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

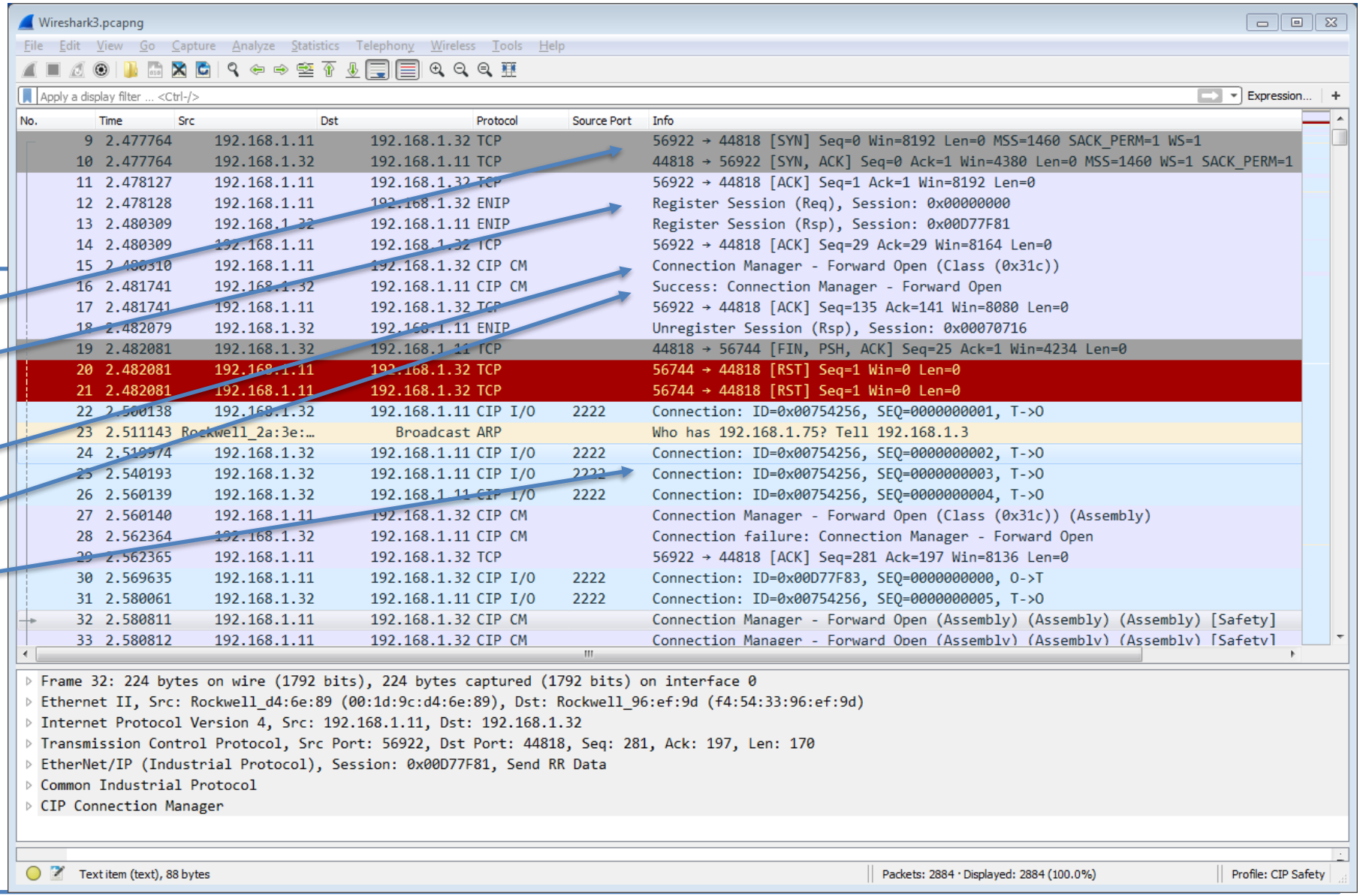
- Configuration of CIP Safety devices (Type 1 vs Type 2 Safety Open)
- Error mitigation techniques (Time Expectation, Redundant Cross-check, End-to-end CRCs)
- Time Coordination and Correction
  - Timestamp is 128us 16-bit counter (Extended format adds 16-bit rollover count)
  - Ping Interval is RPI/EPI-based
- 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

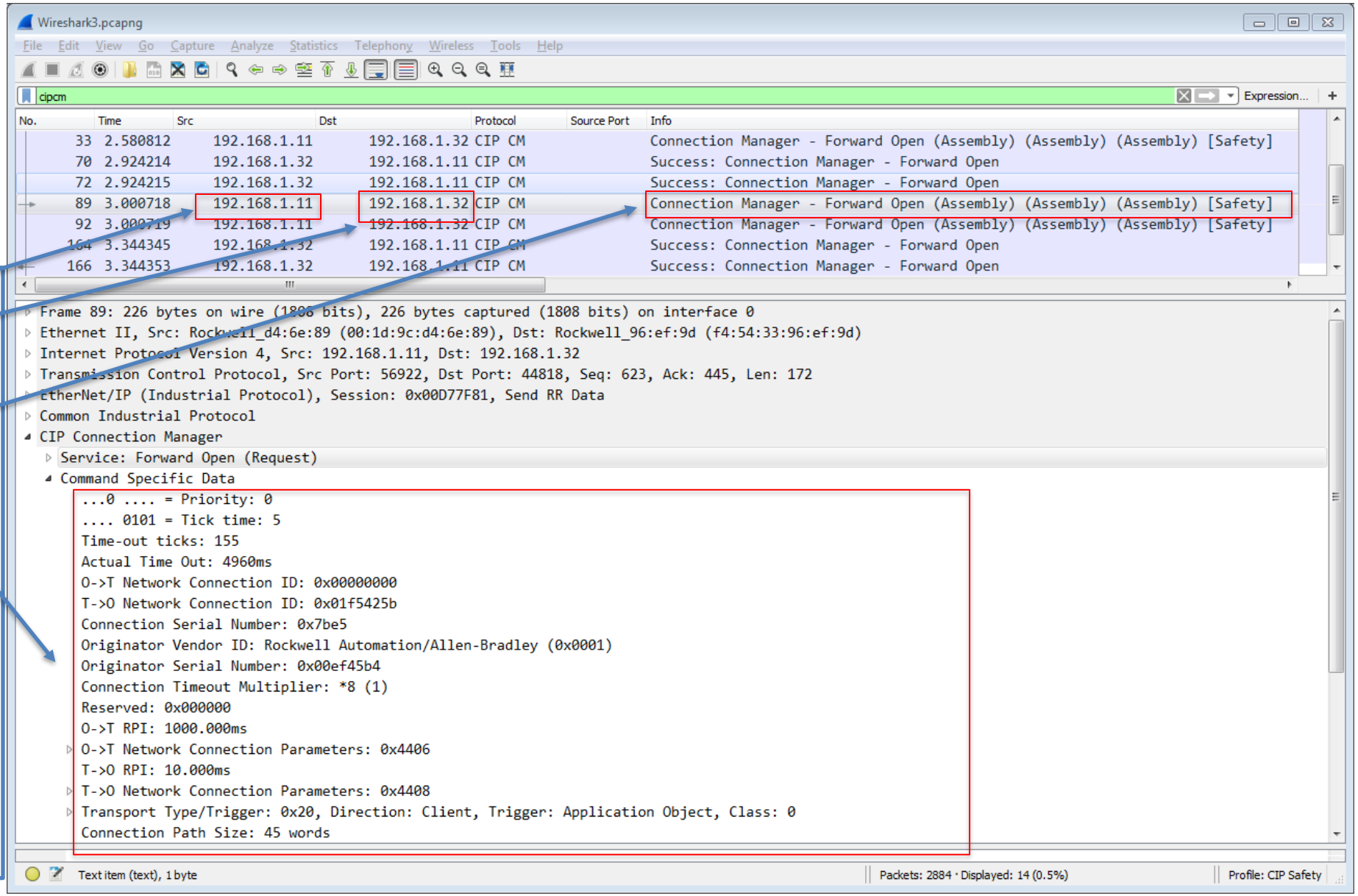
EtherNet/IP Wireshark

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



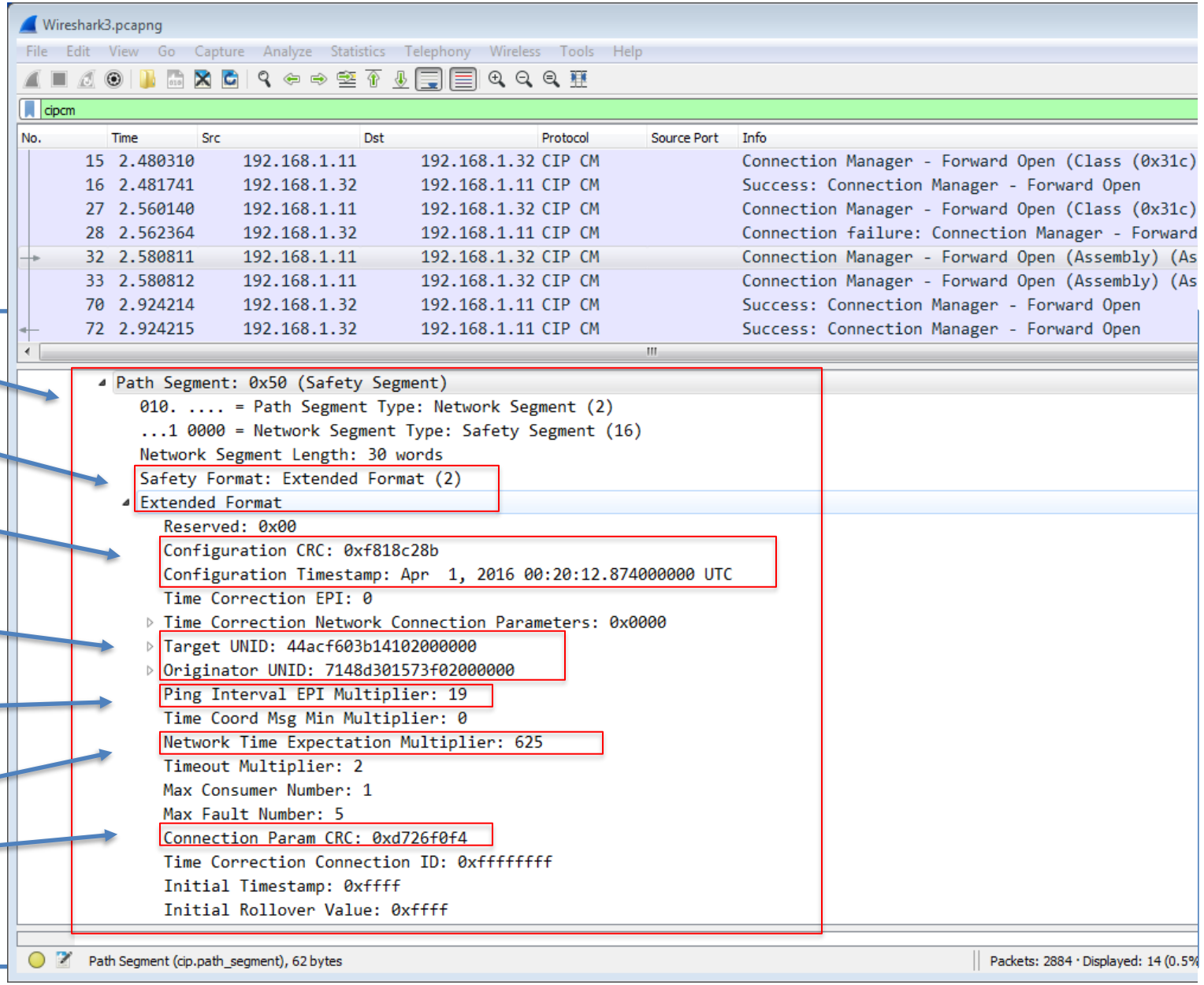
Filtered view "cipcm"

- Originator
- Target
- Forward Open
  - Standard CIP Parameters



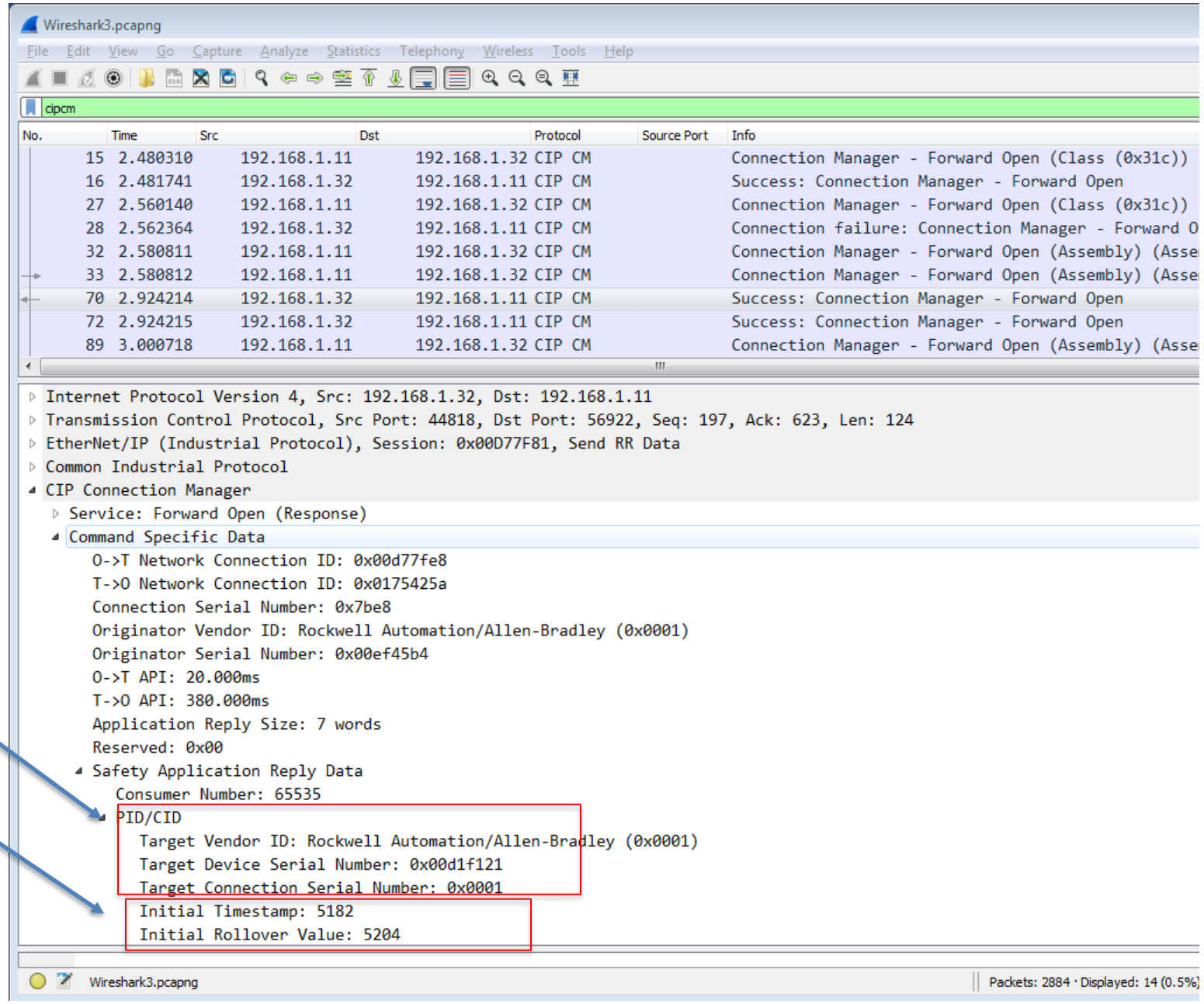
CIP Safety Parameters

- 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



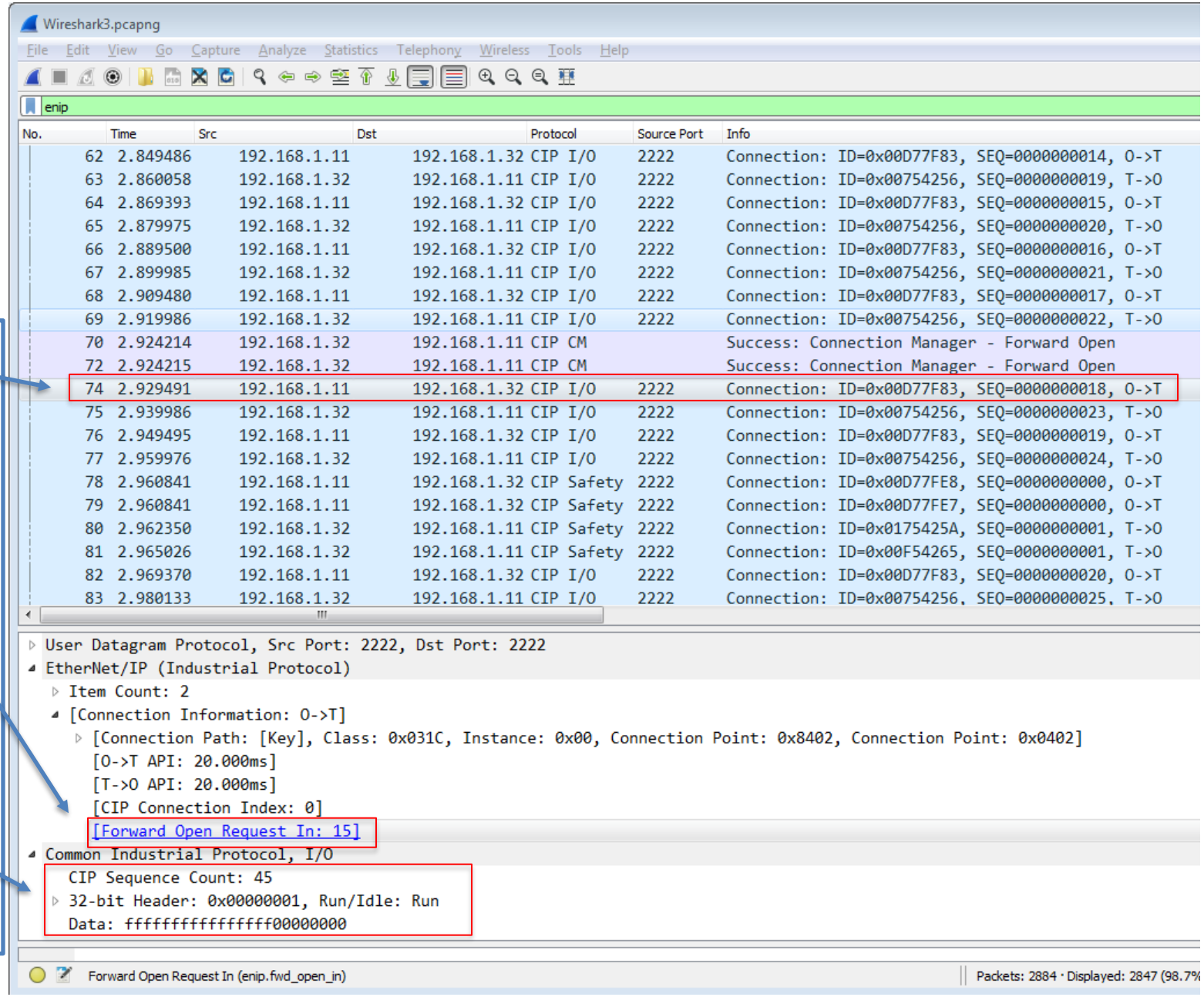
Forward Open Response

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



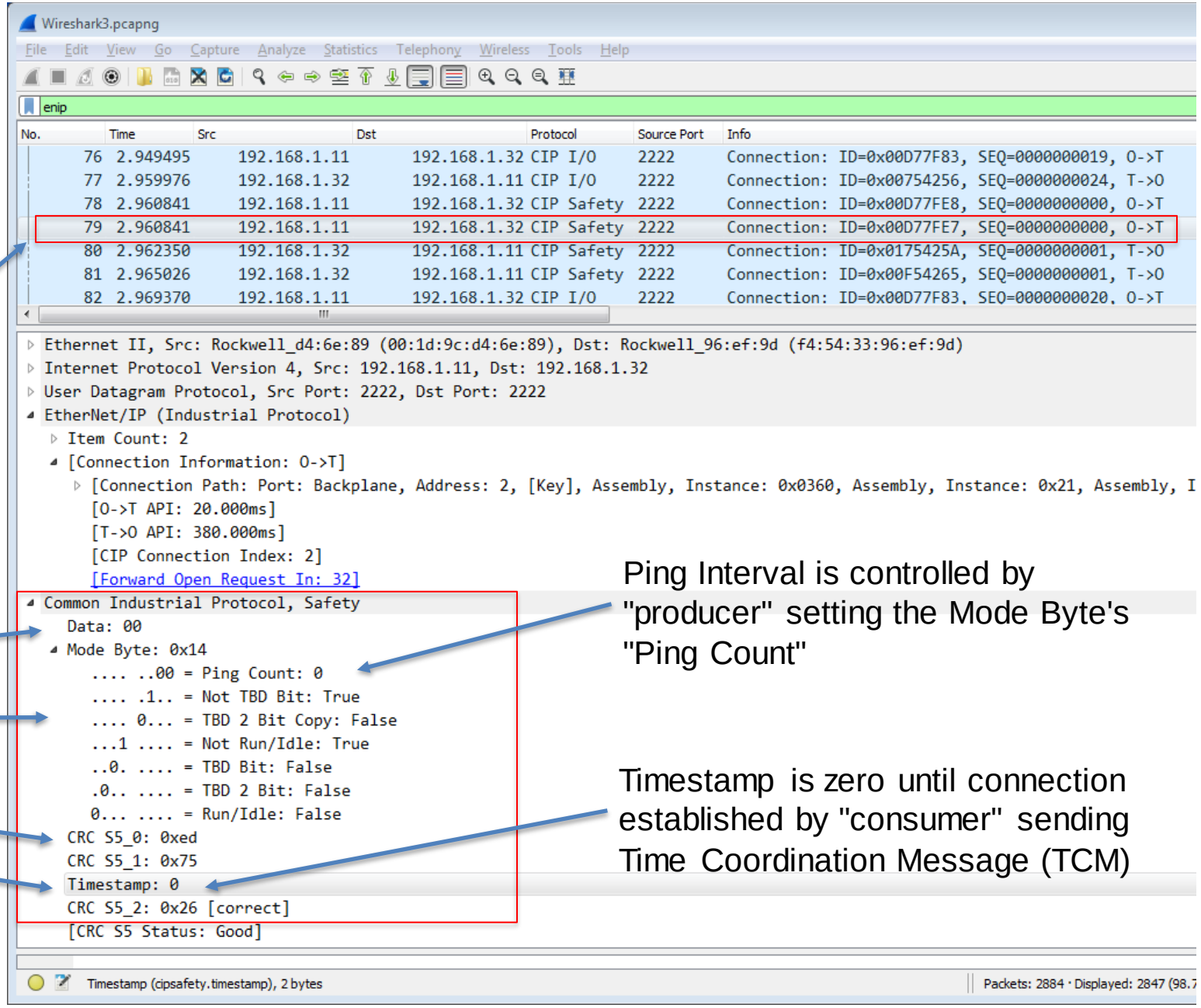
EtherNet/IP I/O "enip" filter

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



CIP Safety I/O "Data"

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

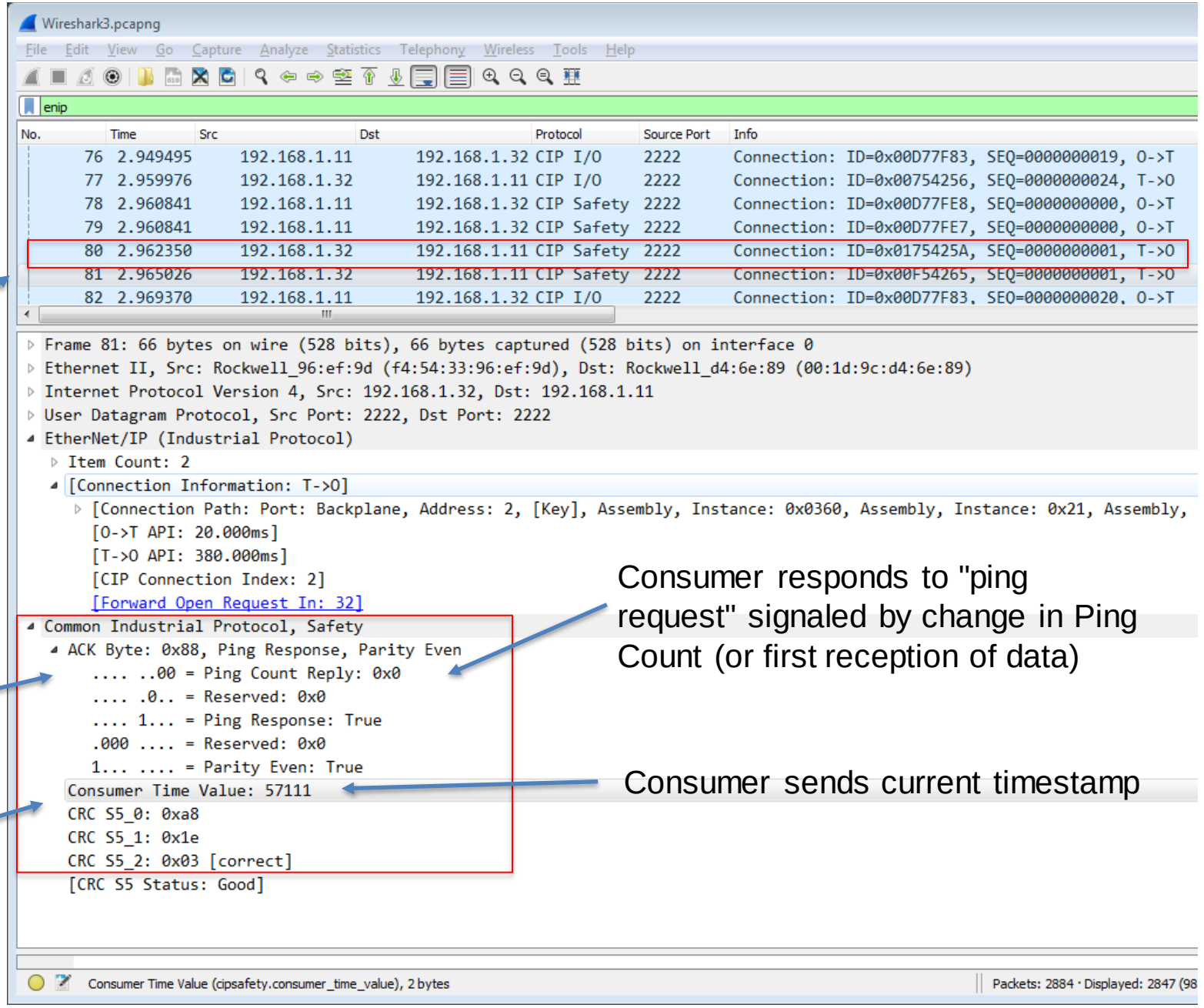


Ping Interval is controlled by "producer" setting the Mode Byte's "Ping Count"

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



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

Consumer sends current timestamp

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

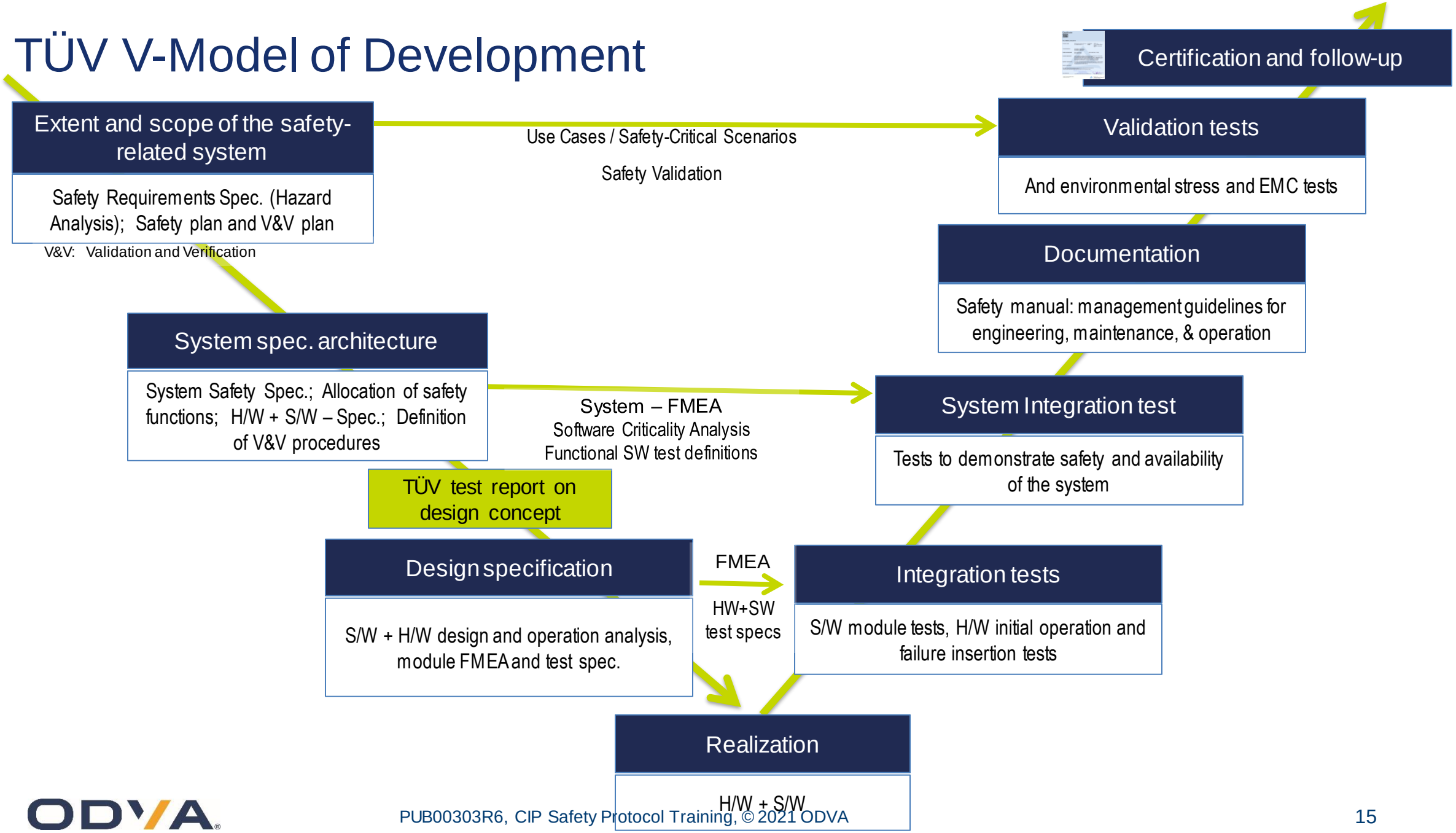
- Who you need
  - Product Manager
  - Lead Safety Engineer
  - Lead Product Engineer
  - Project Manager

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

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

These will form the documents of the Concept Review

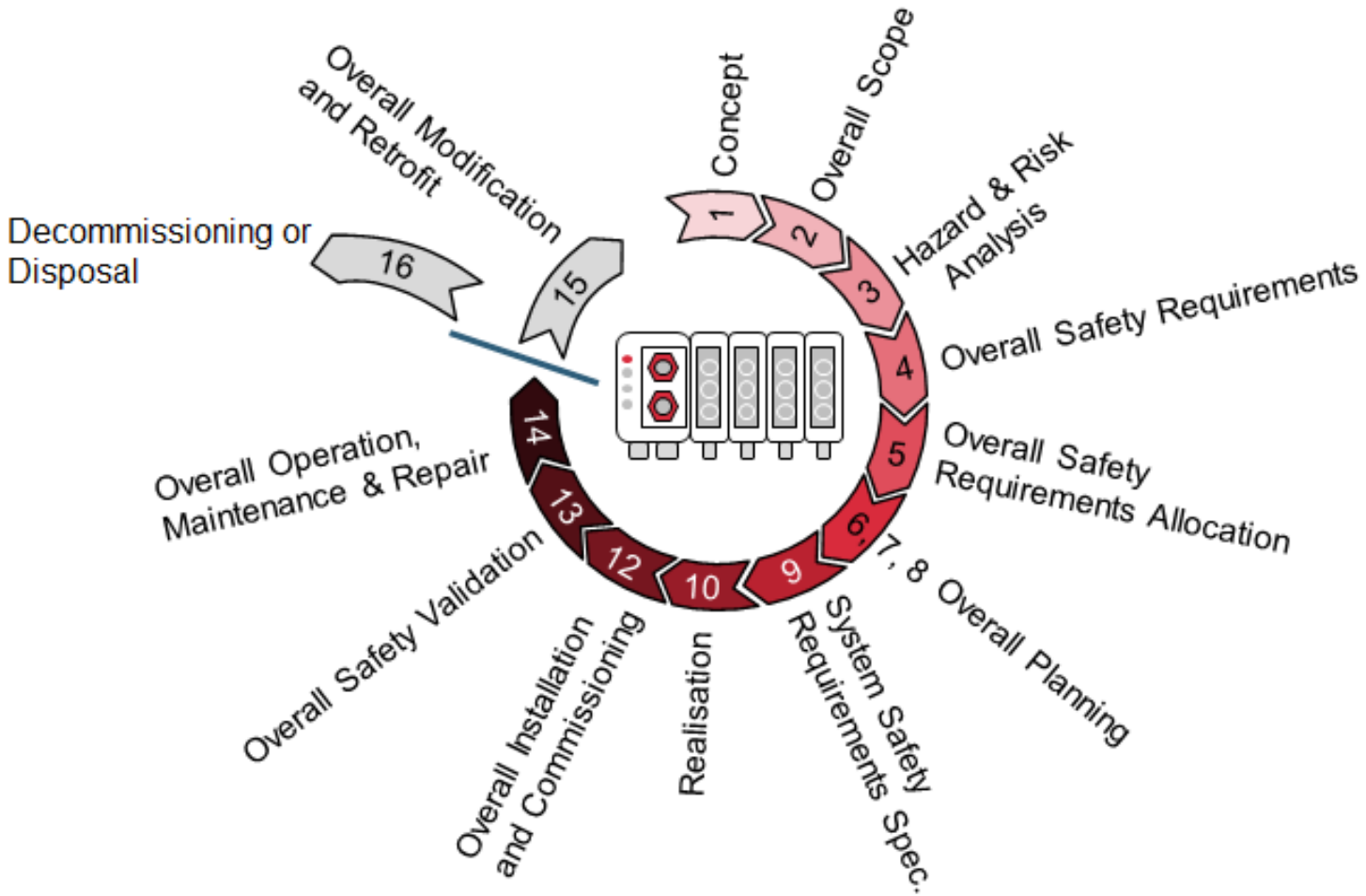
TÜV V-Model of Development



Safety Lifecyle phases (IEC 61508)

Apply in all phases:

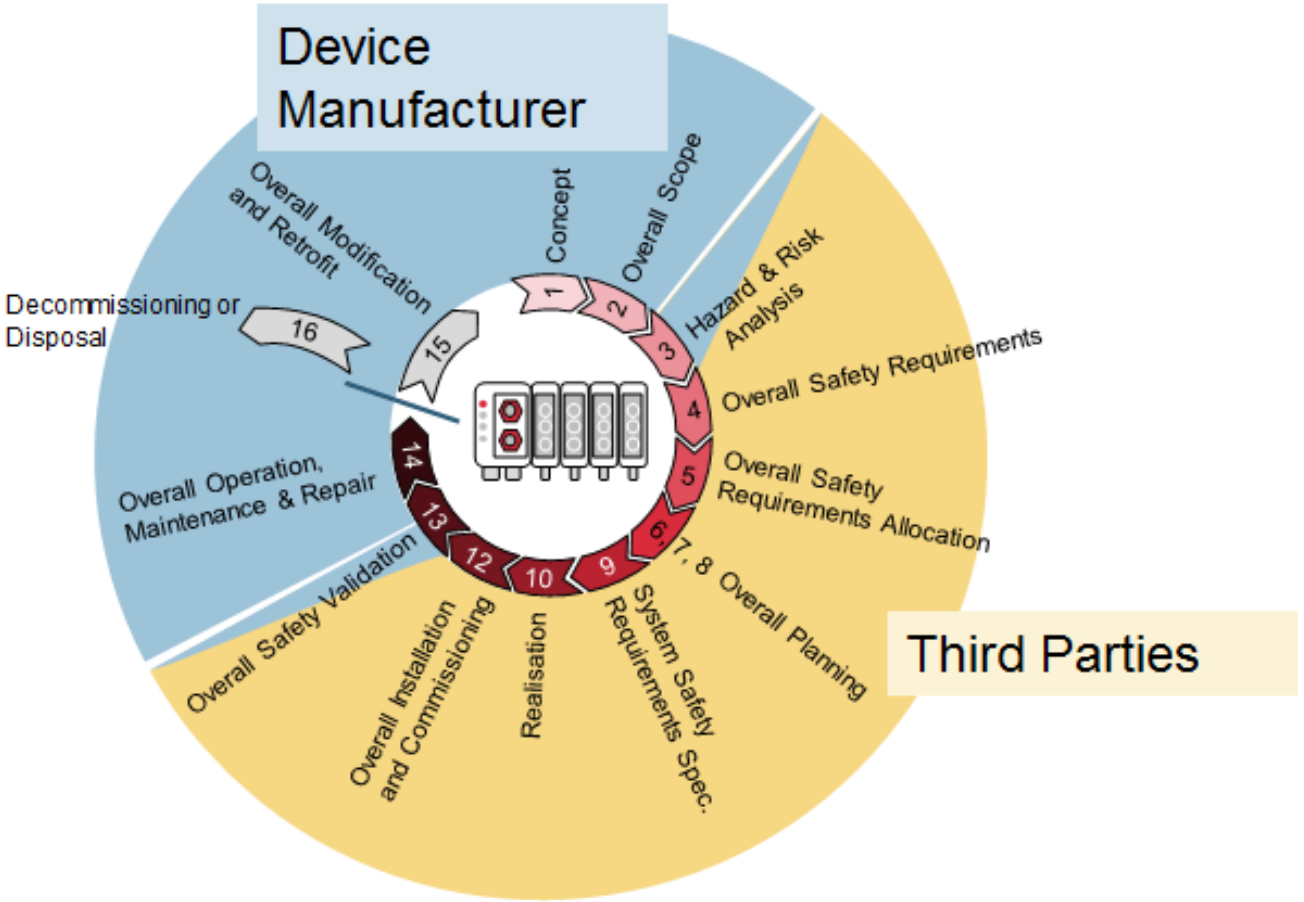
- Documentation
- Reviews
- Verification & Validation Actions



3rd party support in the Safety Lifecyle

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



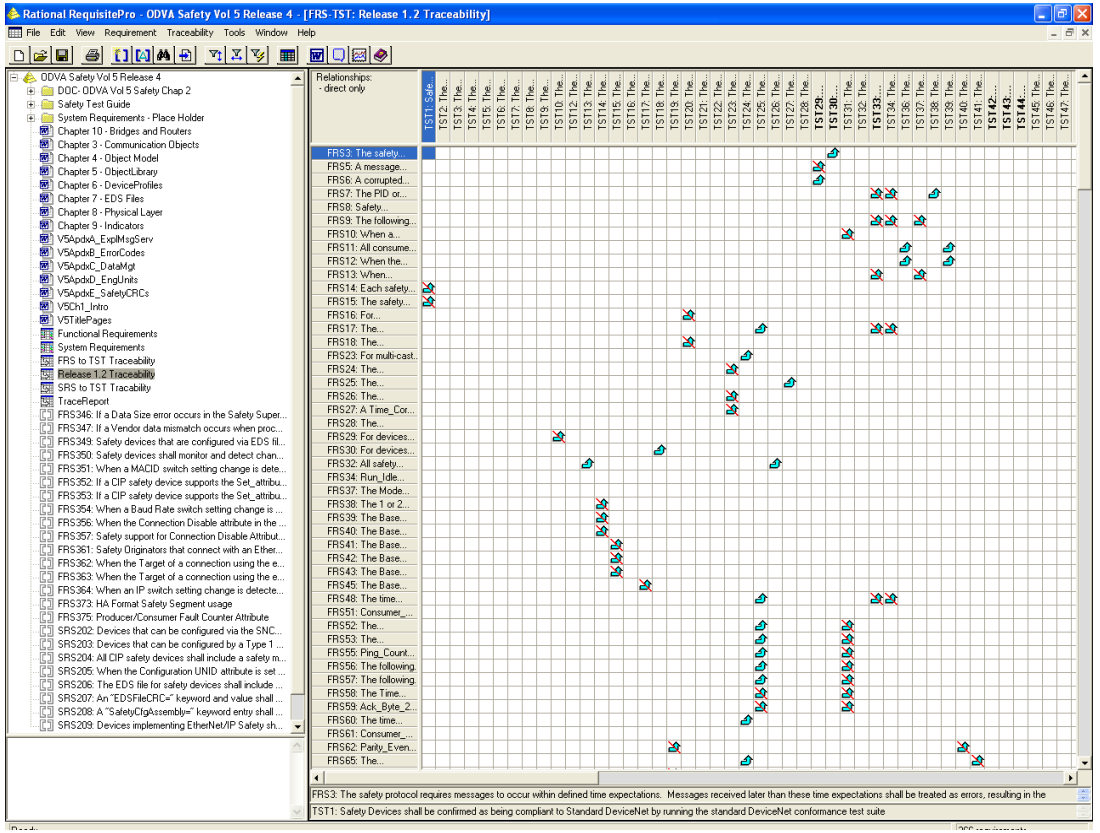
Example: Safety Lifecycle Phase Tasks

Hazard & Risk Analysis

Purpose:

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

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



3rd party H/W support in the Safety Lifecyle

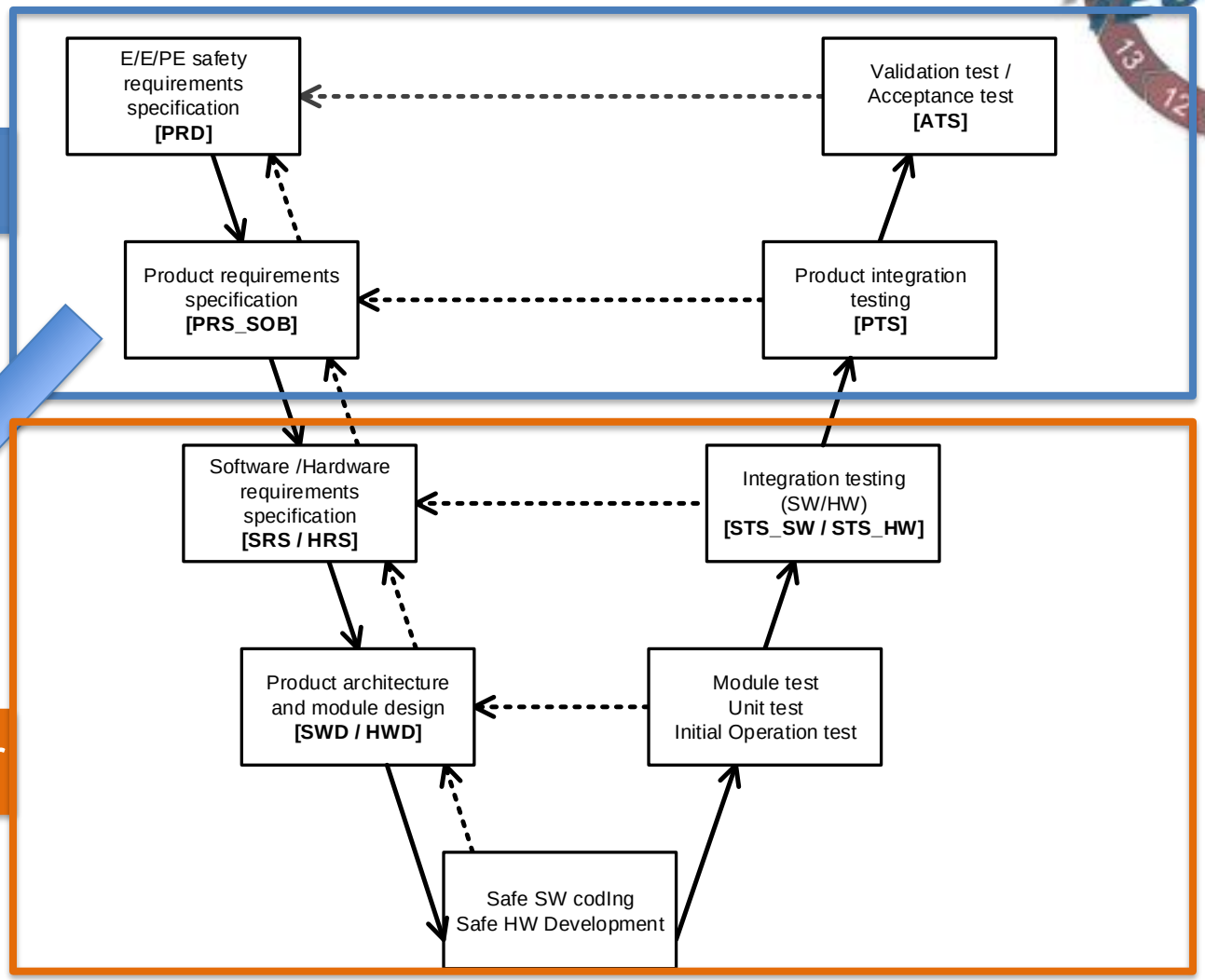
5

Safety Requirement Allocation

Device Manufacturer

Use of ready-made Safety Hardware

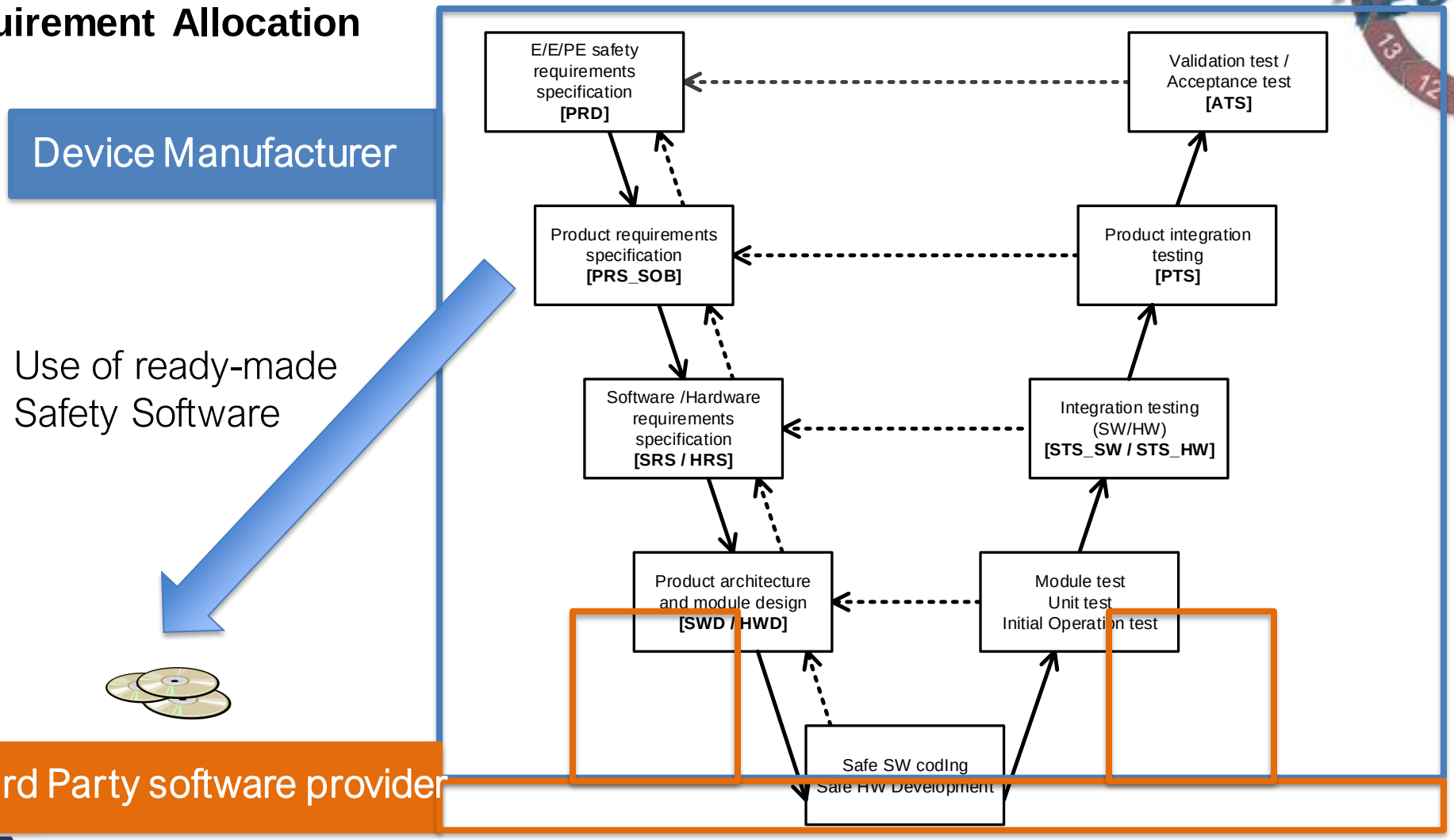
Third party module provider



3rd party S/W support in the Safety Lifecyle

5

Safety Requirement Allocation

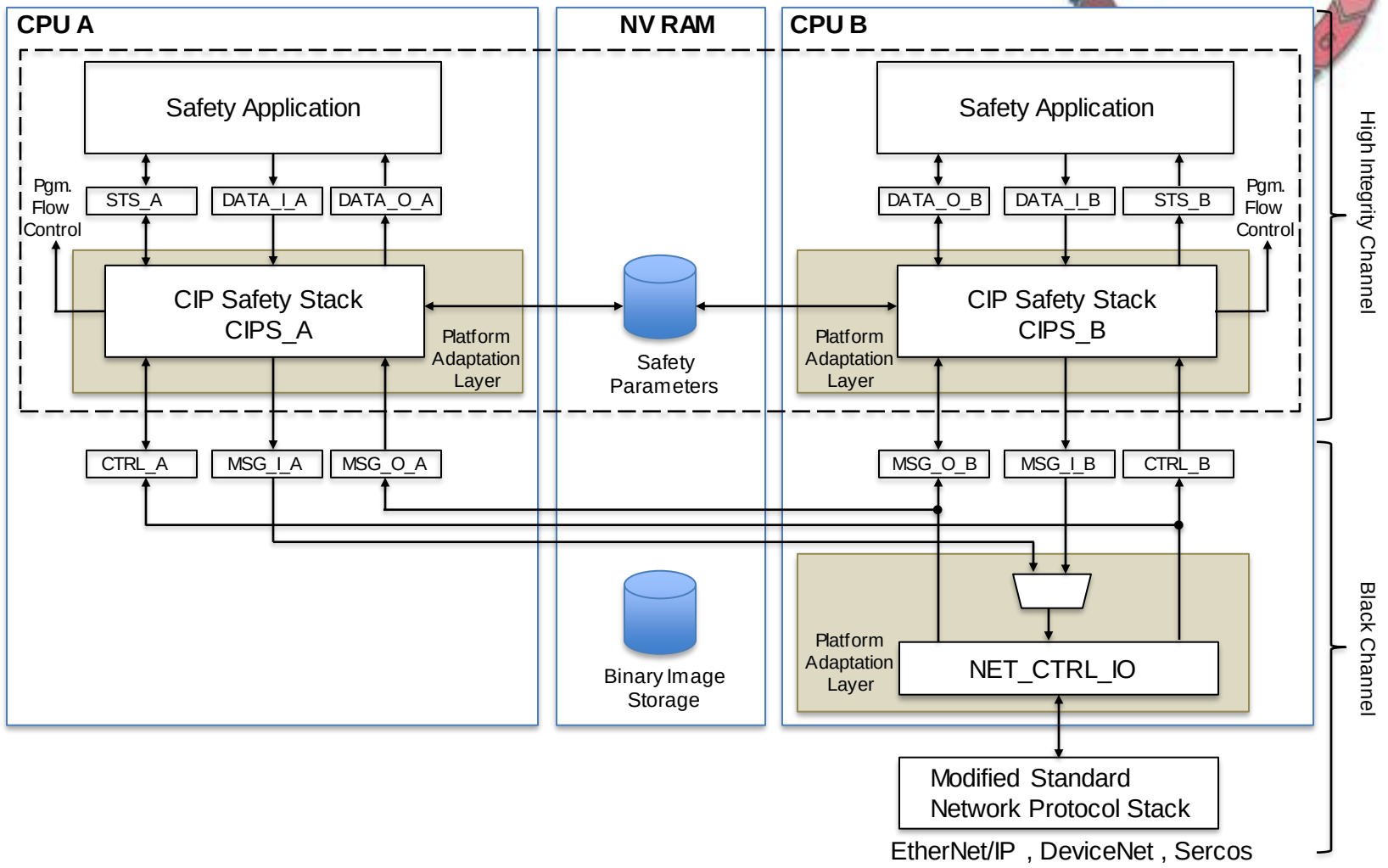


Example: Working with a CIP Safety toolkit

10 Realization

Platform requirements:

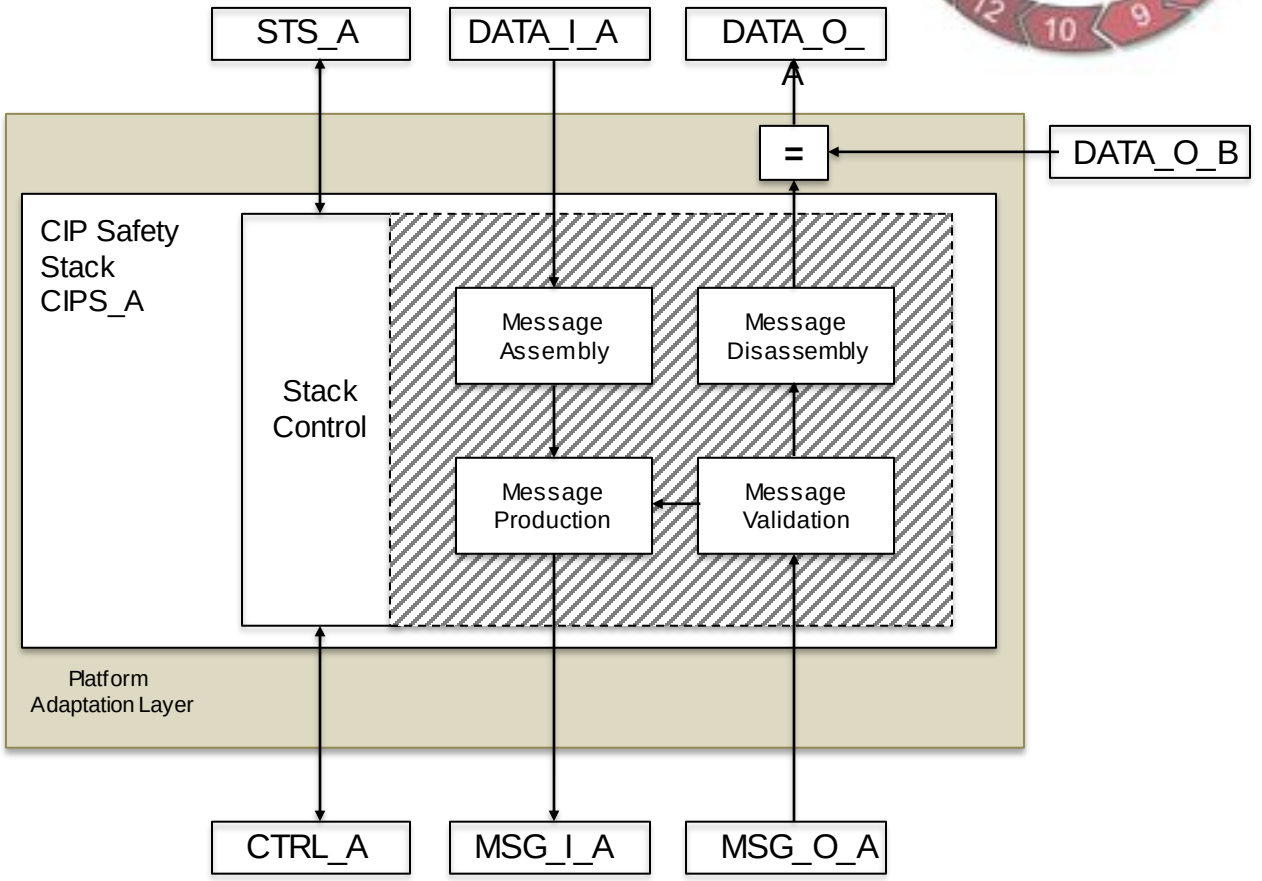
- Dual channel (1oo2)
- Integrity
  - FW binary image
  - non-volatile safety parameters storage
  - CPU and memory integrity
- Isolation
  - Read/write interface between non-safe and safe environments
- Program flow monitoring (Watchdog)
- Memory cross-checking (Soft-Error handling)



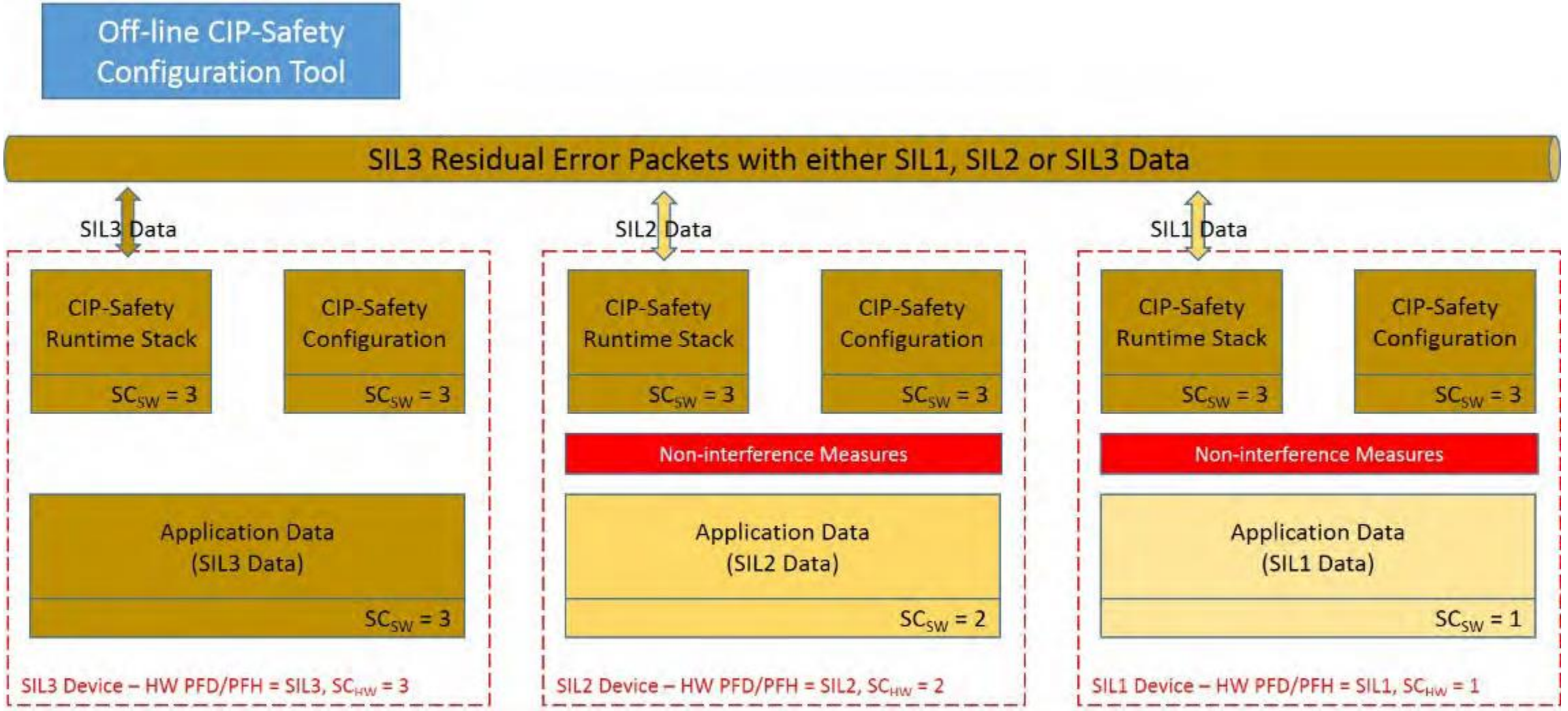
Example Toolkit (cont'd)

10 Realization

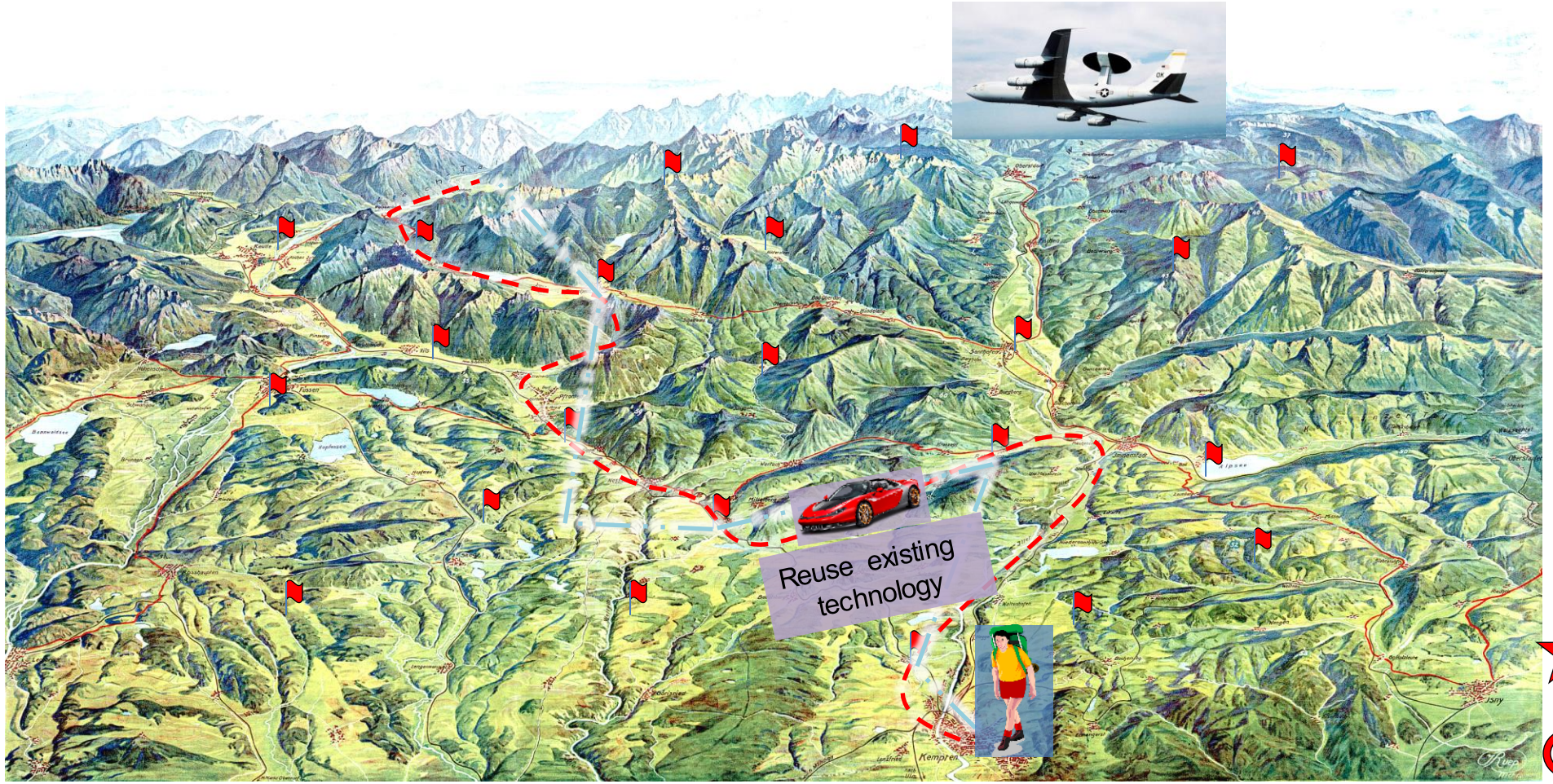
- CIP Safety Stack Implementation
  - The CIP Safety Stack comprises two functionally identical images CIPS_A and CIPS_B
  - Message Validation and Production is initiated by the platform(safe application) periodically.
  - Shall be designed (in both hardware and software) to be compliant with requirements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



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



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

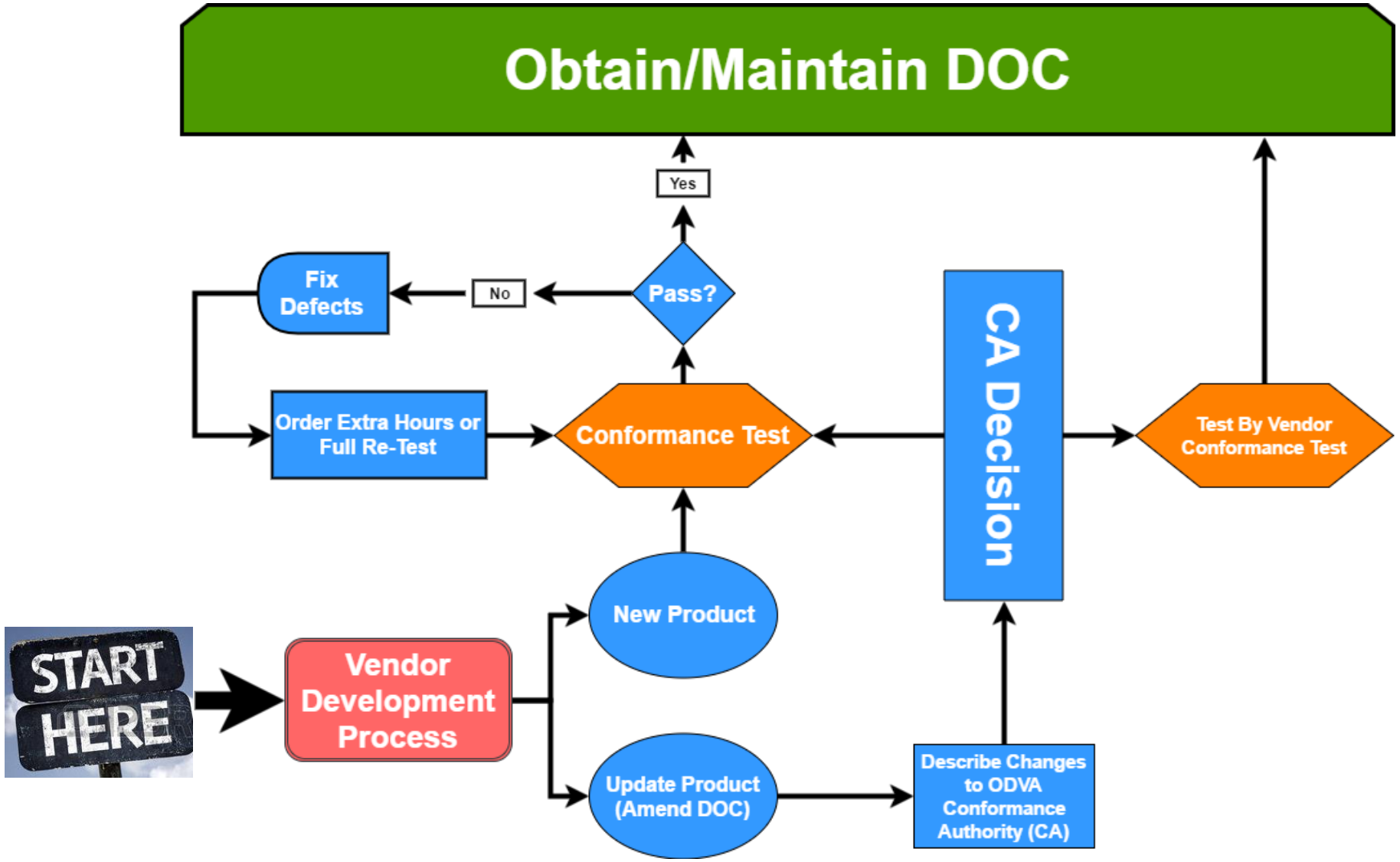
ODVA Composite Conformance Test

- 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

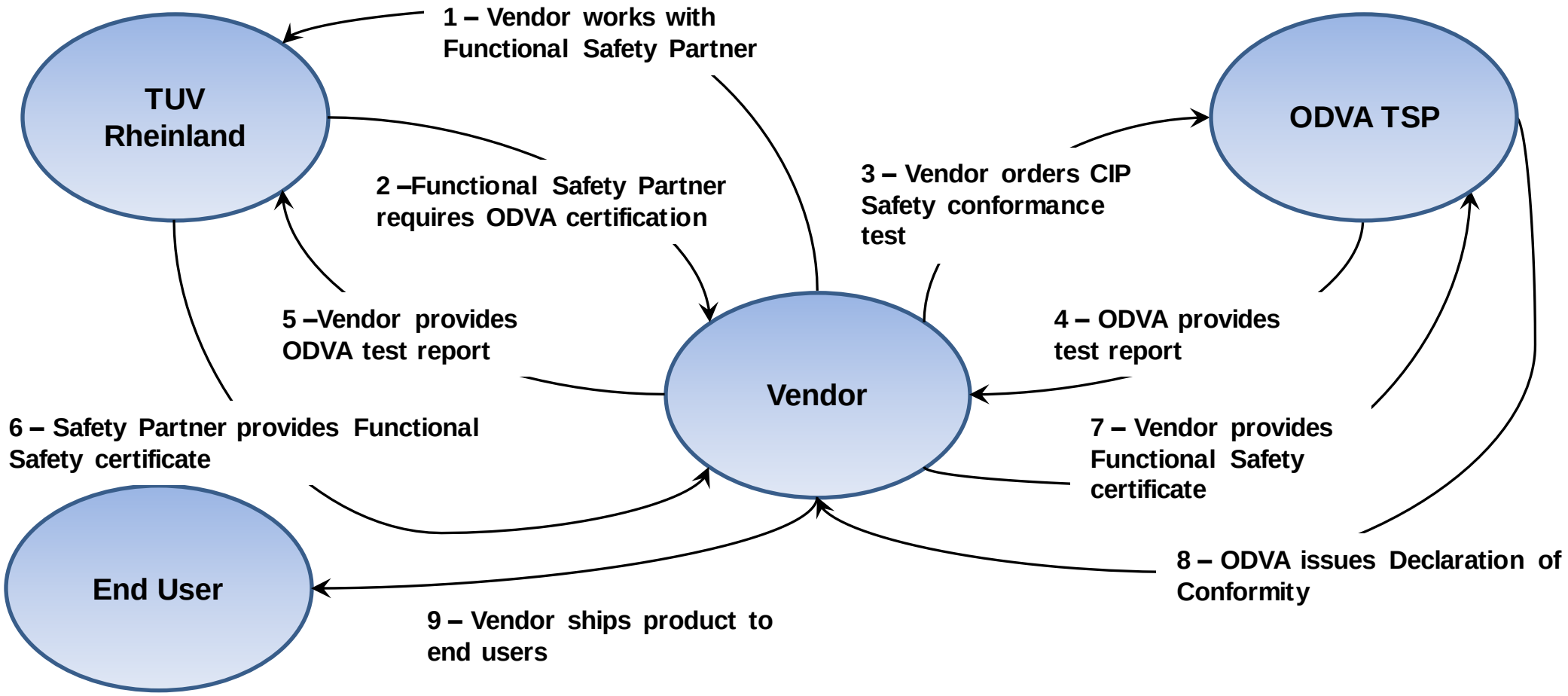
Conformance Process Overview



CIP Safety Conformance Test Process

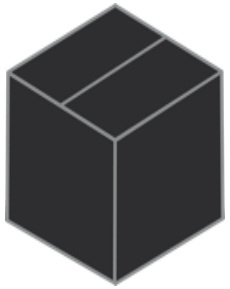
- Requires special version of the conformance test
  - Establishes conformance to the Safety Test Plan
  - Does not test functional safety nor assess the safety of a device implementation
- ODVA test report is an input to the assessment of CIP Safety implementations
  - TÜV Rheinland requires the ODVA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

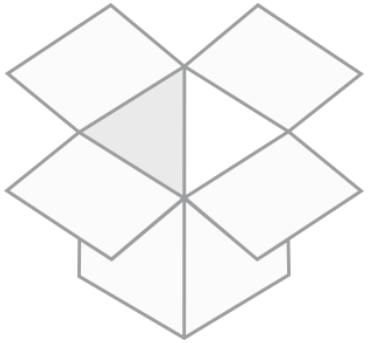
The central role of the Vendor



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 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