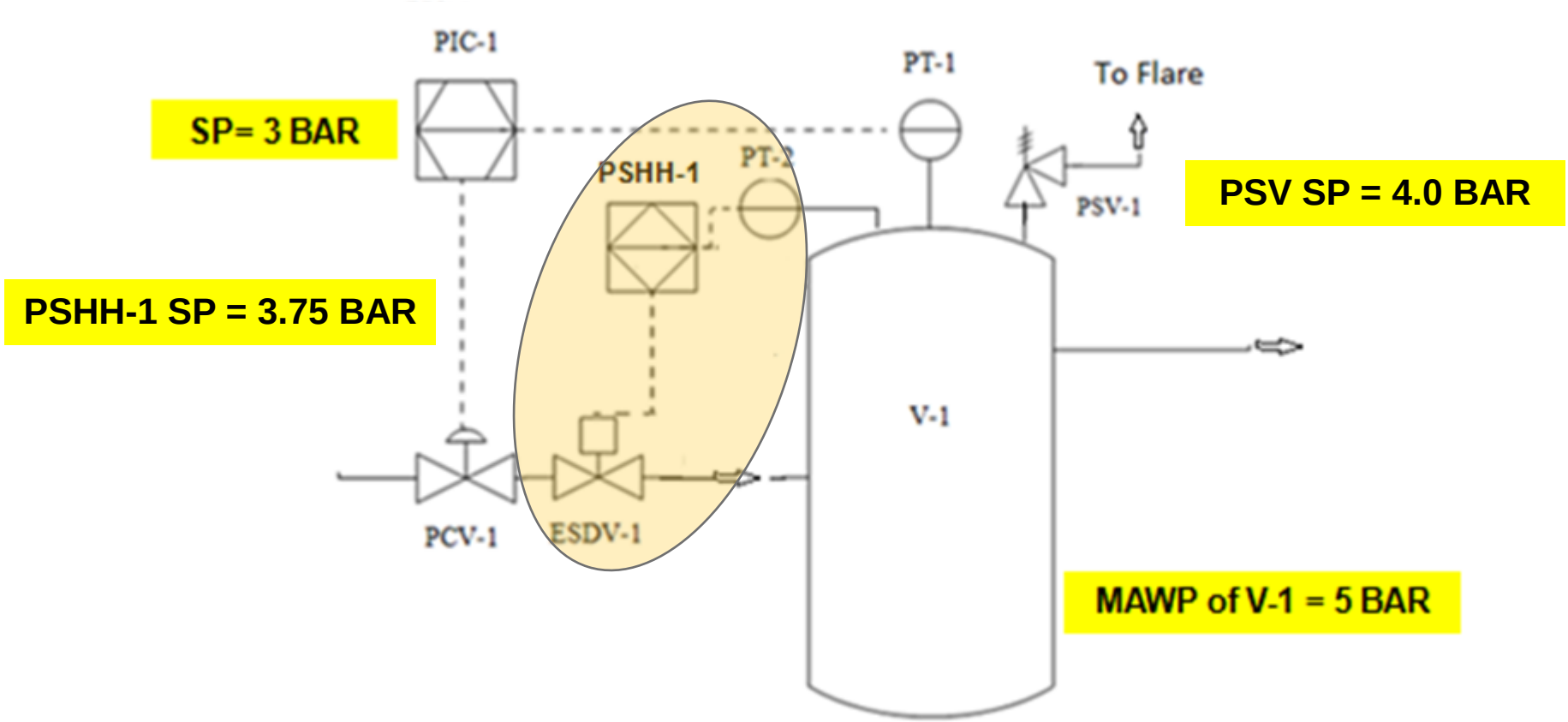
Prasad Goteti
Dec 2017

PARAMETERS THAT DEFINE THE SIL RATING OF A COMMUNICATION PROTOCOL

Honeywell

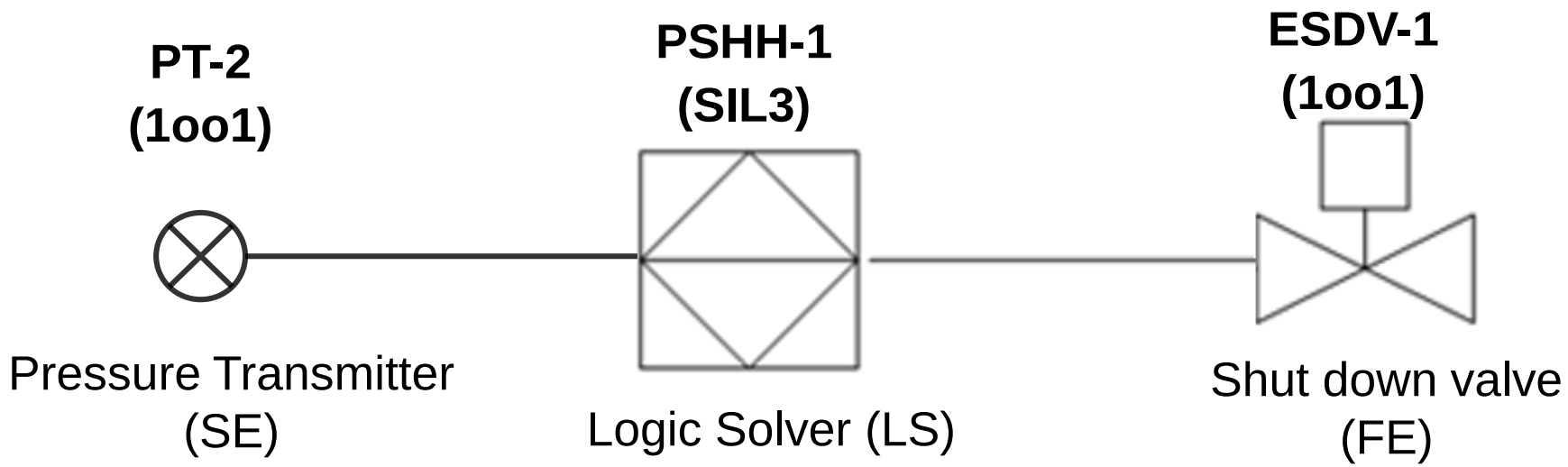
RECAP – by using LOPA technique….we need a SIF



- High Pressure Trip PSHH-1 added (which is SIL2 Reliable, ie 99% Reliable as a minimum)
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

Honeywell
THE POWER OF CONNECTED

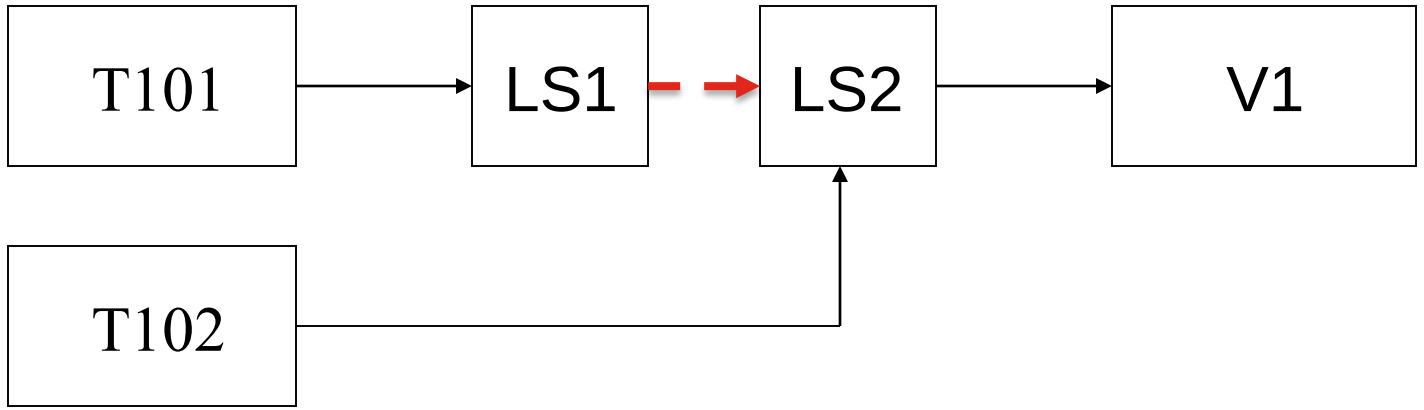
RECAP - Reliability calculations – Safety Function



$PFD_{avg}(SIF\text{-}1) = PFD_{avg}(SE) + PFD_{avg}(LS) + PFD_{avg}(FE)$

Make sure it is SIL2 (at least 99% Reliable)

Application of Secure Data transfer for Safety Systems



LS1 – Accepts and Processes Input T101

- Transfers Processed data to LS2 by data transfer

LS2 – Accepts and Processes Input T102

- Accepts Processed input from LS1 on T101
- Processes the 1oo2 logic for inputs
- Issues Executive action to V1 based on the 1oo2 logic

What is a Communication Protocol ?

- Exchange of information between two devices in a manner that both can interpret, understand and use the information as required

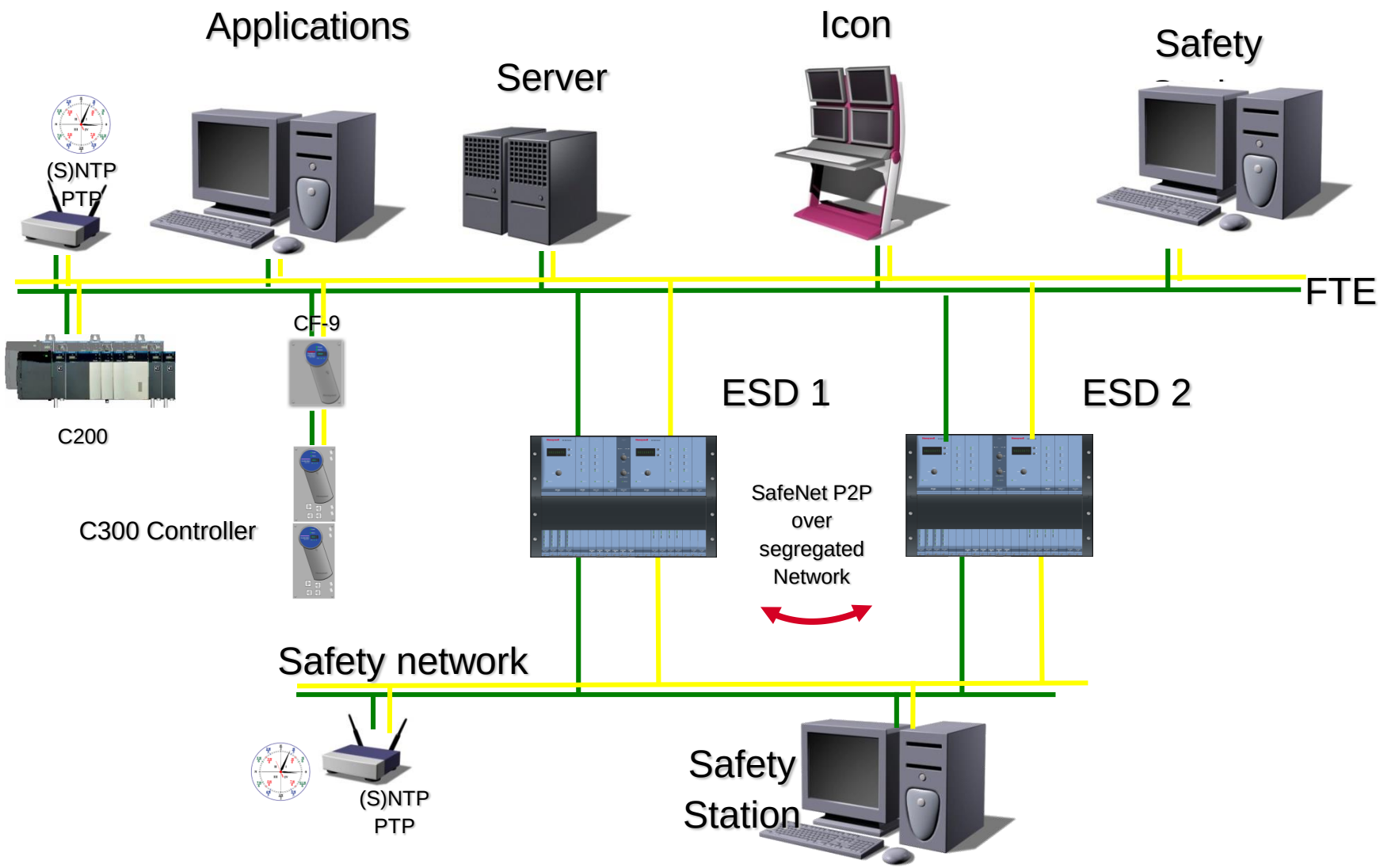
Requirements of Data transfer between two devices

- Data sent by a Transmitting device is received by the intended Receiver
- The Data received by the Receiver is identical to the Data sent by the Transmitter
- If Data gets corrupted during transmission, the Receiver should be able to interpret that the Data is corrupt and implement appropriate action
- Two types of Data transfer :
  - Hard interface – usually “one to one” Analog interface
  - Soft interface – Digital signal interface which is either “one to one” or over a Network

What is Secure Data transmission ?

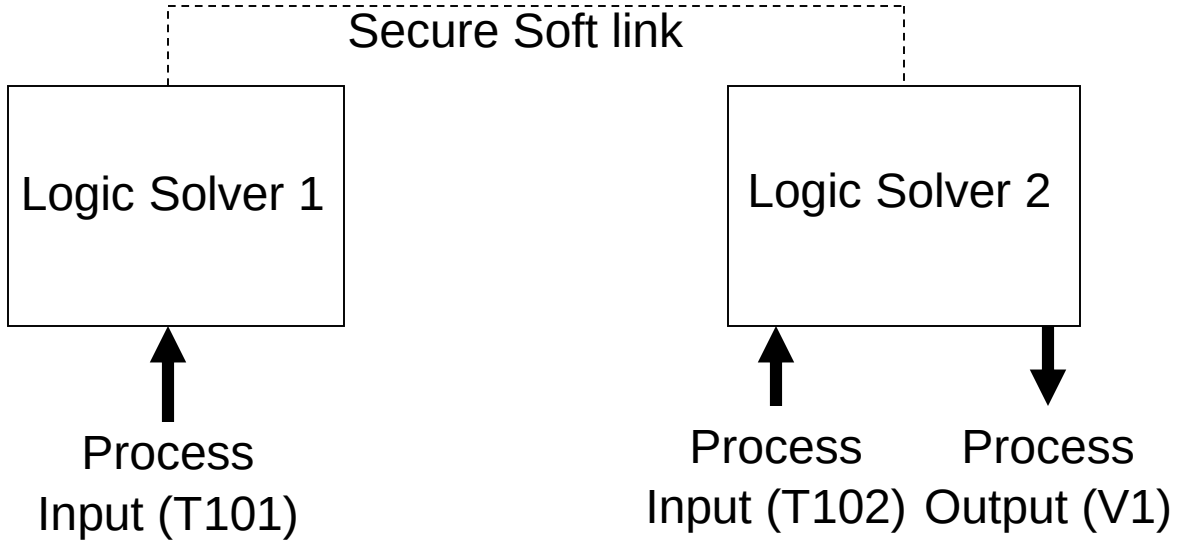
- Referenced for “Soft” Communication between two devices, ie Digital communication.
- Data sent by a Transmitting device is received ONLY by the intended Receiver and interpreted by it.
- The transmission is Reliable

Example - Integrated Control and Safety System architecture

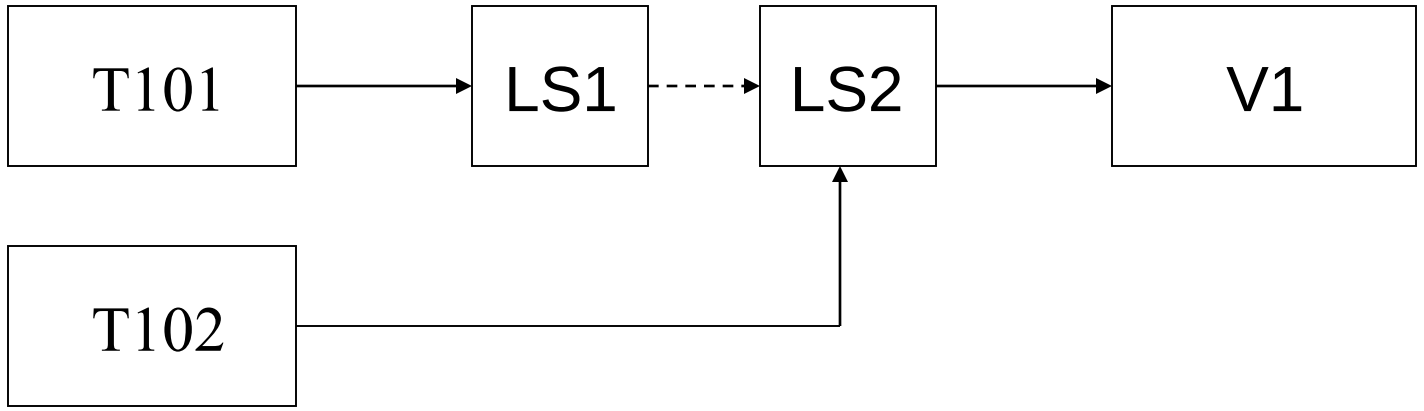


Application of Secure Data transfer for Safety Systems

- A Safety instrumented Function (SIF) is distributed over two Logic Solvers, for example :
  - Consider the following SIF :
    - Sensors T101 and T102 in a 1oo2 configuration
    - T101 is “Hardwired” to Logic Solver LS1
    - T102 is “Hardwired” to Logic Solver LS2
    - “Soft Link” between LS1 and LS2
    - Final Element V1 in a 1oo1 configuration “Hardwired” to LS2



Application of Secure Data transfer for Safety Systems



LS1 – Accepts and Processes Input T101
- Transfers Processed data to LS2

LS2 – Accepts and Processes Input T102
- Accepts Processed input from LS1 on T101
- Processes the 1oo2 logic for inputs
- Issues Executive action to V1 based on the 1oo2 logic

Reliability of the Secure Data Transfer for Safety Systems

- A SIL value may be allocated to the Data transmission based on how Reliably the Data is transferred.
- Two components play a key role :
    1. Hardware involved in the Data transfer should be Reliable to meet the required SIL value
    2. Software protocol, should be Reliable to meet the required SIL value

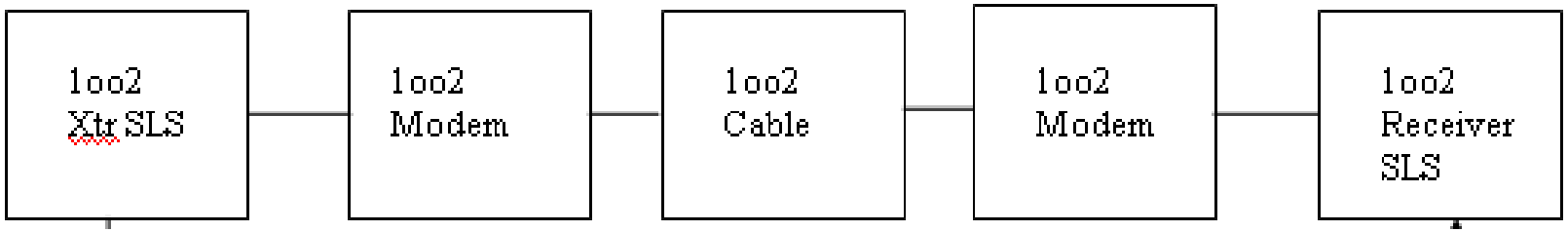
Hardware requirements for Secure data transfer

Assumptions :

- The Hardware components involved in the transmission include the Transmitter (LS1), Receiver (LS2), the transmission medium (Serial cable, CAT5 cable etc), intermediate devices (like a Modem) and connectors
- Data transfer speeds could be critical based on Process Safety Time (PST)
- The Hardware components should be immune to external noise which can corrupt the Data

Hardware configuration for Secure data transfer

Reliability Block Diagram



Software configuration for Secure data transfer

The Communication protocol should :

- Consolidate the data at the Transmitter (LS1) end in a predefined format. This is usually done in “Packets of information”
- Each “Packet of information” should carry the address of the Receiver (LS2) and Data being transmitted to the Receiver (LS2)
- Each packet should have some sort of encryption which helps validate the data when received by the Receiver (LS2)
- The protocol should be designed to take a Fail Safe action in the event the data is not received correctly after a predefined number of attempts

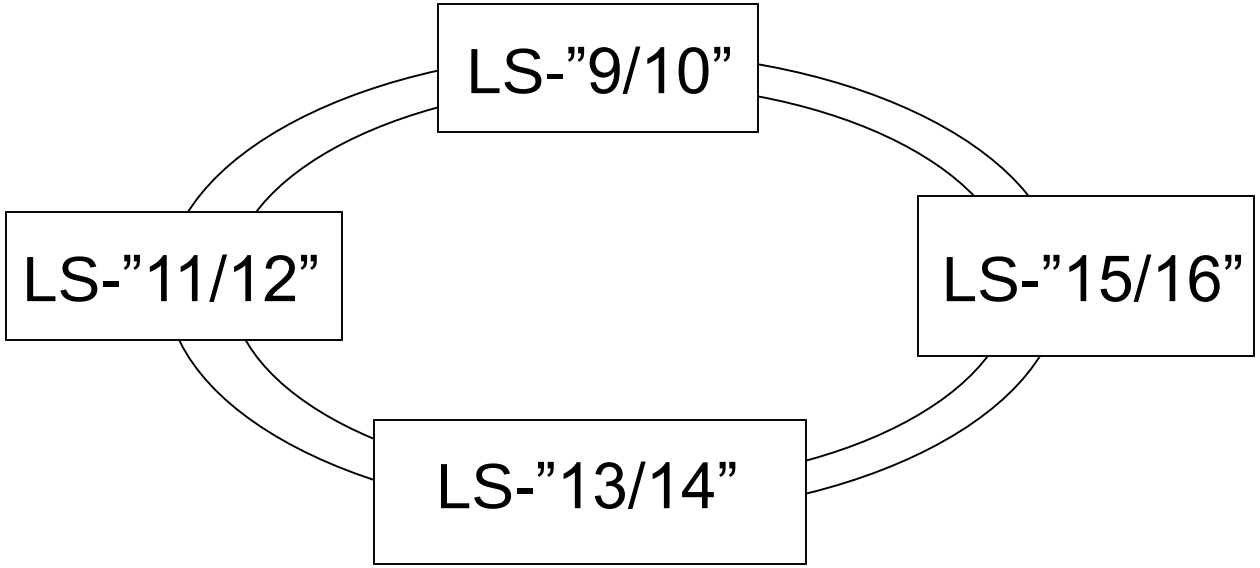
Data consolidation

HEADER		DATA	TRAILER	
Message Start	Address	Data as required	LRC or CRC	Message End

- The Secure data communication protocol may have any format but the following criteria should be met :
  - Data received ONLY by the addressed Logic Solver
  - The Receiving Logic Solver gets the identical data transmitted by the Transmitting Logic Solver
  - In the event the data received is NOT identical, the receiving Logic Solver should take the Process to a Safe State after all attempts to get identical data fail.

Addressing Logic Solvers

Each Logic Solver in ONE network should have a unique address. The Drawing below indicates redundant Logic Solvers on a redundant network.



LRC or CRC

- LRC – Longitudinal Redundancy Check
- CRC – Cyclic Redundancy Check

CRC is more complicated than LRC as it could be based on a polynomial while LRC is a simpler calculation based on addition and subtraction of the Data bits.

Conditions that can go wrong during Data transmission

Following errors may occur during Data transfer :

- The Data transmitted may never be received by the Receiver due to a hardware fault (like Cable open or hardware failure of the Modem etc.)
- The Data is received by the wrong receiver (Addressing problems – hardware and/or software problems)
- The Data is received by the Receiver but is not identical to the message transmitted, due to corruption (detected based on LRC/CRC). This could be due to “Noise” (hardware fault) or Protocol problems (Systematic errors)

Action on Hardware fault

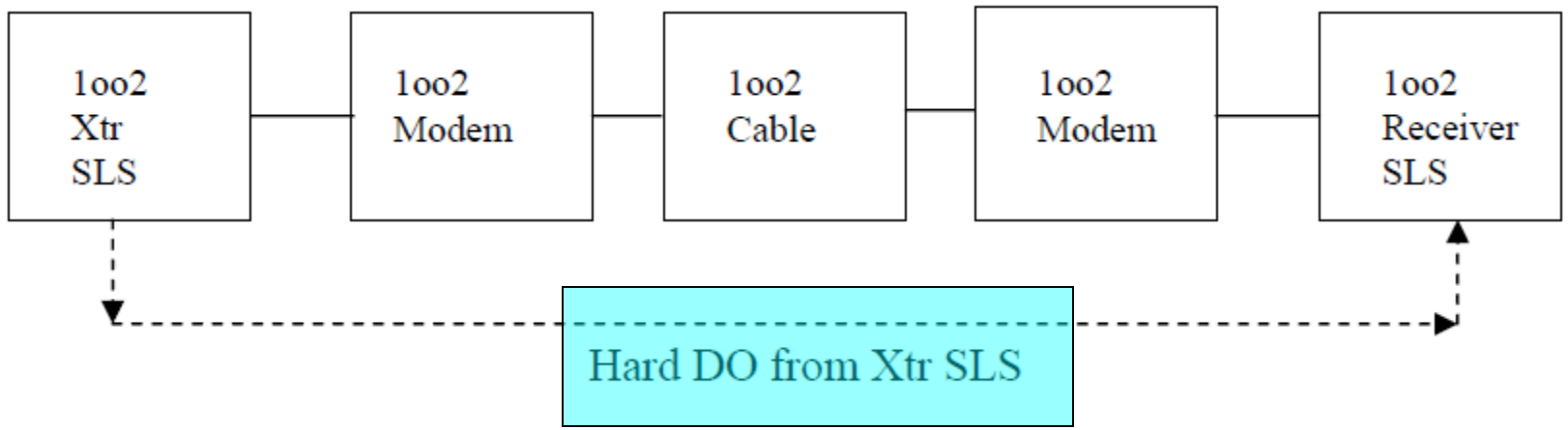
1. The hardware should be designed based on the required Reliability levels. This is done based on failure rates of components involved and providing adequate redundancy to meet the required SIL value

2. Because of a hardware fault, if the Transmitter (LS1) does not receive an acknowledgement from the Receiver (LS2) during a pre-determined time

    - EXECUTIVE ACTION - The transmitting Logic Solver sends a Hard DO which initiates a Safe Process shutdown by the Receiving Logic Solver.

Hardware configuration for Secure data transfer

Reliability Block Diagram



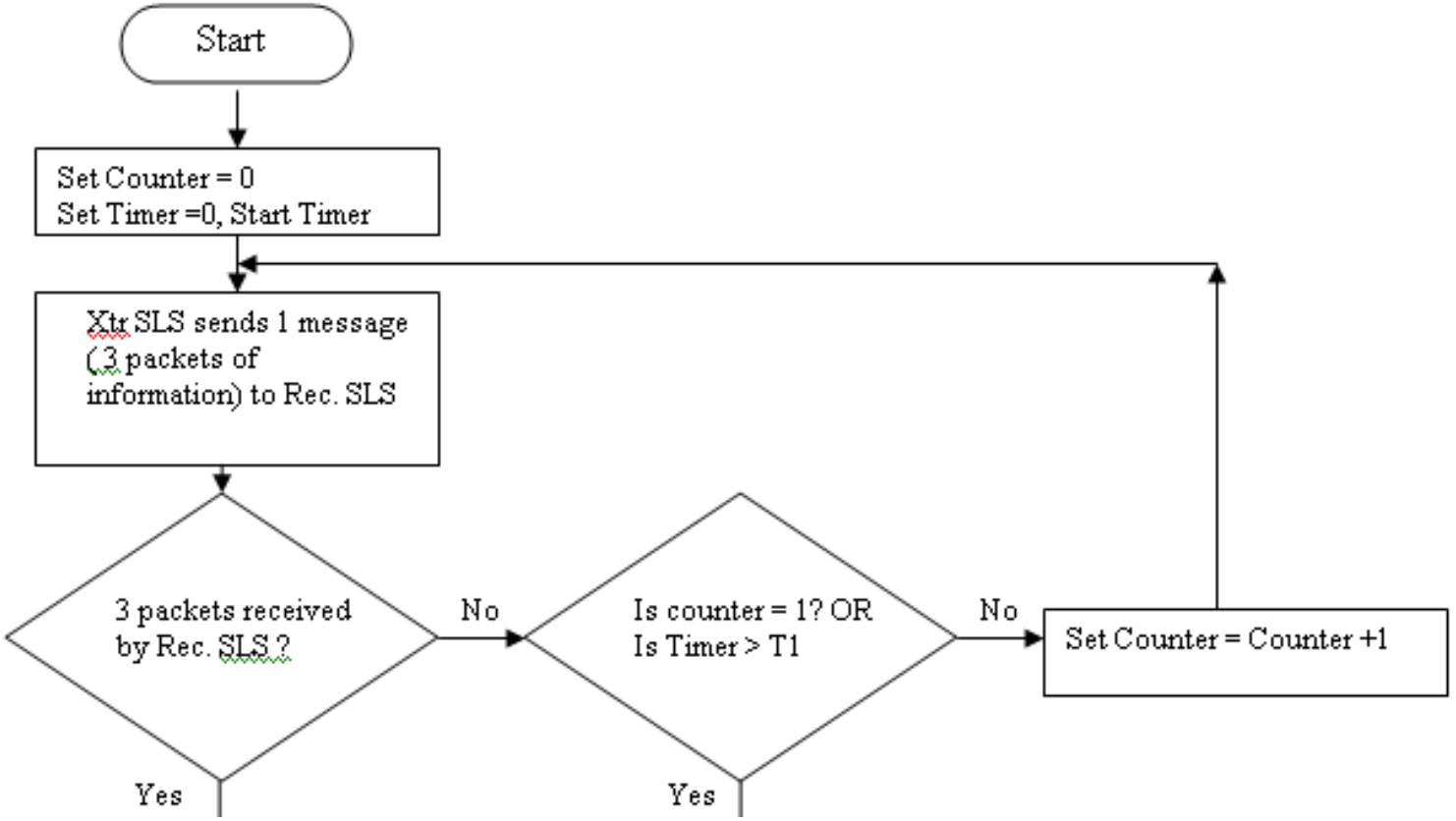
Action on Software fault

1. If the Transmitting Logic Solver does not receive an acknowledgement from the Receiving Logic Solver it means the Data has not reached the Receiving Logic Solver at all (addressing problems)
   - EXECUTIVE ACTION - The transmitting Logic Solver sends a Hard DO which initiates a Safe Process shutdown by the Receiving Logic Solver

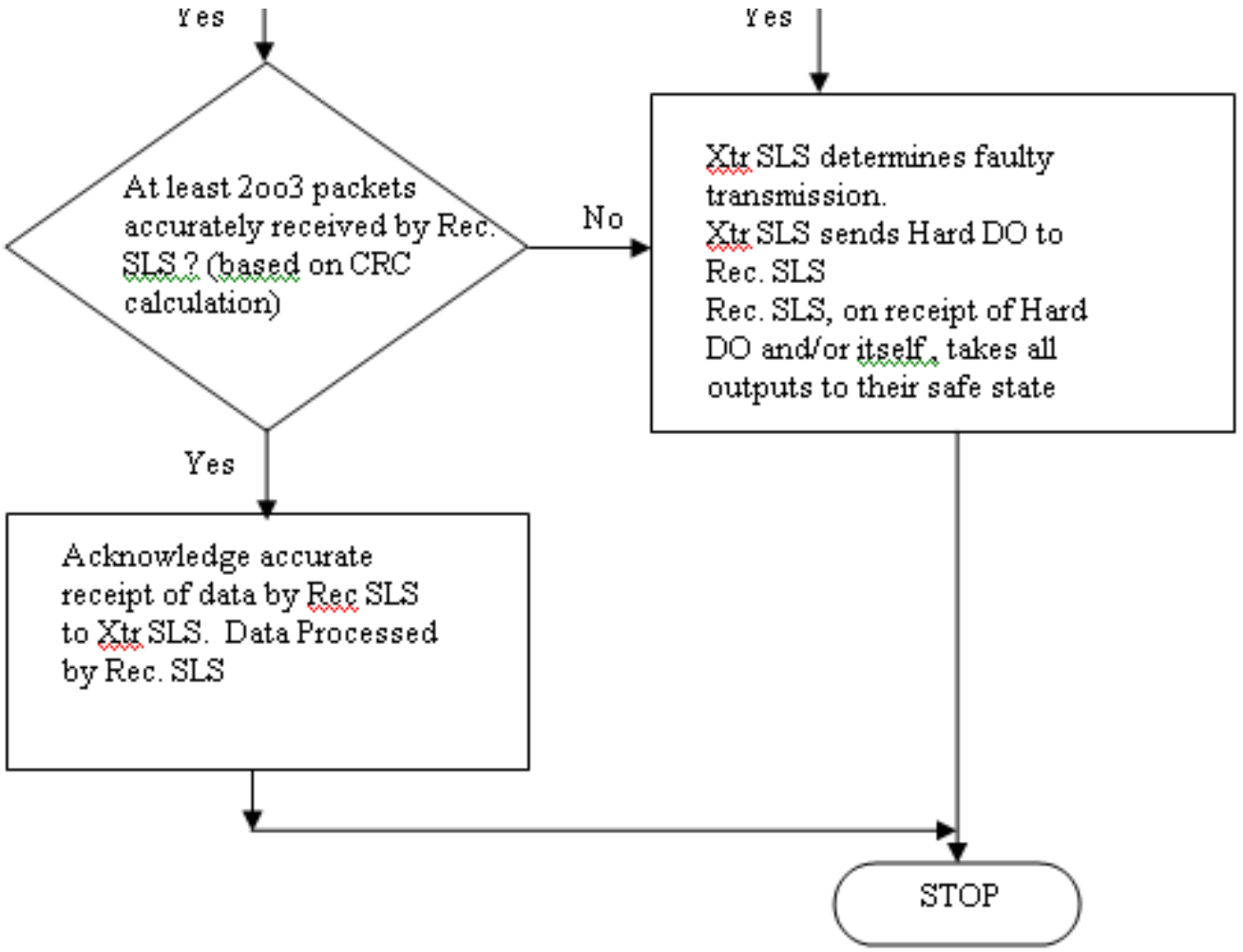
2. If the Receiving Logic Solver acknowledges receipt of data but is corrupted, then either external noise has corrupted the data or there is a systematic error in the protocol which needs to be rectified. After three such attempts (as an example) if there is no resolution :
   - EXECUTIVE ACTION - The transmitting Logic Solver sends a Hard DO which initiates a Safe Process shutdown by the Receiving Logic Solver AND the receiving Logic Solver will itself initiate a Safe Process shutdown

Honeywell
THE POWER OF CONNECTED

Secure Data transfer in flowchart format

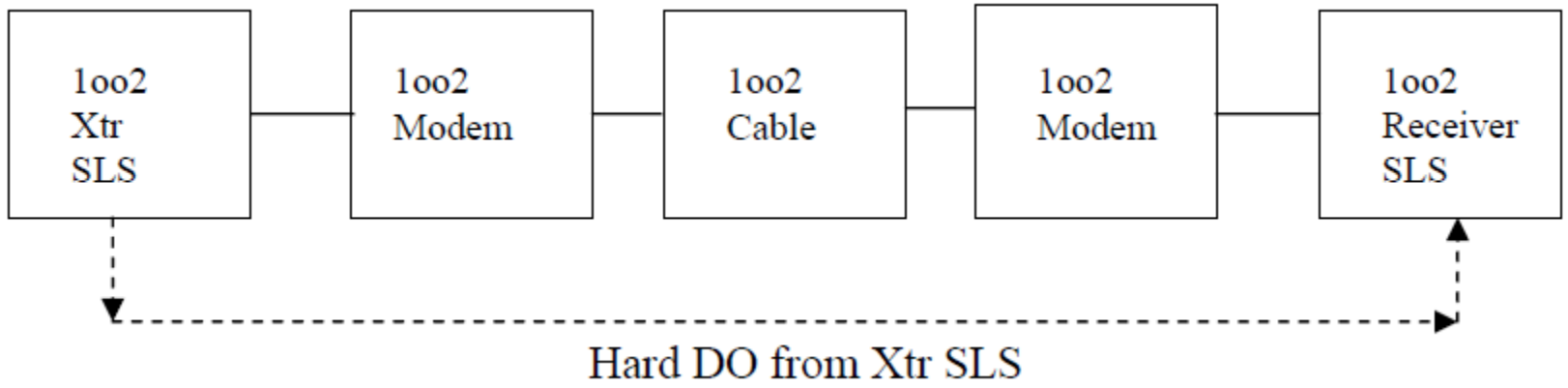


Secure Data transfer in flowchart format



Assign Reliability numbers to the Secure Data communication

Hardware :

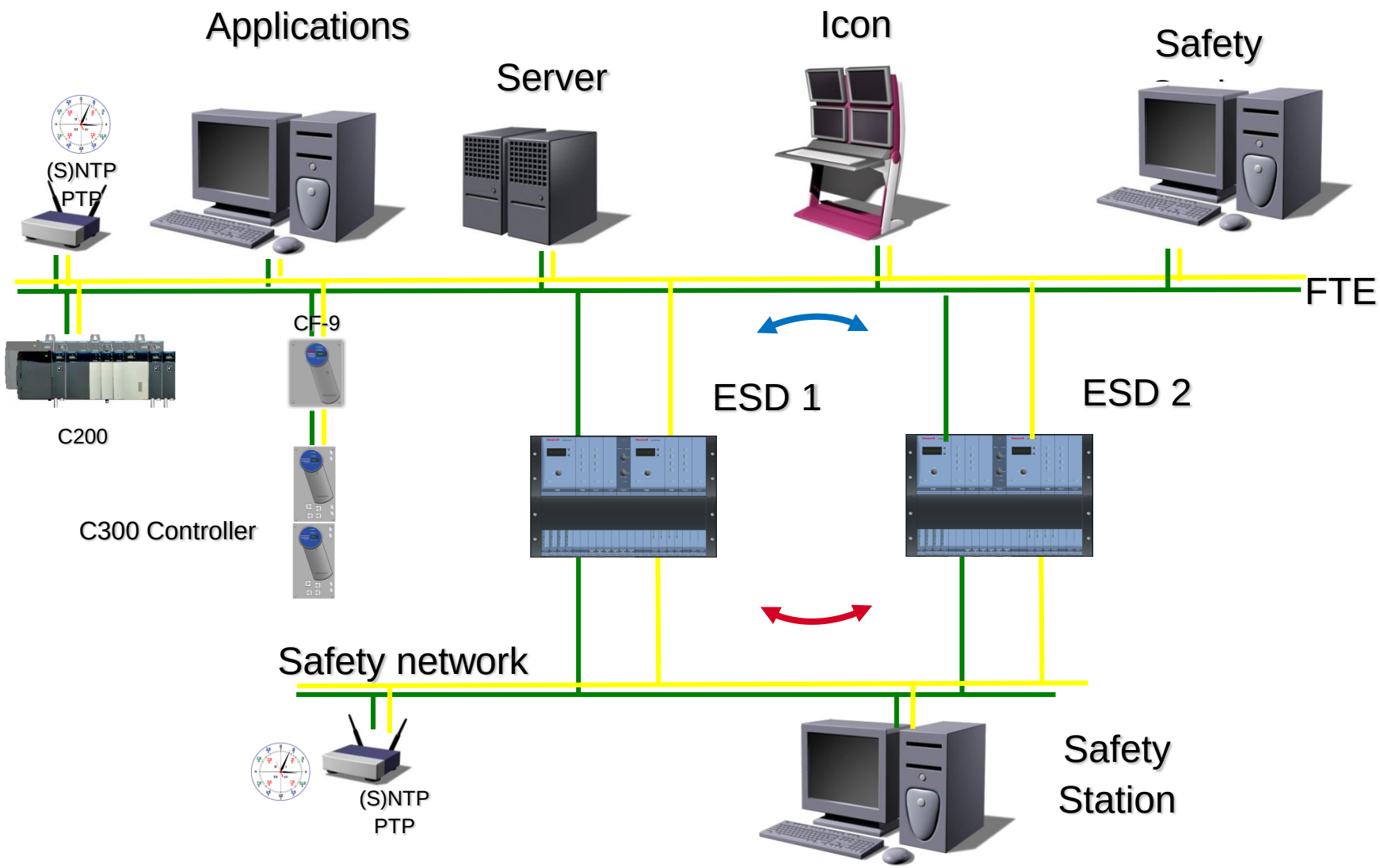


In the event the Receiver Logic Solver does not receive or acknowledge the received Data, the Transmitting Logic Solver sends a Hard DO which initiates a Safe shutdown by the Receiver Logic Solver

This implies, the Reliability value is **independent of the Transmitting medium**

By using SIL3 Logic Solvers, the Hardware Reliability for Secure Data transfer will always be SIL3 !

Example - Integrated Control and Safety System architecture



Assign Reliability numbers to the Secure Data communication

Software :

- Test the Secure Data transfer protocol for accuracy numerous number of times. If the criteria for successful Secure Data transfer statistically meets 1950 out of 2000 attempts (PFD=0.025, RRF = 40), it could be assigned SIL 1
- Other modeling based methods are also available

Conclusion

To qualify for a SIL rating, the Secure Data transmission should meet the following requirements:

- The Data being transferred is received ONLY by the Receiver the message is intended for
- The Data transfer occurs accurately with high integrity (Reliability)
- If the Data gets corrupt after being transmitted because of any noise or random hardware failure of the transmission medium, the Receiver should be able to interpret that the Data being received is corrupt and should implement a Fail Safe scenario