Invensys Tricon Communications

Isolation, Independence, and Data Integrity

Joseph Murray

Nuclear program manager

Invensys Process Systems

29 March 2007

invensys®

Process Systems

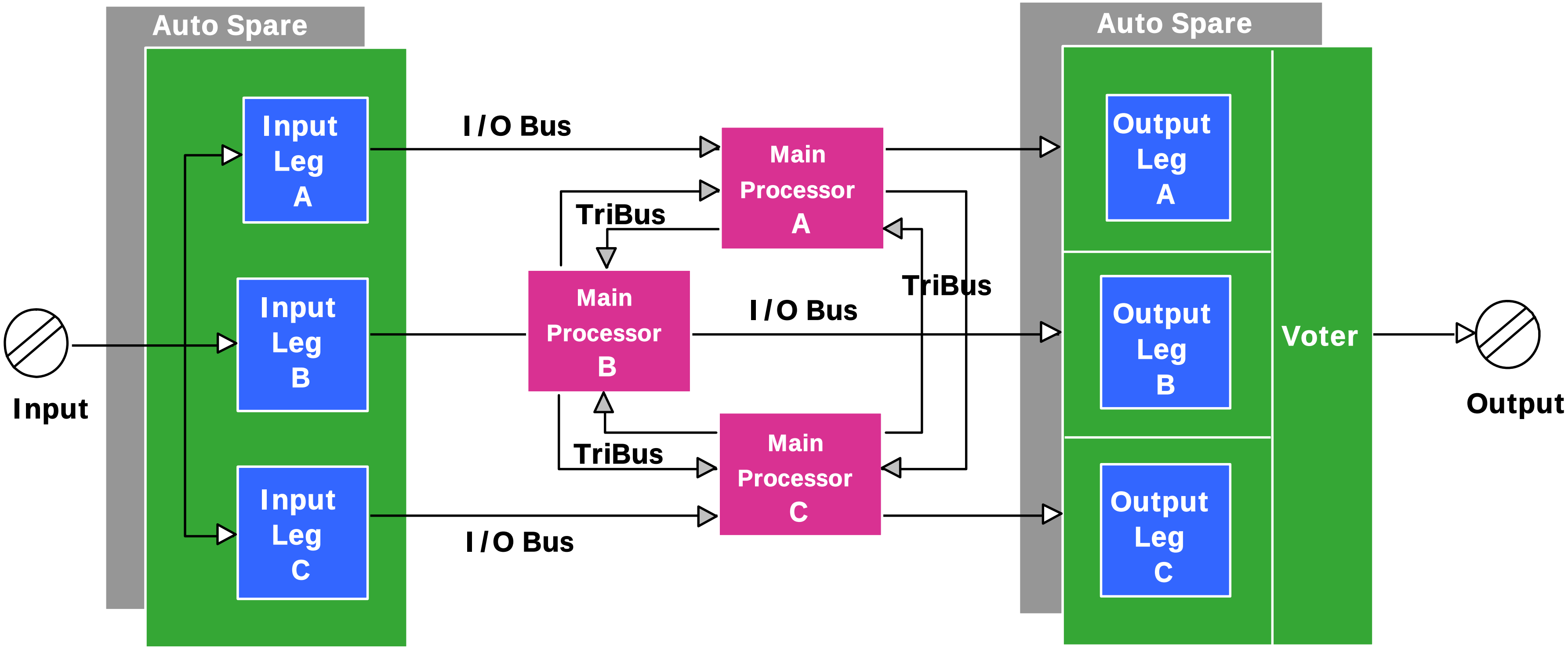
Get More from One

Avantis • Foxboro • SimSci-Esscor • Triconex

Tricon overview

- Triple Modular Redundant
- No Single Point of Failure
- Wide use as safety & critical control across industries
  - > 7000 systems in service
  - > 400,000,000 hours without a failure to perform on demand
  - Same platform as 1E system
- Designed from the ground up as an industrial safety and critical control system
- Full internal diagnostics, self testing and self calibration
- Designed to maintain operation with multiple failures, properly report failures, and allow on-line repairs

Tricon Architecture



Today's Breakdown

- Safety Communications need to be addressed in two distinct areas:

- 1) Hardware Based Isolation / Independence
  - To show that one division's communications function can have no deleterious effect on another division.
- 2) Software Based Message Validation Methodology
  - To show that the data being transmitted between divisions has maintained integrity, is validated and is timely.

Hardware based isolation / independence

Triconex communications basics

- Tricon designed to use “Black Channel” definition.
  - Black Channel means that everything outside of the Tricon is considered an unknown.
  - All design criteria to meet independence / isolation and maintain data integrity is contained within the Tricon.
  - No credit is taken for external devices.
    - External devices outside of our design control.
- Full electrical isolation
  - Opto-Isolators and fiber optics
- Communications isolation from safety application processor
- Shared memory used throughout
- Multi-layered control of access to safety processors

Triconex communications basics, continued

- All processors asynchronous
- All data writes must be in the proper format, have the proper address, be within a given range.
  - No writes allowed to any points not pre-assigned as writeable
  - Those pre-assigned points must also be programmed into sending Tricon.
- No requests for “Reads” into the safety application processor.
  - Full data dump every scan of all pre-assigned (programmed) readable points and all diagnostics values.
- Individual communications cards can be configured for “Read Only”
- Entire Tricon can be key switched to “Read Only”
- Tricon to Tricon Peer-to-Peer is a proprietary protocol that is essentially a point to point UDP/IP non-request transmission with an additional safety communication layer on top of the standard comms layers

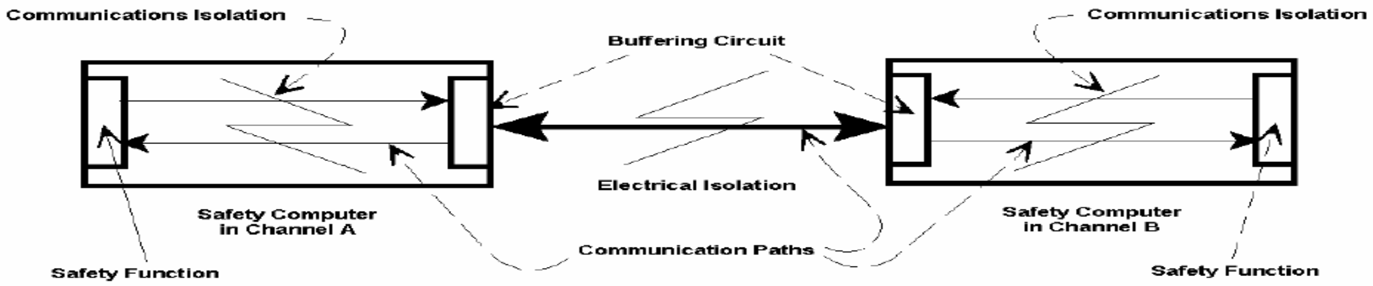
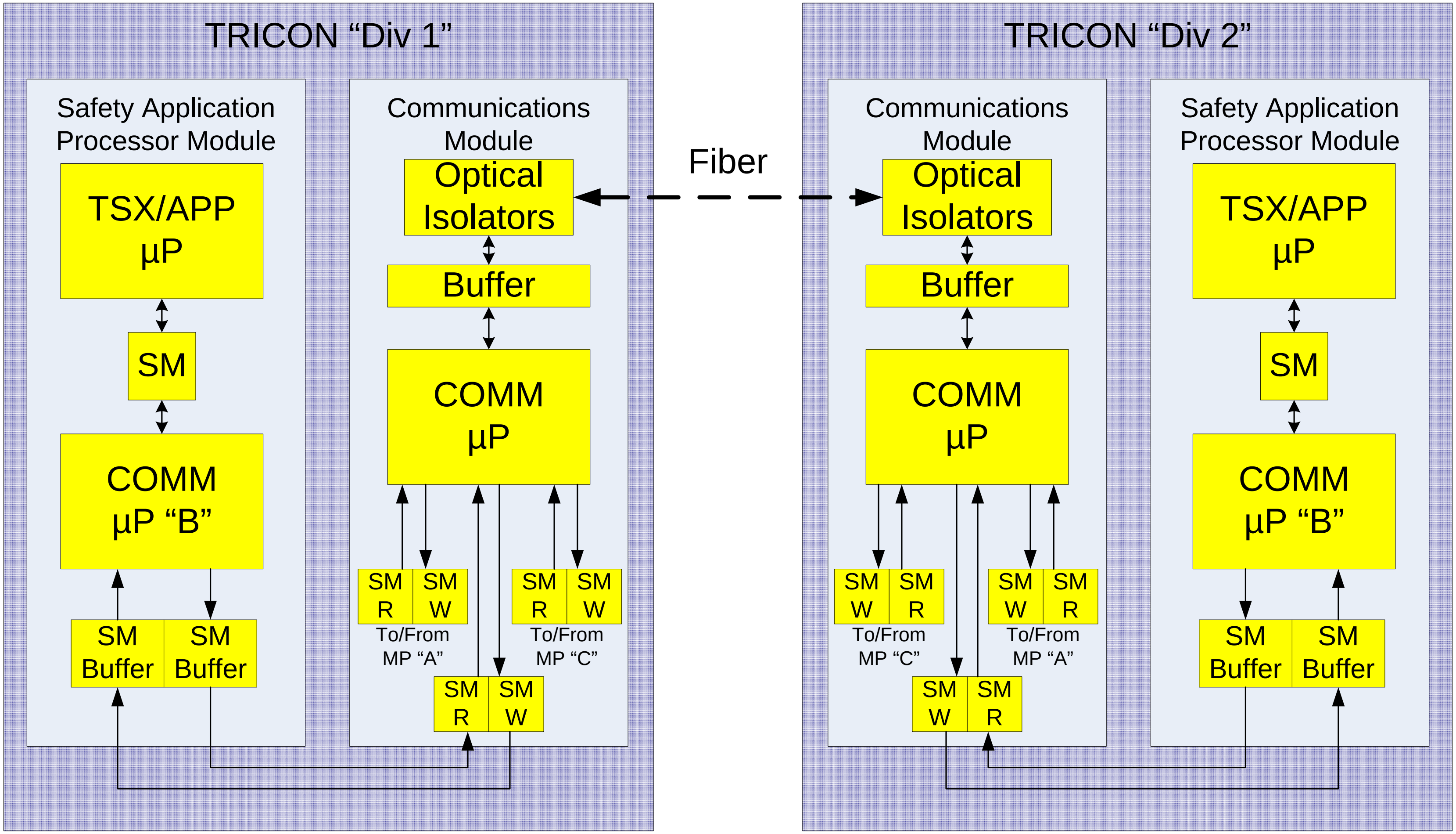


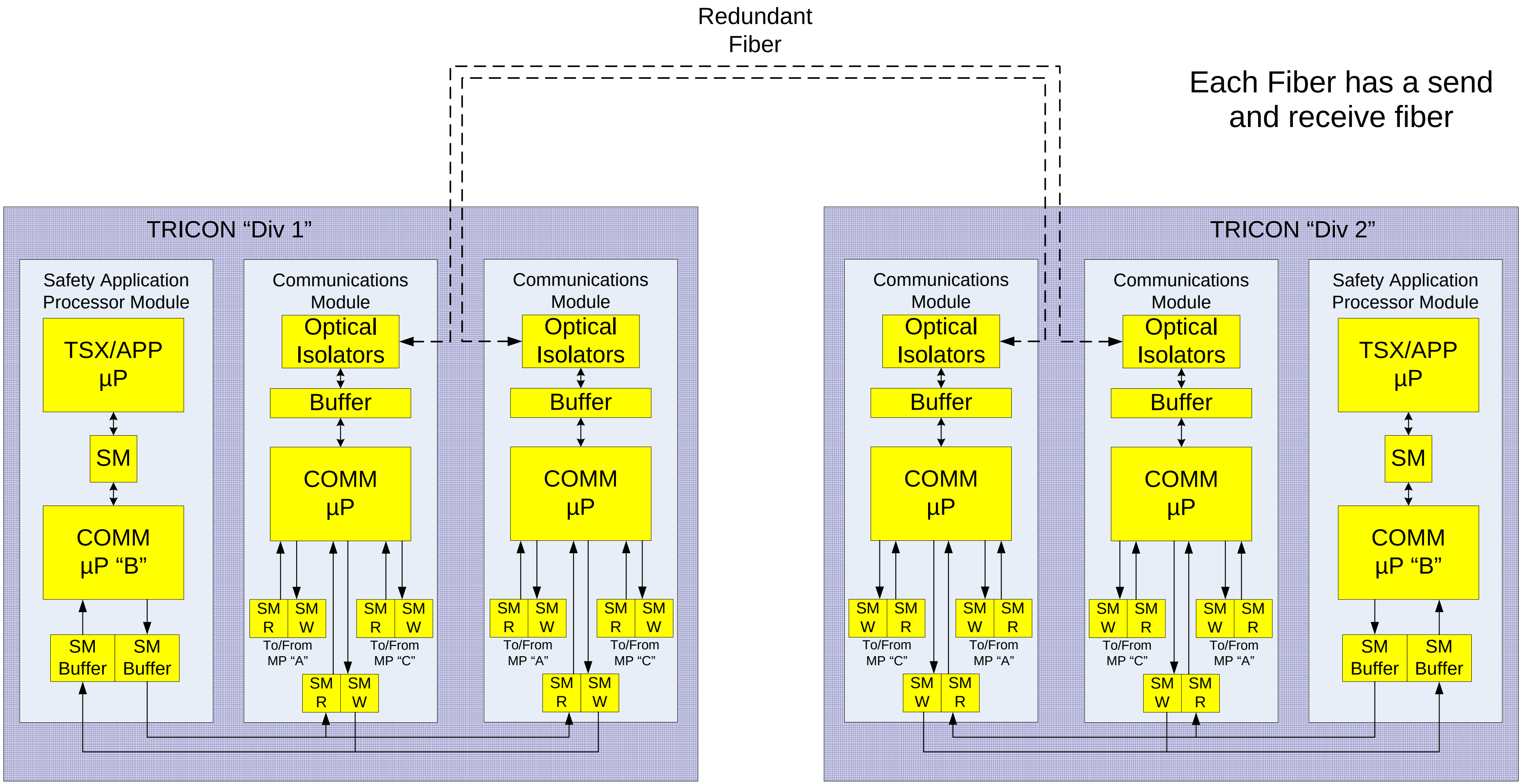
Figure E.2—Communication between safety channels (two-way communication)



invensys
Process Systems

Redundant Safety Peer-to-Peer

Each Fiber has a send and receive fiber



Safety to Non-Safety Comms

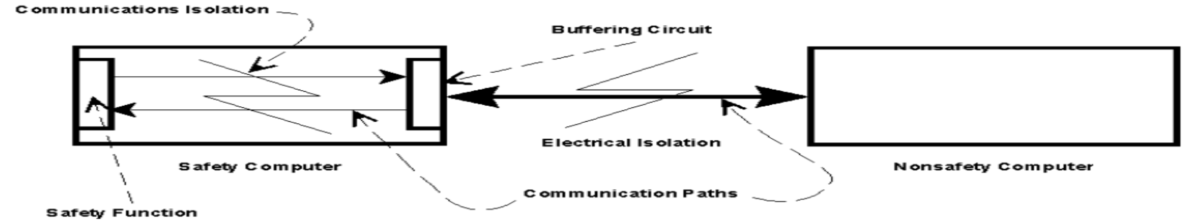
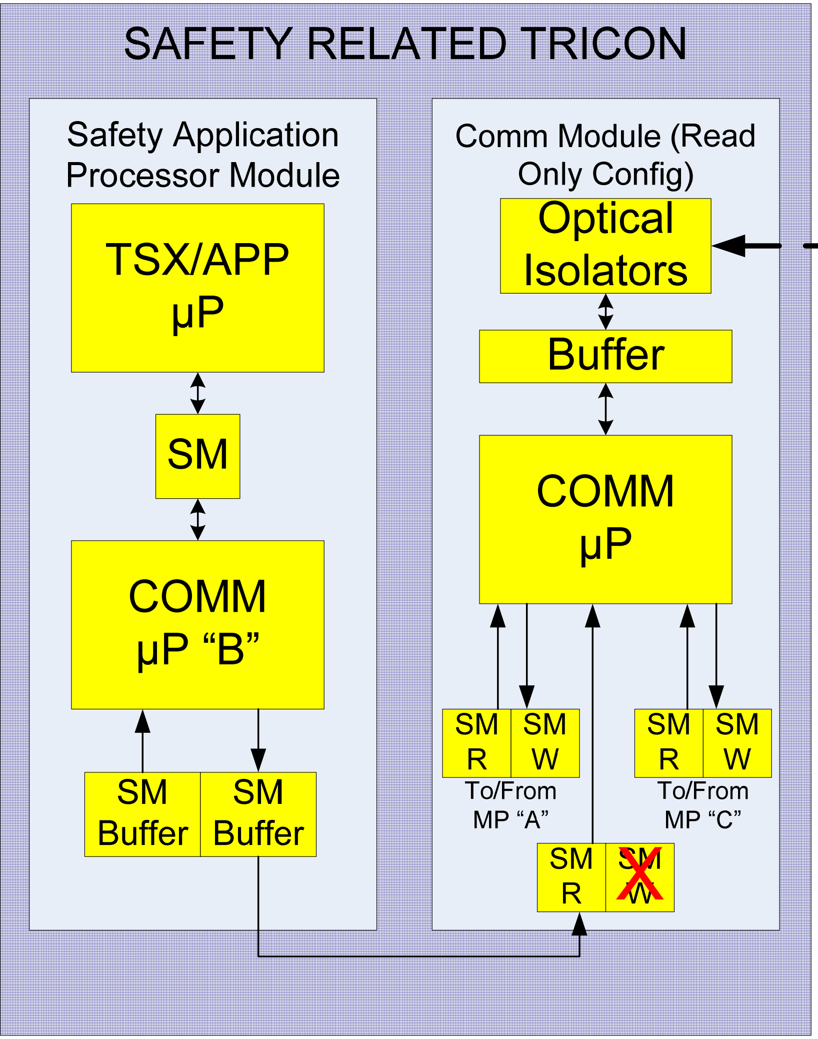


Figure E.4—Communication between safety and nonsafety computers (two-way communication)

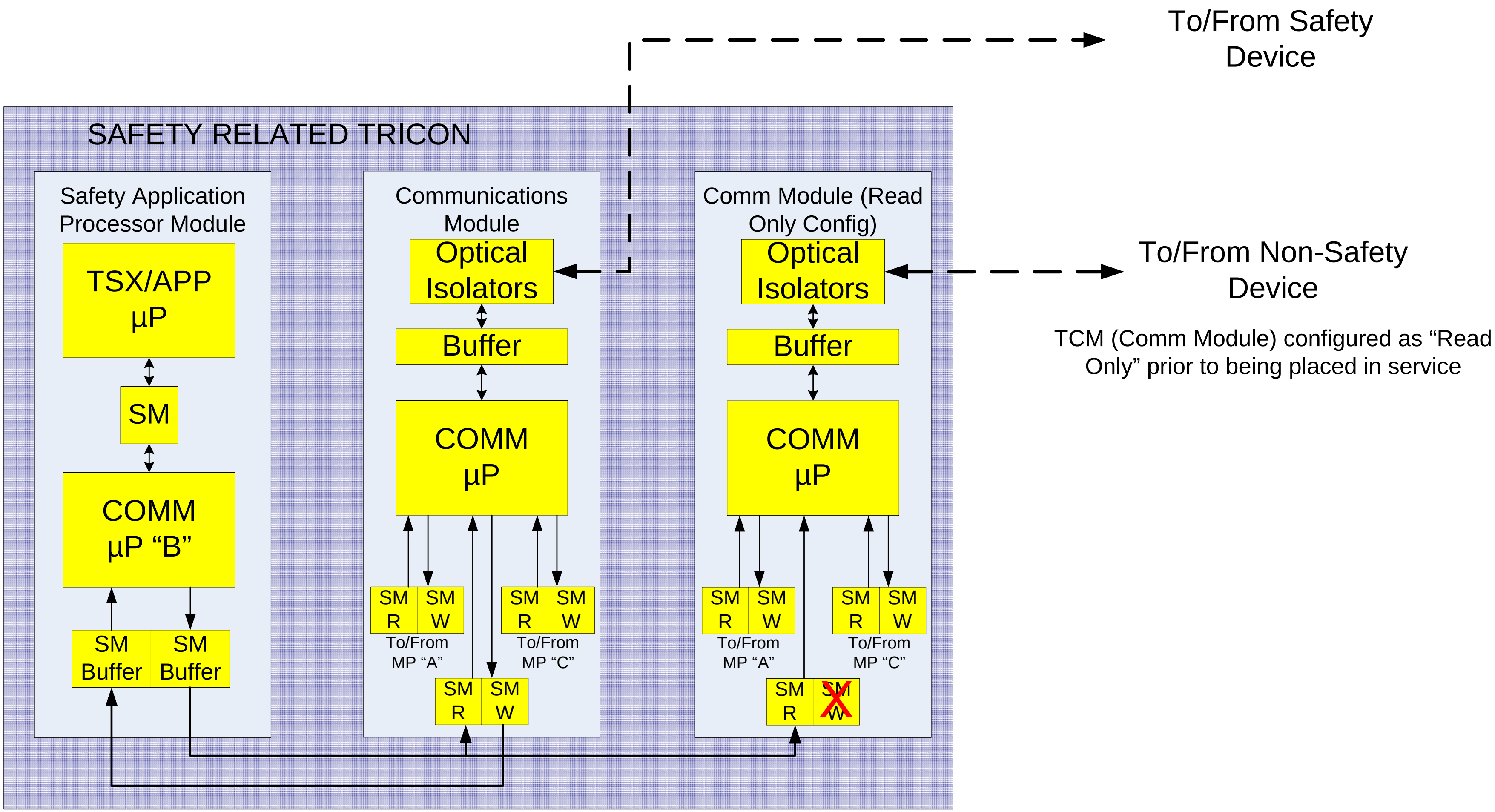


To/From Non-Safety Device

- Comm Card configured as "Read Only." All write functions disabled; write requests ignored.
- At end of every App µP scan, all data preprogrammed as "Read" or "Read-Write" and all diagnostics are dumped all the way to comm card memory; not by request.
- Request for data comes into comm card
- Comm card only looks to it's own memory for available data on a read request
- Read requests can only be for the listed "read" points or request ignored
- Data transmitted out in response

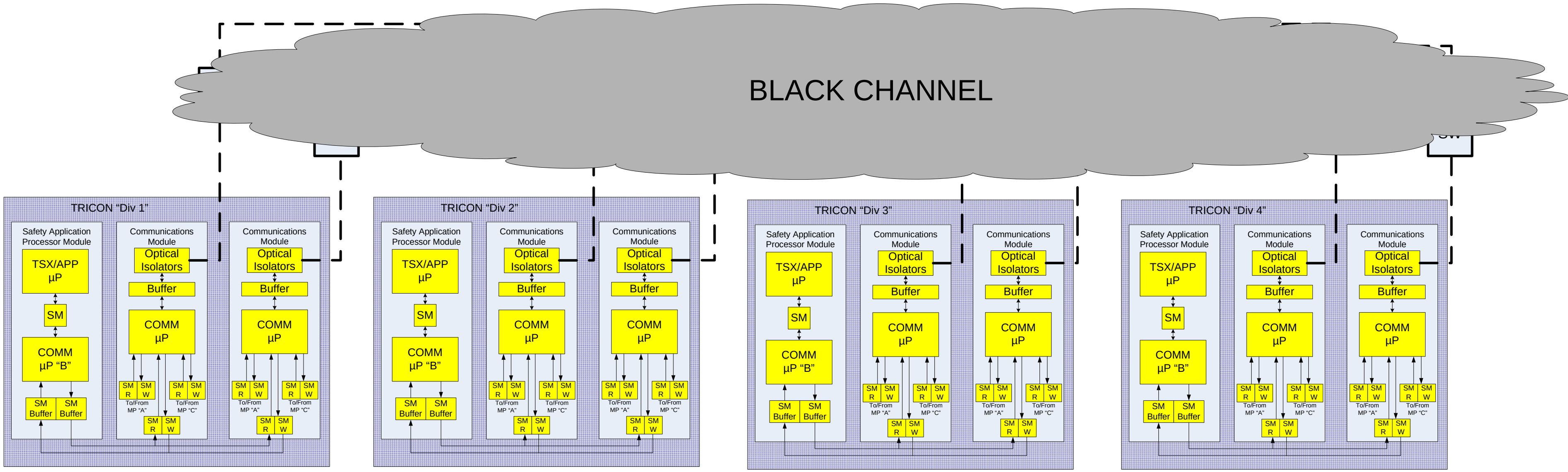
Tricon with SR-SR and SR-NSR communications

Invensys Process Systems



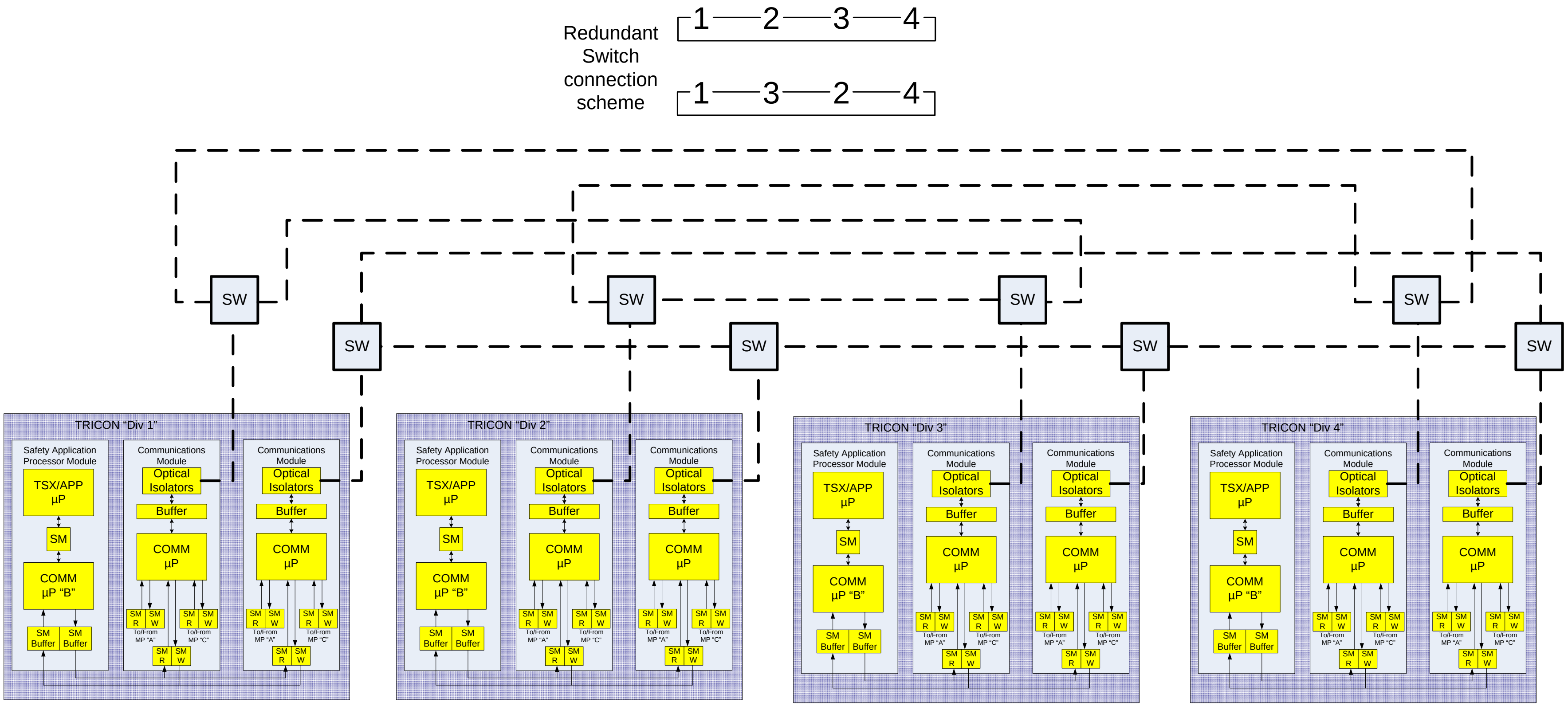
Tricon independent of network topology

- All design features to ensure both data independence, isolation, and integrity reside in Tricon.



Example of Cross Divisional Network

- Dual Redundant Self Healing Ring Fiber Network
  - Multiple fault tolerant
  - COTS dedicated network switches, data integrity independent of switches.



Section Summary

- Tricon system maintains multiple barriers between the safety application processor and the communication process to external devices.
  - Shared Memory
  - Buffers
  - Two barrier processors between the safety application processor and the “outside” world
  - Capability to disable write functions per comm card or for entire system
  - “Read” methodology that ensures no requests go further than the comm card
  - Isolation / Data Independence is independent of external devices and is controlled fully within the Tricon System.

Software Based Message Validation Methodology

Or, How do I know I’m getting what I think I’m getting when I think I should be getting it!

Overview

- Physical independence and isolation is only half the battle.
- Assurance of data integrity is the rest!
- Requirements?   Determination of:
  - Credible faults in communications
  - Acceptable remedial measures
  - Considerations affecting data integrity

New standard

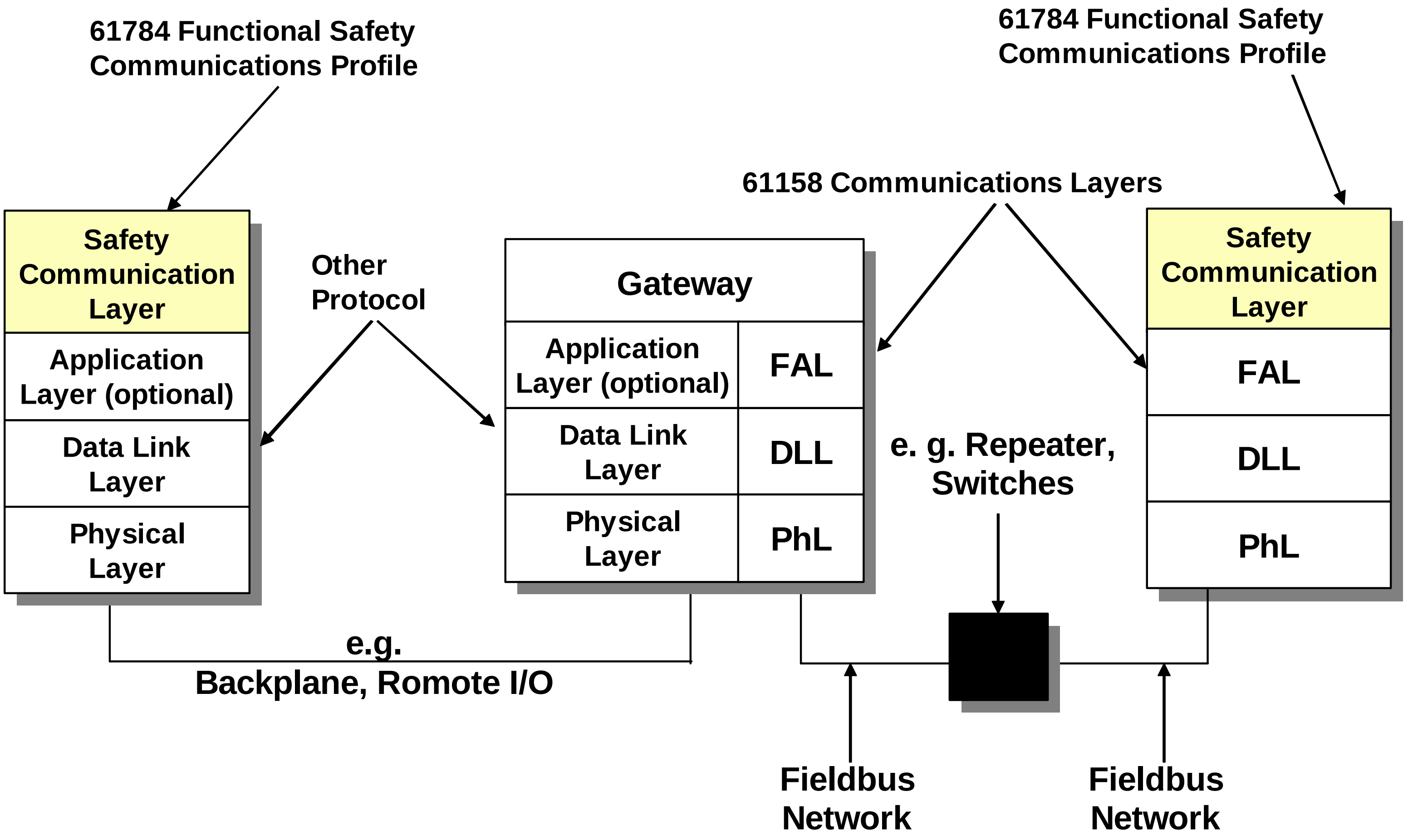
- Triconex is a part of the IEC working group that developed a new standard, IEC 61784-3, “ Industrial Communications – Fieldbus profile – Profiles for functional safety communications in Industrial networks Part 3: General rules and profile definitions.
  - “…provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.”
- In other words
  - Know when the message is good

  AND

  - Know when the message is bad and take specific pre-analyzed actions

Safety Communication Layer

- Communications Protocol Safety layer added on top of communications layers.


61784 Functional Safety Communications Profile
Safety Communication Layer
Application Layer (optional)
Data Link Layer
Physical Layer
Other Protocol
Gateway
Application Layer (optional)
FAL
Data Link Layer
DLL
Physical Layer
PhL
e.g. Backplane, Romote I/O
61158 Communications Layers
61784 Functional Safety Communications Profile
Safety Communication Layer
FAL
DLL
PhL
e. g. Repeater, Switches
Fieldbus Network
Fieldbus Network

Credible Failures

- Corruption
  - Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference.
- Unintended Repetition
  - Due to an error, fault or interference, old not updated messages are repeated at an incorrect point in time.
- Incorrect Sequence
  - Due to an error, fault or interference, the predefined sequence (e.g. natural numbers, time references) associated with messages from a particular source is incorrect.

Credible Failures (continued)

- Loss
  - Due to an error, fault or interference, a message is not received or not acknowledged.
- Unacceptable Delay
  - Messages may be delayed beyond their permitted arrival time window, for example due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied (for example FIFOs in switches, bridges, routers).
- Insertion
  - Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity.

Credible Failures (continued)

- Masquerade
  - Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a non-safety relevant message may be received by a safety relevant participant, which then treats it as safety relevant.
- Addressing
  - Due to a fault or interference, a safety relevant message is sent to the wrong safety relevant participant, which then treats reception as correct.

Deterministic Remedial Measures

- Sequence Number
  - A sequence number is integrated into messages exchanged between message source and message sink. It may be realised as an additional data field with a number that changes from one message to the next in a predetermined way.
- Time Stamp
  - In most cases the content of a message is only valid at a particular point in time. The time stamp may be a time, or time and date, included in a message by the sender.
- Time Expectation
  - During the transmission of a message, the message sink checks whether the delay between two consecutively received messages exceeds a predetermined value. In this case, an error has to be assumed.

Deterministic Remedial Measures (continued)

- Connection Authentication
  - Messages may have a unique source and/or destination identifier that describes the logical address of the safety relevant participant.
- Feedback Message
  - The message sink returns a feedback message to the source to confirm reception of the original message. This feedback message has to be processed by the safety communication layers.
- Data Integrity Assurance
  - The safety-related application process shall not trust the data integrity assurance methods if they are not designed from the point of view of functional safety. Therefore, redundant data is included in a message to permit data corruptions to be detected by redundancy checks.

Deterministic Remedial Measures (continued)

- Redundancy with Cross Checking
  - In safety-related fieldbus applications, the safety data may be sent twice, within one or two separate messages, using identical or different integrity measures, independent from the underlying fieldbus.
  - In addition to this, the transmitted safety data is cross-checked for validity over the fieldbus or over a separate connection source/sink unit. If a difference is detected, an error shall have taken place during the transmission, in the processing unit of the source or the processing unit of the sink.
  - When redundant media are used, then common mode protection should be considered using suitable measures (e.g. diversity, time skewed transmission)

Deterministic Remedial Measures (continued)

- Different data integrity assurance systems
  - If safety relevant (SR) and non-safety relevant (NSR) data are transmitted via the same bus, different data integrity assurance systems or encoding principles may be used (different CRC algorithms, different generator polynomials), to make sure that NSR messages cannot influence any safety function in an SR receiver.

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption (see 5.3.2)					X	X	Only for serial bus[d]	
Unintended repetition (see 5.3.3)	X	X					X	
Incorrect sequence (see 5.3.4)	X	X					X	
Loss (see 5.3.5)	X				X		X	
Unacceptable delay (see 5.3.6)		X	X[c]					
Insertion (see 5.3.7)	X			X[a,b]	X[a]		X	
Masquerade (see 5.3.8)				X[a]	X[a]			X
Addressing (see 5.3.9)				X				

NOTE Table adapted from IEC 62280-2 and [24].

[a] Depends on application.

[b] Only for sender identification. Detects only insertion of an invalid source.

[c] Required in all cases.

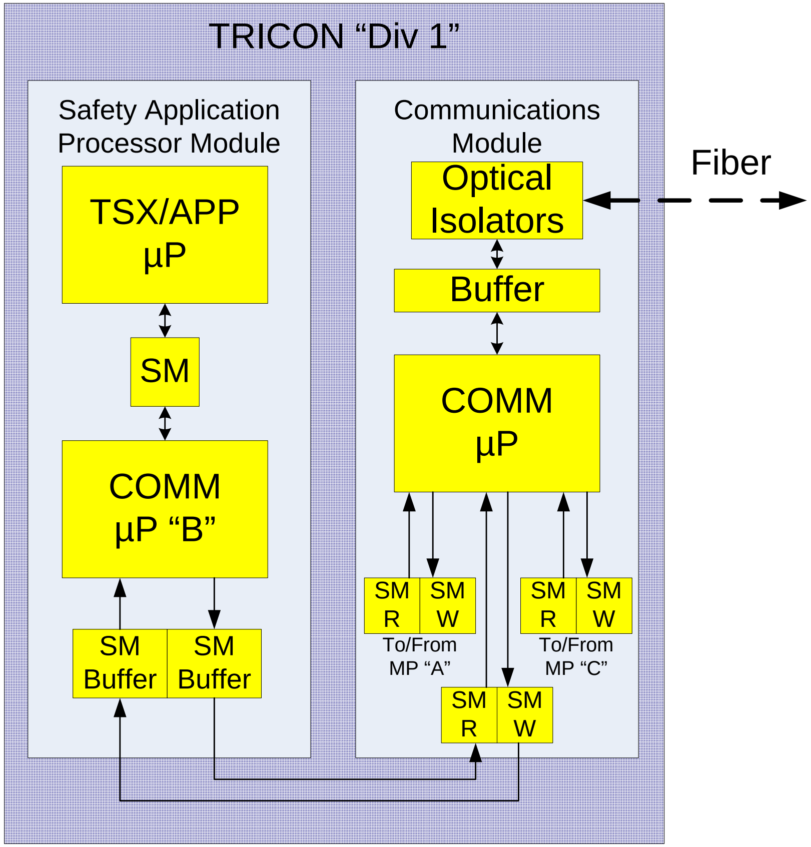
[d] This measure is only comparable with a high quality data assurance mechanism if a calculation can show that the residual error rate Λ reaches the values required in 5.4.9 when two messages are sent through independent transceivers.

Triconex Peer to Peer Safety Layer

Function	Dest. Address & internal address	Source Address & internal address	Seq. #	Data	Hash Function	CRC-64

Assembled in Safety App Processor

Appended in Comm Card



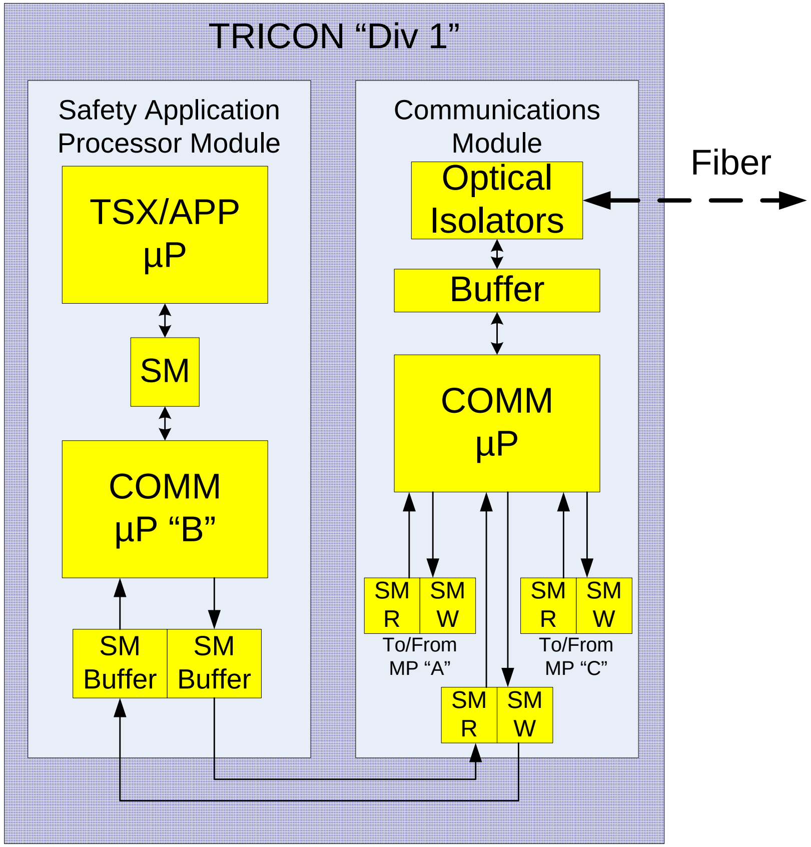
- Application program contains actions to be taken on loss of validated data.
- Tricon expects feedback message for every transmission. If message lost (non-validated) sending unit will take action (alarm) and receiving unit will take action (possibly trip and alarm)
- All remedial safety measures are taken within the safety application processor to ensure integrity of all internal comm links.

Triconex Peer to Peer Safety Layer (continued)

Function	Dest. Address & internal address	Source Address & internal address	Seq. #	Data	Hash Function	CRC-64

Assembled in Safety App Processor

Appended in Comm Card



- Non-responsiveness will cause Tricons to reset sequence numbers. Sequence numbers are not skipped.
- CR-64 added by comm card for extra security.
- Addresses, internal addresses, data formats and ranges, data point ID's are all preprogrammed in each Tricon system. Messages that do not follow proper format are rejected.
- Receiving Tricon verifies message and sends response to Source Tricon

Section Summary

- Invensys Triconex follows methodologies to ensure Physical isolation and independence, and also follows methodologies (spelled out in IEC 61784-3) to ensure Data Validation Integrity and Timeliness.
- Methods employed ensure integrity of message within the safety application processor, thereby ensuring greatest coverage of prospective points of error in comm path.

- Questions / Comments?