CIP Safety Embracing IEC 61784-3 Edition 4

Xiaobo Peng[1], Steven Seidlitz[2], David Crane[3], Arun Guru[4]

[1]Sr. Safety Architect, Rockwell Automation, Shanghai, China.
[2]Sr. Project Engineer, Rockwell Automation, Milwaukee, USA
[3]Sr. Staff Engineer, ODVA, Michigan, USA
[4]Principal Engineer, Rockwell Automation, Mequon, USA

Agenda

- IEC 61784-3 Overview
- Major Changes in IEC 61784-3 Edition 4
  - Extended models (TADI models)
  - Effectiveness of CRC polynomials
  - Transition to new editions
- Description of Changes to CIP Safety
- Impact to Conformance
- Summary
- Q&A

IEC61784-3 Overview

- The Edition 4 of IEC 61784-3 (Functional safety fieldbus - General rules and profile definitions) was published in February of 2021.
- It added significant enhancements to address Timeliness errors, Authenticity errors and Masquerade errors to accompany the previously considered Data Integrity errors.
- Edition 3 introduced “informative” extended models for estimation of the total residual error rate, considering all listed communication errors.
- The latest one, fourth edition made extended models as “normative”

IEC61784-3 Overview

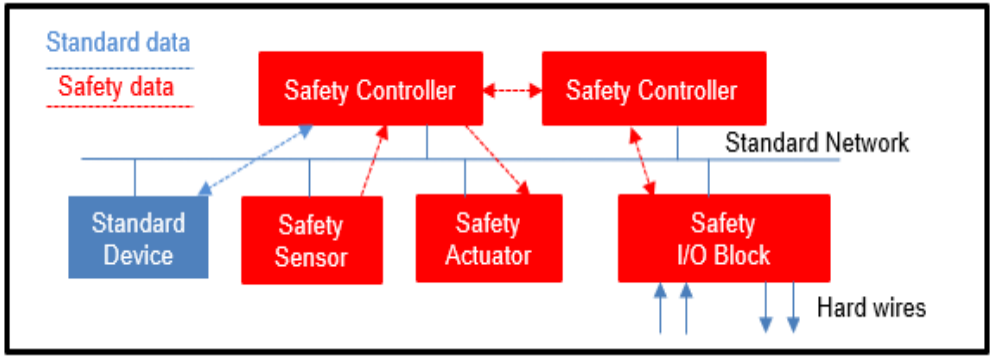


Figure 1: Networked Safety System.

- Safety communication is treated as part of a safety function and thus contributes to the total safety function PFH or PFD_{avg}.
- To simplify system safety calculations, it is recommended that any logical connection between safety communication elements of a safety function does not consume more than 1% of the maximum PFH or PFD_{avg} of the target SIL level [2].

IEC61784-3 Overview

- IEC 61784-3 categorizes communication errors into **corruption, unintended repetition, incorrect sequence, loss, unacceptable delay, insertion, masquerade and addressing** errors.
- This standard further recommends deterministic remedial measures to these communication errors, including the use of a sequence number, time stamp, time expectation, connection authentication, feedback message, data integrity assurance, redundancy with cross checking and different data integrity assurance systems.
- Importantly IEC 61784-3 also defines requirements and/or models for estimation of total residual error rate, which need to be considered and fulfilled by all FSCPs

Major Changes in IEC 61784-3 Edition 4 – Extended Models

- To introduce the extended models, all listed communication errors in the standard were further **grouped** into **Timeliness error, Authenticity error, Data Integrity error and Masquerade error**.
- Edition 4 requests a supplier of FSCP to provide proof of a sufficient overall residual error rate considering all these errors.
- Edition 4 also gives example equations for the calculation of residual error rates for explicit FSCP category, with contribution of residual error rates of data integrity errors (RR_I), authenticity errors (RR_A), timeliness errors (RR_T) and masquerade errors (RR_M).
- The total residual error rate can be based on the summation of the four residual error rates RR_I, RR_A, RR_T and RR_M, or it can be based on other quantitative proofs.

Major Changes in IEC 61784-3 Edition 4 – Effectiveness of CRC Polynomials

- IEC 61784-3 explains safety communication channel (*Binary Symmetric Channel* (*BSC*) model) using CRC-based error checking. The residual error probability based on the detection using a *CRC-mechanism* for a *BSC* can be calculated as

$$R_{CRC}(P_e) = \sum_{i=1}^{n} A_i \times P_e^i \times (1 - P_e)^{n-i} \quad \text{…Equation (1)}$$

Where *Ai* is the distribution factor of the code, *n* is the number of bits in block and *Pe* is the bit error probability.

- As indicated by the Equation (1), exploration of *Ai* is critical for R_{CRC} *(Pe)* calculation.
- Noting no conservative approximation formulas, IEC 61784-3 Edition 4 has an additional requirement to **explicitly calculate R_{CRC} *(Pe)* for the selected generator polynomial over all values of *n* in use and all relevant values of *Pe***

Major Changes in IEC 61784-3 Edition 4 – Transition to new editions

- A transition strategy was provided in Edition 4 to allow products to conform to new ‘normative’ requirements.
- Basically, the philosophy is that critical new requirements come to the standard as informative first and then become normative in next edition.
- The TADI models were informative in generic part Edition 3 so FSCPs were expected to update specifications based on TADI models during Edition 3 validity period.
- Upon the publication of Edition 4 of the generic part(February 2021), FSCPs should be assessed using the methods from Edition 4.

Description of Changes to CIP Safety

- There have been a few changes to the CIP Safety specification to accommodate the recent updates to the IEC 61784-3 standard as discussed in the previous section.
- In summary, Changes include deprecation of the Base Format and setting the Maximum Fault Number (Max_Fault_Number) of the Extended Format to a fixed value of 2.

Description of Changes to CIP Safety – Base Format Deprecation

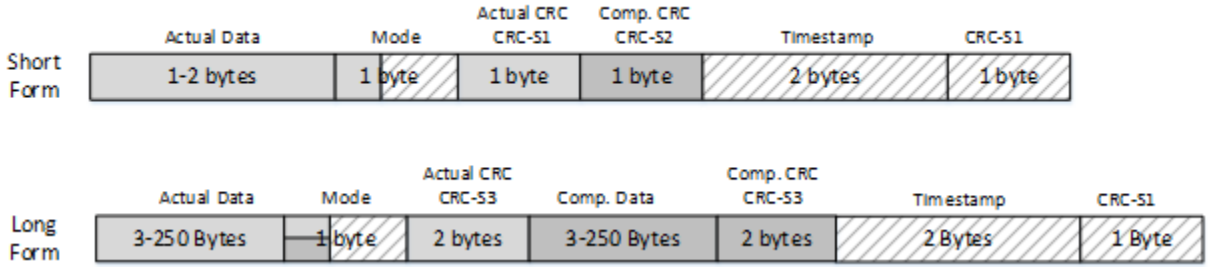


Figure 2: Base Format Messages.

- Figure 2 above illustrates the layout of the safety protocol data unit, SPDU, for each form of the Base Format.
- Both Short Form and Long Form employ an 8-bit CRC across the Time Stamp field.

Description of Changes to CIP Safety – Base Format Deprecation

- It turns out that Timeliness Errors are the major contributor to the overall Residual Error Probability. Let us dig a bit deeper to understand the reason

$$RR(Timeliness\_DataSection) \approx R(T)_{Data} \cdot \left[1 + RP\left(CRC_{Timestamp}\right)\right] \cdot RP(NTE_{check})$$ … Equation (2)

where:

RR = Residual Error Rate (faults per hour)

$R(T)_{Data}$ = Timeliness Error Rate (per hour)

RP = Residual Error Probability

NTE = Network Time Expectation

Description of Changes to CIP Safety – Base Format Deprecation

- $\boldsymbol{R(T)_{Data}}$, this is the error rate of Timeliness errors in units of faults per hour. This is how often Timeliness error can occur in a system, regardless of whether they can be detected or not.
- $\boldsymbol{RP\left(CRC_{Timestamp}\right)}$ makes use of that CRC field. It represents the probability that data integrity errors within the Time Stamp field will not be detected by the corresponding 8-bit CRC across it.
- $\boldsymbol{CRC_{Timestamp}}$ effectiveness is directly related to the strength and properness of the corresponding CRC polynomial and the number of bits of that CRC. Mathematically, this is represented by the value of 2^{-r}, where r is the number of bits of the CRC.
- For the Base Format in both forms, r has a length of 8 bits.

Description of Changes to CIP Safety – Base Format Deprecation

- From a practical standpoint, if a message containing stale or inaccurate safety data had reached a safety consumer in an end device, this represents the probability that:

  The Time Stamp may have been corrupted such that its value yet falls within the proper time window when otherwise it would not have

  -and-

  The CRC check had failed to detect this changed Time Stamp value up to a small probability of $2^{-8} = 3.9 \times 10^{-3}$.

- Old and stale safety data would be applied within the safety function of a system, thereby, potentially causing indeterminate behavior in the system and safety actuator(s).

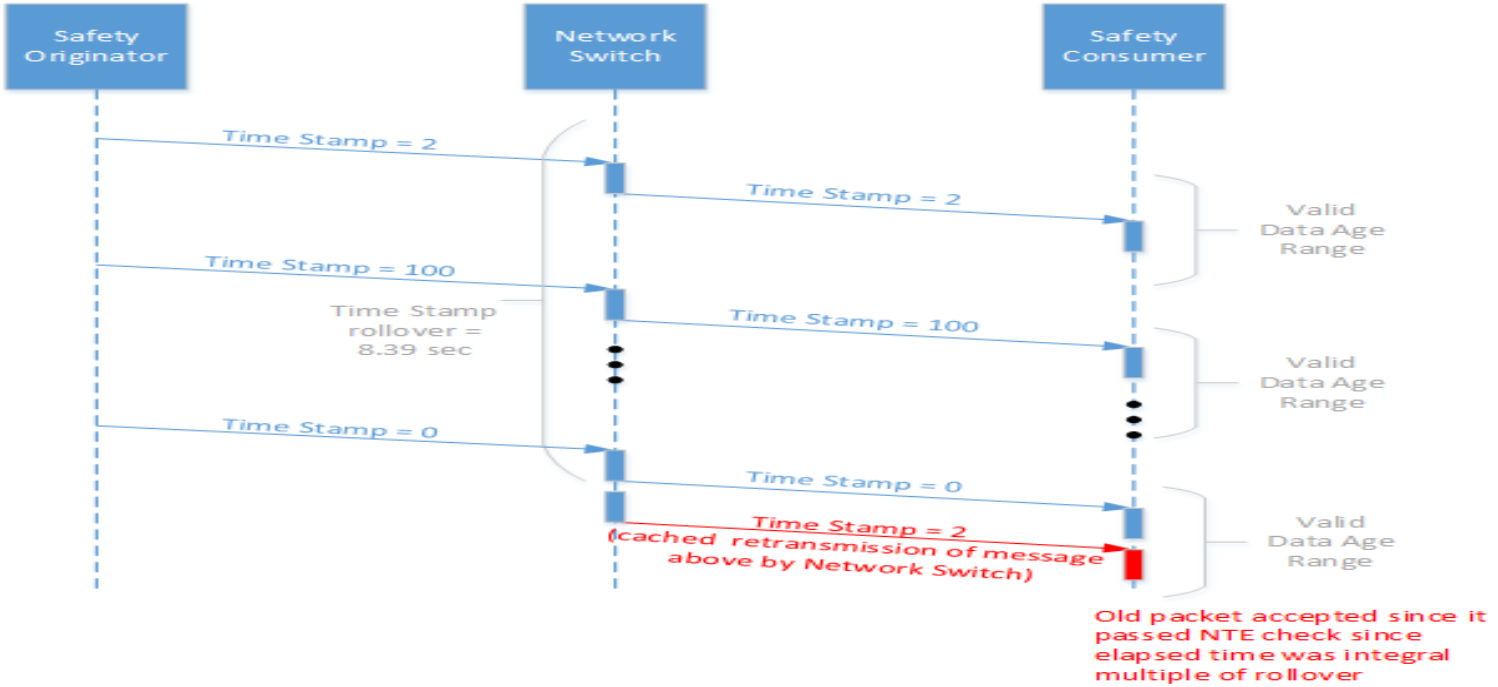
Description of Changes to CIP Safety – Base Format Deprecation

- $\boldsymbol{RP(NTE_{check})}$ is the second layer of defense in detecting Timeliness errors after the Time Stamp CRC check. As it turns out, this is the primary factor for why the Base Format cannot achieve a resultant PFH value of under 10^{-9}
- In short, this is due to the size of the Time Stamp field and not being able to detect Time Stamp rollovers. This term represents the probability that an invalid or stale packet will pass the Network Time Expectation check.

Description of Changes to CIP Safety – Base Format Deprecation

- There is a small chance that a Time Stamp of a stale message could be wrongly considered valid, if the time value just happens to fall within the valid window either through data corruption that is undetected by the *CRC* check or if the *CRC* check does pass but the Time Stamp value happens to be so old that the NTE check evaluates the data age associated with the Time Stamp to yet be valid. That's why the second term in Equation 2 contains a "1 +" factor.
- The Time Stamp could be corrupted, or it may not be but rather just old enough such that the data age check passes because of a rollover. The old age is not attributable to data corruption or from random hardware faults but from **systematic anomalies such as retransmission of cached messages.**

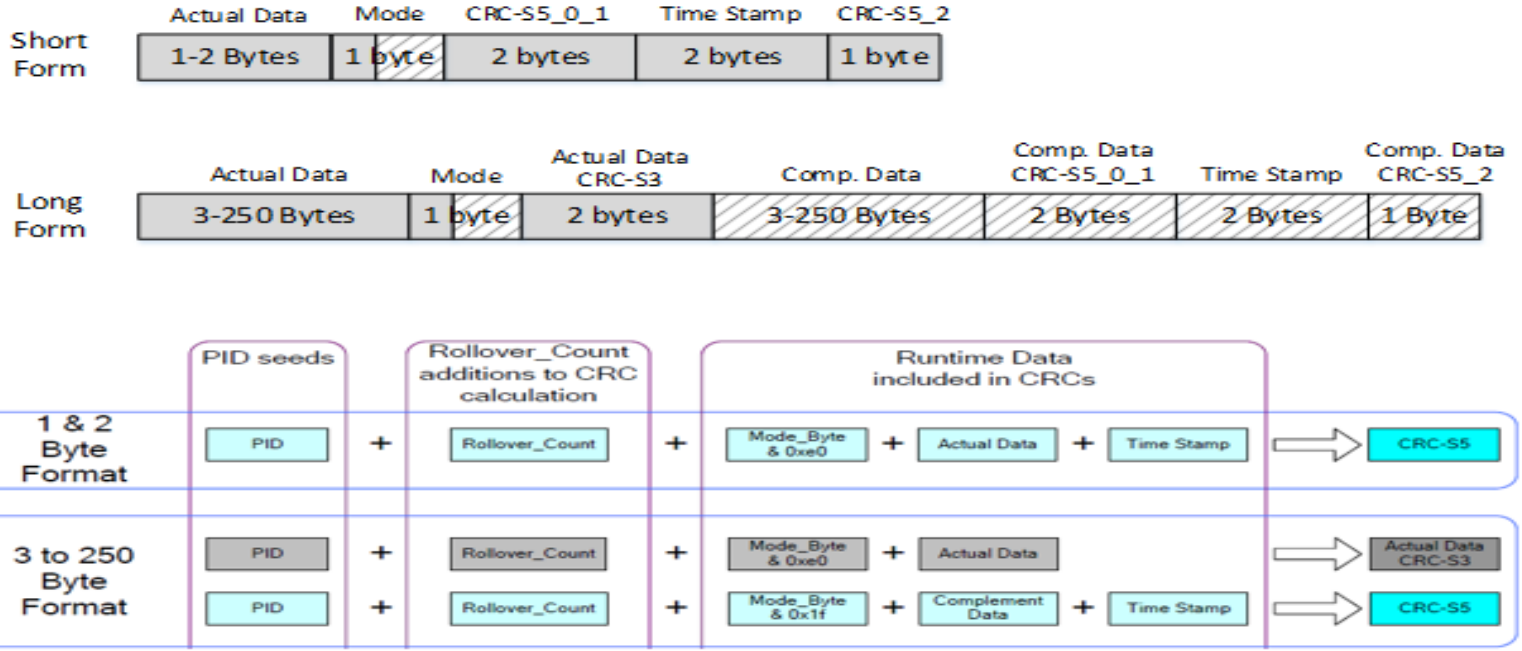
Description of Changes to CIP Safety – Base Format Deprecation



Description of Changes to CIP Safety – Base Format Deprecation

- What this all means is if a large EPI value is selected by an end user, the NTE value will be quite large, especially in comparison to the Time Stamp rollover time.
- Given the Time Stamp field of the Base Format has a length of 16 bits with no provisions for counting the number of rollovers and each bit count corresponds to a time increment tick of 128us, this translates to a Time Stamp rollover time of **(128us * 2^{16}) = 8.39 seconds**.
- That's **not a very large rollover time when considering contemporary store-and-forward network routers** in the marketplace.
- The probability that the NTE_{check} does not detect a Timeliness error is based on how big the NTE window is in comparison to the time it takes for the Time Stamp to rollover, which in this case is 8.39 seconds.
- The higher the NTE window for a safety connection, the higher the residual error probability becomes for CIP Safety. When calculating the final residual error rate for the Base Format, this term is just too high of a probability to overcome to stay under the **1 FIT (10^{-9} per hour) threshold without making format changes, and therefore is not compliant with Edition 4 changes to the IEC 61784-3.**

Description of Changes to CIP Safety – Extended Format



Description of Changes to CIP Safety – Max_Fault_Number

- There was one additional change needed for it to be compliant to Edition 4 of IEC 61784-3. The Extended Format provides for a certain amount of error tolerance through a parameter called the Maximum Fault Number (Max_Fault_Number). It had previously defaulted to a value of 5. This parameter was variable and set during the connection establishment process.
- This parameter is included the Type 1 Safety Open message. When considering the new changes from Edition 4 of IEC 61784-3 in relation to the Extended Format, Timeliness errors also became the same dominating factor as was the case for the Base Format. Unlike the Base Format, though, the residual error rate for the Extended Format can be made to stay under the threshold of 10-9 per hour.
- The format did not need to be completely deprecated but rather slightly modified. To stay under this probability error rate threshold the Maximum Fault Number (Max_Fault_Number) is now fixed to a constant value of 2 and is no longer variable from this point forward.
- Since Maximum Fault Number is a parameter included in a safety open message, Originators will be checked to verify that they do not send any value other than 2 for Max_Fault_Number parameter in the Safety Open.

Impact of Changes on CIP Safety Devices

- Installed legacy products will continue to be covered by their certifications accorded by certifying bodies. However, when significant modifications to an installed safety system are done, this modified safety system would need to comply with the most current version of the standards. Product owners and end users should consult their certifying bodies for specific guidance. Also note that support for Base Format will continue to exist in the originator devices to support legacy installations.

Impact to Conformance

- The changes to the specification described above impact the ODVA conformance test in the following ways:
  - Devices with safety originator functionality will be checked for correct setting of the Maximum Fault Number (Max_Fault_Number) parameter. The evaluation of this behavior may require review of accompanying documentation and configuration software tools.
  - Devices with safety target functionality will be checked for rejection of Base Format connection requests. Eligible target-only devices still supporting base format and seeking to maintain a previously issued DOC (Declaration of Conformity) may use the Amended DOC test process according to ODVA policy in Pub 8 and Pub 261.
- The grace period provided for gradual adoption of these requirements ended on January 1, 2022. Since that time, target-only devices which have not deprecated the Base Format cannot obtain a new Declaration of Conformity from ODVA.

Summary

- We described changes in IEC 61784-3 Edition 4 which had an impact on the CIP Safety protocol as a FSCP when it became normative in February 2021.
- We described in detail the impact of changes in the total residual error rate calculations for both Base and Extended Formats of CIP Safety messages while considering those additional errors in communications channels as required by the Edition 4.
- We explained rationale for deprecating Base Format and change in the Max_Fault_Number parameter value.
- These changes along with specification enhancements have been released in Edition 2.22 of CIP Safety Volume 5.
- Conformance testing will be used to govern these changes in the CIP Safety specification as new devices undergo conformance certification testing beyond January 2022.

Q&A

2022 ODVA

INDUSTRY CONFERENCE AND 21ST ANNUAL MEETING