intertek
Total Quality. Assured.

FUNCTIONAL SAFETY

Jason Mauldin
Senior Consulting Engineer
Intertek Assurance

WHAT IS FUNCTIONAL SAFETY?

Functional safety concerns hazards that may arise from the installation, commissioning, use, maintenance and decommissioning of a device.

Functional safety addresses that hazards that go above the typical electrical fire and shock hazards often associated with product standards.

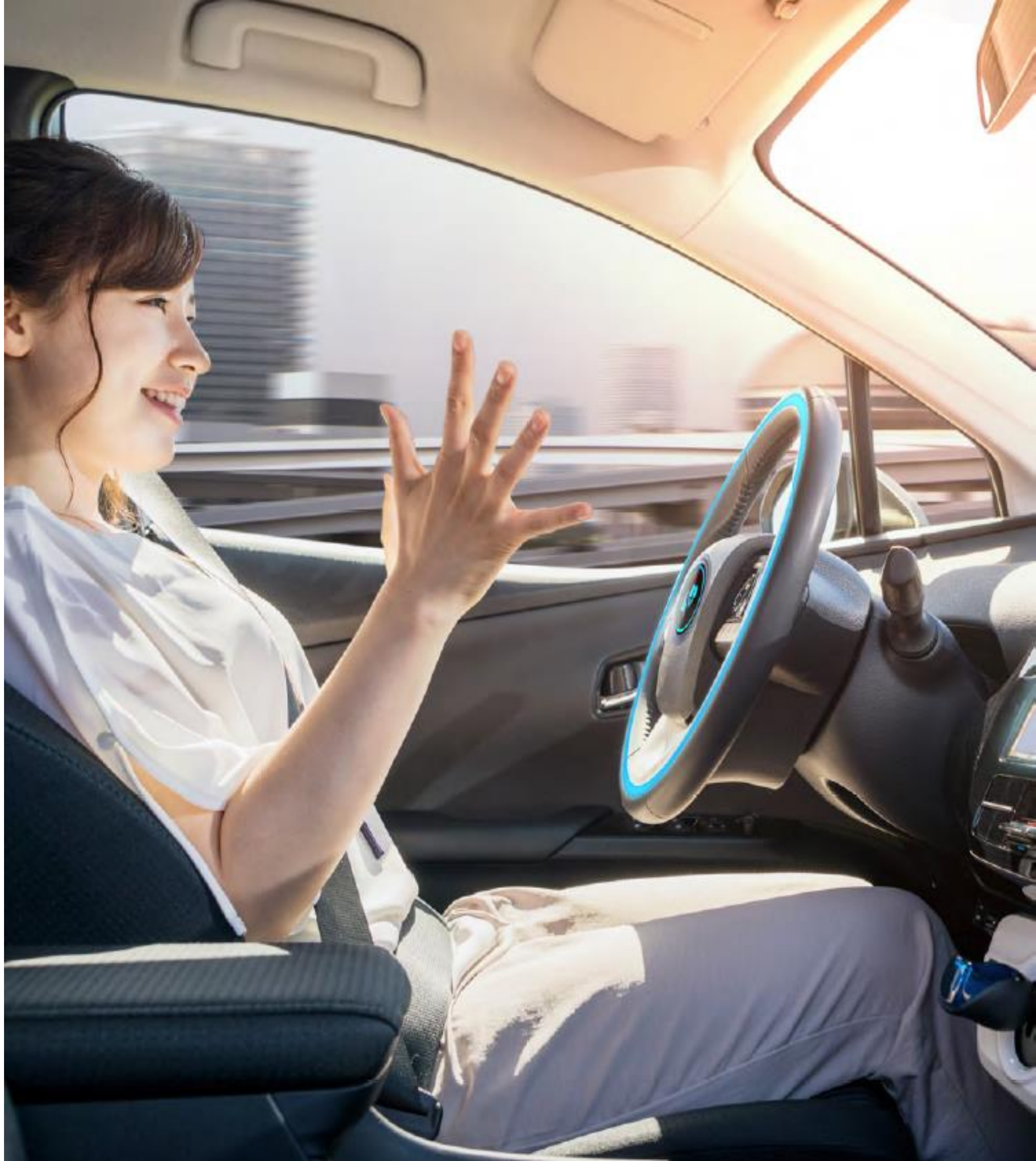
Every engineered system has risks, to people, to the environment, other equipment and the facilities.

Functional safety is the identification and planned mitigation of these risks.

WHY IS FUNCTIONAL SAFETY IMPORTANT?

Functional safety allows for a more complete evaluation of the hazards associated with a product. Traditional safety standards are static, prescriptive and slow to change.

Today’s markets move quickly and grow faster than standards can adapt. Functional Safety allows these new products to be evaluated against a common safety approach.

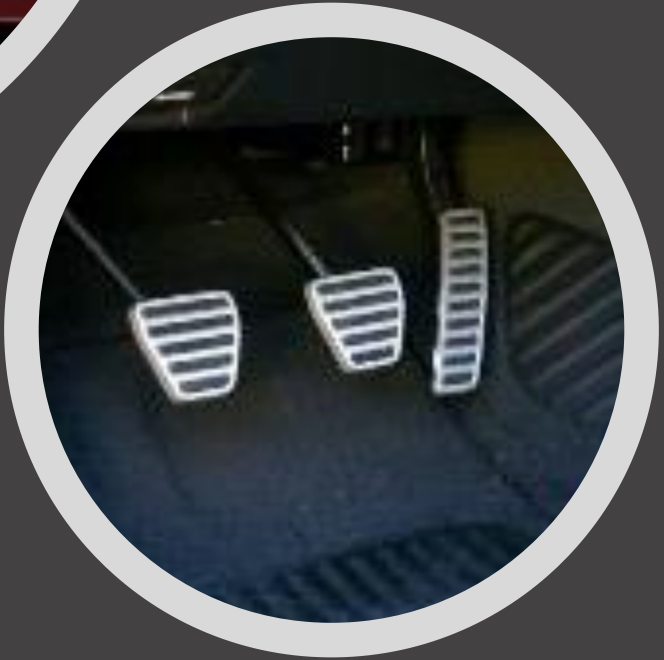


HOW DO I KNOW IF FUNCTIONAL SAFETY APPLIES TO MY PRODUCT?

Conducting a Risk Assessment is the best approach to determine if functional safety applies to your product. When risks are identified that are not covered by the safety standard, then additional functional safety requirements may be beneficial.

It is often necessary to review the risk assessment with your customers to confirm complete coverage of all risks.

The product safety standard may specify a functional safety evaluation for certain functions.



FUNCTIONAL SAFETY - EXAMPLES

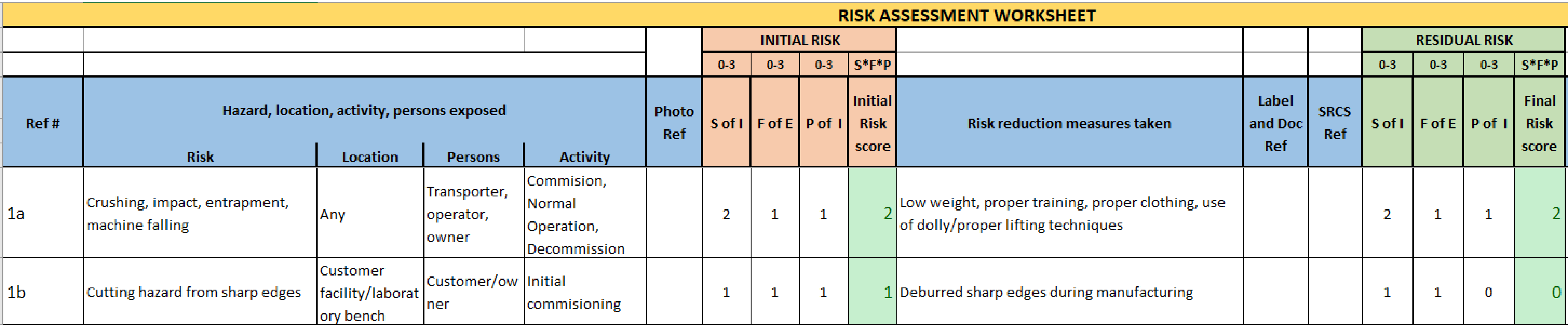
- Object avoidance in AGV
- Water Temperature Regulation in Water Heater
- Automotive Brake Control
- Access Control with Light Curtain
- Lawn Mower – Blade Torque

WHAT IS A RISK ASSESSMENT?

A risk assessment is a development activity that is used to identify and analyze potential hazards associated with a product.

The process begins by identifying hazards based on normal and abnormal use cases. Once the hazards are identified, they are assessed based on their severity and other factors.

Conducting a risk assessment allows your company to focus on the highest level risks associated with your product and affords you the opportunity to either accept those risks in the product, or engineer means to remove them.



RISK ASSESSMENT WORKSHEET																
						INITIAL RISK							RESIDUAL RISK			
						0-3	0-3	0-3	S*F*P				0-3	0-3	0-3	S*F*P
Ref #	Hazard, location, activity, persons exposed				Photo Ref	S of I	F of E	P of I	Initial Risk score	Risk reduction measures taken	Label and Doc Ref	SRCS Ref	S of I	F of E	P of I	Final Risk score
	Risk	Location	Persons	Activity												
1a	Crushing, impact, entrapment, machine falling	Any	Transporter, operator, owner	Commision, Normal Operation, Decommission		2	1	1	2	Low weight, proper training, proper clothing, use of dolly/proper lifting techniques			2	1	1	2
1b	Cutting hazard from sharp edges	Customer facility/laboratory bench	Customer/owner	Initial commisioning		1	1	1	1	Deburred sharp edges during manufacturing			1	1	0	0

SAFETY CLASSIFICATIONS

IEC 61508 - SIL: Safety Integrity Level

SIL 1, 2, 3, 4

ISO 13849 – PL: Performance Levels

PLA, PLB, PLC, PLD, PLE

ISO 26262 – ASIL: Automotive Safety Integrity Level

QM, ASIL A, B, C, D

Frequency	5	SIL 3	SIL 4	X	X	X
	4	SIL 2	SIL 3	SIL 4	X	X
	3	SIL 1	SIL 2	SIL 3	SIL 4	X
	2	-	SIL 1	SIL 2	SIL 3	SIL 4
	1	-	-	SIL 1	SIL 2	SIL 3
		1	2	3	4	5
		Severity				

IEC 61508 – THE UMBRELLA STANDARD

Process Industry:
IEC 61511
ANSI/ISA S84.00.01

Machinery:
IEC 62061
ISO 13849

Automotive:
ISO 26262

Software:
UL 1998

Solid-State controllers:
UL 991

Nuclear:
IEC 61513
IEC 60880-2
IEC 61238

Railway:
EN 50126
EN 50128
EN 50129

Military:
MIL STD 882

Communication:
IEC 61784-3

EMC:
IEC 61000-1-2

Immunity:
IEC 61326-3

Gas Detection:
EN 50402

Power Drives:
IEC 61800-5-2

Medical Software:
IEC 62304

End-Product standards:
IEC/UL 60730-1
IEC 60335-1
IEC 61010-1

DOES MY DESIGN REQUIRE REDUNDANCY?

Not necessarily!

The redundancy requirement will depend on many factors:

The specific safety rating.

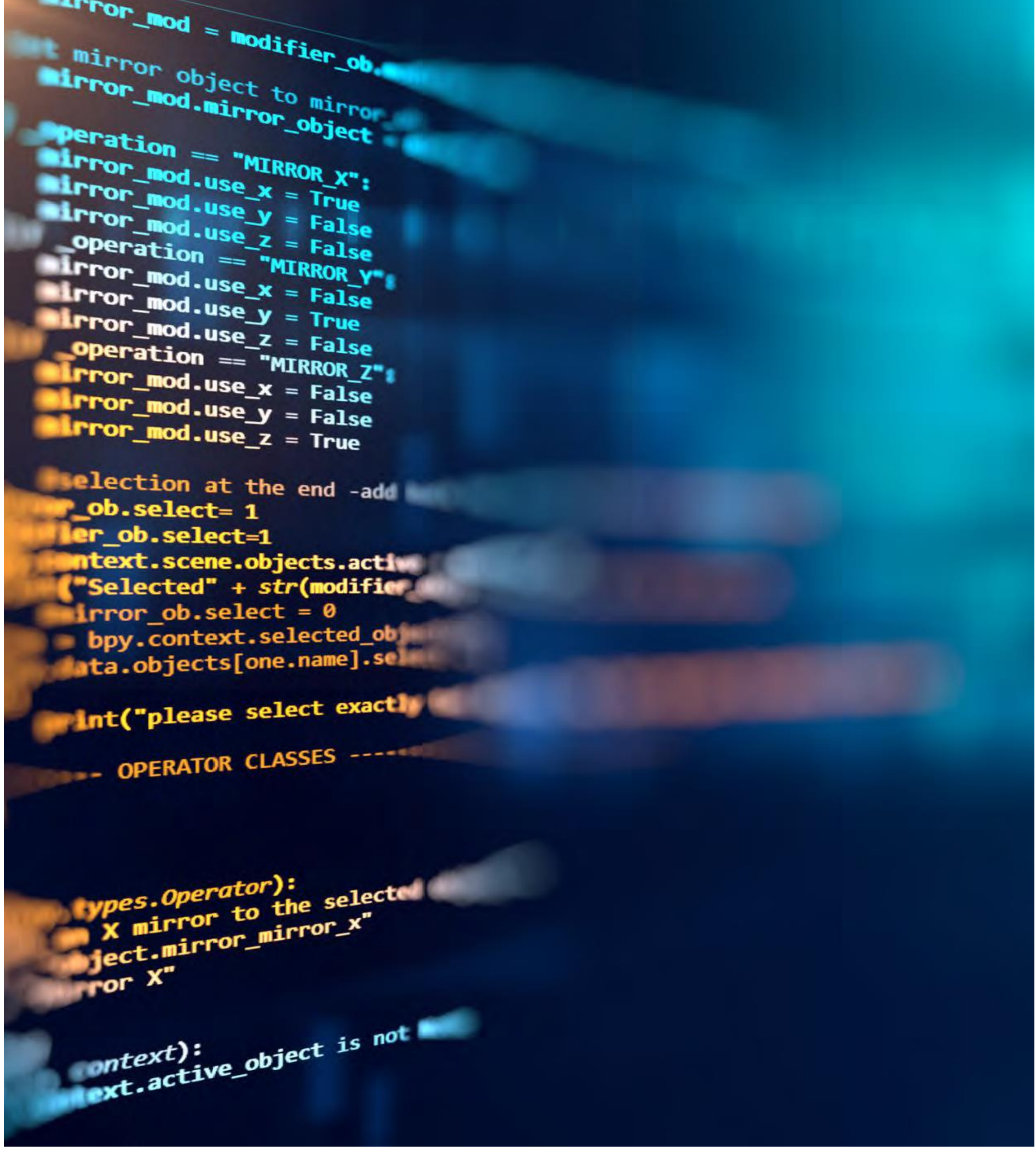
The level of supervision or diagnostic coverage of your product.

Other factors based on how the product is incorporated into the process or product.

DO FUNCTIONAL SAFETY REQUIREMENTS APPLY TO SOFTWARE?

The output of the risk assessment can be used to identify specific functions and "parts" of your system that are responsible for functional safety functions.

Does software play a part in one of those functions?



SOFTWARE EVALUATION

The evaluation focuses on the following items:

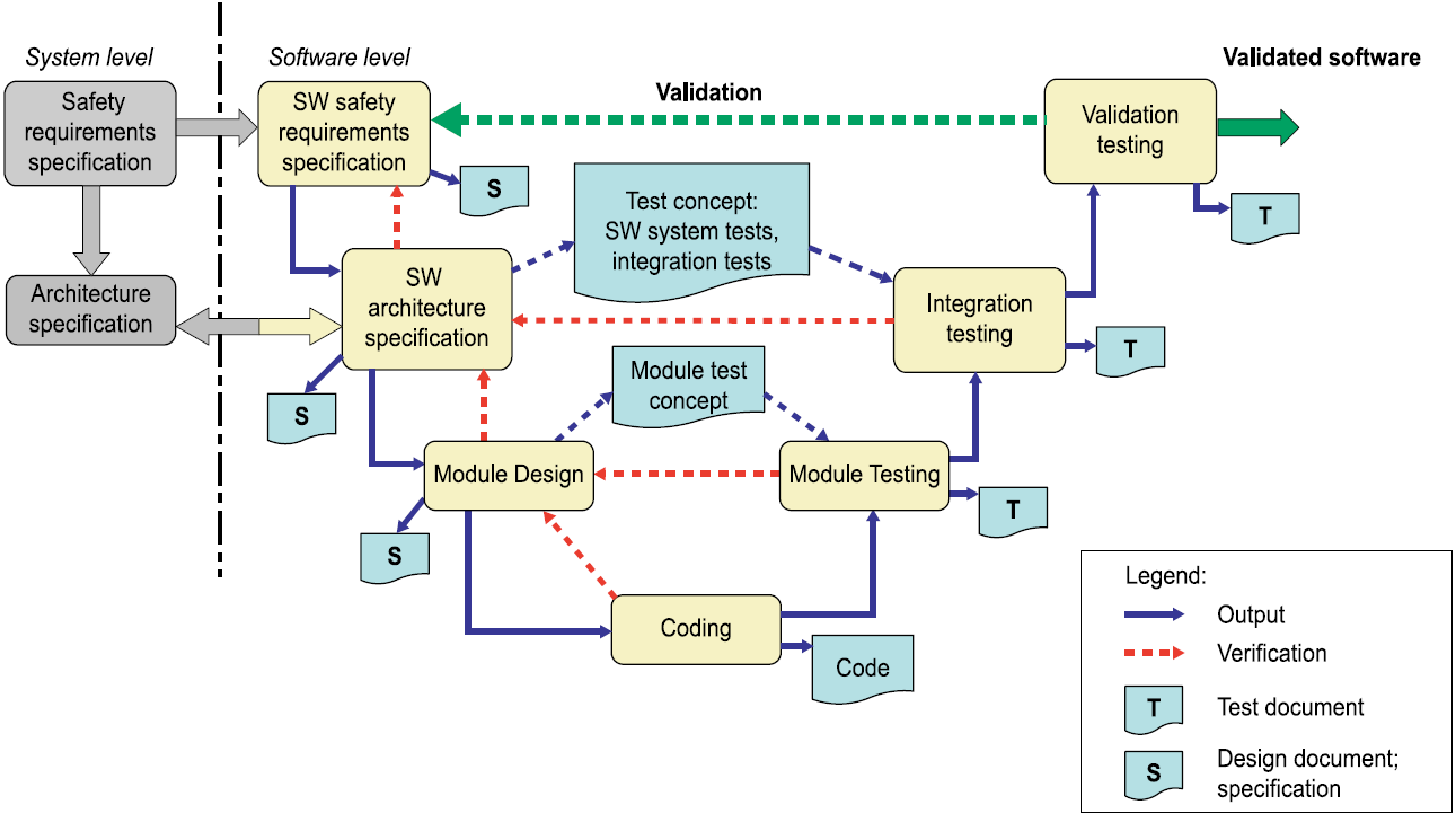
- The development process

- Review of critical portions of software code

- Review of the electrical architecture and components of the safety circuit

- Review of the tests conducted

FUNCTIONAL SAFETY - DEV. LIFECYCLE


System level
Software level
Validated software
Safety requirements specification
SW safety requirements specification
Validation
Validation testing
S
T
Test concept: SW system tests, integration tests
Architecture specification
SW architecture specification
Integration testing
T
S
Module test concept
Module Design
Module Testing
T
S
Coding
Code
Legend:
Output
Verification
T
Test document
S
Design document; specification

IS A CERTIFICATION REQUIRED?

- It depends.

- Certification is not always required, depending on the type of product. Automotive products typically do not require a certification. Household appliances are generally certified by an independent third party.

In either case, a complete documentation package will provide a level of confidence to correspond with a declared safety rating.

Questions???

Jason Mauldin, Senior Consultant Engineer

☎ +1 (919) 247-4497

✉ jason.mauldin@intertek.com

🖱 intertek.com