Fieldbusses

awaiting ...

formal stuff

- Fieldbus is the name of a family of industrial computer network protocols used for real-time distributed control,

  ...
- standardized as IEC 61158.

- private company versions exists

- but interoperability is a “must”

IEC 61158

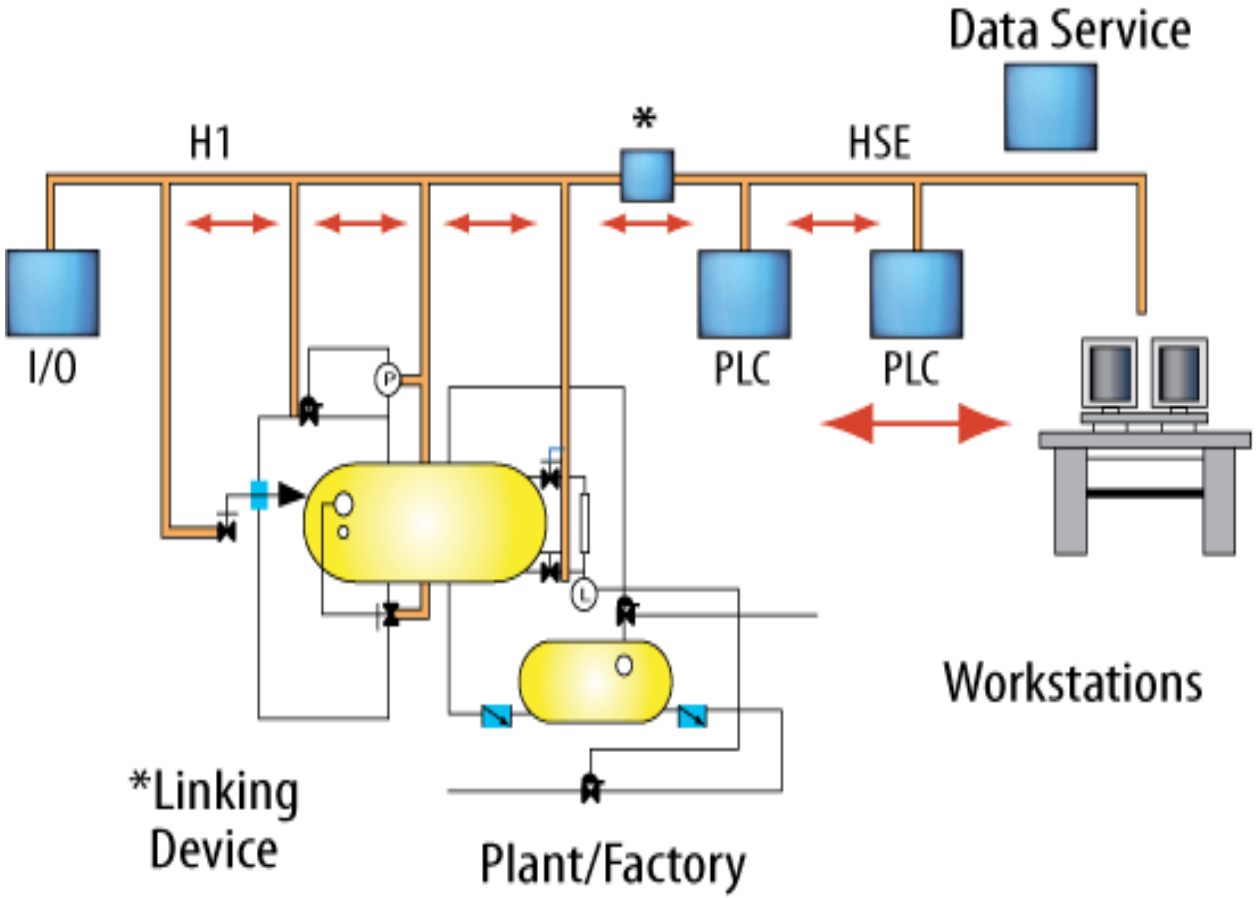
- IEC 61158 consists of the following parts, under the general title Digital data communications for measurement and control – Fieldbus for use in industrial control systems:
-
- Part 1: Overview and guidance for the IEC 61158 series
- Part 2: Physical Layer specification and service definition
- Part 3: Data Link Service definition
- Part 4: Data Link Protocol specification
- Part 5: Application Layer Service definition
- Part 6: Application Layer Protocol specification

- *and the standard is expensive ...*

What is it all about ?

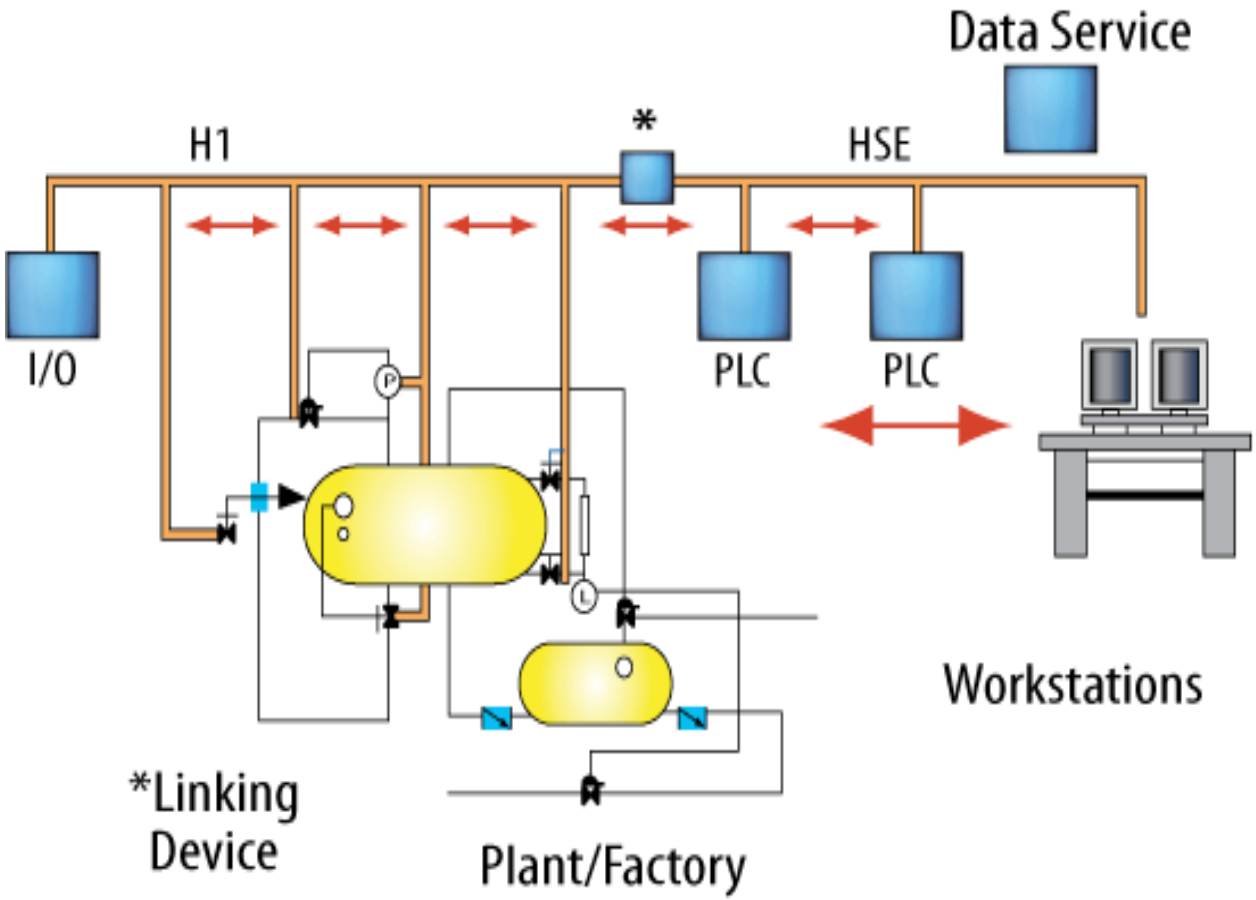
- Reliable networking
- Real time behaviour
- Safety Criticial ?

- Reliable (sub)systems
- Cheap ?
- + 10 year lifetime
- testet, documented
- vendor independent ?!

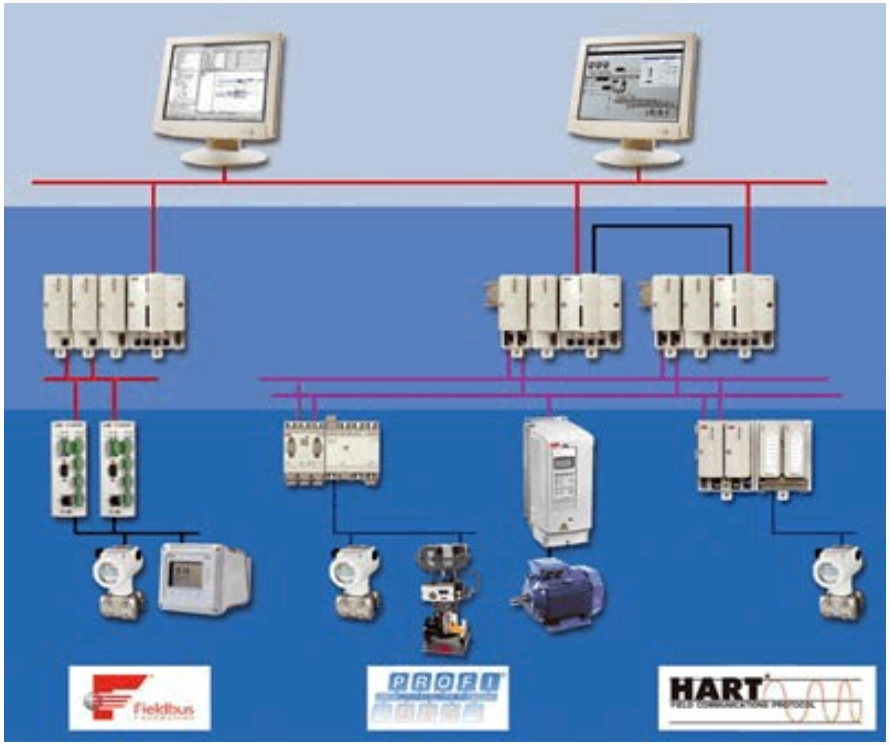


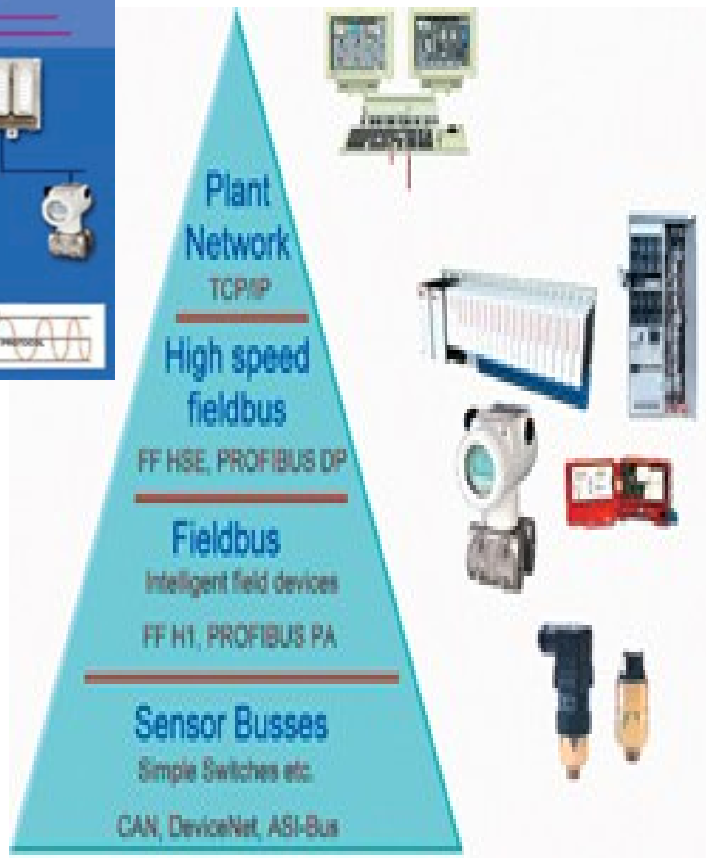
Standards

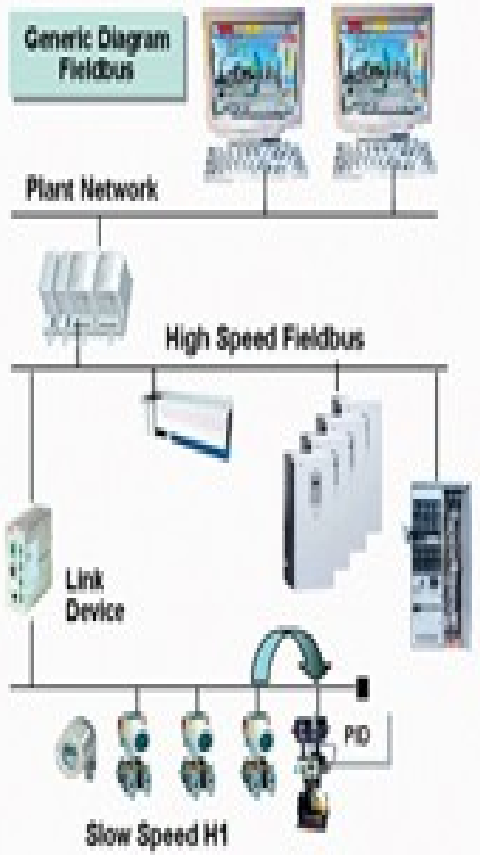
- Reliable (sub)systems
- Cheap ?
- + 20 year lifetime
- testet, documented
- vendor independent ?!



Hierachy / concepts







Fieldbus	Bus power	Cabling redundancy	Max devices	Synchronisation	Sub millisecond cycle
AFDX	No	Yes	Almost unlimited	No	Yes
AS-Interface	Yes	No	62	No	No
CANopen	No	No	127	Yes	No
CompoNet	Yes	No	384	No	Yes
ControlNet	No	Yes	99	No	No
CC-Link	No	No	64	No	No
DeviceNet	Yes	No	64	No	No
EtherCAT	No	Yes	65,536	Yes	Yes
Ethernet Powerlink	No	Optional	240	Yes	Yes
EtherNet/IP	No	Optional	Almost unlimited	Yes	Yes
Interbus	No	No	511	No	No
LonWorks	No	No	32,000	No	No
Modbus	No	No	246	No	No
PROFIBUS DP	No	Optional	126	Yes	No
PROFIBUS PA	Yes	No	126	No	No
PROFINET IO	No	Optional	Almost unlimited	No	No
PROFINET IRT	No	Optional	Almost unlimited	Yes	Yes
SERCOS III	No	Yes	511	Yes	Yes
SERCOS interface	No	No	254	Yes	Yes
Foundation Fieldbus H1	Yes	No	240	Yes	No
Foundation Fieldbus HSE	No	Yes	Almost unlimited	Yes	No
RAPIEnet	No	Yes	256	Under Development	Conditional
Fieldbus	Bus power	Cabling redundancy	Max devices	Synchronisation	Sub millisecond cycle

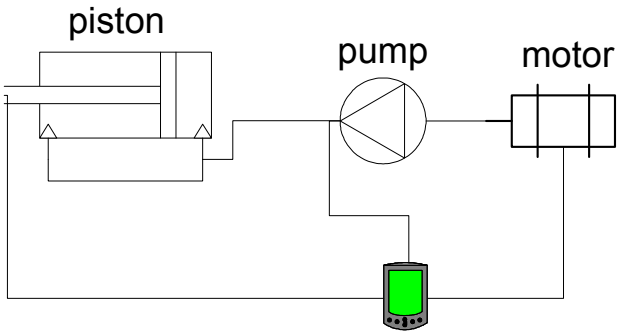
Safety critical systems

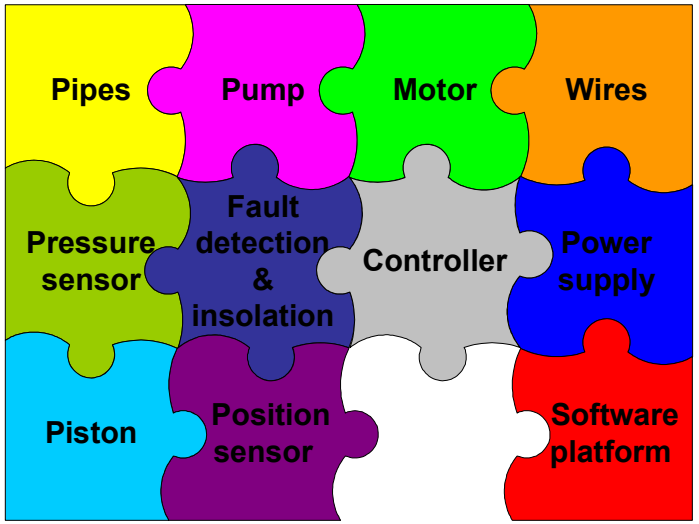
- Example of safety critical systems

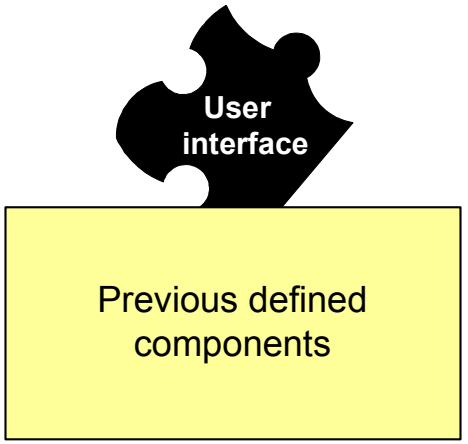
Safety critical systems

- Design of safety critical systems by components

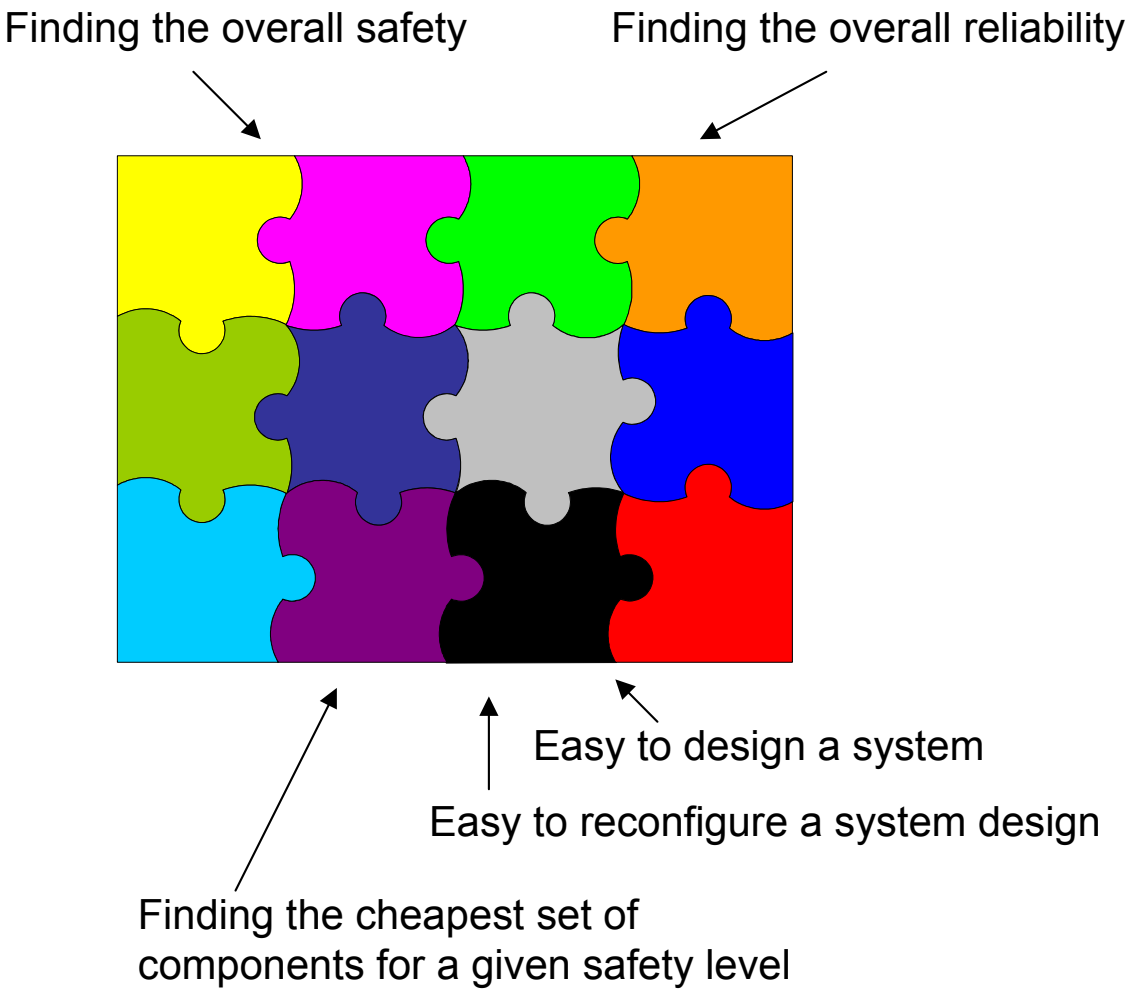
Example: Drive
by wire system



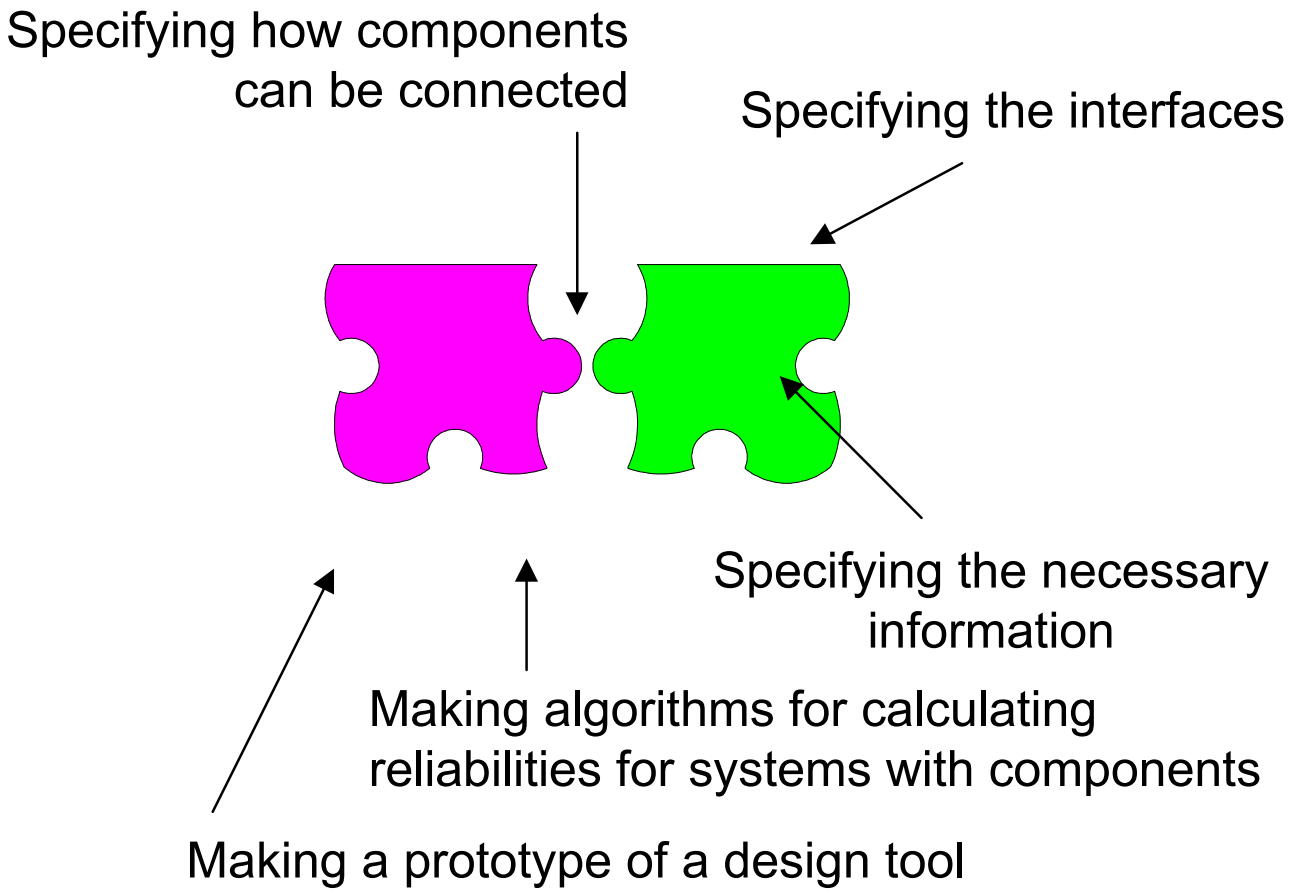




Safety critical systems



Safety critical systems



IEC 61508 – safety
a very short introduction

- IEC 61508 - **Functional** safety of electrical/electronic/programmable electronic safety-related systems

- The safety life cycle has 16 phases which roughly can be divided into three groups as follows:

- Phases 1-5 address analysis
- Phases 6-13 address realisation
- Phases 14-16 address operation.

- can kill small new uprising companies.

Beware ...


certifire
UL
Lloyd's Register
DNV
Lloyd's Register
TYPE APPROVAL
GL
Germanischer Lloyd

Categories of likelihood of occurrence

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Consequence categories

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

These are typically combined into a risk class matrix

	Consequence			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Where:

- Class I: Unacceptable in any circumstance;
- Class II: Undesirable: tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained;
- Class III: Tolerable if the cost of risk reduction would exceed the improvement;
- Class IV: Acceptable as it stands, though it may need to be monitored.

SIL 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 $< 10^{-7}$ (1 dangerous failure in 1140 years)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

for download see https://en.wikipedia.org/wiki/IEC_61508

canbus as an example

- Bosch
- Automotive Industry
- AAU satellites :-)
-