Realizing Greater System Robustness Through Combining CIP Safety and CIP Security

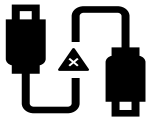
Industrial Communications

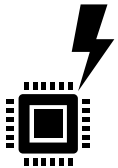
- Basic functional requirements:
    1. Quick connect/disconnect of devices
    2. Simple integration of new devices
    3. Easy configuration and communication between devices
    4. Diagnostic data
    5. Simple IT – OT integration

- Extra requirements for Functional Safety:
    1. Messages delivered as intended in a timely manner, or an expected action will be taken (e.g. the device goes to the safe state)
    2. Suitably small quantitative risk (residual error) that a corrupted message will not be detected and therefore the device will not go to the safe state

- Extra requirements for Security:
    1. If messages are not delivered as sent, prevent the message from affecting operations
    2. Provide logging and alarming to alert operators to the potential thread
    3. Confidentiality: ensuring that intellectual property is protected

Known Challenges With Industrial Ethernet

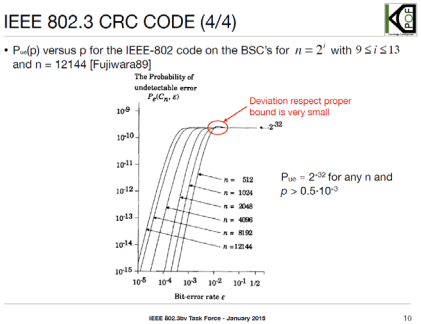


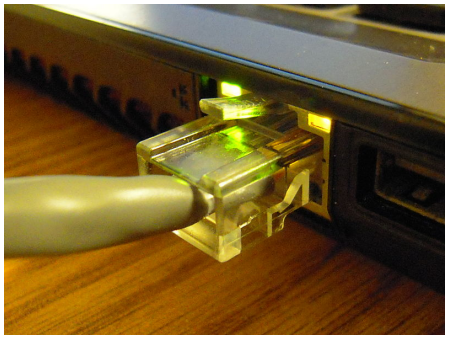


Risk	Consequence
– Electrical noise – Cable breaks & aging	– Loss – Repetition – Corruption – Delay
– Hardware failures – Software bugs	– Incorrect message routing – Coupling with other packets – Mixing with other packets
– Security threats	– Loss of production – Damage – Compromised Intellectual Property

Data Integrity Protection – Ethernet CRC

- Ethernet packets have a CRC that is 32 bits long
- Primary function is detecting corrupted data
- Network components will discard frames in the event of an error
- What is the chance that an error is not detected?
  - Applying the birthday paradox, collisions are likely to occur approx. every $2^{\frac{32}{2}} = 2^{16} = 65536$ messages
  - Note this assumption is likely overly conservative
- Even though the space is small this will still catch many possible errors
- Note that assumptions are likely overly conservative: even if a collision occurs after about 65,000 messages, the collision must also be coincident with some kind of environmental error (e.g. EMC noise)





Error Detection Requirements for Functional Safety

IEC 61784-3 defines errors that must be mitigated for functional safety communications and possible corresponding remedial measures

Communication errors:

1. Corruption
2. Unintended Repetition
3. Incorrect Sequence
4. Loss
5. Unacceptable Delay
6. Insertion
7. Masquerade
8. Addressing

- Not necessarily one-on-one mapping
- One measure can cover several errors
- Not all listed measures are required
- Each error covered by at least one measure

- Addressed by safety measures:
- Sequence number
- Time stamp
- Time expectation
- Connection authentication
- Feedback message
- Data integrity assurance
- Redundancy with cross checking
- Different data integrity assurance systems

Binary Symmetric Channel (BSC) disturbance or background noise - modelled with Bit Error Probability of $P_e = 0.01$

How Do Safety Protocols Mitigate These Risks?

White Channel vs Black Channel

- IEC 61508-2 7.4.11.2 describes two possible approaches for safety communications
  - White channel (entire network must be developed according to 61508 and certified)
  - Black channel (only safety network protocol subject to certification)

	Advantages	Disadvantages
White Channel	• All components certified	• Additional development cost and complexity • May not be feasible to account for all potential errors and communication technologies
Black Channel	• Architectural flexibility • Broader choice of network components • Simpler deployment of other features	• Requires a conservative approach to error modelling

- IEC 61784-3 extends IEC 61158 fieldbus specifications to Functional Safety Communication Profiles (FSCP)
  - All defined 61784-3 FSCPs use the black channel approach
- Safety protocols make use of various diverse CRC polynomials (distinct from that used for ethernet)

How Does CIP Security Mitigate Against Threats?

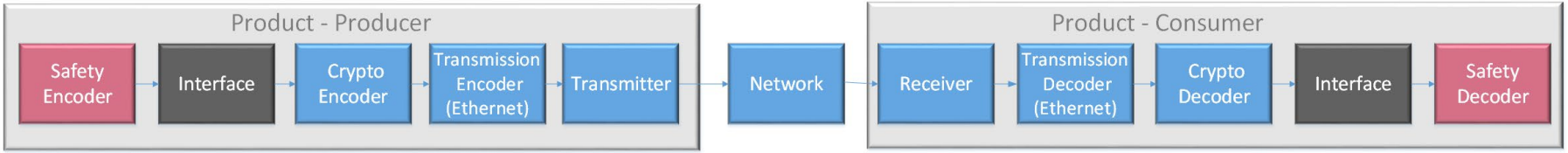
Security Property	Common Technology
Device Identity	X.509 Digital Certificates are used to provide cryptographically secure identities to devices
Device Authentication	TLS/DTLS cryptographic handshake provides authentication via the certificate verification and challenge.
Data Integrity	Hashes or HMAC (keyed-Hash Message Authentication Code) as a cryptographic method of providing data integrity and message authenticity; the HMAC relies on a secret symmetric key to generate and/or verify. In TLS/DTLS this key is derived as part of the handshake.
Data Confidentiality	Data encryption as a means of encoding messages or information in such a way as to help prevent reading or viewing of data by unauthorized parties; this generally involves a symmetric key applying an algorithm like AES to the data. Similar to the HMAC key, this key is generally derived as part of the handshake in TLS and DTLS.

Data Integrity Protection – Cryptographic Hashing

- For CIP Security using TLS and DTLS the cryptographic hash is applied to data at the transport layer
- Commonly used one is SHA-256
  - As the name implies, hash space is 256 bits
- Birthday attack: $2^{\frac{256}{2}} = 2^{128} \approx 3.402 \times 10^{38}$
- This is a *big* number; it would be hard to cover this space in our lifetime
  - As an example, a system sends a 1,000 messages every microsecond, that is 3.1536×10^{18} messages in 100 years
- If you'd like to be even more conservative, take SHA-512: $2^{\frac{512}{2}} = 2^{256} \approx 1.157 \times 10^{77}$ this is getting close to some estimates about the number of atoms in the universe (10^{77} to 10^{82})
- Also note, this is the probability that *any* two hashes collide
  - Probability that a hash collision is also coincident with a data error is *much* smaller, but even the probability of any collision is already extremely small

Conclusion: we can safely ignore the theoretical probability of a (properly working) cryptographic hash failing to detect a bit error

System View



Trend in Safety: Detect Events Causing “Heavy Corruption”

- Recognition that BSC disturbance alone may not provide sufficient error detection capability
  - Bit stuffing/destuffing
  - Bit slipping
  - Symbol coding/decoding
  - Block coding/decoding
  - Compression/Decompression
  - Encryption/Decryption
  - Error correction
  - Buffer overwritten
  - EMI
  - ...

Can lead to heavily corrupted SPDU error pattern which cannot be covered by the Binary Symmetric Channel (BSC) with P_e=0.01

Uniformly Distributed Segment (UDS) Errors could conservatively be modelled with a Bit Error Probability of P_e = 0.5 but is not representative of real world.

What is the Value to Use?

- **p=0.000** Increasing Functional Safety System Reliability by Adding Communication Security
- **p=0.001** Increasing FunctionaL Safety System Reliability by`Adding Communication Security
- **p=0.010** inãreasing Functional Safety System RelhabIlity bx Adding Communica|io. Secubity
- **p=0.500** ÷Q½Xé♀×#aö☼Yë♫►♦û<ÕÖî«rS¶Ú♥§Q¥×¹]ßÀ£O☻^i⌂Q▼@e+T©7cÕ‼gmKXôÿàÆACÜ◄}Ù;¸~ã·°§

If the bit error probability is 50% then the data is unusable

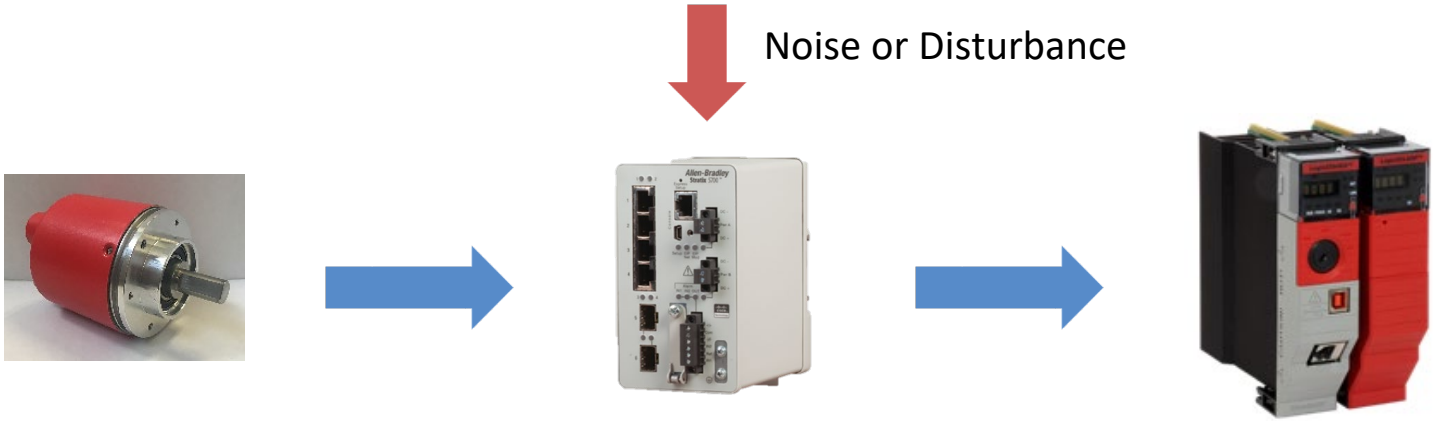
Mathematics Versus the Real World

Real World Evidence

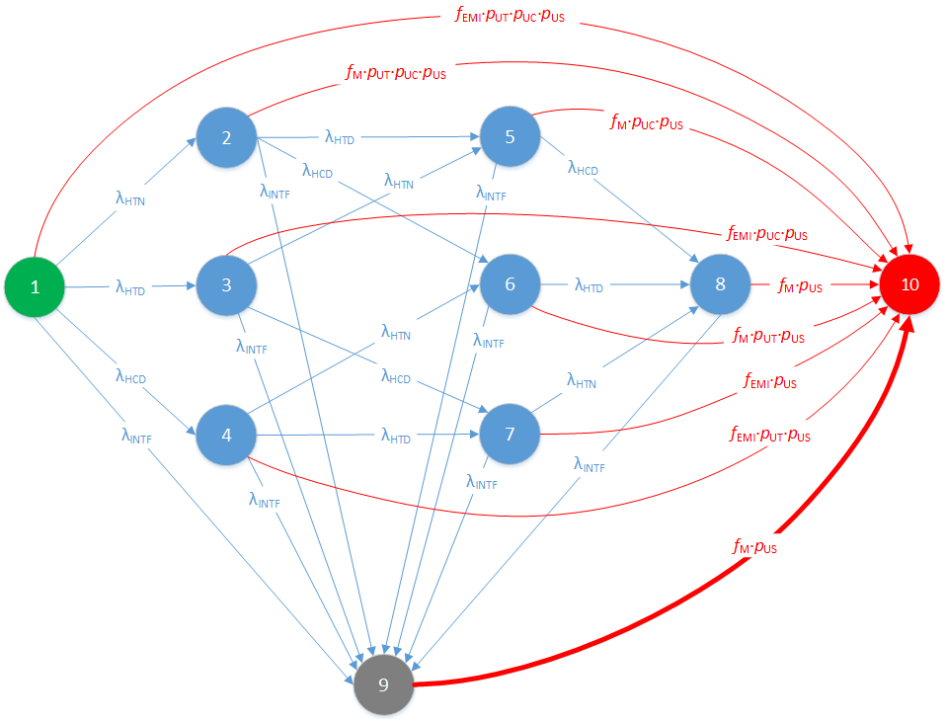
- Assuming a safety system goes into a safe state if an error is detected, a P_e value of 0.5 would imply a noticeably high rate of trips owing to errors in the installed base of safety systems
- Would imply that safety systems are unusable with an unacceptable level of availability
- No empirical evidence that safety systems are experiencing an unusually high level of safe state transition
- What is really happening?
  - Something other than the safety communication layer is addressing the problem to some degree
  - The P_e value assumption of 0.5 is too high (without considering additional factors to reduce effective failure rate)

Discrepancy between the mathematical assumption and real-world evidence

System View

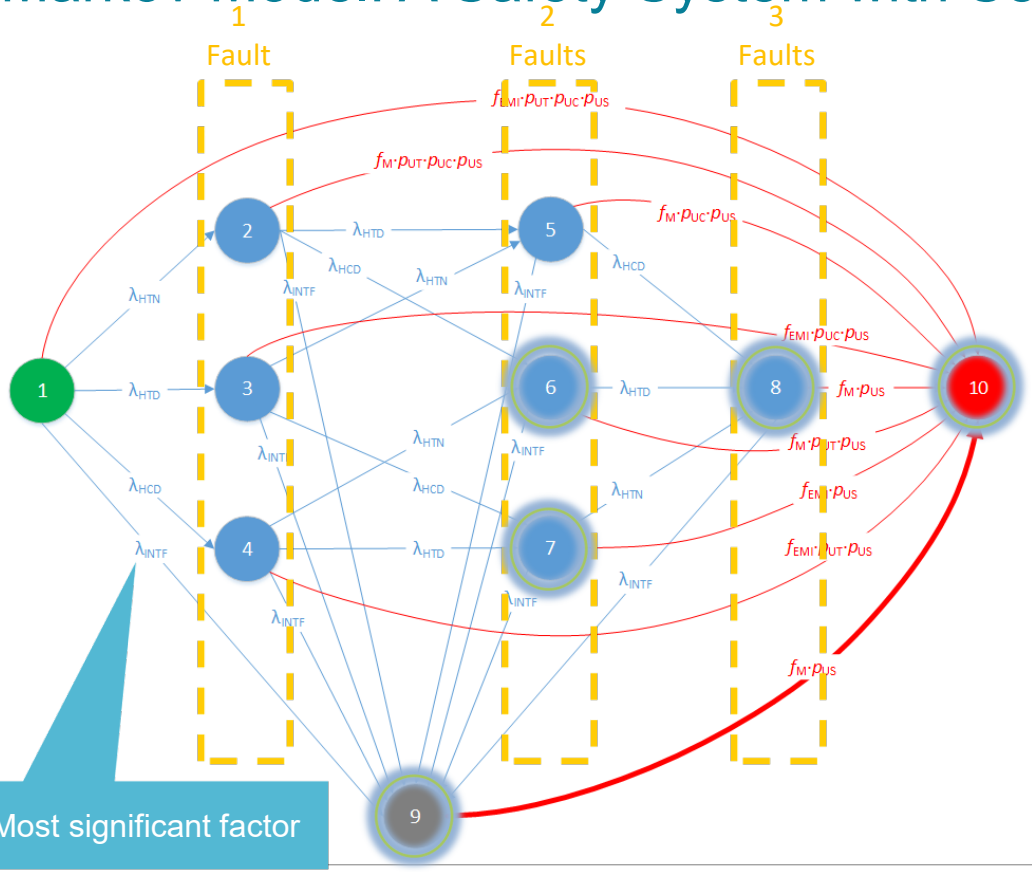


Markov Model: A Safety System with Security



State	State Description
1	The transmission system is operational without faults. Transmissions occur under the potential of EMI disturbances or soft errors.
2	State of the transmission system when random HW fault(s) have occurred within either the transmitting device, the transmission media, network components, the receiver in the target device, or any combination thereof.
3	State of the transmission system when random HW fault(s) have occurred ONLY within the transmission decoder of a target device, such that it cannot perform its normal function, but itself does not inject faults into the message. An example of this state would be when the transmission decoder is fully bypassed.
4	State of the transmission system when random HW fault(s) have occurred ONLY within the cryptographic decoder of a target device, such that it cannot perform its normal function, but itself does not inject faults into the message. An example of this state would be when the cryptographic decoder is fully bypassed.
5	State of the transmission system when random HW fault(s) have occurred within either the transmitting device, the transmission media, network components, the receiver in the target device, or any combination thereof, AND random HW fault(s) have occurred within the transmission decoder such that it cannot perform its normal function.

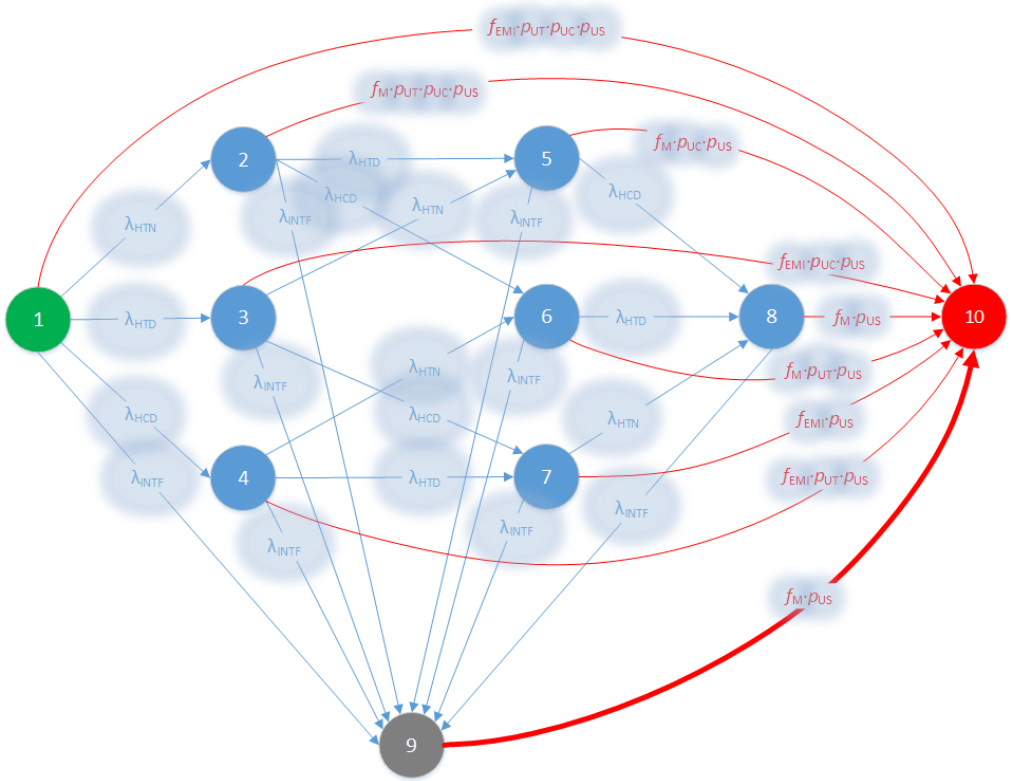
Markov Model: A Safety System with Security



Most significant factor

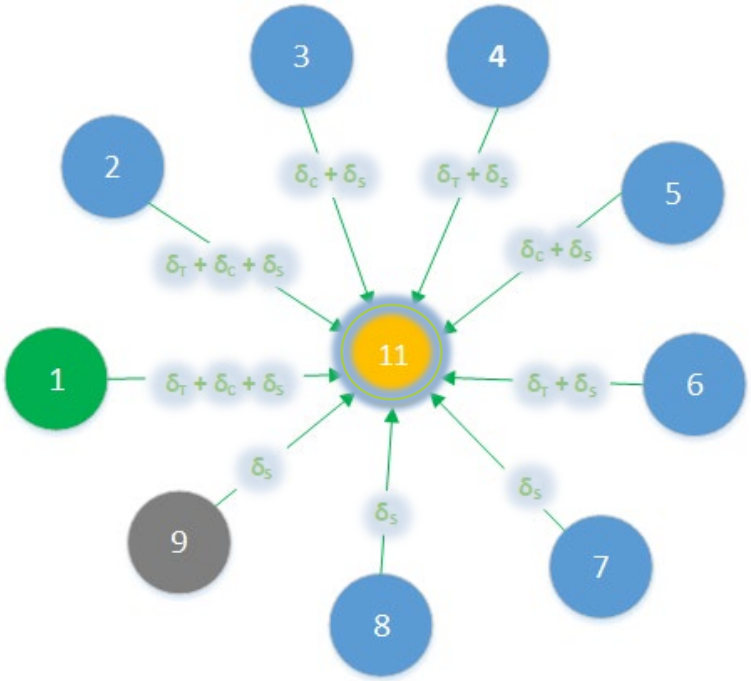
State	State Description
6	State of the transmission system when random HW fault(s) have occurred within either the transmitting device, the transmission media, network components, the receiver in the target device, or any combination thereof, AND random HW fault(s) have occurred within the cryptographic decoder such that it cannot perform its normal function.
7	State of the transmission system when random HW fault(s) have occurred within both the transmission decoder AND the cryptographic decoder such that neither of them cannot perform their normal function. In this state, EMI is the only mechanism modelled to cause a corrupted message.
8	State of the transmission system when random HW fault(s) have occurred within both the 1) transmission decoder AND 2) the cryptographic decoder such that neither of them cannot perform their normal function, AND 3) within either the transmitting device, transmission media, network components, the receiver of the target device, or any combination thereof. This state represents the condition when only the safety decoder is the only decoder functional, and an error has corrupted the message somewhere during transmission.
9	State of the transmission system when random HW fault(s) have occurred within the interface blocks between the cryptographic decoder and the safety blocks at either the encoder or decoder. In this state the transmission and cryptographic decoder offer no detection capability for these errors. The safety decoder is the last and only line of defense once this state is reached.
10	State of the transmission system when a safety hazard is present and not detectable.

Markov Model: A Safety System with Security



Symbol	The meaning of a Symbol
λ_{HTN}	Random HW failure rate of a transmitting device, transmission media, network components, and the receiver of a target device. This includes soft errors, such as from high energy, atmospheric particles.
λ_{HTD}	Random HW failure rate of a transmission decoder within a target device. This represents random hardware-based failures of the decoder such that it cannot perform its function, but not injection of faults into a message. This also includes soft errors resulting in bit flips, such as from high energy, atmospheric particles.
λ_{HCD}	Random HW failure rate of a cryptographic decoder within a product. This represents random hardware-based failures of the decoder such that it cannot perform its function, but not the injection of faults into a message. This also includes soft errors resulting in bit flips, such as from high energy, atmospheric particles.
λ_{INTF}	Random HW failure rate within the interface between the cryptographic decoder and the safety decoder. This could represent a serial channel or a simple memory interface. This also includes soft errors resulting in bit flips, such as from high energy atmospheric particles.
f_{EMI}	Mean frequency of corrupted messages caused by EMI.
f_M	Mean frequency of messages generated by a transmitter.
p_{UT}	Probability of the transmission decoder not detecting an error.
p_{UC}	Probability of the cryptographic decoder not detecting an error.
p_{US}	Probability of the safety decoder not detecting an error.

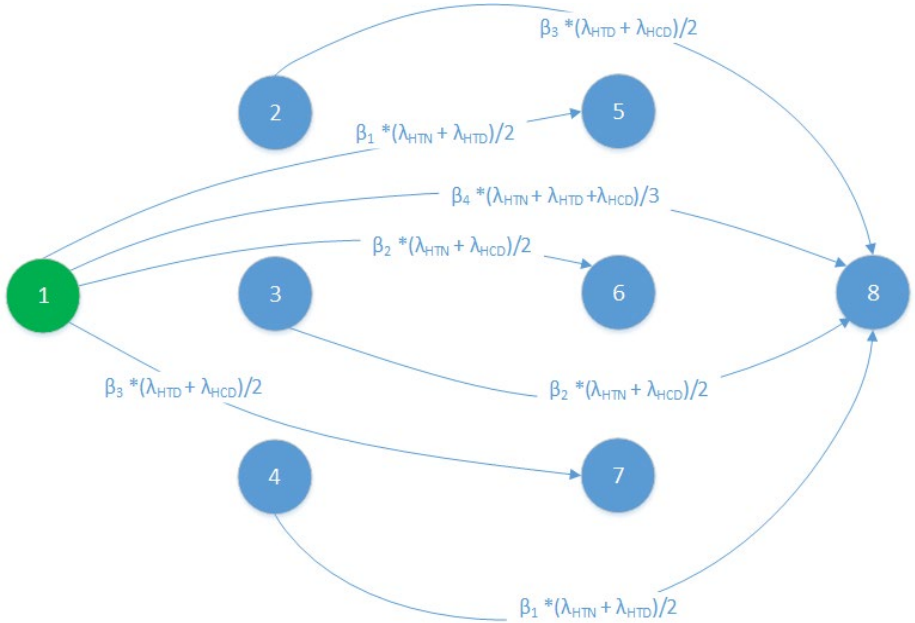
Markov Model: A Safety System with Security



State	State Description
11	State of the transmission system when a fault has been detected and controlled by either the transmission decoder, cryptographic decoder, or safety decoder such that a safety state is entered.

Symbol	The meaning of a Symbol
δ_T	Fault detection rate from the transmission decoder.
δ_C	Fault detection rate from the cryptographic decoder.
δ_S	Fault detection rate from the safety decoder.

Markov Model: A Safety System with Security



Symbol	The meaning of a Symbol
β_1	Common Cause Factor of λ_{HTD} occurring at the same time as λ_{HTN}.
β_2	Common Cause Factor of λ_{HTC} occurring at the same time as λ_{HTN}.
β_3	Common Cause Factor of λ_{HTD} occurring at the same time as λ_{HTC}.
β_4	Common Cause Factor of λ_{HTD}, λ_{HTC}, and λ_{HTN} all occurring at the same time.

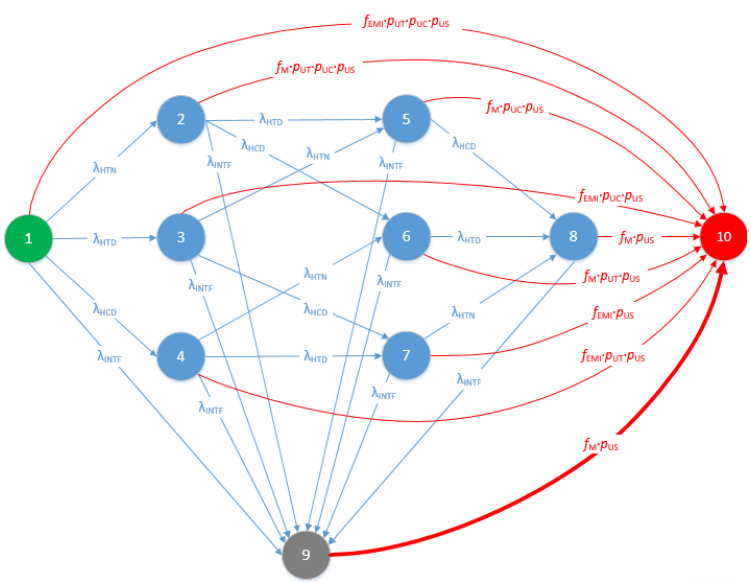
This is shown for completeness – but, impact is statistically insignificant

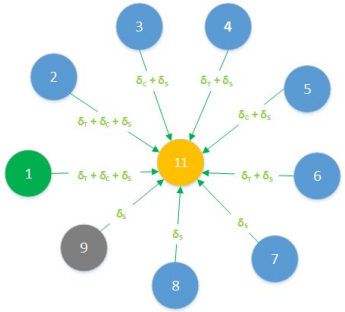
Summary

- The number of States of Markov Model is related to combinations of λ_{HTN}, λ_{HTD}, λ_{HCD}, λ_{INTF}
  - 2^4 = 16 states, plus two additional states for the Hazard and Safe state
  - However, since Ethernet and Security checkers cannot detect λ_{INTF} faults, the number of states can be collapsed down to 11 states

- As the number of checkers increases in the black channel, the probability of undetected failures as seen by Safety Communication Layer gets smaller
  - Not in accordance with IEC 61508, but as a lower effective bit error rate when modelling the black channel
  - More states means there are more multiplicative factors to reduce the overall undetected failure rate in the black channel
  - Adding security helps in a positive and significant way due to the strong coverage provided

- Mathematically, according to the Markov model the biggest impact on the probability of undetected failures comes from the interface $\boldsymbol{\lambda_{INTF}}$ term.
  - Since Ethernet and Security checkers cannot detect these type of faults, the safety check is the last and only line of defense





Conclusions

- Although non-safety rated fault detection mechanisms in the black channel cannot be used formally to provide diagnostic coverage of a safety function per IEC 61508, adding a security layer to a safety system results in a lower effective bit error rate as seen by the safety communication layer

- The most significant factor affecting the reliability of a system is the interface (λ_{INTF}) between the safety and security layers
  - However, this interface forms part of a certified product (IEC61508, IEC62443 or both)
  - Systematic errors can be minimised owing to the processes defined in these standards
  - Failure rate can be managed and controlled

- Data security is a necessary function in Safety systems to prevent attackers from compromising the safety system

- In applications where security and safety are deployed together there is an opportunity to increase the reliability (and availability) of systems without adding additional capabilities to the safety layer

- Encourage the development of safety standards that consider the presence of security features as a way for modelling error probabilities, and the means for delivering safe and secure solutions

References

[1] K. Rastocny, M. Franekova, “Modelling in development of safety-related communication systems”, in Communications - Scientific Letters of the University of Zilina, vol. 10, no. 1, p. 24-30, 2008.

[2] M. Franekova, K. Rastocny, “Safety evaluation of fail-safe fieldbus in safety related control system”, in *Journal of Electrical Engineering*, vol. 61, no. 6, p. 350-356, 2010.

[3] M. Franekova, P. Luley, T. Ondrasina, “Modelling of Failures Effect of Open Transmission System for Safety Critical Applications with the Intention of Safety”, in *Elektronika IR Elektrotechnika, ISSN 1392-1215*, vol. 20, no. 1, 2014.

[4] M. Bellare, T. Kohno, “Hash Function Balance and Its Impact on Birthday Attacks”, in Cachin C., Camenisch J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_24

2022 ODVA

INDUSTRY CONFERENCE AND 21ST ANNUAL MEETING