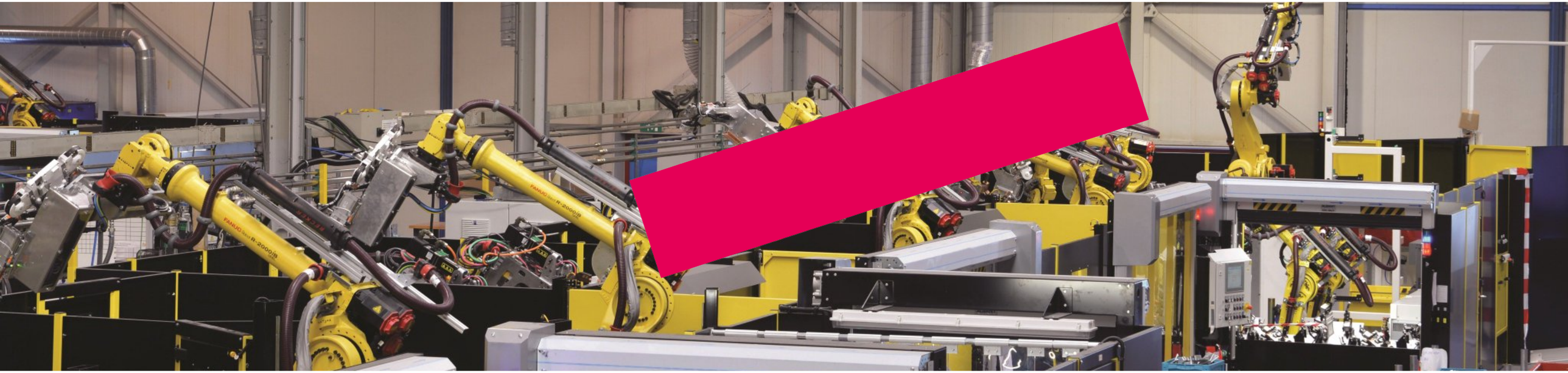
Connected Factories/IIoT lecture 5/6: Safety



Associate Degree Smart Industry / Technische Bedrijfskunde
Faculty of Engineering and Automotive

johan.korten@han.nl

V1.2 May 23, 2022

HAN_UNIVERSITY
OF APPLIED SCIENCES

Schedule

	Theme	
Lecture 1	Introduction	
Lecture 2	Network connections	
Lecture 3	Network protocols	
Lecture 4	Interconnections	
Lecture 5	**Today: Safety**	
Lecture 6	Security	
Assessment		

Functional Safety

Brief definition:

Protection of people an assets from hazards caused by incorrect functioning of a system.

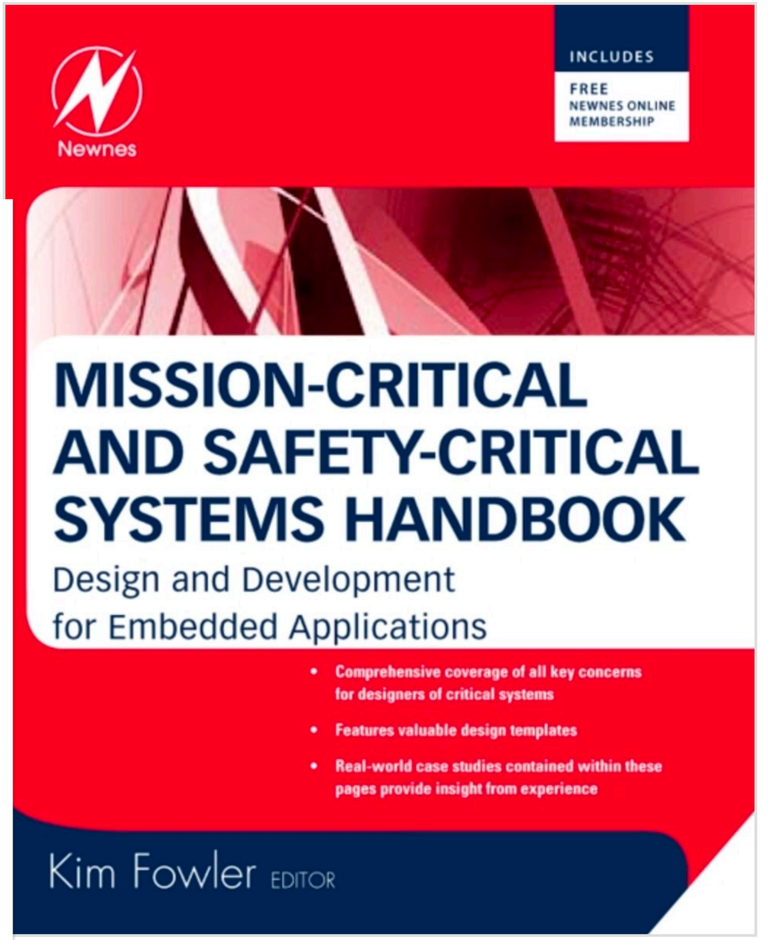
Full definition:

Functional safety is a part of overall safety, responsible for correct operation of system or equipment in response to input changes including safety management taking into account the possibility of human error and/or system/equipment or hardware failure and environmental changes.

Protection: halting system and putting it in to a predicable *safe state*.

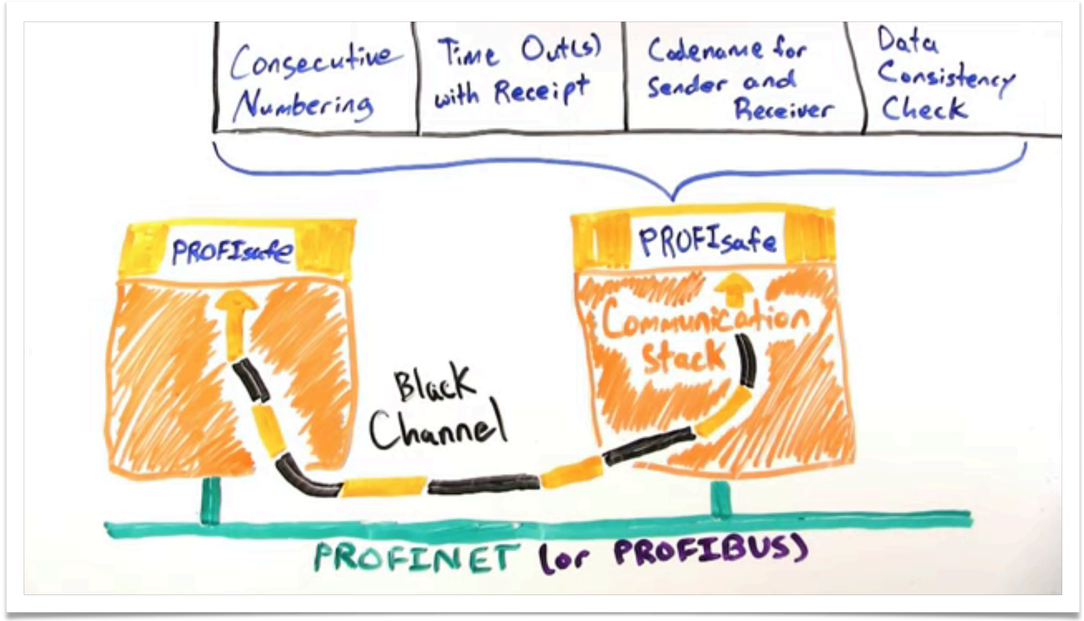
https://www.sciencedirect.com/topics/engineering/functional-safety

Safety by design



PROFIsafe

One minute video: https://youtu.be/S3tbB9-8X4Y



PROFIsafe Live Demonstration: https://youtu.be/QjEeRvgO6jc

Safety

- physical level

- data level

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion

Insertion

Re-sequencing

Data corruption

Masquerade

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition – malfunction of a bus device causes old / obsolete safety messages to be repeated at the wrong time Example: guard door is reported closed when it is already open.

Deletion

Insertion

Re-sequencing

Data corruption

Masquerade

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion – malfunction of a bus device deletes a safety message
For example: request for “safe operational stop”.

Insertion

Re-sequencing

Data corruption

Masquerade

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion

Insertion – malfunction of a bus device inserts a safety message.
For example: deselection of the “safe operational stop”.

Re-sequencing

Data corruption

Masquerade

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion

Insertion

Re-sequencing – malfunction of a bus device modifies the safety message sequence.
For example: prior to initiating the safe operational stop one wants to select the safely reduced velocity.
The machine will continue running while these messages are swapped, no stop is necessary.

Data corruption

Masquerade

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion

Insertion

Re-sequencing

Data corruption – malfunction of a bus device or the transmission link perturbs safety messages.

Masquerade

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion

Insertion

Re-sequencing

Data corruption

Masquerade – malfunction of a bus device causes safety messages and non-safety messages mixed up.

Revolving memory failure (FIFO)

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

What can possibly go wrong?

Different network communication issues:

Repetition

Deletion

Insertion

Re-sequencing

Data corruption

Masquerade

Revolving memory failure (FIFO) – malfunction of a bus device causes an overload situation by simulating incorrect safety messages to a service that belongs to the message is delayed or prevented.

https://profinetuniversity.com/functional-safety/profisafe-profile-details/

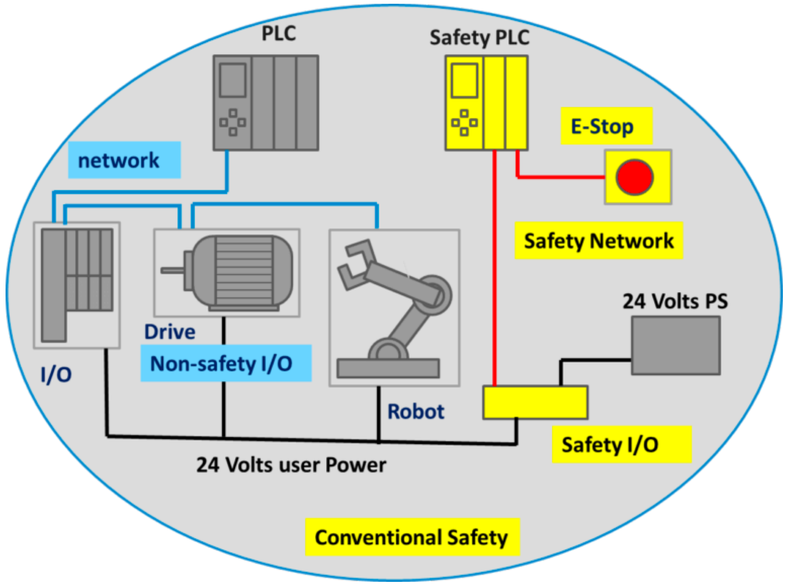
PROFIsafe countermeasures

Remedy: / Error type:	(Virtual) Consecutive Number	Time Out with Receipt	Codename for Sender and Receiver	Cyclic Redundancy Check
Repetition	✓			
Deletion	✓	✓		
Insertion	✓	✓	✓	
Resequencing	✓			
Data Corruption				✓
Delay		✓		
Masquerade (standard message mimics failsafe)		✓	✓	✓
Revolving memory failures	✓			

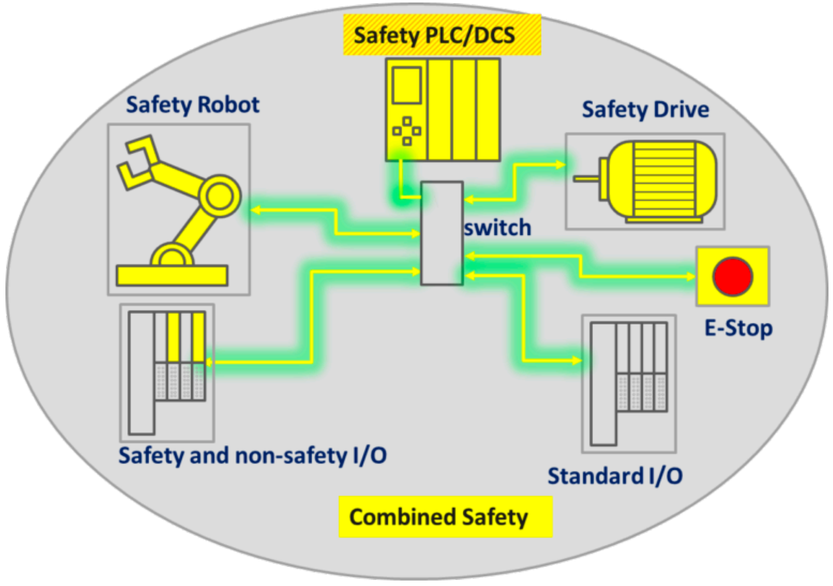
https://profinetuniversity.com/functional-safety/profisafe-profile-details/

Integrated Safety

Conventional safety system:



Integrated safety system:



Safety Integrity Levels

SIL	Low demand mode: average probability of failure on demand	High demand or continuous mode: probability of dangerous failure per hour
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

Safety Integrity Levels

PROFIsafe can support up to:

- Safety Integrity Level 3 (SIL 3) IEC 61508,
- or Category 4, EN 954-1.

To meet SIL 3 requirements, the probability of an undetected error must be < 1 error for every 10^(7) hours of operation (once every 1140.8 years).

The allowable PROFIsafe communication portion of the error probability is < 1 undetected error for every 10^(9) hours (one undetected error every 114,077 years).

Standard IEC 61511

- defines the functional safety requirements established by IEC 61508 (*master standard*) in process industry sector terminology.

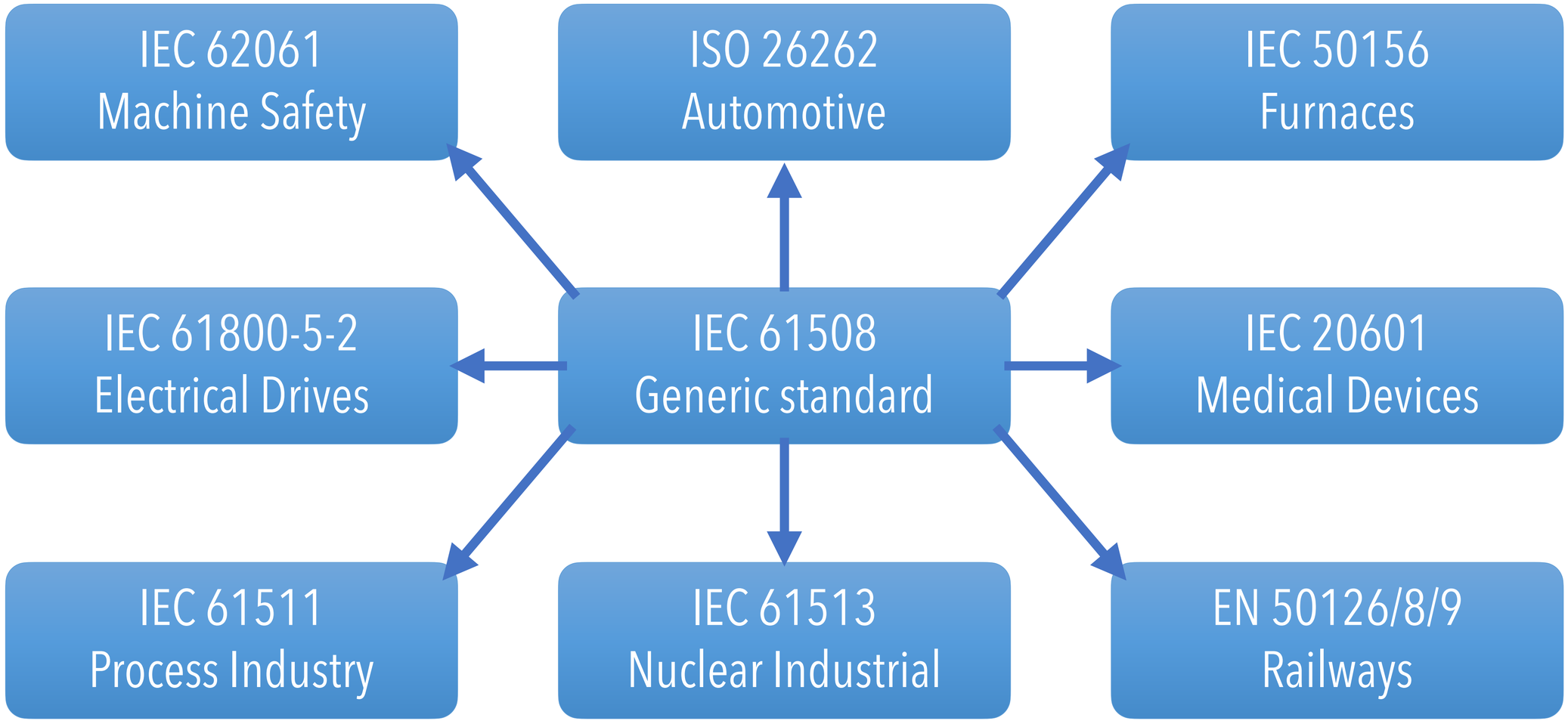
- focuses attention on one type of instrumented safety system used within the process sector, the Safety Instrumented System (SIS).

- consists of three parts:

1. Framework, definitions, system, hardware and software requirements
2. Guidelines in the application of IEC 61511-1
3. Guidance for the determination of the required safety integrity levels

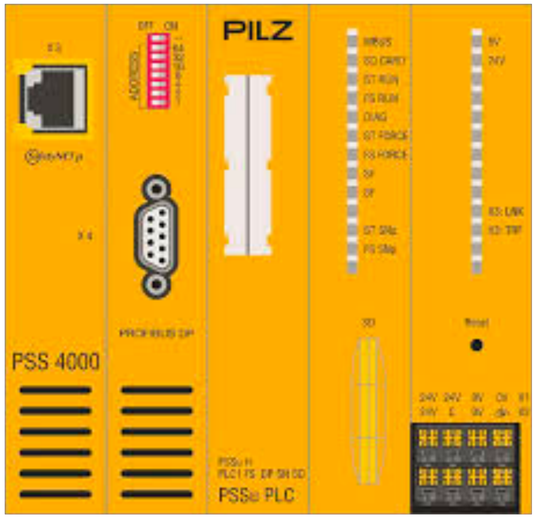
https://en.wikipedia.org/wiki/IEC_61511

IEC 61508 and related standards (not exhaustive)



https://en.wikipedia.org/wiki/IEC_61511

PiLZ (also: SICK, Phoenix Contact, ABB, etc.)



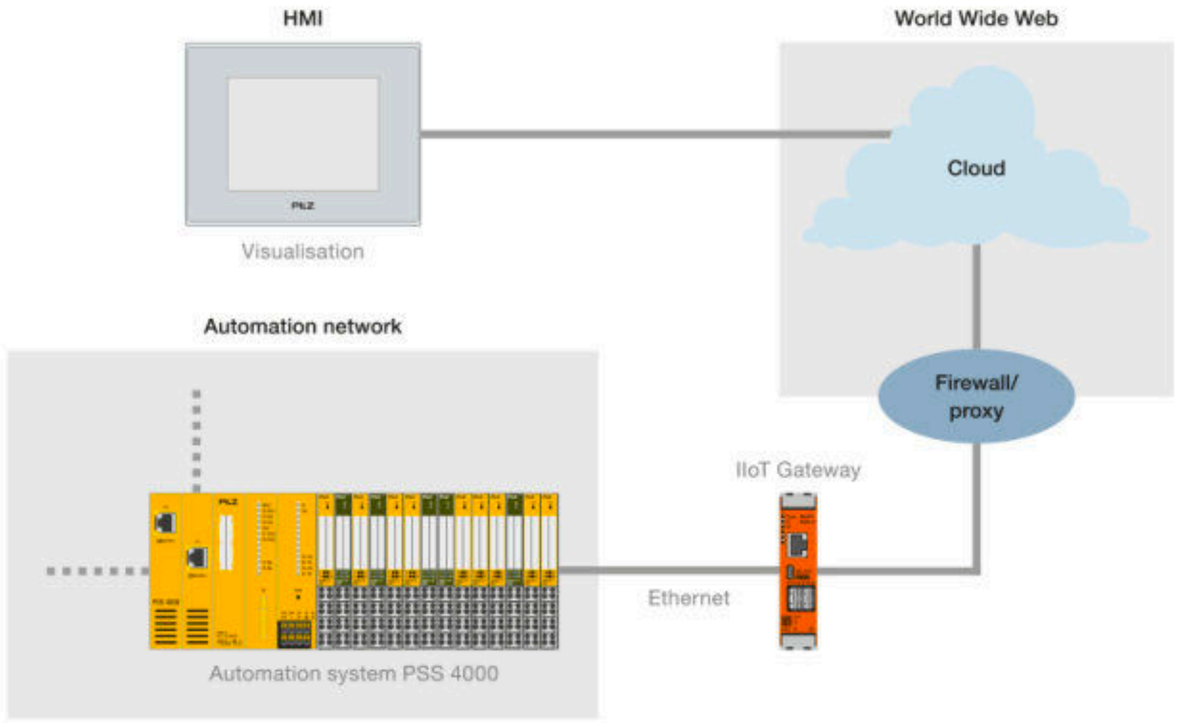
Raspberry Pi and safety…

Revolution Pi

EN 61131-2 compliant

Operation conditions: -40 till +55 °C

Raspbian with Real Time Patch

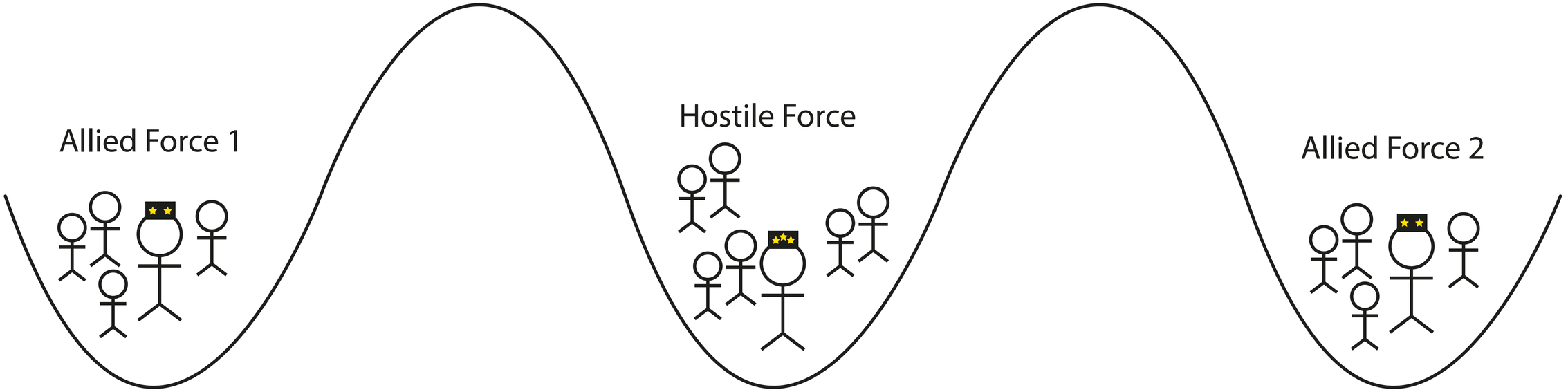


https://www.pilz.com/nl-NL/eshop/00103002137157/Revolution-Pi

https://www.pilz.com/download/open/Fly_Revolution_Pi_1004838-EN-01.pdf

Remember: the two army problem.

Two army / general problem



Allied forces can only win with a coordinated attack, but how do they know when to attack?

TCP: Transmission Control Protocol

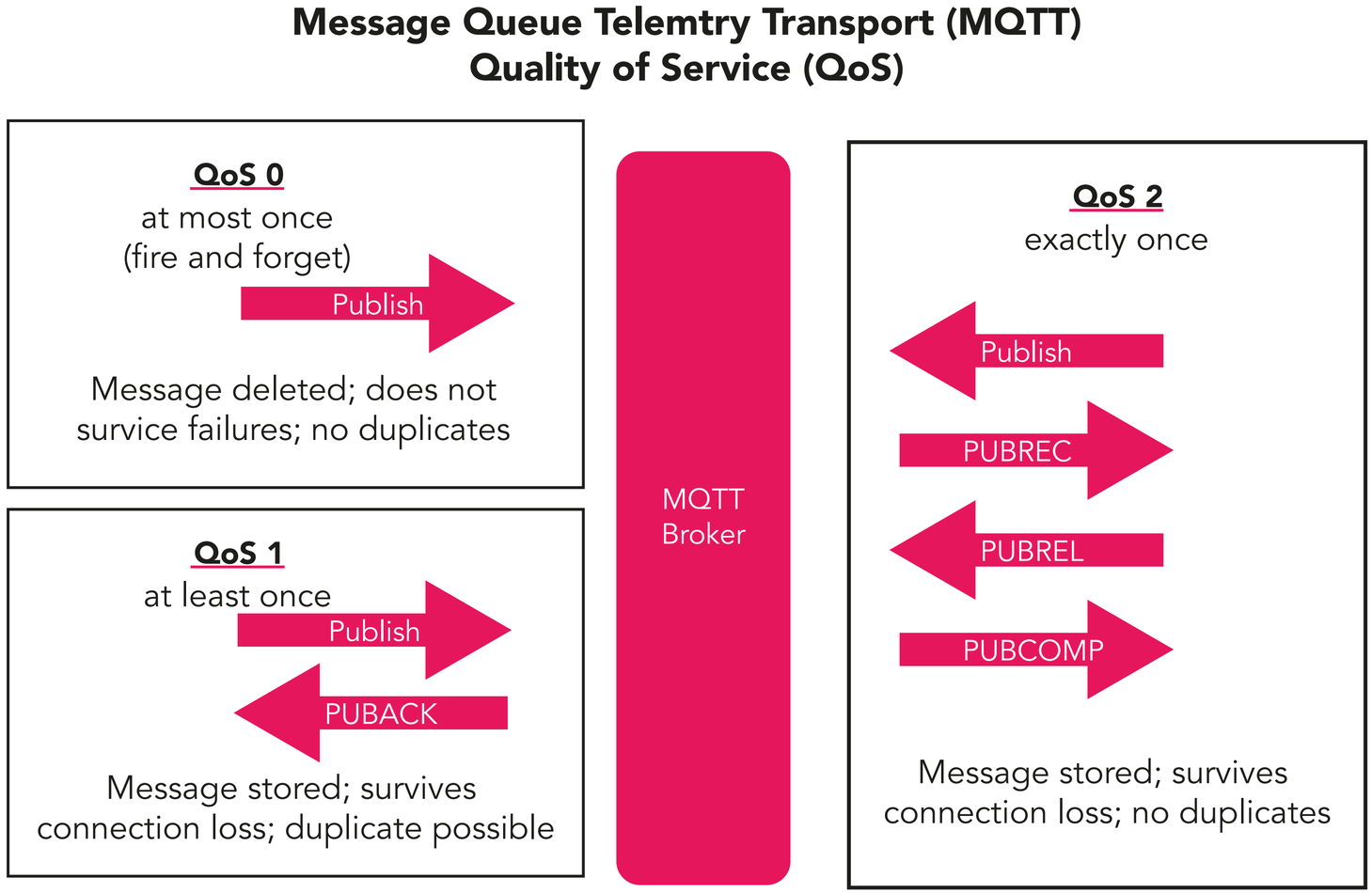
TCP program layer in the client computer:

- waits until all the packets have arrived,
- then acknowledges those it received
- asks for the re-transmission of any it did not (based on missing packet numbers)

How does it deal with the *two generals problem*?

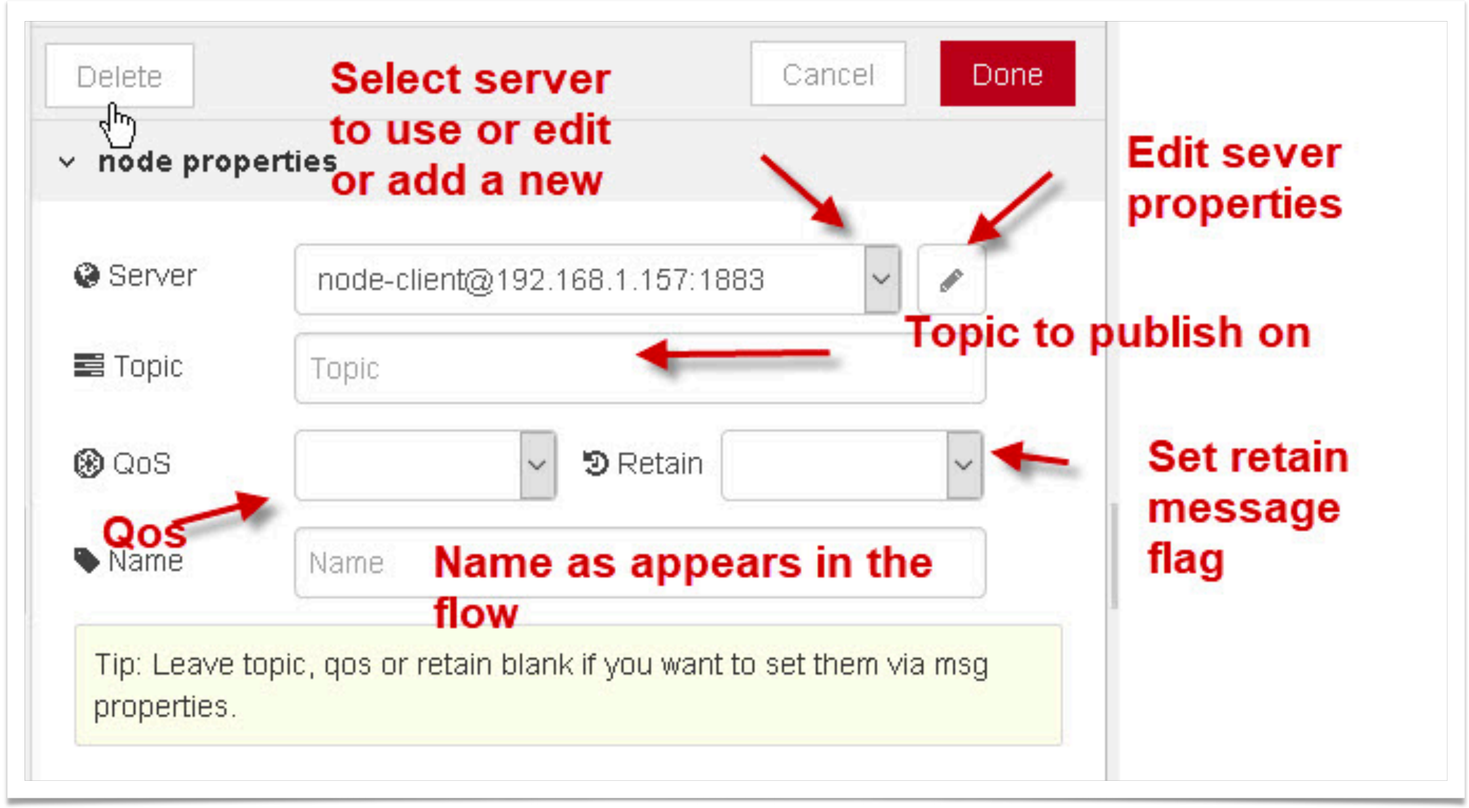
- TCP can't guarantee state consistency between endpoints
- timeouts

Quality of Service: QoS



Source: https://dzone.com/articles/internet-things-mqtt-quality

QoS with MQTT in Node-RED



http://www.steves-internet-guide.com/configuring-the-mqtt-publish-node/

Final tip

Do more with your Arduino Nano 33 IoT board:

https://www.amazon.com/Arduino-Nano-IoT-Development-Workshop-ebook/dp/B07WK9Y7YV

or

https://books.google.nl/books/about/Arduino_Nano_33_IoT_Development_Workshop.html?id=cZCpDwAAQBAJ&redir_esc=y

More Links…

https://skkynet.com/mqtt-answer-iiot/

“

That’s all…

Any questions?

Next week: Security