

CIP Safety Protocol Training

Session 4: Implementation, Testing, and Next Steps

Virtual Training Courses



ODVA[®]

Before We Begin

- Introductions
- All attendees are automatically muted with no video connection as a default.
- Please use the Q&A to ask questions, not the chat. We will address questions as they come in.
- At the end if there is time, we will take questions verbally from the attendees. We will advise if and when there is time for you to “raise your hand” if you have a question.
- Please complete the 5 question post session survey. The survey will launch when you close out of the webinar.

Review - Yesterday We Covered:

CIP Safety Details

- Configuration of CIP Safety devices (Type 1 vs Type 2 Safety Open)
- Error mitigation techniques (Time Expectation, Redundant Cross-check, End-to-end CRCs)
- Time Coordination and Correction
 - Timestamp is 128us 16-bit counter (Extended format adds 16-bit rollover count)
 - Ping Interval is RPI/EPI-based
- Safety I/O packet format
 - Base/Extended
 - Short/Long (1-2 byte vs 3-250 byte)
- Originator/Target roles
- Producer/Consumer relationship to Input/Output and Time Coordination
 - Producers send Data Message with timestamp; maintain coordinated time for consumer(s)
 - Consumers send Time Coordination message once per Ping Interval
 - Multicast consumers receive Time Correction message to translate common timestamp
- Safety protocol messages composed of sections according to format
- Safety I/O connections provide high-integrity, functionally safe application data

CIP Safety WireShark Demo

David Crane
ODVA

ODVA[®]

EtherNet/IP Wireshark

- TCP/IP session
- Encapsulation
- Forward Open
 - Request
 - Response
- EtherNet/IP I/O

The image shows a Wireshark capture of an EtherNet/IP session. The main pane displays a list of network packets with columns for No., Time, Src, Dst, Protocol, Source Port, and Info. The packets are numbered 9 through 33. The 'Info' column provides details for each packet, such as TCP flags, session IDs, and connection manager actions. The bottom pane shows the detailed view of a selected packet (No. 32), which is an EtherNet/IP I/O packet. The detailed view shows the encapsulation layers: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and EtherNet/IP (Industrial Protocol). The EtherNet/IP details include the Session ID (0x00D77F81) and the action (Send RR Data). The status bar at the bottom indicates that 2884 packets are displayed (100.0%) and the profile is CIP Safety.

No.	Time	Src	Dst	Protocol	Source Port	Info
9	2.477764	192.168.1.11	192.168.1.32	TCP		56922 → 44818 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 WS=1
10	2.477764	192.168.1.32	192.168.1.11	TCP		44818 → 56922 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
11	2.478127	192.168.1.11	192.168.1.32	TCP		56922 → 44818 [ACK] Seq=1 Ack=1 Win=8192 Len=0
12	2.478128	192.168.1.11	192.168.1.32	ENIP		Register Session (Req), Session: 0x00000000
13	2.480309	192.168.1.32	192.168.1.11	ENIP		Register Session (Rsp), Session: 0x00D77F81
14	2.480309	192.168.1.11	192.168.1.32	TCP		56922 → 44818 [ACK] Seq=29 Ack=29 Win=8164 Len=0
15	2.480310	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Class (0x31c))
16	2.481741	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open
17	2.481741	192.168.1.11	192.168.1.32	TCP		56922 → 44818 [ACK] Seq=135 Ack=141 Win=8080 Len=0
18	2.482079	192.168.1.32	192.168.1.11	ENIP		Unregister Session (Rsp), Session: 0x00070716
19	2.482081	192.168.1.32	192.168.1.11	TCP		44818 → 56744 [FIN, PSH, ACK] Seq=25 Ack=1 Win=4234 Len=0
20	2.482081	192.168.1.11	192.168.1.32	TCP		56744 → 44818 [RST] Seq=1 Win=0 Len=0
21	2.482081	192.168.1.11	192.168.1.32	TCP		56744 → 44818 [RST] Seq=1 Win=0 Len=0
22	2.500138	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=0000000001, T->O
23	2.511143	Rockwell_2a:3e:...	Broadcast	ARP		Who has 192.168.1.75? Tell 192.168.1.3
24	2.519974	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=0000000002, T->O
25	2.540193	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=0000000003, T->O
26	2.560139	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=0000000004, T->O
27	2.560140	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Class (0x31c)) (Assembly)
28	2.562364	192.168.1.32	192.168.1.11	CIP CM		Connection failure: Connection Manager - Forward Open
29	2.562365	192.168.1.11	192.168.1.32	TCP		56922 → 44818 [ACK] Seq=281 Ack=197 Win=8136 Len=0
30	2.569635	192.168.1.11	192.168.1.32	CIP I/O	2222	Connection: ID=0x00D77F83, SEQ=0000000000, O->T
31	2.580061	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=0000000005, T->O
32	2.580811	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (Assembly) [Safety]
33	2.580812	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (Assembly) [Safety]

▶ Frame 32: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface 0
▶ Ethernet II, Src: Rockwell_d4:6e:89 (00:1d:9c:d4:6e:89), Dst: Rockwell_96:ef:9d (f4:54:33:96:ef:9d)
▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.32
▶ Transmission Control Protocol, Src Port: 56922, Dst Port: 44818, Seq: 281, Ack: 197, Len: 170
▶ EtherNet/IP (Industrial Protocol), Session: 0x00D77F81, Send RR Data
▶ Common Industrial Protocol
▶ CIP Connection Manager

Text item (text), 88 bytes | Packets: 2884 · Displayed: 2884 (100.0%) | Profile: CIP Safety

Filtered view "cipcm"

- Originator
- Target
- Forward Open
 - Standard CIP Parameters

No.	Time	Src	Dst	Protocol	Source Port	Info
33	2.580812	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (Assembly) (Assembly) [Safety]
70	2.924214	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open
72	2.924215	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open
89	3.000718	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (Assembly) (Assembly) [Safety]
92	3.000719	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (Assembly) (Assembly) [Safety]
164	3.344345	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open
166	3.344353	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open

```
...0 .... = Priority: 0
.... 0101 = Tick time: 5
Time-out ticks: 155
Actual Time Out: 4960ms
O->T Network Connection ID: 0x00000000
T->O Network Connection ID: 0x01f5425b
Connection Serial Number: 0x7be5
Originator Vendor ID: Rockwell Automation/Allen-Bradley (0x0001)
Originator Serial Number: 0x00ef45b4
Connection Timeout Multiplier: *8 (1)
Reserved: 0x000000
O->T RPI: 1000.000ms
O->T Network Connection Parameters: 0x4406
T->O RPI: 10.000ms
T->O Network Connection Parameters: 0x4408
Transport Type/Trigger: 0x20, Direction: Client, Trigger: Application Object, Class: 0
Connection Path Size: 45 words
```

CIP Safety Parameters

- Logical Segment "Safety"
- Extended Format
- Safety Configuration ID
 - SCID (CRC + Timestamp)
- Device Unique IDs
 - TUNID
 - OUNID
- PIEM
 - EPIs per Ping Interval
- NTEM
 - Max age of data (128us ticks)
- CPCRC
 - CRC over safety parameters

The image shows a Wireshark capture of CIP CM (Connection Manager) packets. The packet list pane shows several packets between 192.168.1.11 and 192.168.1.32. Packet 32 is selected, and its details pane is expanded to show the Path Segment structure. The details pane is annotated with red boxes and arrows pointing to the list on the left.

No.	Time	Src	Dst	Protocol	Source Port	Info
15	2.480310	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Class (0x31c)
16	2.481741	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open
27	2.560140	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Class (0x31c)
28	2.562364	192.168.1.32	192.168.1.11	CIP CM		Connection failure: Connection Manager - Forward
32	2.580811	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (As
33	2.580812	192.168.1.11	192.168.1.32	CIP CM		Connection Manager - Forward Open (Assembly) (As
70	2.924214	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open
72	2.924215	192.168.1.32	192.168.1.11	CIP CM		Success: Connection Manager - Forward Open

Details of Path Segment: 0x50 (Safety Segment):

- 010. = Path Segment Type: Network Segment (2)
- ...1 0000 = Network Segment Type: Safety Segment (16)
- Network Segment Length: 30 words
- Safety Format: Extended Format (2)
- Extended Format
 - Reserved: 0x00
 - Configuration CRC: 0xf818c28b
 - Configuration Timestamp: Apr 1, 2016 00:20:12.874000000 UTC
 - Time Correction EPI: 0
 - Time Correction Network Connection Parameters: 0x0000
 - Target UNID: 44acf603b14102000000
 - Originator UNID: 7148d301573f02000000
 - Ping Interval EPI Multiplier: 19
 - Time Coord Msg Min Multiplier: 0
 - Network Time Expectation Multiplier: 625
 - Timeout Multiplier: 2
 - Max Consumer Number: 1
 - Max Fault Number: 5
 - Connection Param CRC: 0xd726f0f4
 - Time Correction Connection ID: 0xffffffff
 - Initial Timestamp: 0xffff
 - Initial Rollover Value: 0xffff

Forward Open Response

- PID or CID
- Extended format initial value of 32-bit timestamp

The image shows a Wireshark capture of a CIP Forward Open Response packet. The packet list pane shows a sequence of packets between 192.168.1.11 and 192.168.1.32. Packet 70 is the selected packet, a CIP CM response from 192.168.1.32 to 192.168.1.11. The packet details pane shows the following structure:

- Internet Protocol Version 4, Src: 192.168.1.32, Dst: 192.168.1.11
- Transmission Control Protocol, Src Port: 44818, Dst Port: 56922, Seq: 197, Ack: 623, Len: 124
- EtherNet/IP (Industrial Protocol), Session: 0x00D77F81, Send RR Data
- Common Industrial Protocol
- CIP Connection Manager
 - Service: Forward Open (Response)
 - Command Specific Data
 - O->T Network Connection ID: 0x00d77fe8
 - T->O Network Connection ID: 0x0175425a
 - Connection Serial Number: 0x7be8
 - Originator Vendor ID: Rockwell Automation/Allen-Bradley (0x0001)
 - Originator Serial Number: 0x00ef45b4
 - O->T API: 20.000ms
 - T->O API: 380.000ms
 - Application Reply Size: 7 words
 - Reserved: 0x00
 - Safety Application Reply Data
 - Consumer Number: 65535
 - PID/CID
 - Target Vendor ID: Rockwell Automation/Allen-Bradley (0x0001)
 - Target Device Serial Number: 0x00d1f121
 - Target Connection Serial Number: 0x0001
 - Initial Timestamp: 5182
 - Initial Rollover Value: 5204

EtherNet/IP I/O "enip" filter

- EtherNet/IP I/O (UDP)
- Related Forward Open
- Standard CIP I/O Message

The image shows a Wireshark capture of EtherNet/IP traffic. The packet list pane shows a series of CIP I/O messages. Packet 74 is highlighted with a red box and an arrow pointing to the list. The packet details pane for packet 74 is expanded, showing the following structure:

- User Datagram Protocol, Src Port: 2222, Dst Port: 2222
- EtherNet/IP (Industrial Protocol)
 - Item Count: 2
 - [Connection Information: 0->T]
 - [Connection Path: [Key], Class: 0x031C, Instance: 0x00, Connection Point: 0x8402, Connection Point: 0x0402]
 - [0->T API: 20.000ms]
 - [T->O API: 20.000ms]
 - [CIP Connection Index: 0]
 - [Forward Open Request In: 15]
 - Common Industrial Protocol, I/O
 - CIP Sequence Count: 45
 - 32-bit Header: 0x00000001, Run/Idle: Run
 - Data: ffffffff00000000

The status bar at the bottom indicates: Forward Open Request In (enip.fwd_open_in) | Packets: 2884 · Displayed: 2847 (98.7%)

CIP Safety I/O "Data"

- CIP Safety I/O Data
 - Sent by Producer
- Safety data message
 - Application Data
 - Mode Byte
 - CRCs
 - Timestamp

Wireshark3.pcapng

No.	Time	Src	Dst	Protocol	Source Port	Info
76	2.949495	192.168.1.11	192.168.1.32	CIP I/O	2222	Connection: ID=0x00D77F83, SEQ=0000000019, O->T
77	2.959976	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=0000000024, T->O
78	2.960841	192.168.1.11	192.168.1.32	CIP Safety	2222	Connection: ID=0x00D77FE8, SEQ=0000000000, O->T
79	2.960841	192.168.1.11	192.168.1.32	CIP Safety	2222	Connection: ID=0x00D77FE7, SEQ=0000000000, O->T
80	2.962350	192.168.1.32	192.168.1.11	CIP Safety	2222	Connection: ID=0x0175425A, SEQ=0000000001, T->O
81	2.965026	192.168.1.32	192.168.1.11	CIP Safety	2222	Connection: ID=0x00F54265, SEQ=0000000001, T->O
82	2.969370	192.168.1.11	192.168.1.32	CIP I/O	2222	Connection: ID=0x00D77F83, SEQ=0000000020, O->T

▶ Ethernet II, Src: Rockwell_d4:6e:89 (00:1d:9c:d4:6e:89), Dst: Rockwell_96:ef:9d (f4:54:33:96:ef:9d)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.32
 ▶ User Datagram Protocol, Src Port: 2222, Dst Port: 2222
 ▲ EtherNet/IP (Industrial Protocol)
 ▶ Item Count: 2
 ▲ [Connection Information: O->T]
 ▶ [Connection Path: Port: Backplane, Address: 2, [Key], Assembly, Instance: 0x0360, Assembly, Instance: 0x21, Assembly, I
 [O->T API: 20.000ms]
 [T->O API: 380.000ms]
 [CIP Connection Index: 2]
 [Forward Open Request In: 32]

▲ Common Industrial Protocol, Safety
 Data: 00
 ▲ Mode Byte: 0x14
 00 = Ping Count: 0
 1.. = Not TBD Bit: True
 0... = TBD 2 Bit Copy: False
 ...1.... = Not Run/Idle: True
 ..0.... = TBD Bit: False
 .0.... = TBD 2 Bit: False
 0.... = Run/Idle: False
 CRC S5_0: 0xed
 CRC S5_1: 0x75
 Timestamp: 0
 CRC S5_2: 0x26 [correct]
 [CRC S5 Status: Good]

Timestamp (cipsafety.timestamp), 2 bytes

Packets: 2884 · Displayed: 2847 (98.7%)

Ping Interval is controlled by "producer" setting the Mode Byte's "Ping Count"

Timestamp is zero until connection established by "consumer" sending Time Coordination Message (TCM)

CIP Safety I/O "TCM"

- CIP Safety I/O TCM
 - Sent by Consumer
- Time coordination message (a.k.a. "ping response")
 - ACK Byte
 - Consumer time

Wireshark3.pcapng

No.	Time	Src	Dst	Protocol	Source Port	Info
76	2.949495	192.168.1.11	192.168.1.32	CIP I/O	2222	Connection: ID=0x00D77F83, SEQ=000000019, O->T
77	2.959976	192.168.1.32	192.168.1.11	CIP I/O	2222	Connection: ID=0x00754256, SEQ=000000024, T->O
78	2.960841	192.168.1.11	192.168.1.32	CIP Safety	2222	Connection: ID=0x00D77FE8, SEQ=000000000, O->T
79	2.960841	192.168.1.11	192.168.1.32	CIP Safety	2222	Connection: ID=0x00D77FE7, SEQ=000000000, O->T
80	2.962350	192.168.1.32	192.168.1.11	CIP Safety	2222	Connection: ID=0x0175425A, SEQ=000000001, T->O
81	2.965026	192.168.1.32	192.168.1.11	CIP Safety	2222	Connection: ID=0x00F54265, SEQ=000000001, T->O
82	2.969370	192.168.1.11	192.168.1.32	CIP I/O	2222	Connection: ID=0x00D77F83, SEQ=000000020, O->T

Frame 81: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

- Ethernet II, Src: Rockwell_96:ef:9d (f4:54:33:96:ef:9d), Dst: Rockwell_d4:6e:89 (00:1d:9c:d4:6e:89)
- Internet Protocol Version 4, Src: 192.168.1.32, Dst: 192.168.1.11
- User Datagram Protocol, Src Port: 2222, Dst Port: 2222
- EtherNet/IP (Industrial Protocol)
 - Item Count: 2
 - [Connection Information: T->O]
 - [Connection Path: Port: Backplane, Address: 2, [Key], Assembly, Instance: 0x0360, Assembly, Instance: 0x21, Assembly, [O->T API: 20.000ms]
 - [T->O API: 380.000ms]
 - [CIP Connection Index: 2]
 - [Forward Open Request In: 32]
 - Common Industrial Protocol, Safety
 - ACK Byte: 0x88, Ping Response, Parity Even
 -00 = Ping Count Reply: 0x0
 -0.. = Reserved: 0x0
 - 1... = Ping Response: True
 - .000 = Reserved: 0x0
 - 1... = Parity Even: True
 - Consumer Time Value: 57111
 - CRC S5_0: 0xa8
 - CRC S5_1: 0x1e
 - CRC S5_2: 0x03 [correct]
 - [CRC S5 Status: Good]

Consumer responds to "ping request" signaled by change in Ping Count (or first reception of data)

Consumer sends current timestamp

Consumer Time Value (cpsafety.consumer_time_value), 2 bytes

Packets: 2884 · Displayed: 2847 (98)

Implementation Strategies

Rob Lodesky
HMS Networks

ODVA[®]

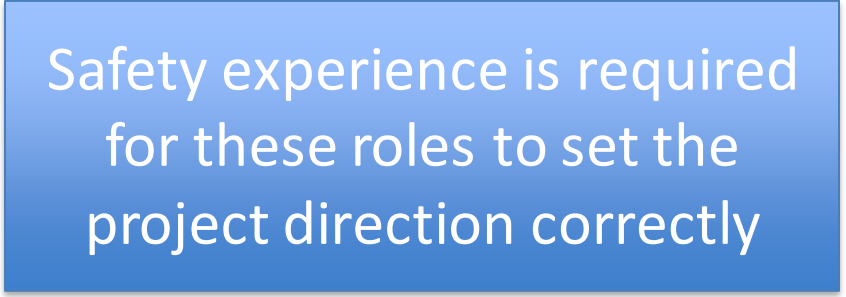
Decisions to make

- What class of device
 - Safety scanner/adapter
- Which safety SW and HW architecture shall be used
- What standards and integrity levels does the product need to meet:
 - IEC 62061 Safety of machinery / IEC 61508 - Functional safety of E/E/PE Systems
 - Product- or Sector-specific standards
 - IEC 61511 Functional Safety: Safety Instrumented Systems for the process industry
 - IEC 61800-5-2 Variable speed drives – Safety requirements
- Which non-safe network(s) shall be supported?
 - CIP Safety is available on DeviceNet, EtherNet/IP, Sercos
- Which Certification body
 - TÜV Rheinland is specified according to ODVA Pub 261 section 7-2
 - others allowed – may incur extra cost
- Who implements the CIP Safety stack?
 - There are available toolkits and development partners

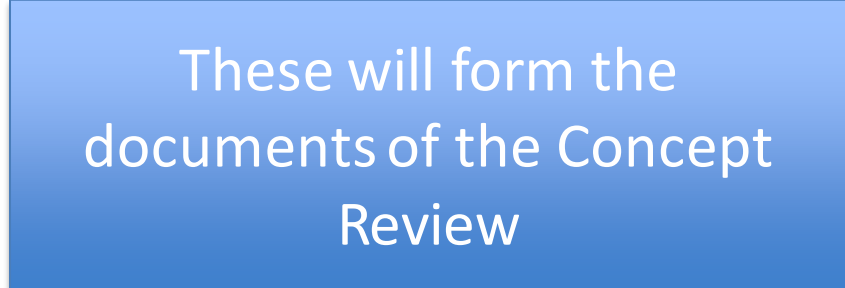
Kicking Off the Project

- Who you need
 - Product Manager
 - Lead Safety Engineer
 - Lead Product Engineer
 - Project Manager

- What you need to create
 - Functional Requirements
 - Safety Requirements Specification
 - Functional Safety Plan
 - Verification & Validation Plan
 - Safety Concept

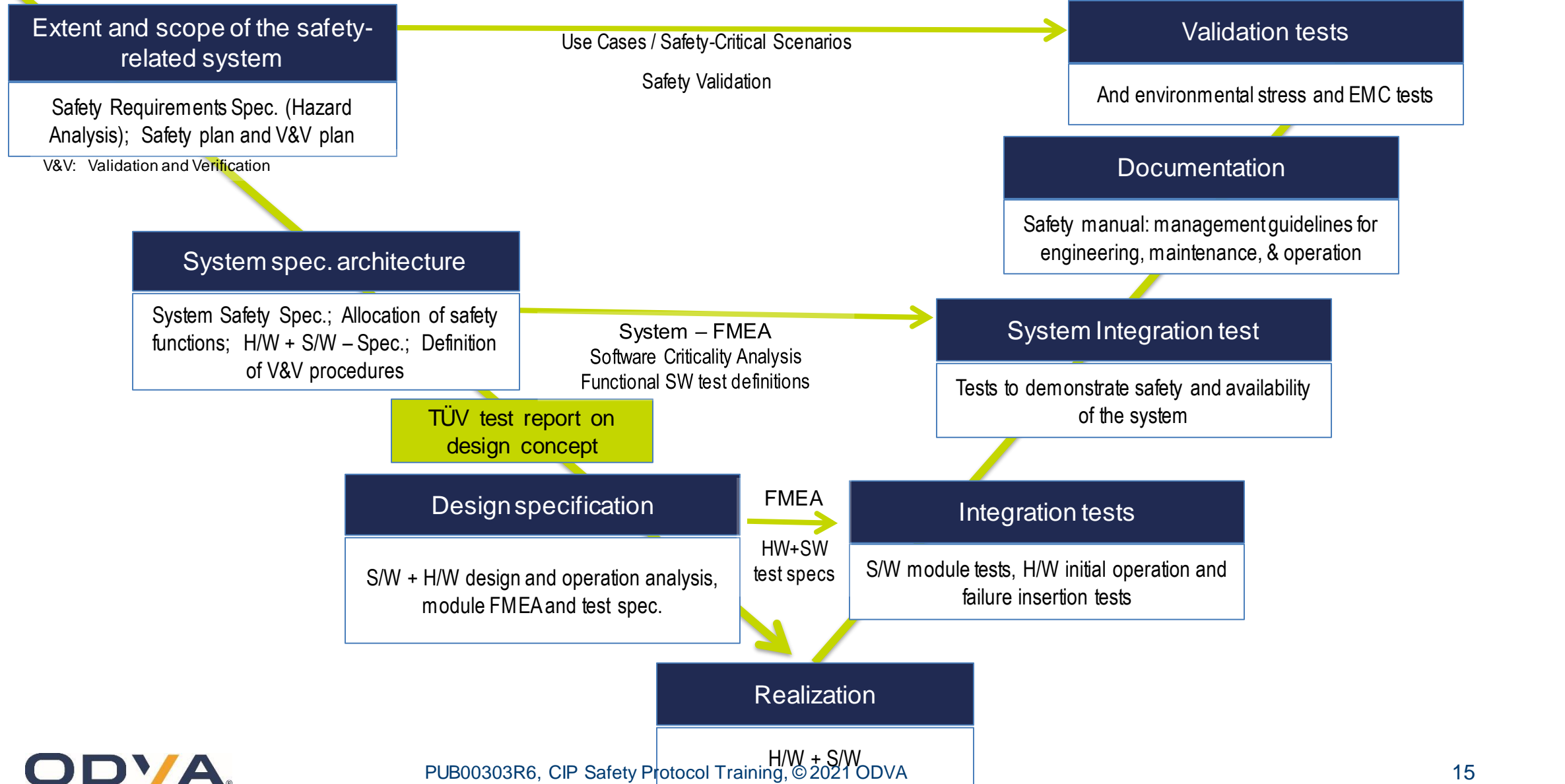


Safety experience is required for these roles to set the project direction correctly



These will form the documents of the Concept Review

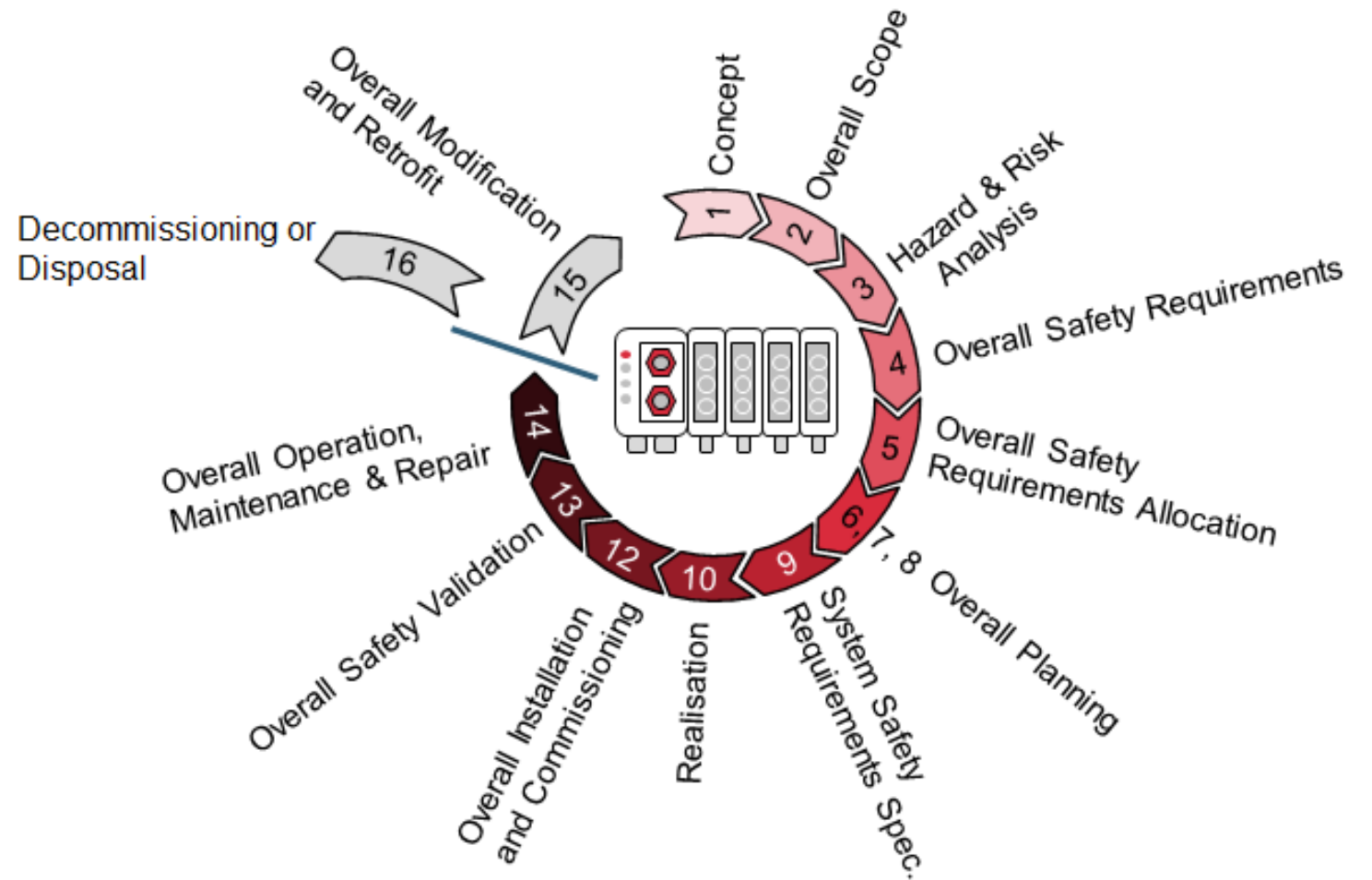
TÜV V-Model of Development



Safety Lifecycle phases (IEC 61508)

Apply in all phases:

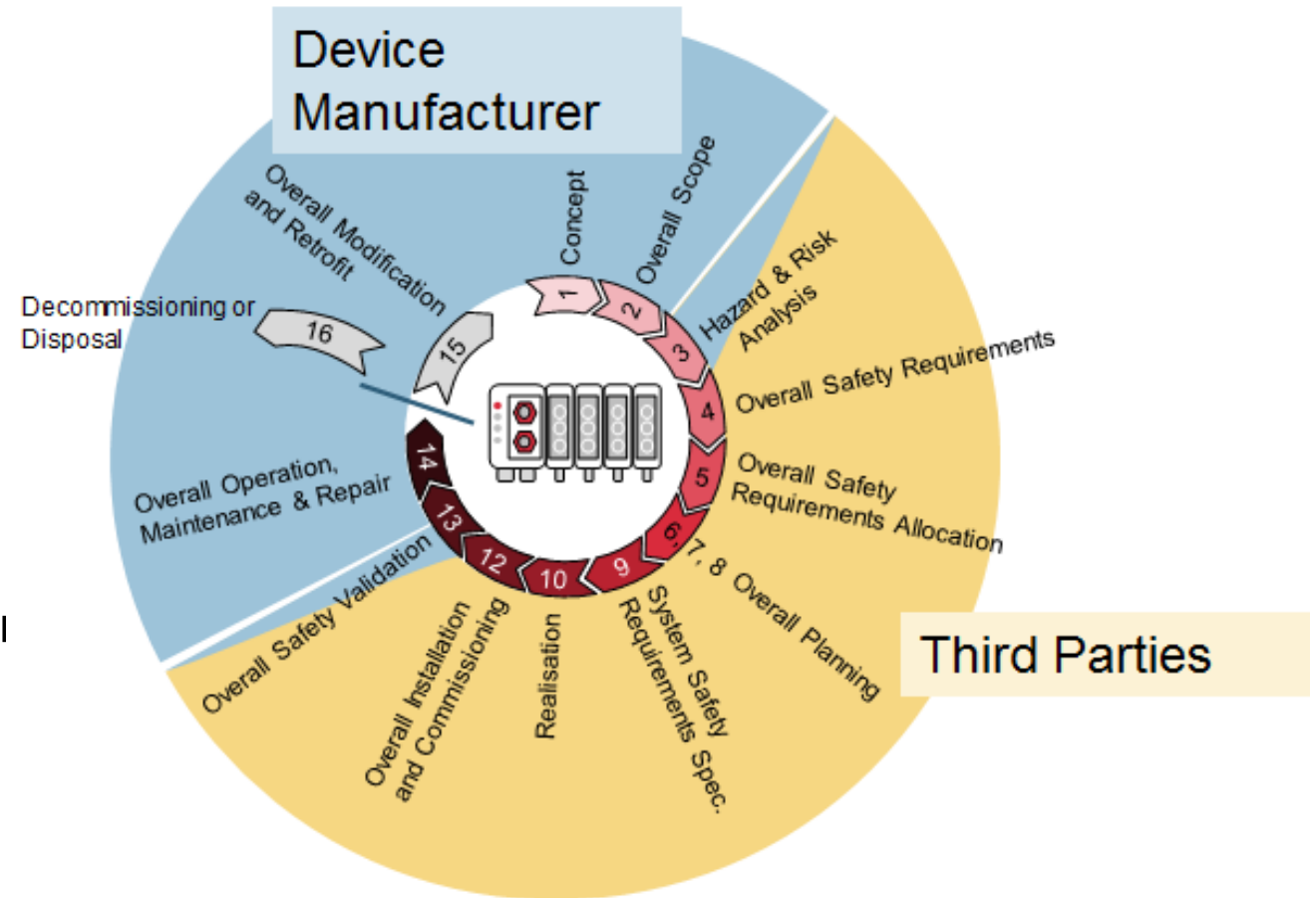
- Documentation
- Reviews
- Verification & Validation Actions



3rd party support in the Safety Lifecycle

Where assistance can be used:

- Some Analysis can be done
 - Overall Safety Req's
 - Overall Safety Req's allocation
- Realization
 - Overall Planning
 - Specification
 - Overall Installation & Commissioning
 - Overall Safety Validation
- Operation done by the Manufacturer



Example: Safety Lifecycle Phase Tasks

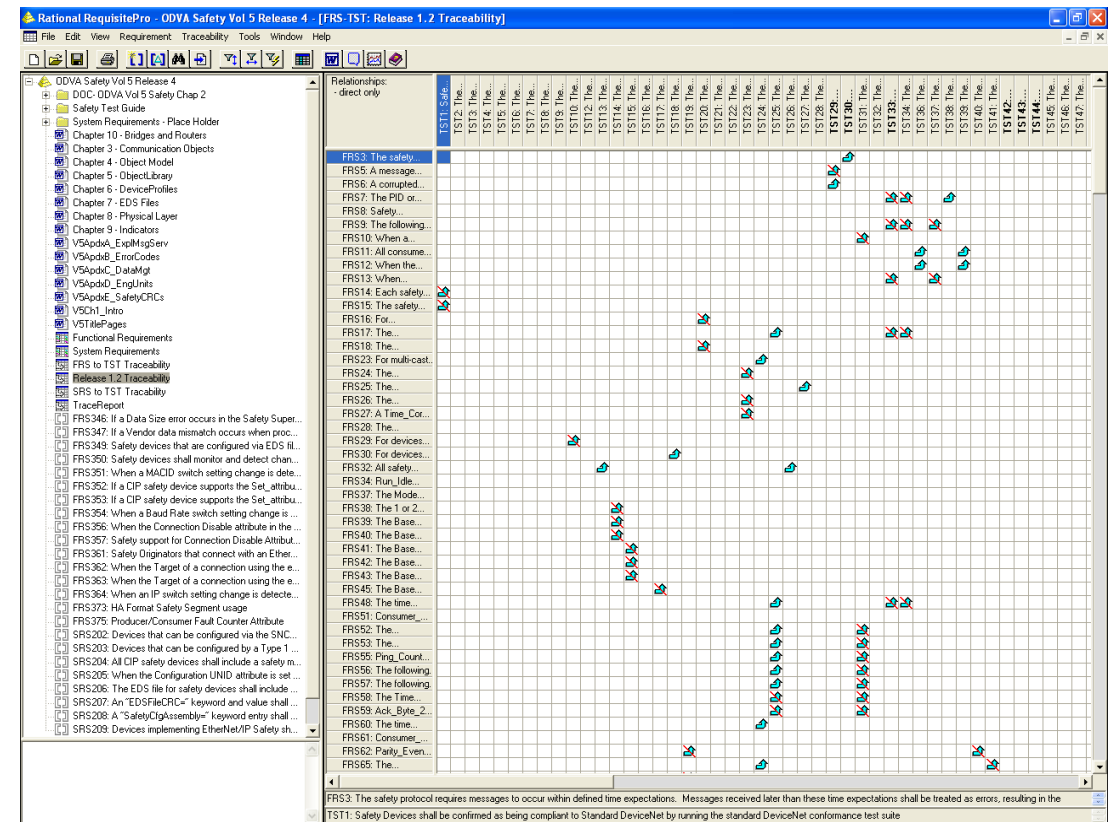


Hazard & Risk Analysis

Purpose:

- **What** could go wrong?
- Hardware, Software, Cosmic, others
- FRS/SRS linkage tests
- Trace \leftrightarrow Test

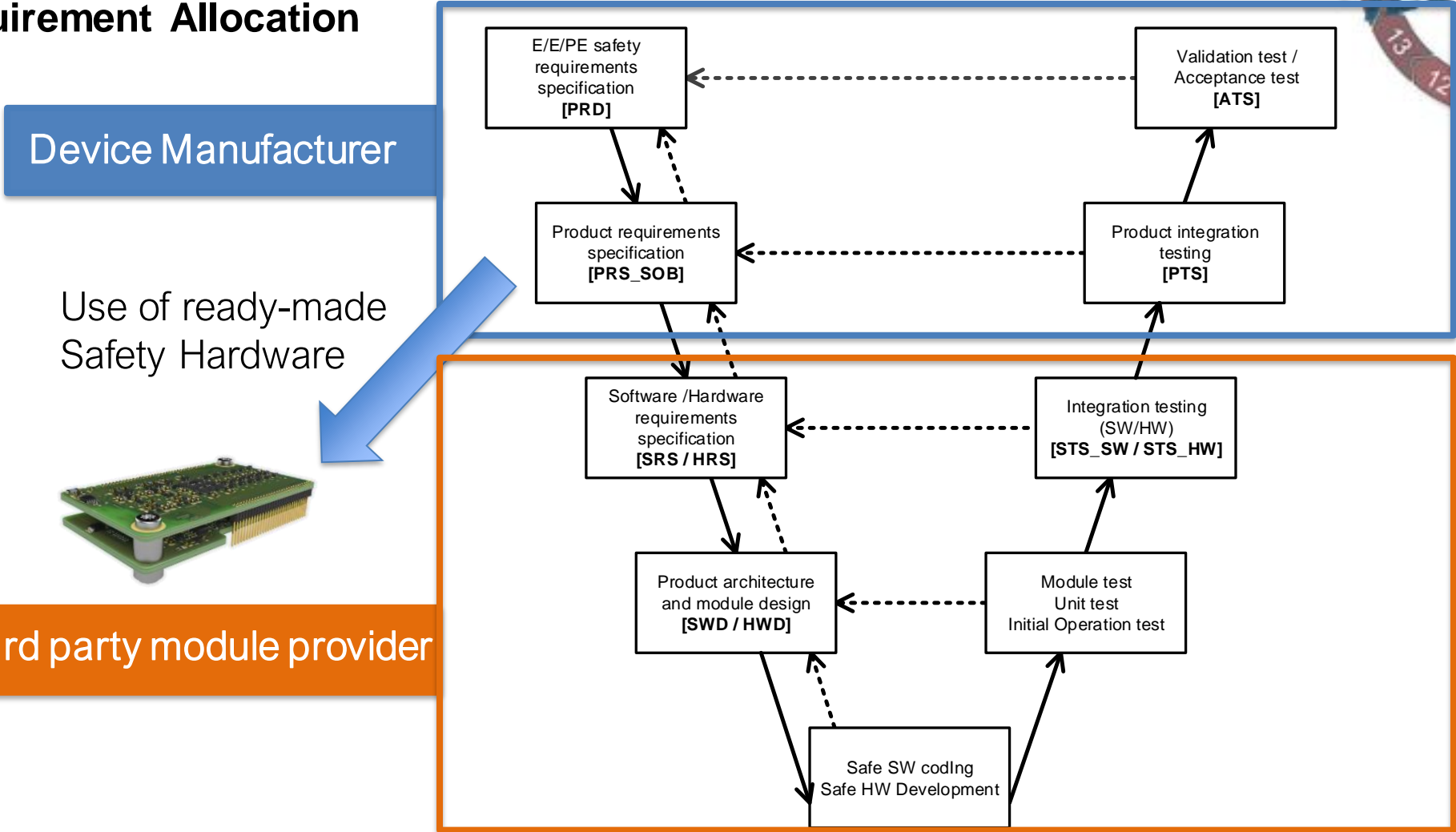
→ Safety development and safety product must provide countermeasures for the identified hazards and risks



3rd party H/W support in the Safety Lifecycle

5

Safety Requirement Allocation



Use of ready-made Safety Hardware

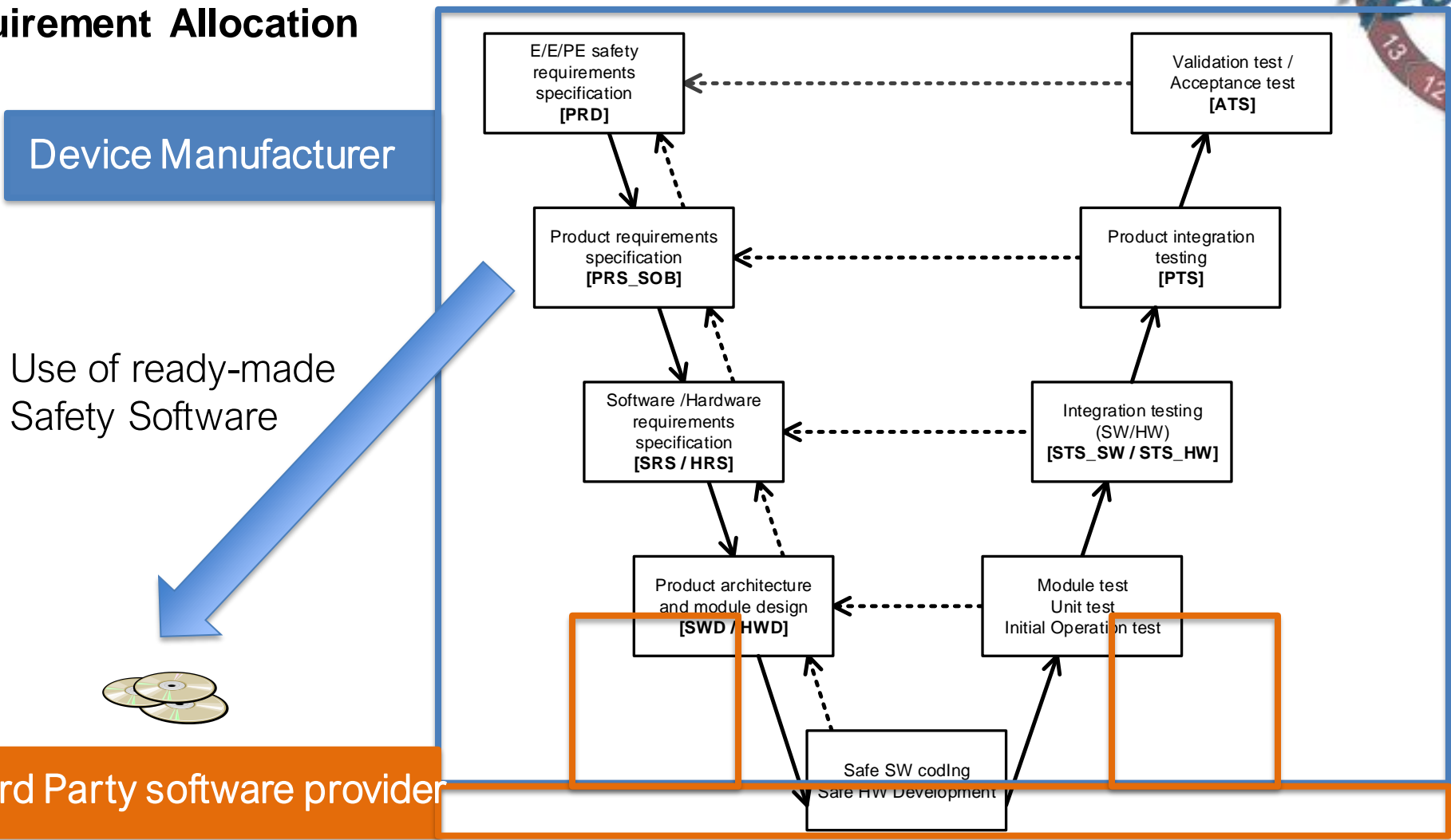


Third party module provider

3rd party S/W support in the Safety Lifecycle

5

Safety Requirement Allocation



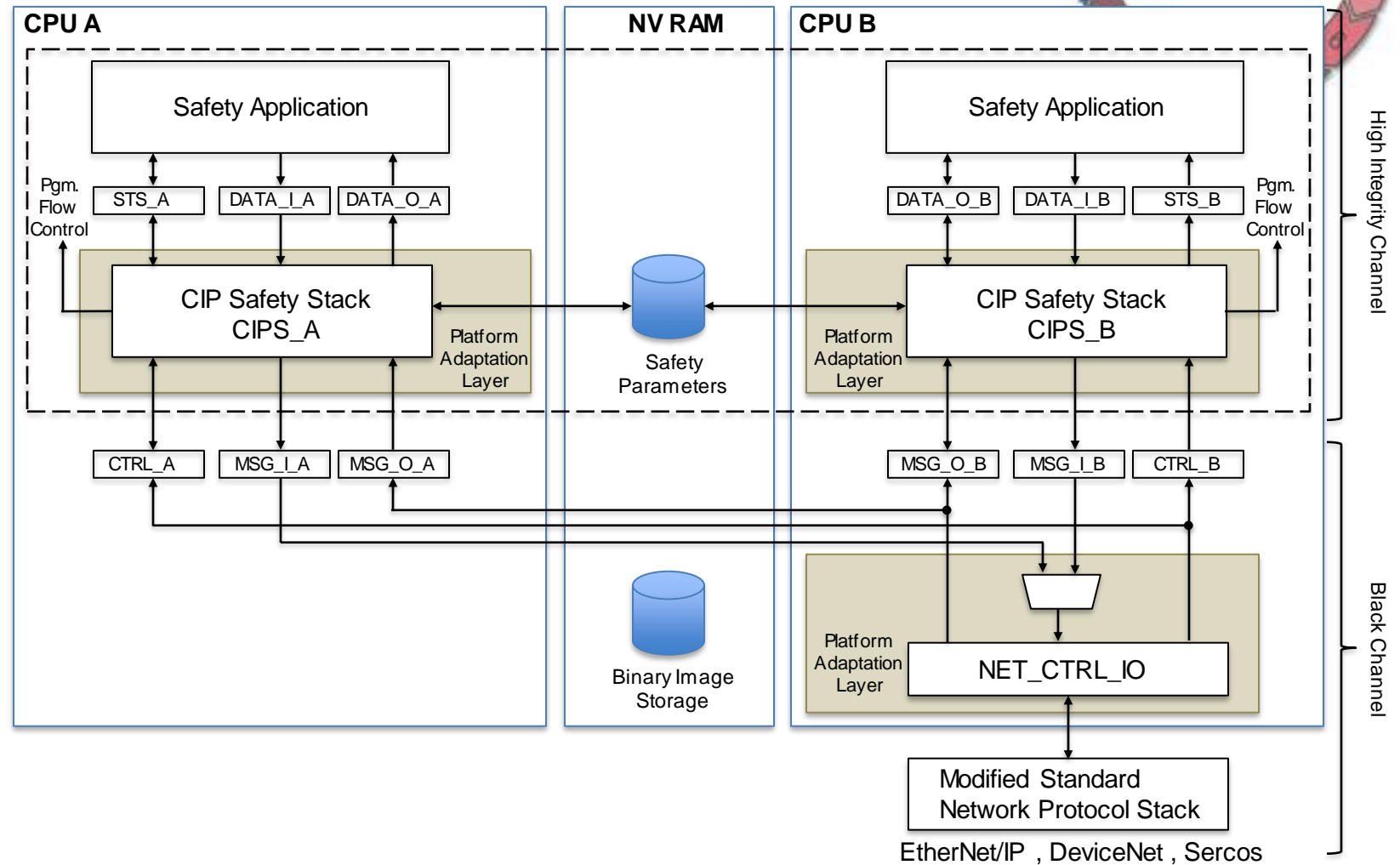
Example: Working with a CIP Safety toolkit



10 Realization

Platform requirements:

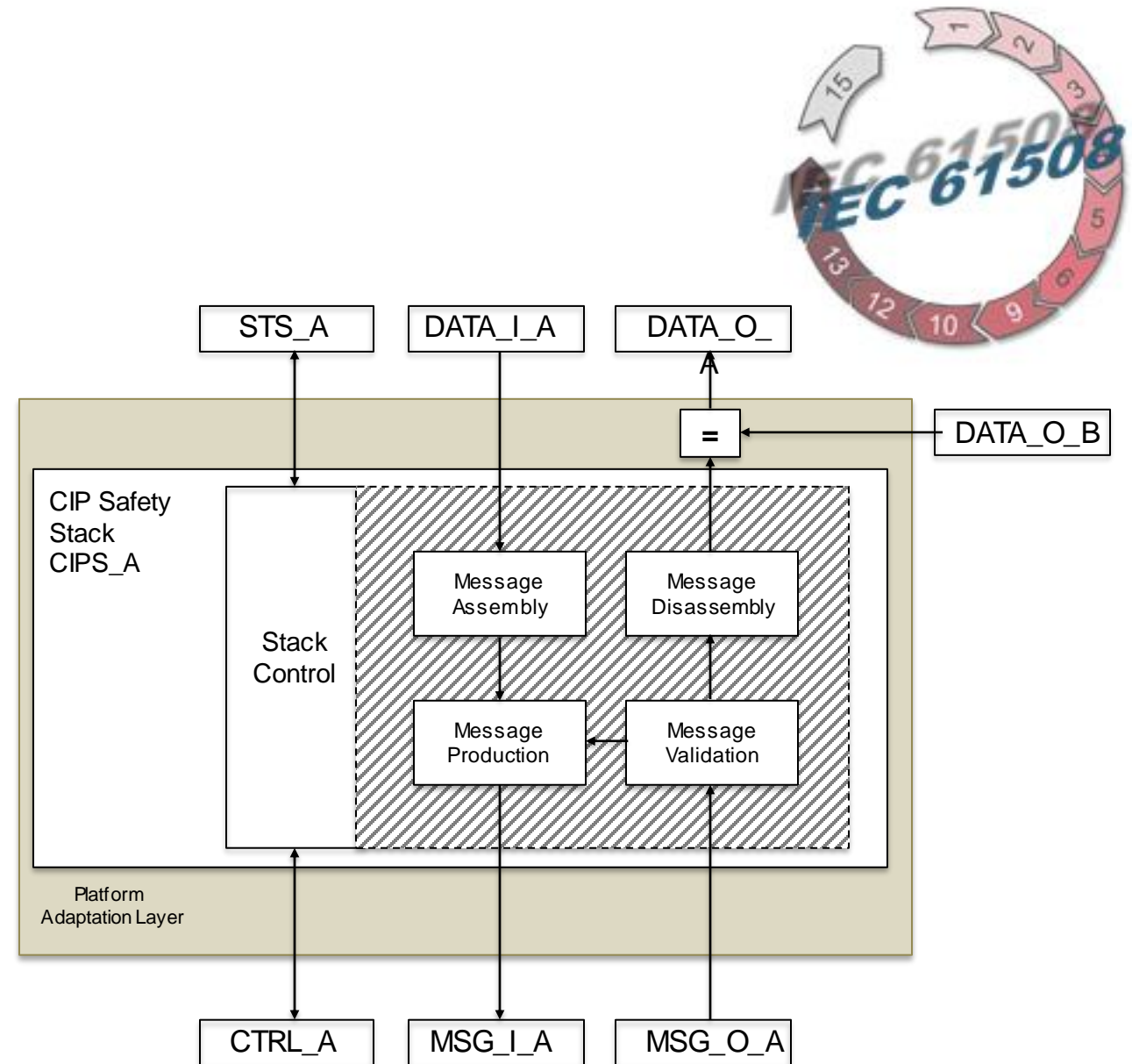
- Dual channel (1oo2)
- Integrity
 - FW binary image
 - non-volatile safety parameters storage
 - CPU and memory integrity
- Isolation
 - Read/write interface between non-safe and safe environments
- Program flow monitoring (Watchdog)
- Memory cross-checking (Soft-Error handling)



Example Toolkit (cont'd)

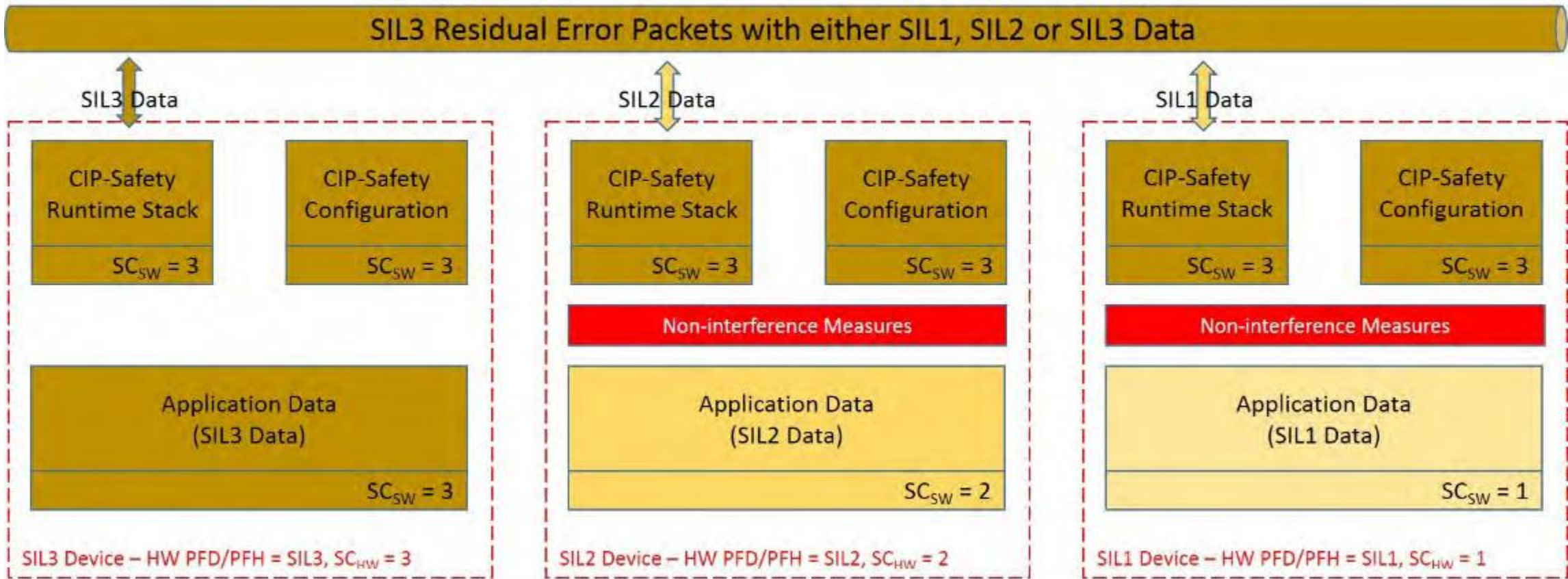
10 Realization

- CIP Safety Stack Implementation
 - The CIP Safety Stack comprises two functionally identical images CIPS_A and CIPS_B
 - Message Validation and Production is initiated by the platform(safe application) periodically.
 - Shall be designed (in both hardware and software) to be compliant with requirements for SIL3 systems according to IEC 61508.

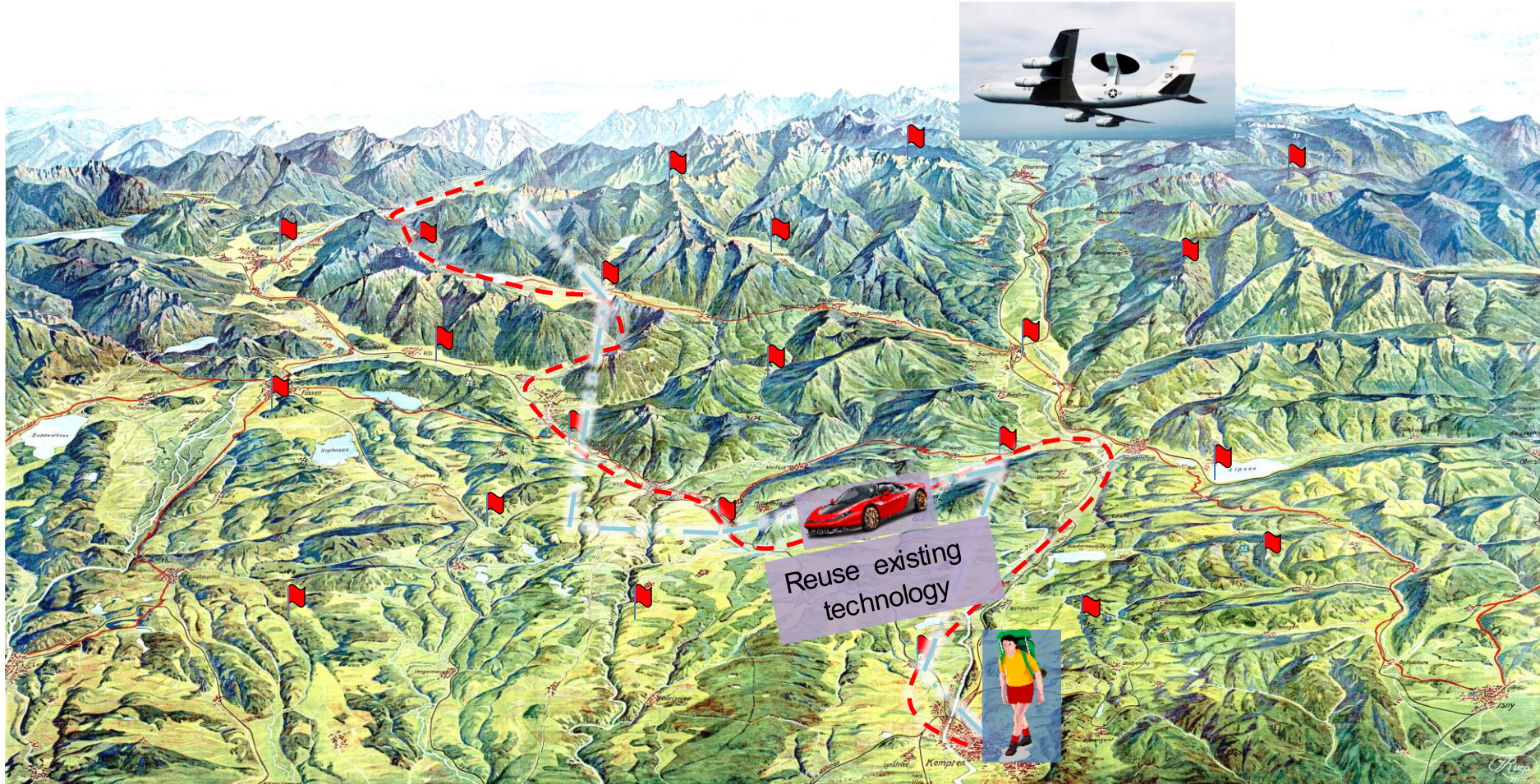


Architectures for CIP Safety (Vol 5 Ed 2.16 2-2.1)

Off-line CIP-Safety Configuration Tool



The Safety Hike



- Project Supervision / Product Assessment (TUV)
- Run the Project (Development / Project Manager)
- Track Planning (Project Manager)
- Set Waypoints (Available technology, consultant, system architect)
- ★ Define end product (Product Management)
- Project starting point

CIP Safety Enabling Technologies

- CIP Safety protocol stacks are available for licensing
- Simplify development and certification
- Available from ODVA Member companies
 - HMS Industrial Networks / IXXAT
 - Molex
 - Online Development Inc



Conformance Testing & Certification

Hamza Choudhry
ODVA

ODVA[®]

ODVA Composite Conformance Test

- Conformance Testing Purpose
 - Provide vendor-independent Quality Assurance to industry – Product Conformance to CIP Specification
 - Improve Customer Satisfaction with CIP technologies – Ensure Interoperability between products
 - Terms of Usage (TOU) compliance – You're obligated to.

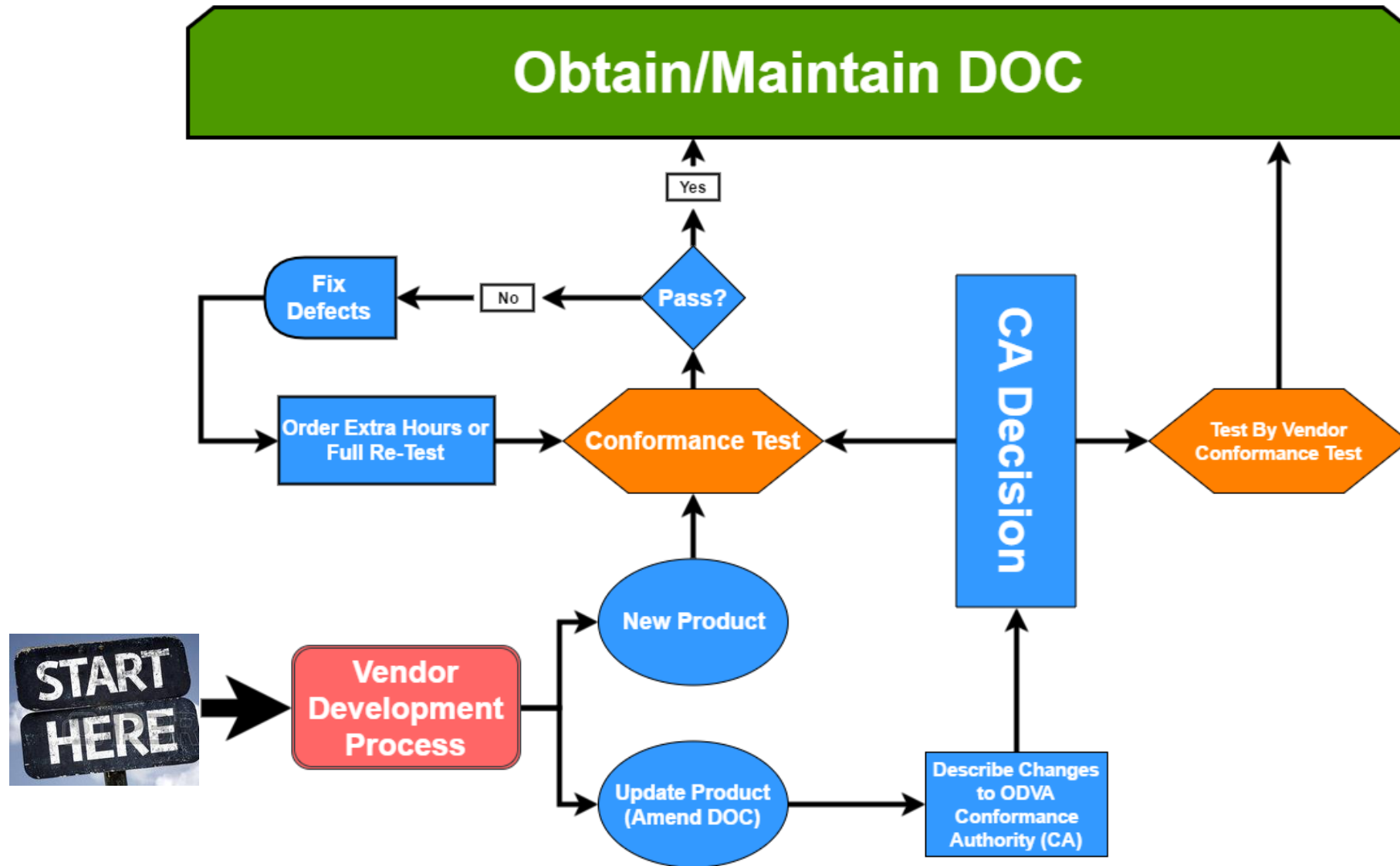


ODVA Composite Conformance Test

- Conformance Testing – What is it?
 - Protocol Test – Automated test covered using our Conformance Test ware
 - EtherNet/IP CT revision: CT18
 - EtherNet/IP Safety CT revision: CT18-ES
 - Physical Layer Test – Documented in the PCTS and Test Report
 - Interoperability Test



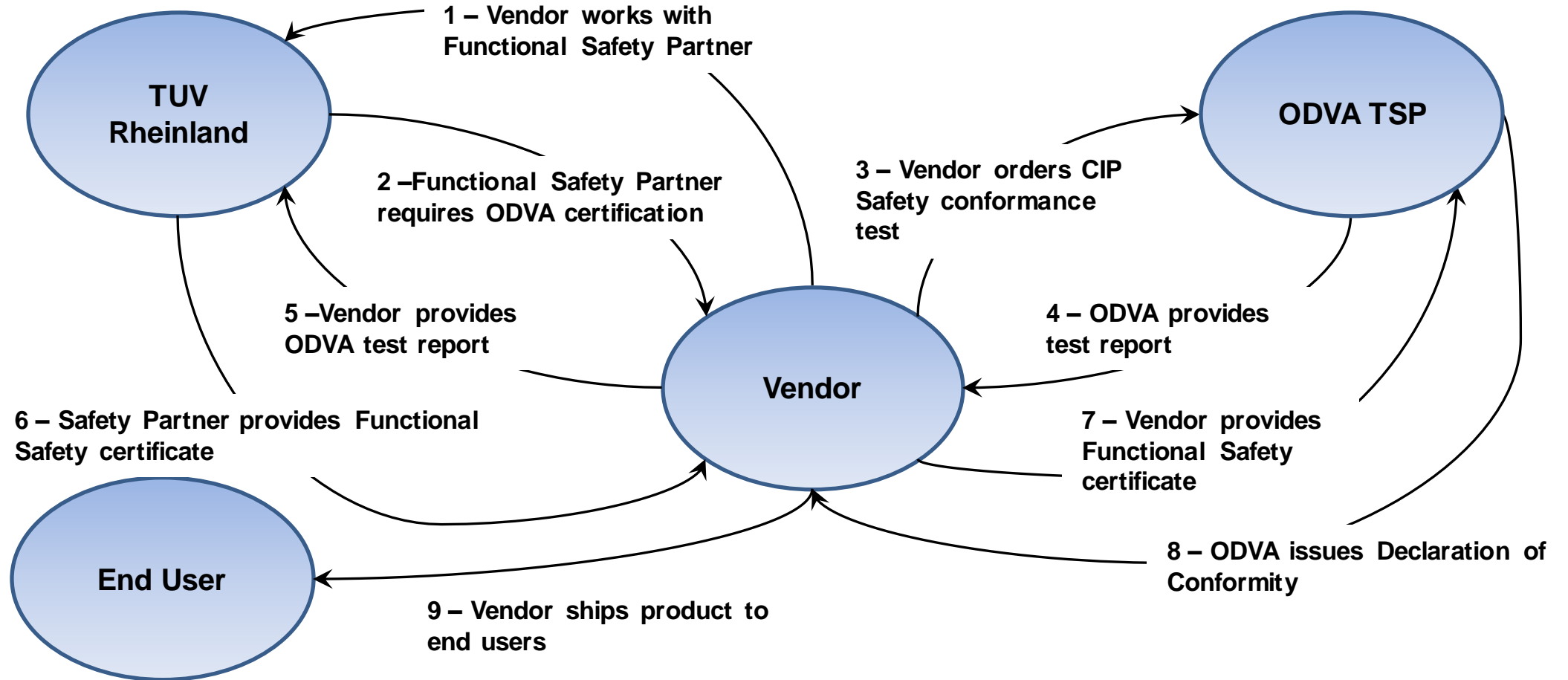
Conformance Process Overview



CIP Safety Conformance Test Process

- Requires special version of the conformance test
 - Establishes conformance to the Safety Test Plan
 - Does not test functional safety nor assess the safety of a device implementation
- ODVA test report is an input to the assessment of CIP Safety implementations
 - TÜV Rheinland requires the ODVA test report
 - ODVA requires the functional safety certificate before issuing a DOC
- The Vendor has a central role in this process...

The central role of the Vendor

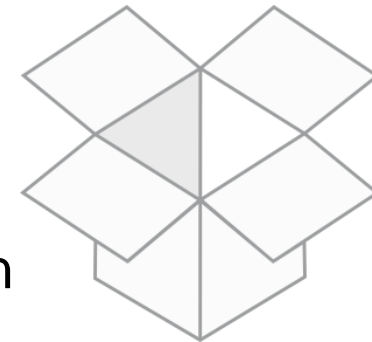
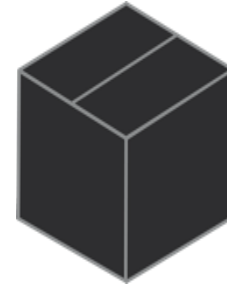


CIP Safety Test Plan

- What is the Safety Test Plan?

- Volume 5 – Appendix F

- Links to traceable requirements (FRSxxx, SRSxxx)
 - Consists of “Black Box” and “White Box” tests
 - Black Box – tests that can be externally verified
 - Volume 5 Appendix F-3
 - e.g., TST101 SafetyClose Processing by Targets
 - White Box – tests that require visibility into the implementation and are executed by the product developer (i.e., code inspection, design review, etc.)
 - Volume 5 Appendix F-4
 - e.g., TST93 – Safety Device Hardware Validation Tests



ODVA Conformance Policy – SIL/SC

- The CIP Networks Library Volume 5 Edition 2.16 Section 2-2.1
 - “The assessment of the systematic capability, SIL level requirements, and appropriate non-interference measures is carried out by the safety certification body.”
 - “All implementations of CIP Safety technology shall use a safety certifying agency to ensure that the design and implementation of the CIP Safety protocol (safety-related communication software) provides a Systematic Capability of SC3 according to IEC 61508.”
 - “The CIP Safety protocol must be considered as part of a complete device, and the integration of the CIP Safety protocol into the device must be done to achieve/maintain SC3.
 - “For example, a Vendor cannot use a separately certified CIP Safety stack (one that does provide SIL3 and SC3) in their product without regard to the need to provide SC3 for the integration of the safety communication software in the integrated product.”

CIP Safety Conformance Policy Publications

- PUB00206 – Terms of Usage Agreement
- PUB00008 - Policy Regarding Compliant Products
 - Appendix A (“Test by Vendor” option)
- PUB00261 - Technology Management for Conformance Test Policy
 - Section 3.2 (CIP Devices – modular and non-modular)
 - Section 7.2 (Third-party certifications)

Conformance Test Preparation

- Plan ahead for your product conformance test
 - Integrate the conformance testing process into your product development process
 - Self-testing with the latest CT release
 - Understand manual test procedures and test tools from the Sample Test Report.
- Have questions? Contact ODVA staff at conformance@odva.org

Specification Enhancement

David Crane
ODVA

ODVA[®]

ODVA CIP Safety SIG

- Mission Statement
 - The CIP Safety Special Interest Group (SIG) has been charged with enhancing and maintaining the CIP Safety Specification. The CIP Safety SIG will work cooperatively with the Conformance Authority of ODVA to enhance and maintain conformance testing for devices incorporating this capability
- Specification Enhancements
 - Reviews for technical accuracy
 - Authors new content (e.g., Safe Motion Objects)
- Operating Procedures
 - SIG Work Plan
 - CIP Safety SIG Specification Enhancement Process
 - ODVA Safety Anomaly Notification Process

Questions?

ODVA[®]

Thank you for your participation in the virtual

CIP Safety Protocol Training

EtherNet/IP[®]

Please visit www.odva.org Developer Hub

for additional resources

PUB00303R6, CIP Safety Protocol Training, © 2021 ODVA