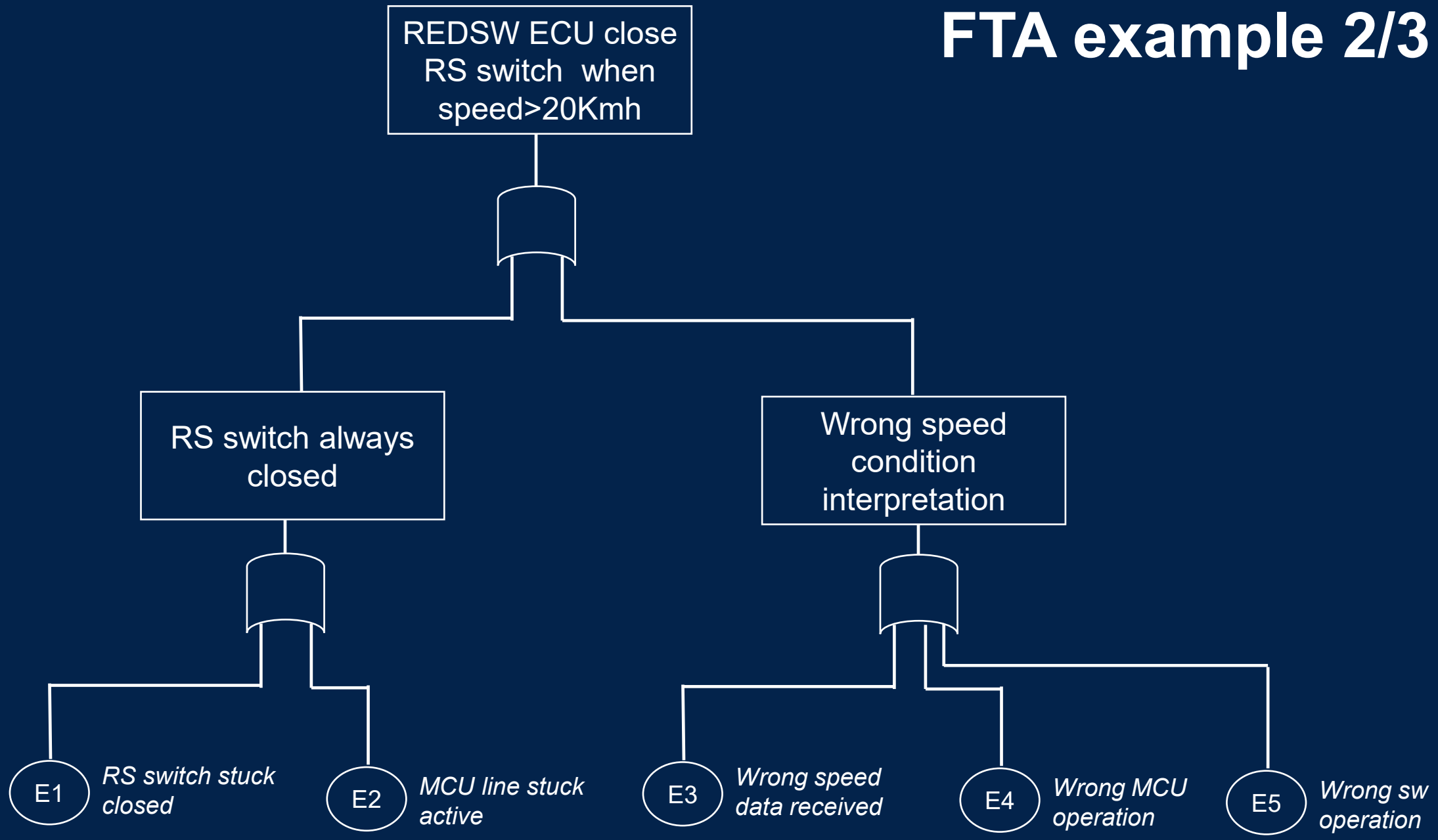


FTA example 1/3



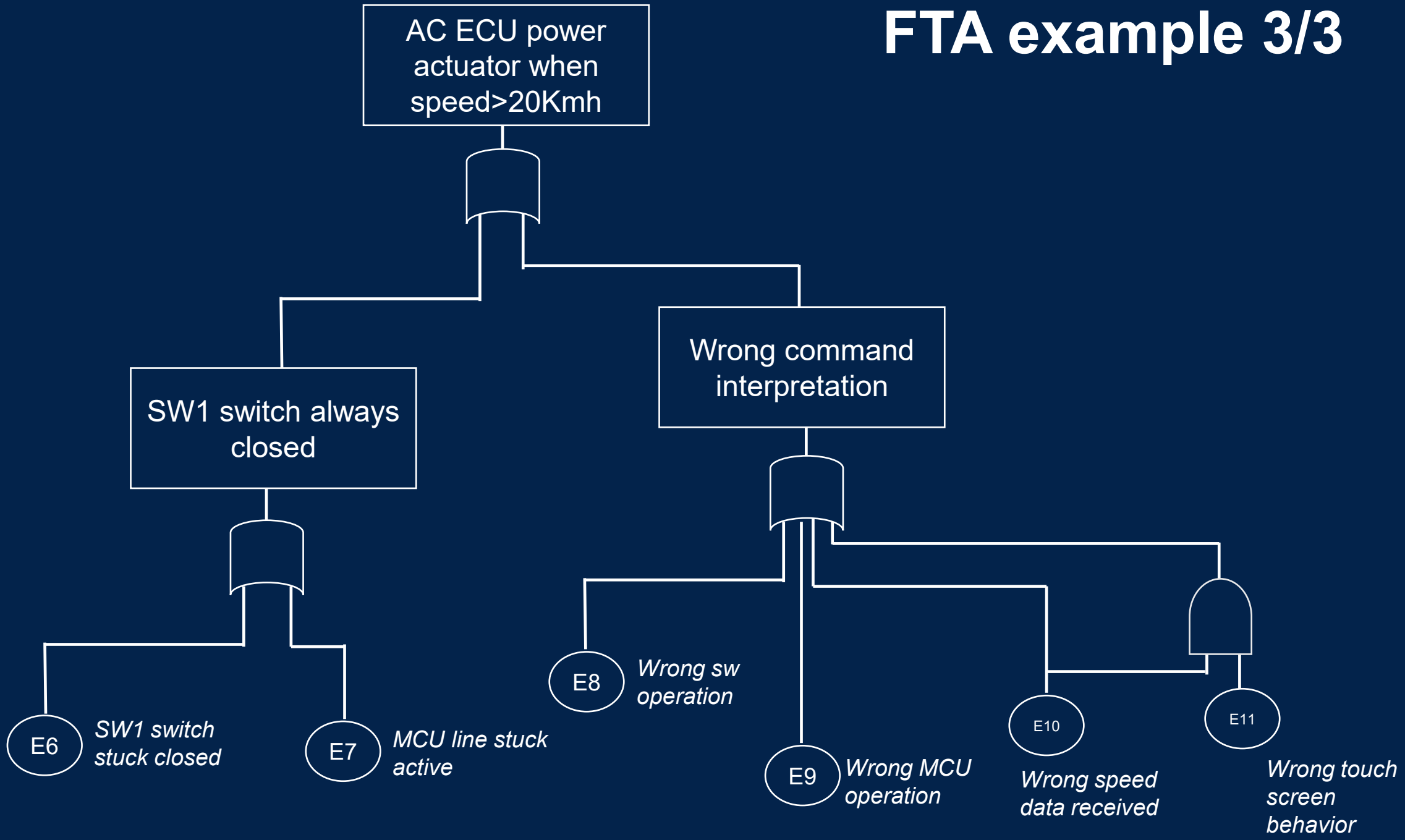
life.augmented

FTA example 2/3

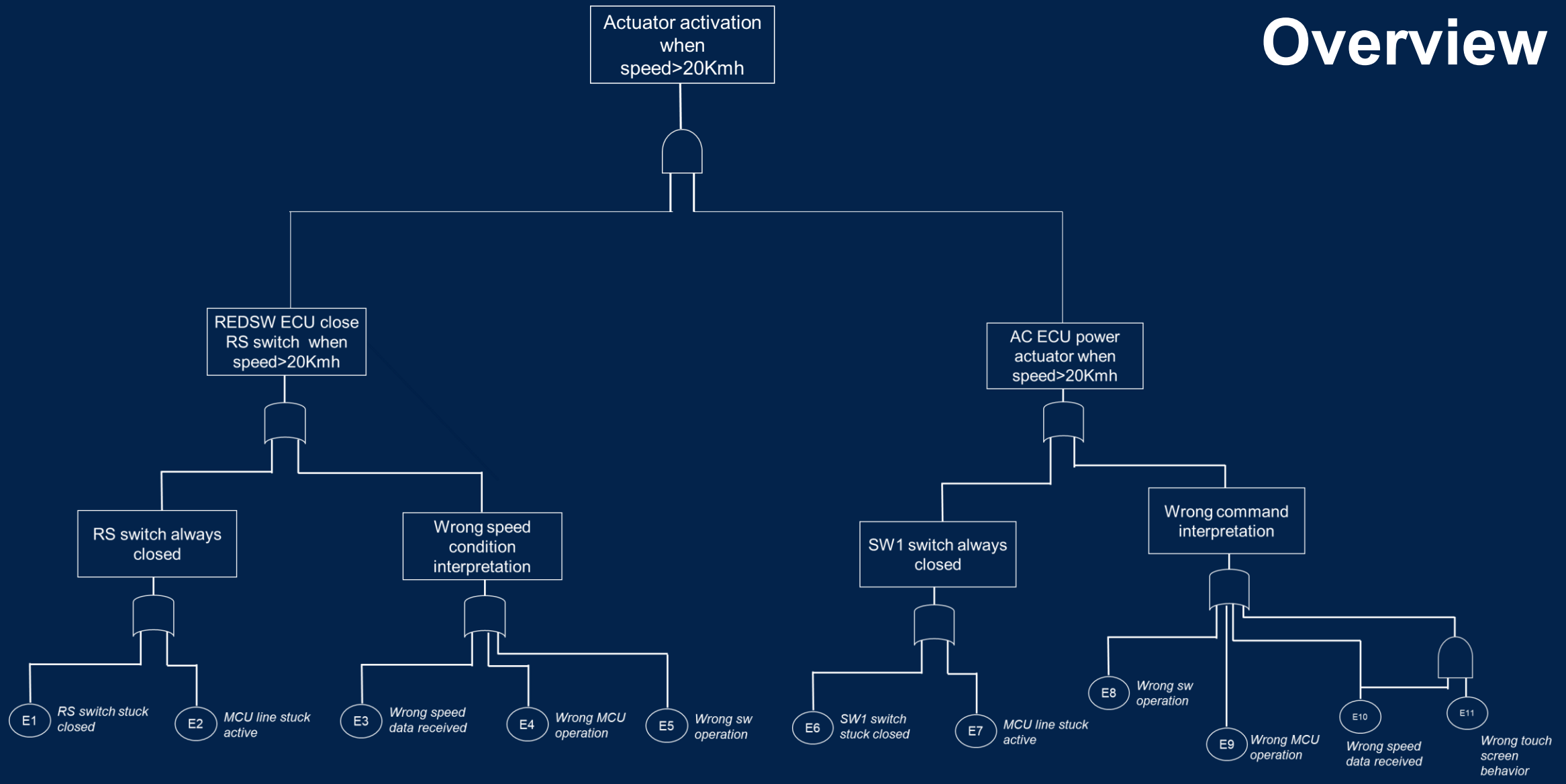


life.augmented

FTA example 3/3



Overview



life.augmented

Exercitations

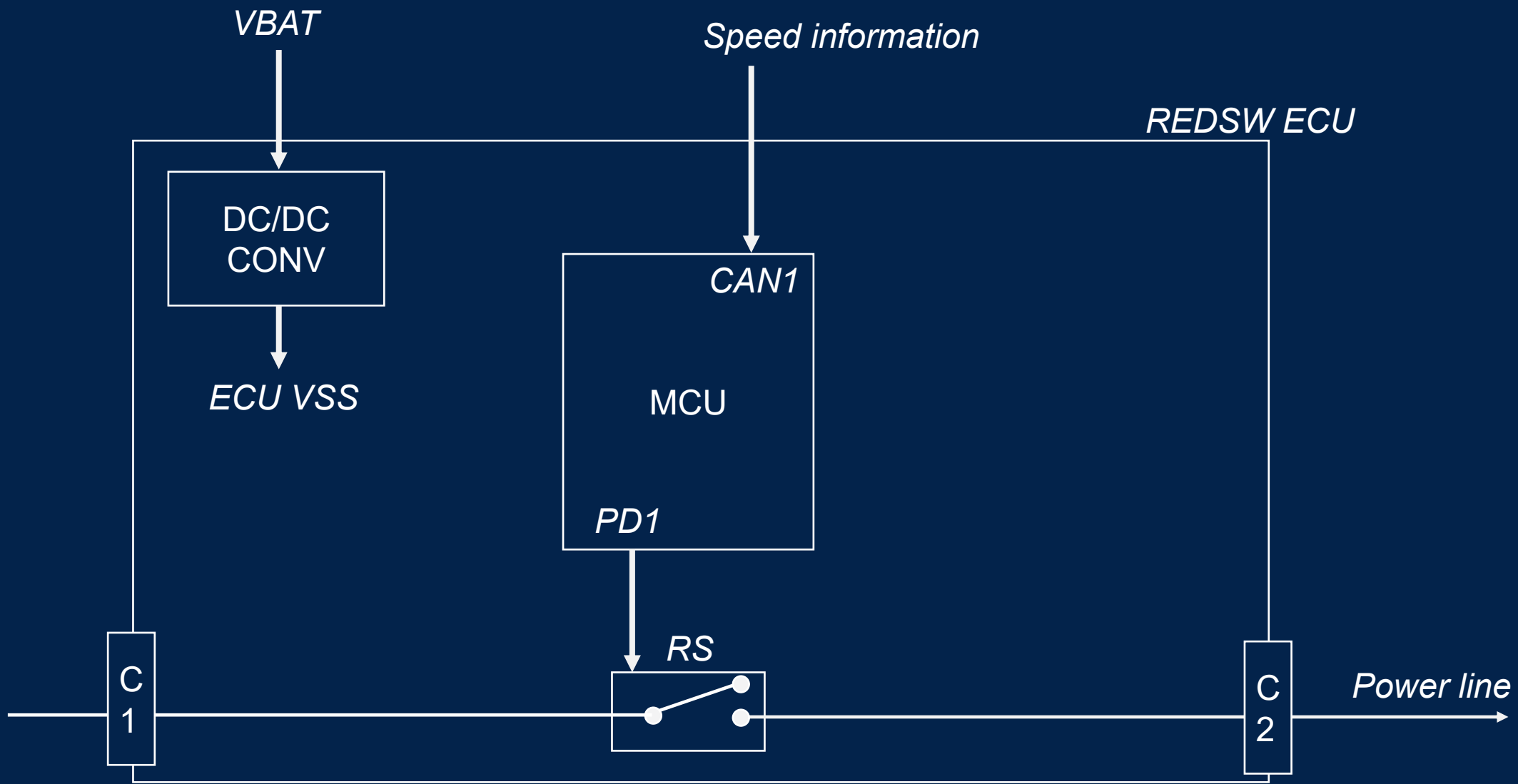
Ex #4 – FMEDA example

Summary:

- **FMEDA before diagnostics**
- **Improvement with diagnostics**

life.augmented

REDSW ECU implementation



FMEDA example – before diagnostics 1/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
RS switch	Open	Power line not connected	50	50%	100%	n/a	0%	0
	Closed	Power line always connected		50%	0%			25
DC/DC conv	Overvoltage	MCU not working correctly	30	33%	0%			10
	Undervoltage	MCU not working correctly		33%	0%			10
	No voltage	MCU unresponsive RS switch open		33%	100%	n/a	0%	0

FMEDA example 2/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
MCU/CAN1	Stuck-at	Speed wrongly computed as >20Km/h	9	33%	100%	n/a	0%	0
	Stuck-at	Speed wrongly computed as <20Km/h		33%	0%			3
	Stuck-at, open	No speed available		33%	0%			3
MCU/PD1	Stuck-at	PD1 output always on (RS closed)	4	50%	0%			2
	Stuck-at	PD1 output always off (RS open)		50%	100%	n/a	0%	0

FMEDA example 3/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
MCU	Stuck-at	No program execution	100	20%	0%		0%	0
	Stuck-at	Wrong decision/ computation (RS wrongly closed)		20%	0%			20
	Stuck-at	Wrong decision/ computation (RS wrongly open)		20%	100%	n/a		0
	Stuck-at	Wrong speed acquisition = V<20KM/h		20%	0%			20
	Stuck-at	Wrong speed acquisition = V>20KM/h		20%	100%	n/a	0%	0

FMEDA example 4/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
CN1	Open	No power supply propagation	10	50%	100%	n/a	0%	0
	Short	Short to GND on Power supply output		50%	0%			5
CN2	Open	No power supply propagation	10	50%	100%	n/a	0%	0
	Short	Short to GND on Power supply output		50%	0%			5

FMEDA example – before diagnostics

$\lambda SR(tot) = \sum \lambda SR = 50 + 30 + 9 + 4 + 100 + 10 + 10 = 213$ FIT

$\lambda SAFE = \lambda SR \times (1 - \%safe)$

$\lambda D = \lambda SR - \lambda SAFE$

$\lambda SAFE(tot) = \sum \lambda SAFE = 25 + 10 + 3 + 2 + (20 + 20) + 5 + 5 = 90$

$\lambda DD = \lambda D \times DC$, $\lambda DU = \lambda D \times (1-DC)$

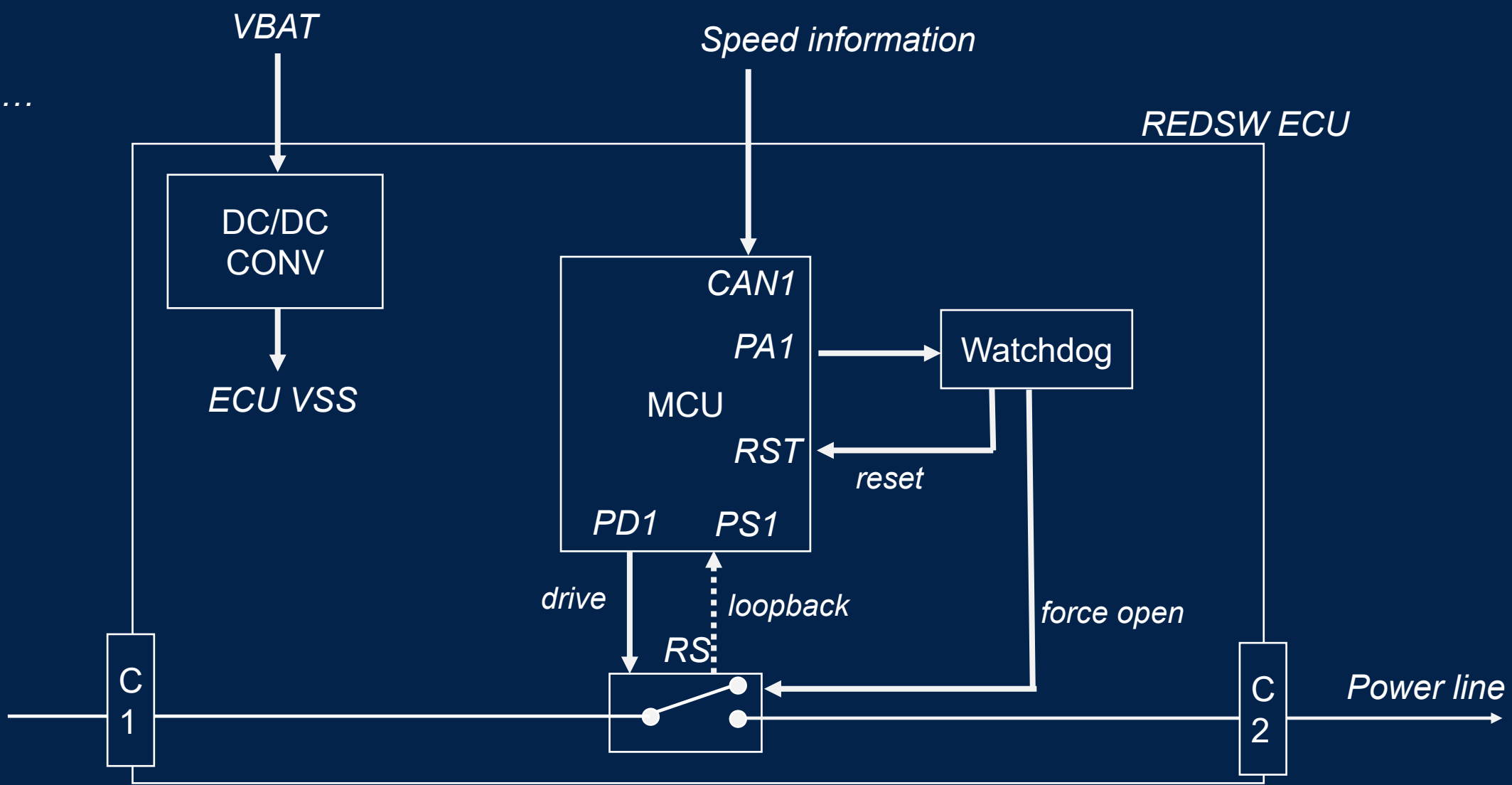
$\lambda DD(tot) = \sum \lambda DD = 0$ FIT (NO DIAGNOSTICS)

$SPF = (\sum \lambda SAFE + \sum \lambda DD) / (\sum \lambda SAFE + \sum \lambda DD + \sum \lambda DU)$

$SFF = (90 + 0)/213 = 42\%$

REDSW ECU implementation - update

Adding the needed diagnostics…



Safety mechanism table - example

Component/ Sub-component	Failure	Safety Mechanism	DC
MCU (whole)	Wrong program flow	Watchdog	90%
MCU (whole)	Wrong computation/wrong decision	Parity	60%
MCU (whole)	MCU not working correctly	Watchdog	60%
MCU/CAN block	Stuck-at	E2E protection on data	99%
MCU/GPIO driver	Stuck-at	Loopback	99%
System/power supply	Shorts to GND	AoU_powersupply	99%

FMEDA example (+diags) 1/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
RS switch	Open	Power line not connected	50	90%	100%	n/a	0%	0
	Closed	Power line always connected		10%	0%			5
DC/DC conv	Overvoltage	MCU not working correctly	30	33%	0%	Watchdog	60%	6
	Undervoltage	MCU not working correctly		33%	0%	Watchdog	60%	6
	No voltage	MCU unresponsive RS switch open		33%	100%	n/a	0%	0

FMEDA (+diags) example 2/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
MCU/CAN1	Stuck-at	Speed wrongly computed as >20Km/h	9	33%	100%	n/a	0%	0
	Stuck-at	Speed wrongly computed as <20Km/h		33%	0%	E2E protection on data	99%	0,03
	Stuck-at, open	No speed available		33%	0%	E2E protection on data	99%	0,03
MCU/PD1	Stuck-at	PD1 output always on (RS closed)	4	50%	0%	Loopback	99%	0,02
	Stuck-at	PD1 output always off (RS open)		50%	100%	n/a	0%	0

FMEDA (+diags) example 3/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
MCU	Stuck-at	No program execution	100	20%	0%	Watchdog	90%	2
	Stuck-at	Wrong decision/ computation (RS wrongly closed)		20%	0%	Parity	60%	8
	Stuck-at	Wrong decision/ computation (RS wrongly open)		20%	100%	n/a		0
	Stuck-at	Wrong speed acquisition = V<20KM/h		20%	0%	Parity	60%	8
	Stuck-at	Wrong speed acquisition = V>20KM/h		20%	100%	n/a	0%	0

FMEDA (+diags) example 4/4

Component	Failure mode	Effect	λSR	F.D.	%safe	Safety Mechanism	DC	λRF
CN1	Open	No power supply propagation	10	50%	100%	n/a	0%	0
	Short	Short to GND on Power supply output		50%	0%	AoU_powersupply	99%	0,05
CN2	Open	No power supply propagation	10	50%	100%	n/a	0%	0
	Short	Short to GND on Power supply output		50%	0%	AoU_powersupply	99%	0,05

FMEDA example – after diagnostics

λSR(tot)= ∑ λSR = 50 + 30 + 9+ 4 + 100 +10 +10 = 213 FIT

λSAFE = λSR x (1- %safe)

λD = λSR-λSAFE

λSAFE(tot)= ∑ λSAFE = 25 + 10 + 3 + 2 + (20 + 20) + 5 + 5 = 90

λDD = λD x DC , λDU = λD x (1-DC)

λDD(tot)= ∑ λDD = 71,6 FIT

DC = ∑ λDD / (∑ λDD + ∑ λDU)

DC = 103 / (103 + 71,6) = 70%

SPF = (∑ λSAFE + ∑ λDD) / (∑ λSAFE + ∑ λDD + ∑ λDU)

SFF = (110 + 71,6)/213 = 85%

Exercitations

Ex #5 – IEC61800-5-2 safety functions

Summary:

- General information
- List of safety functions and their safe state
- Implementation example

life.augmented

About IEC 61800-5-2

IEC 61800-5-2 is a product-specific standard that defines the functional safety requirements and safety functions for adjustable speed electrical power drive systems. It focuses on the implementation of safety functions like Safe Torque Off (STO) and others to ensure safe operation and risk reduction in motor control applications.

- IEC 61800-5-2 derives its safety requirements and performance levels from IEC 61508 principles.
- IEC 61800-5-2 specifies how to implement safety functions in drives to achieve the required SIL or Performance Level (PL) as defined by IEC 61508.
- Compliance with IEC 61800-5-2 ensures that drive systems meet the functional safety lifecycle and integrity requirements established by IEC 61508.
- Essentially, IEC 61800-5-2 translates the generic safety concepts and processes of IEC 61508 into concrete requirements and safety functions specific to adjustable speed drives.

About IEC 61800-5-2

IEC 61800-5-2 incorporates concepts that align with the Performance Level (PL) and modes of operation similar to those defined in IEC 61508, but with terminology and application specific to adjustable speed drive systems..

Concept	IEC 61508 Term	IEC 61800-5-2 Equivalent/Notes
Process Safety Time (PST)	PST	Response time / reaction time of safety functions
Modes of Operation	Low Demand (LD), High Demand (HD), Continuous Mode (CM)	Demand rate considerations implicit in safety function design and validation
Safety Integrity Level	SIL 1 to SIL 4	SIL or Performance Level (PL) requirements for safety functions

About IEC 61800-5-2 in this exercitation

.In this part, a survey of the main safety functions (and related safe states) defined by IEC 61800-5-2 is provided.

The safety functiosn can be split in three main categories:

- Motor stop control (safe stop)
- Motor speed control (safe speed)
- Generic control of motor/actuator

Safety functions

Safety functions related to motor stop:

Safety Function	Explanation	Related Safe State
Safe Torque Off (STO)	Prevents the drive from generating torque by disabling power to the motor power stage.	No torque generation; power to the motor power stage is removed, ensuring the motor cannot rotate.
Safe Stop 1 (SS1)	Controlled stop with deceleration, followed by removal of power to ensure safe stop.	Motor decelerates to stop, then torque off (STO) applied; motor is stationary with no torque.
Safe Stop 2 (SS2)	Controlled stop with deceleration, then power remains applied to maintain safe braking torque.	Motor decelerates to stop, brake applied and monitored; power remains applied to hold position.
Safe Operating Stop (SOS)	Motor is safely stopped but power remains applied to maintain holding torque or position.	Motor remains stationary with safe torque applied to hold position.

Safety functions

Safety functions related to control of motor speed:

Safety Function	Explanation	Related Safe State
Safe Limited Speed (SLS)	Limits the motor speed to a predefined safe maximum value.	Motor speed is limited; exceeding the limit triggers transition to safe state (e.g., STO).
Safe Direction (SDI)	Ensures the motor only rotates in a predefined safe direction.	Motor rotation allowed only in safe direction; rotation in opposite direction triggers safe state.
Safe Speed Range (SSR)	Ensures motor speed remains within a safe range (minimum and maximum limits).	Motor speed maintained within safe range; exceeding limits triggers safe state.
Safe Brake Control (SBC)	Controls and monitors the brake to ensure it is applied when required.	Brake is applied and monitored; failure to apply brake triggers safe state.

Safety functions

Safety functions related to general control of motor/actuator:

Safety Function	Explanation	Related Safe State
Safe Position (SP)	Ensures motor or actuator is in or moves to a safe position.	Motor or actuator position is maintained or moved to a safe position; deviation triggers safe state.
Safe Cam (SCA)	Ensures motor movement follows a predefined safe cam profile or path.	Motor movement follows cam profile; deviation triggers safe state.
Safe Reset (SR)	Ensures system reset only occurs under safe conditions after a fault or stop.	System reset allowed only when safe; otherwise remains in safe or fault state

Backup slides

life.augmented

Simplified Block Diagram of STO Implementation

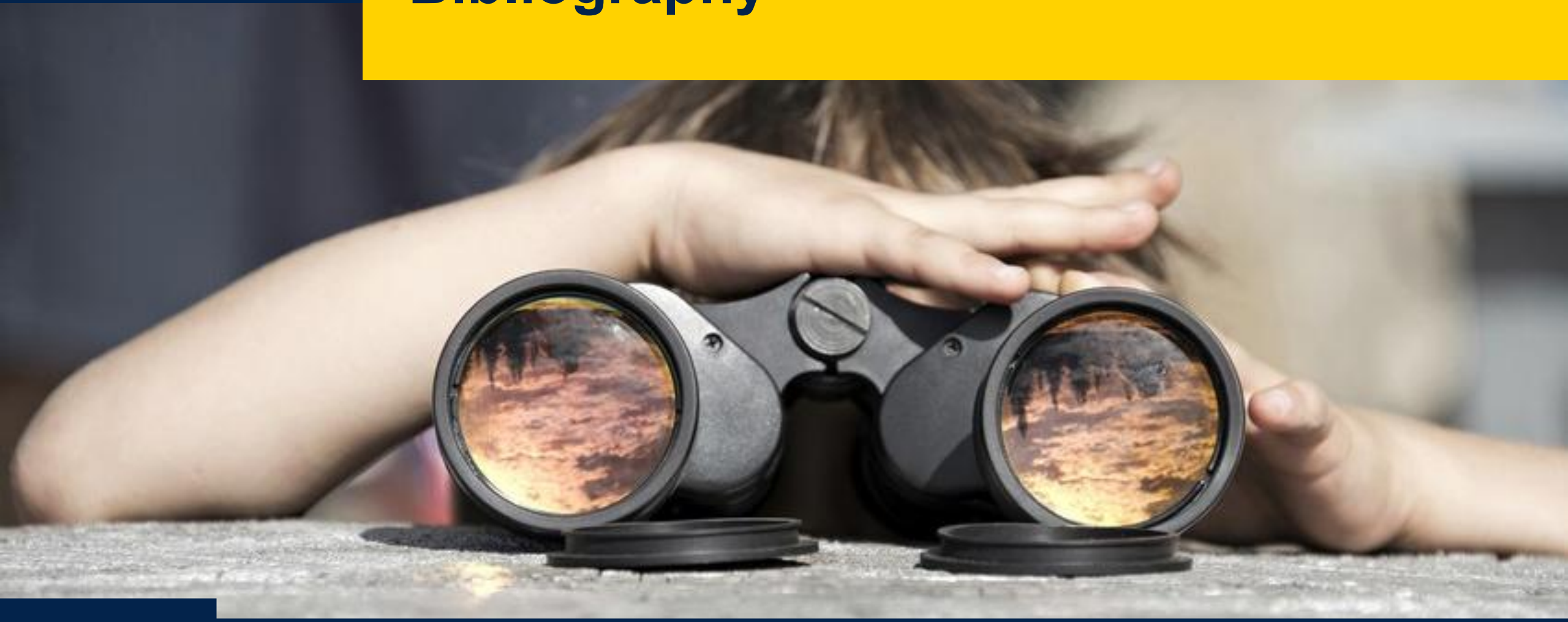
Safety Devices provide redundant STO signals.

STO Input Circuit monitors and validates dual-channel signals.

STO Logic Circuit processes inputs and controls power stage enable/disable.

Power Stage Gate Driver disables gate signals to inverter transistors to remove torque

Bibliography



life.augmented

Thank you

life.augmented