

# PEMS - Bridging The Gap

Lorit Consultancy – EuroSPI 2019

Alastair Walker & Stuart Hardie

19 Sep 2019



# The medical device challenge

## Automotive

ISO 26262

IATF 16949

A few  
supporting docs

HW Team



SW Team



Functional Safety Team



Quality Management Team



18 Sep 19

## Medical

MDR

ISO 13485

ISO 14971

IEC 60601-1

IEC

IEC

IEC 60601-1-x

FDA Guidance

ISO 10993-x

IEC 62304

IEC 62366

IEC 60601-2-x

HW Team



SW Team

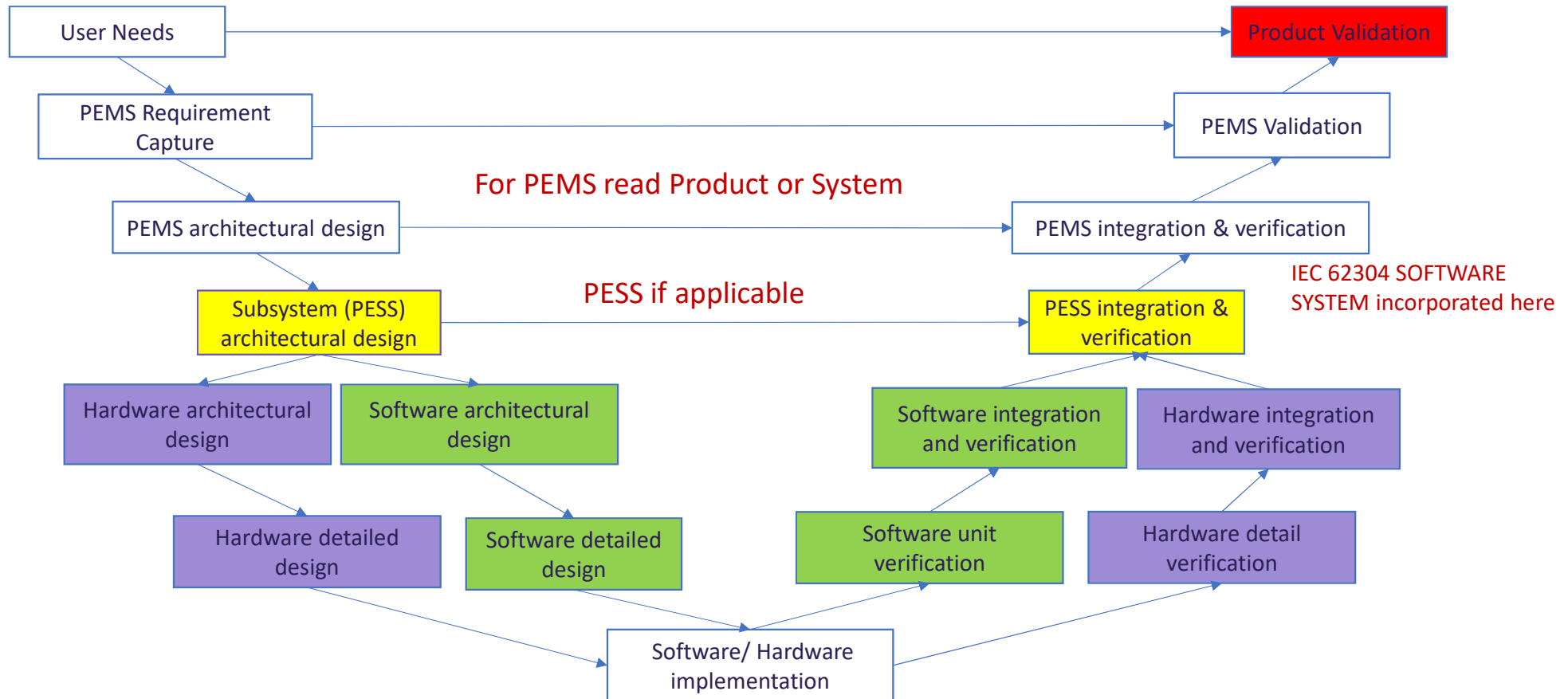


Quality Management Team

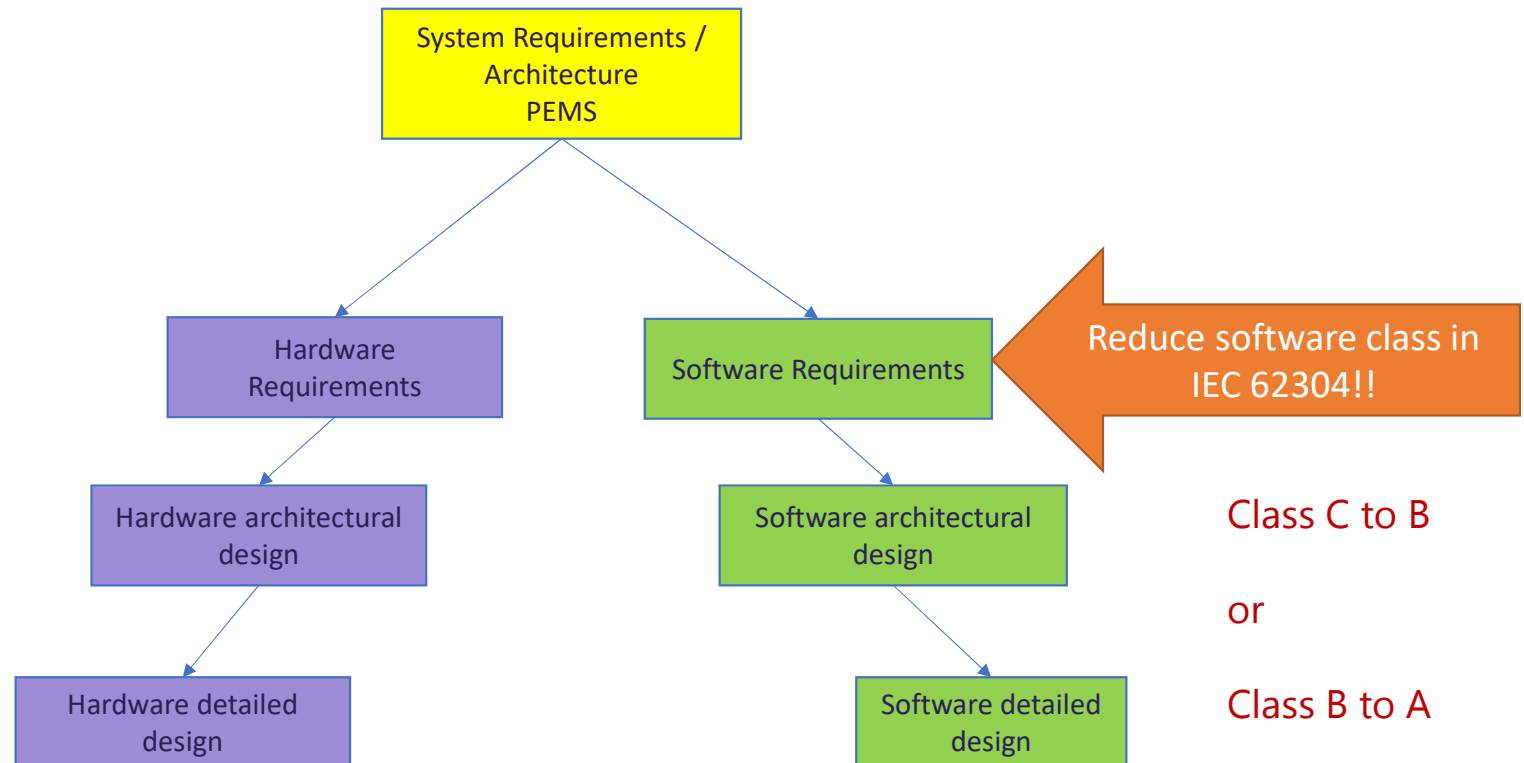


EuroSPI 2019

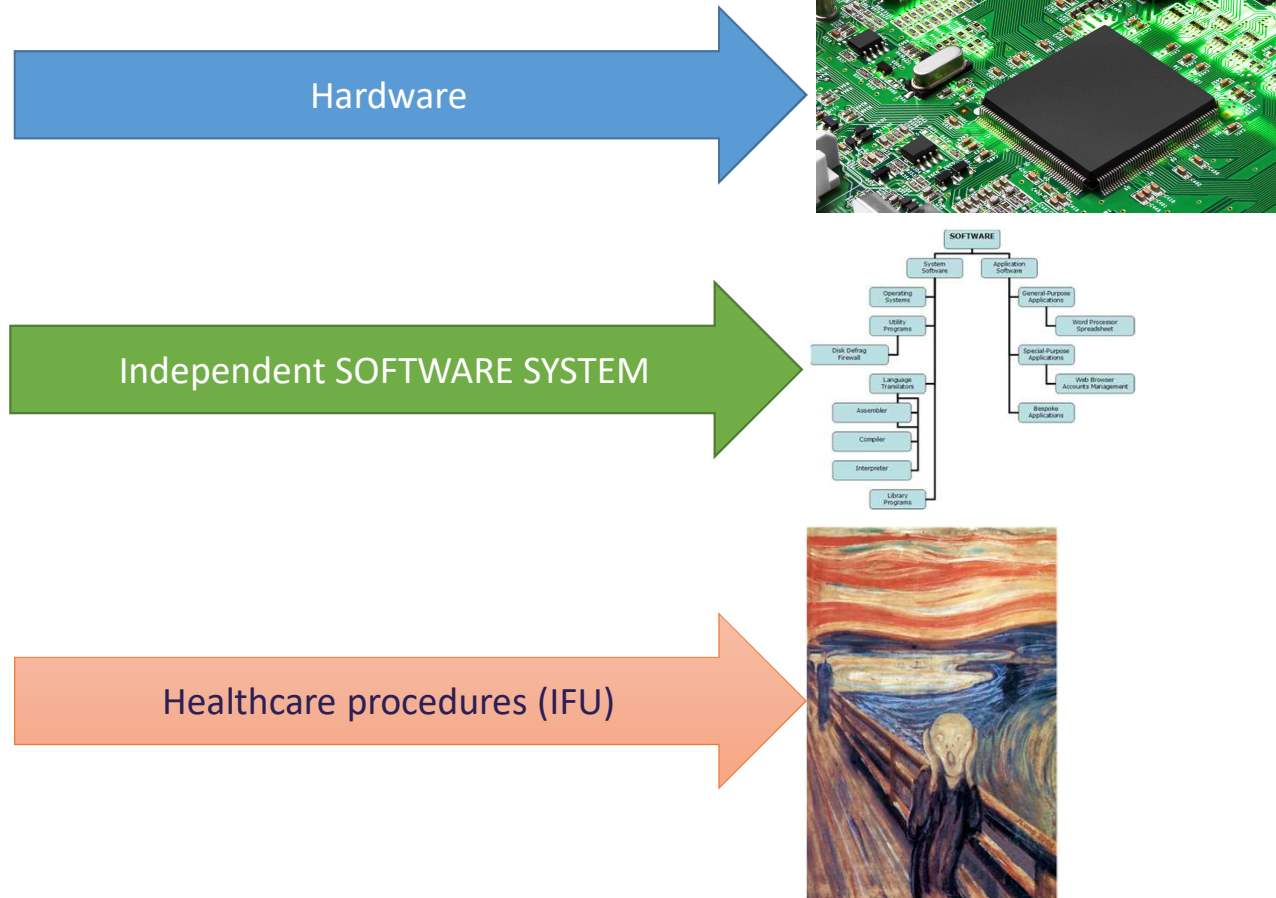
# The infrastructure IEC 60601



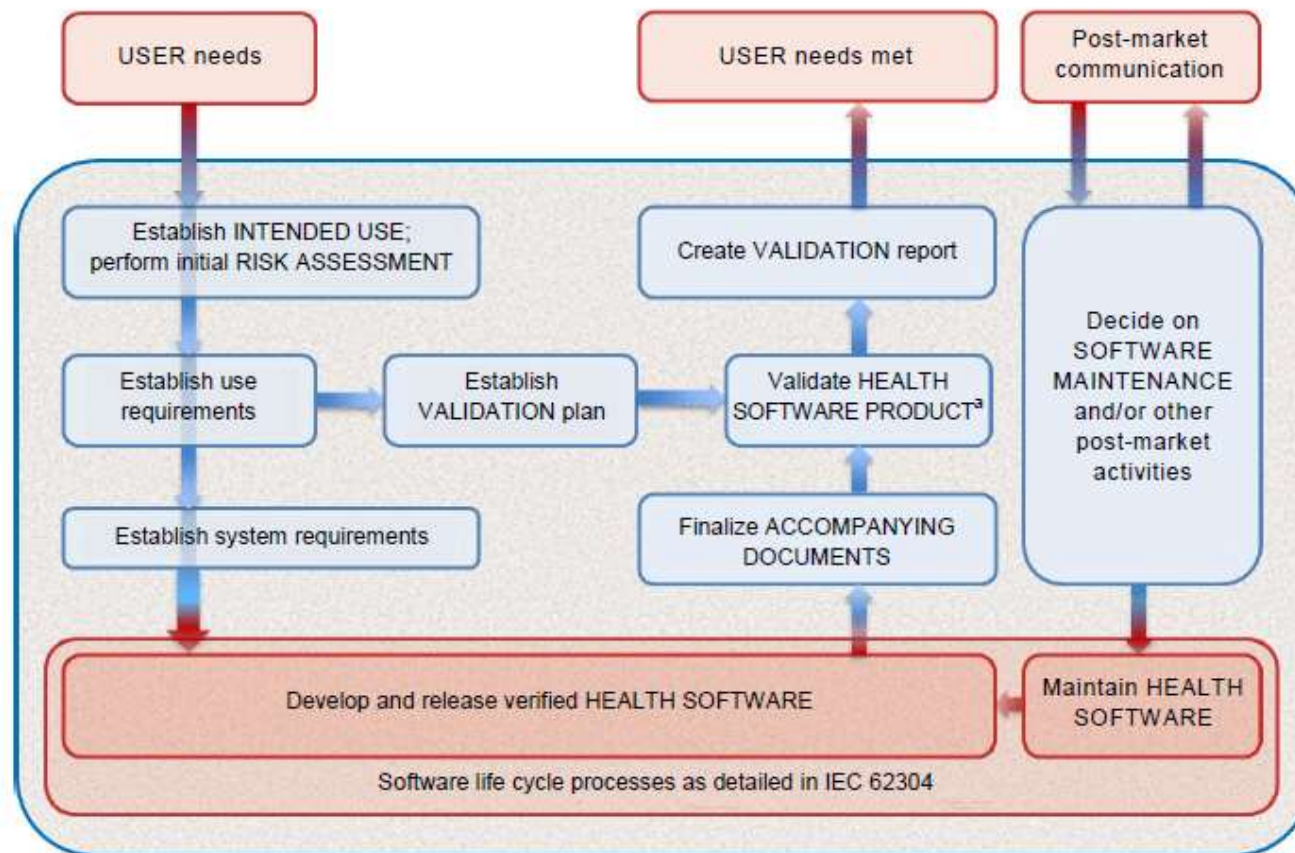
# The infrastructure IEC 60601 with IEC 62304



# SW Class Decomposition Options



# SW Class Decomposition IEC 82304-1

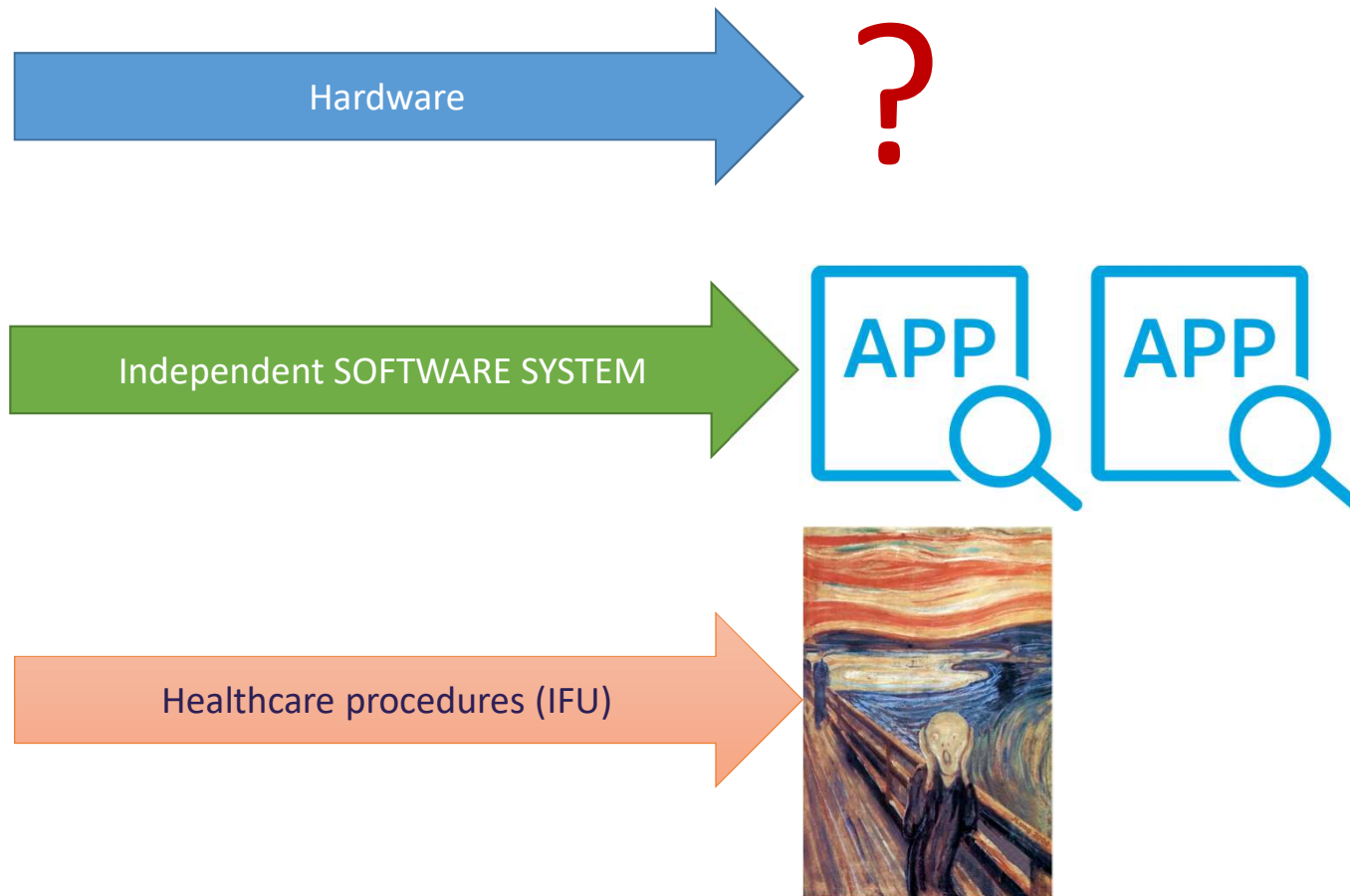


<sup>a</sup> HEALTH SOFTWARE PRODUCT: HEALTH SOFTWARE plus ACCOMPANYING DOCUMENTS

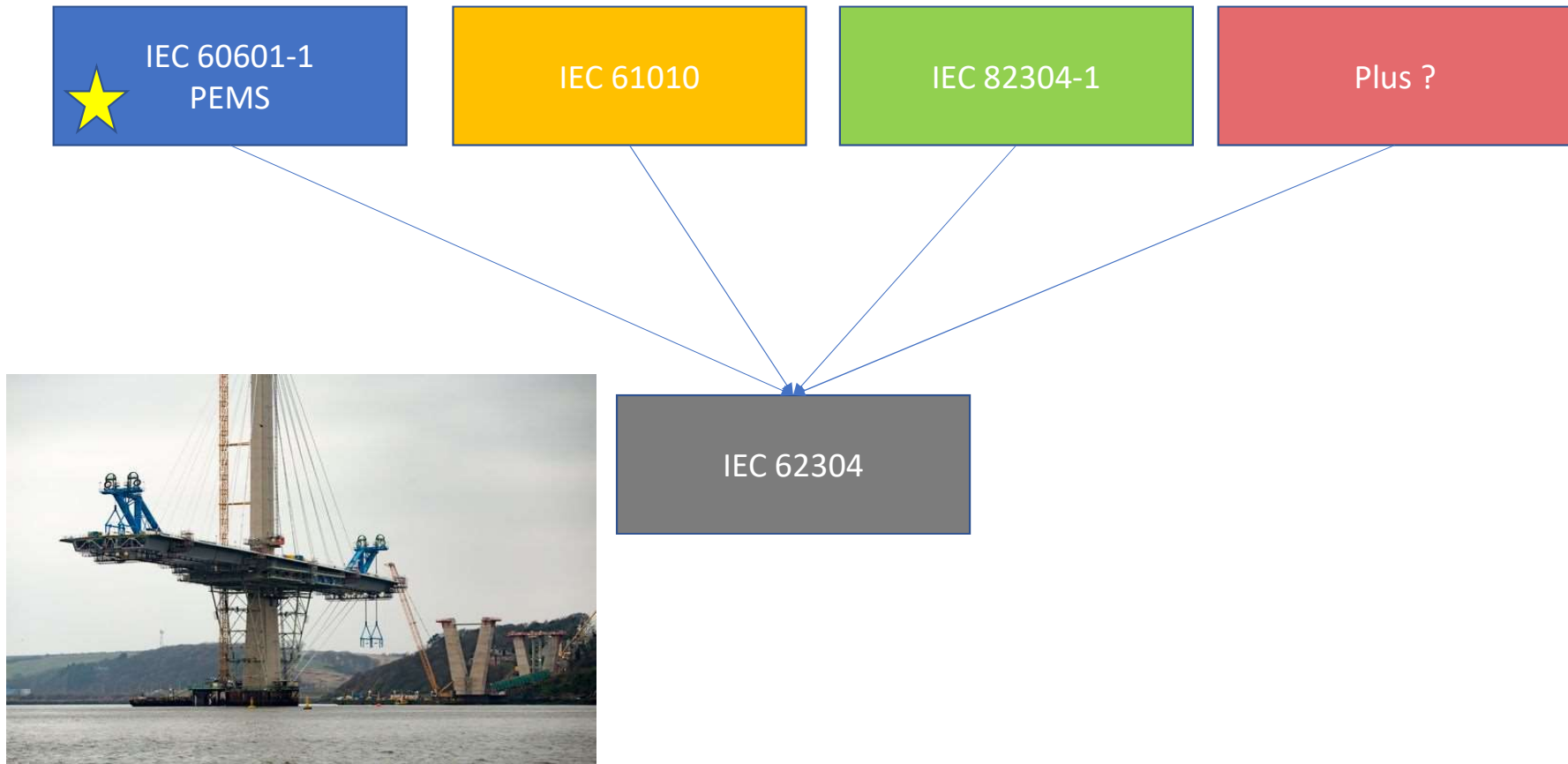
IEC



# SW Class Decomposition Options



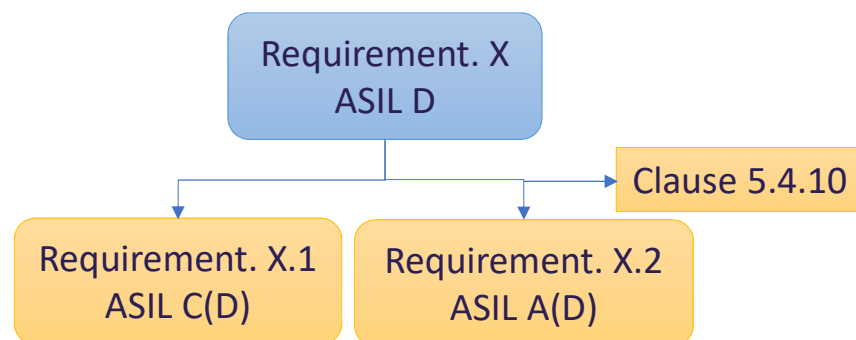
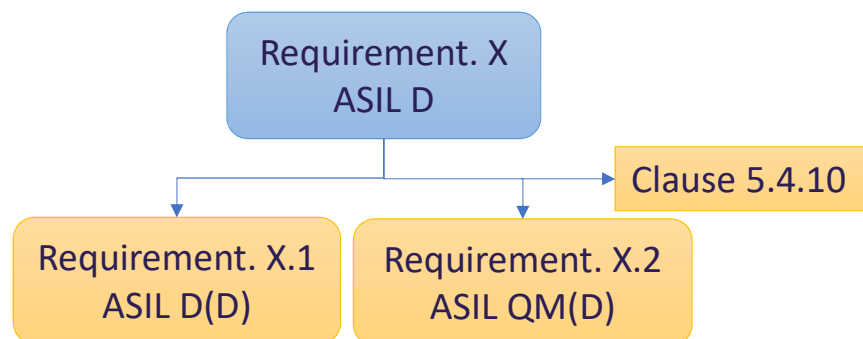
# SW Class Decomposition Options





# SW Class Decomposition Options

How do other industries approach this topic?



ISO 26262

Decomposition at system level

Clause 5.4.10 is proving '**Freedom from Interference**' to justify the acceptability of the decomposition

Safety Mechanisms take the higher ASIL intended functionality the lower ASIL

# What's in IEC 60601-1 AMD2?

Scheduled release October 2020  
Committee SC 62A  
Working Group MT 28  
Status AFDIS



# What's in IEC 60601-1 AMD2?

Nothing earth-shattering its an amendment!

- Mandatory IFU symbol 😊
- Obsolescence of IEC 60950-1
- ISO 14971 updates
- IEC 60601-1-8 updates
- Relation to other 60601-x-x standards



# What's in IEC 60601-1 AMD2?

Refer to ACCOMPANYING DOCUMENTS

IEC 60601-1 **AMD2 will make this symbol mandatory** if RISK CONTROL measures have been applied in the ACCOMPANYING DOCUMENTS



Otherwise

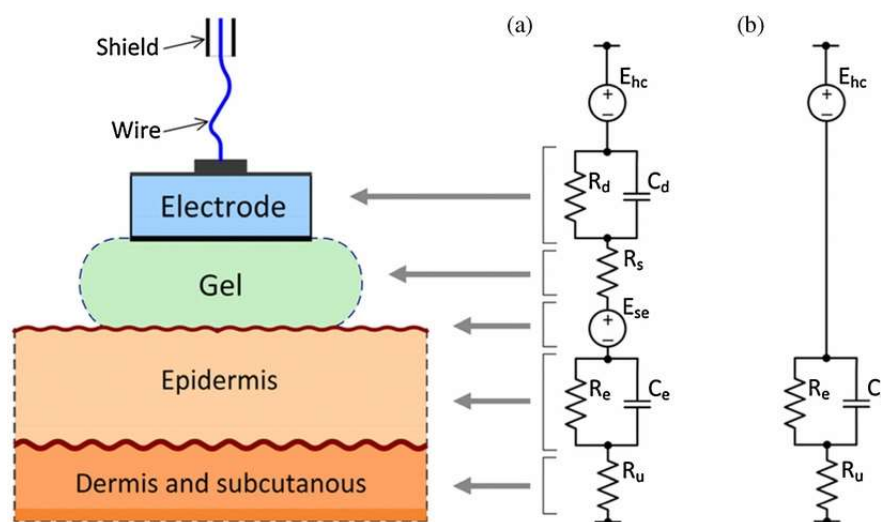


# What's in IEC 60601-1 AMD2?

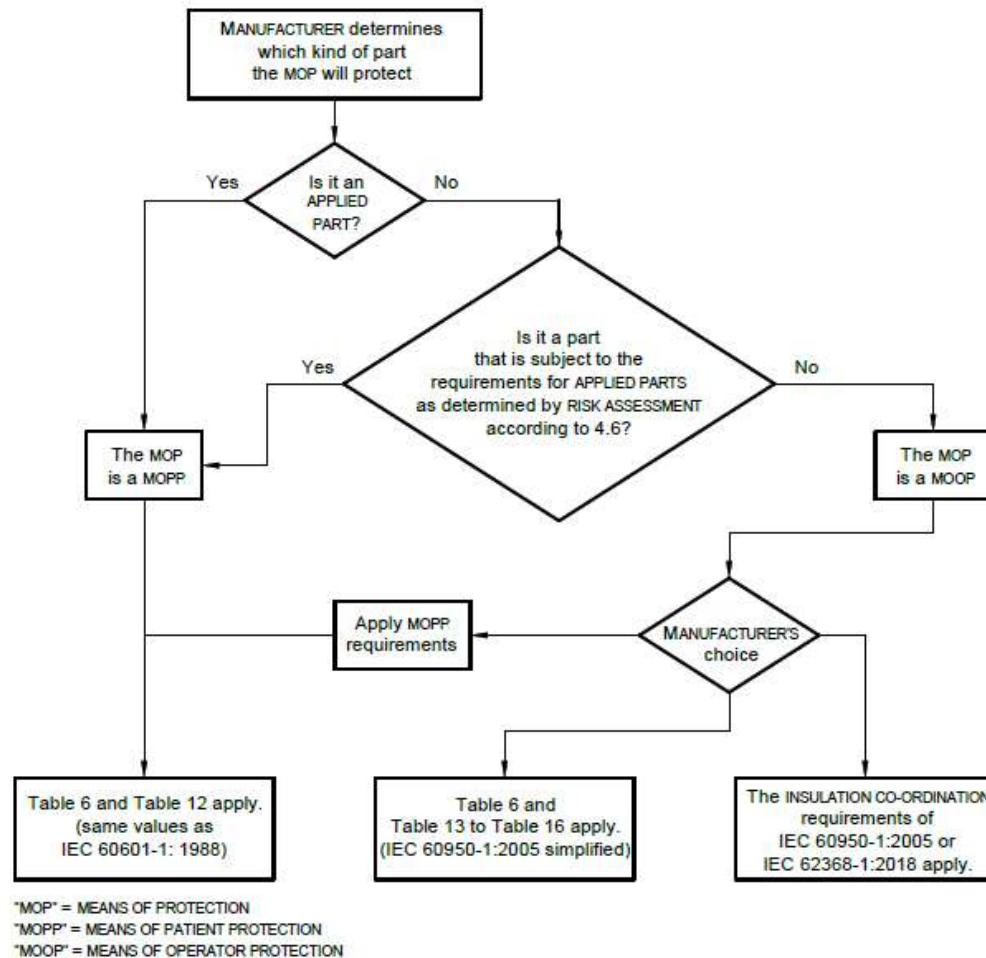
Retirement of IEC 60950-1

Impedance to the heart from the surface of the skin can drop > **factor of 10** with skin preparation and gelled electrodes.

e.g.  $60\text{k}\Omega$  to  $2\text{k}\Omega$  is typical.



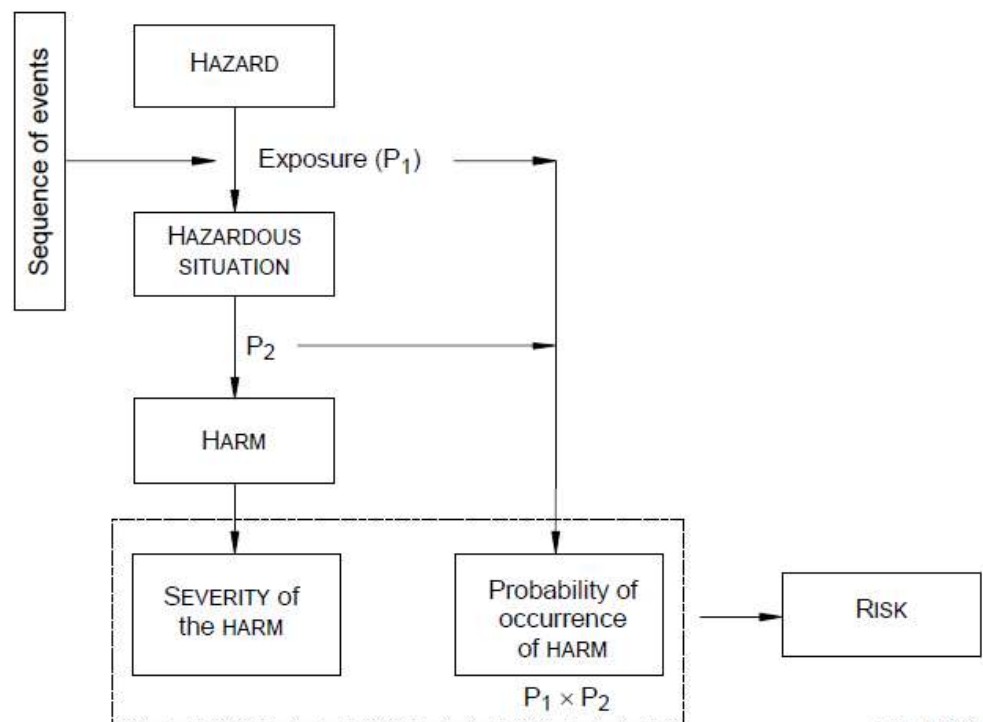
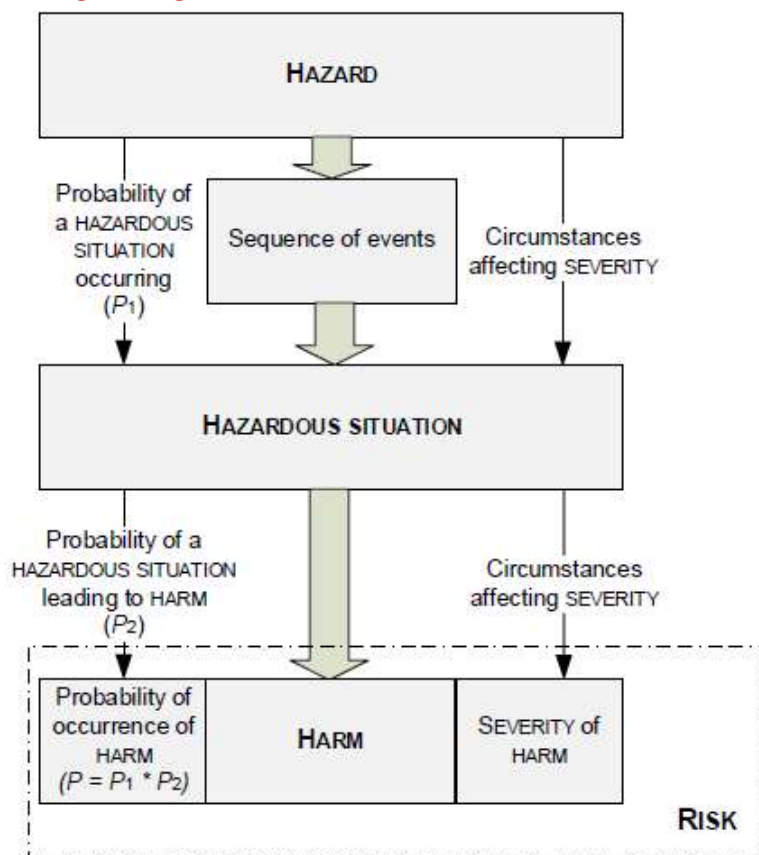
# What's in IEC 60601-1 AMD2?





# What's in IEC 60601-1 AMD2?

## Annex A new



IEC 2430/05

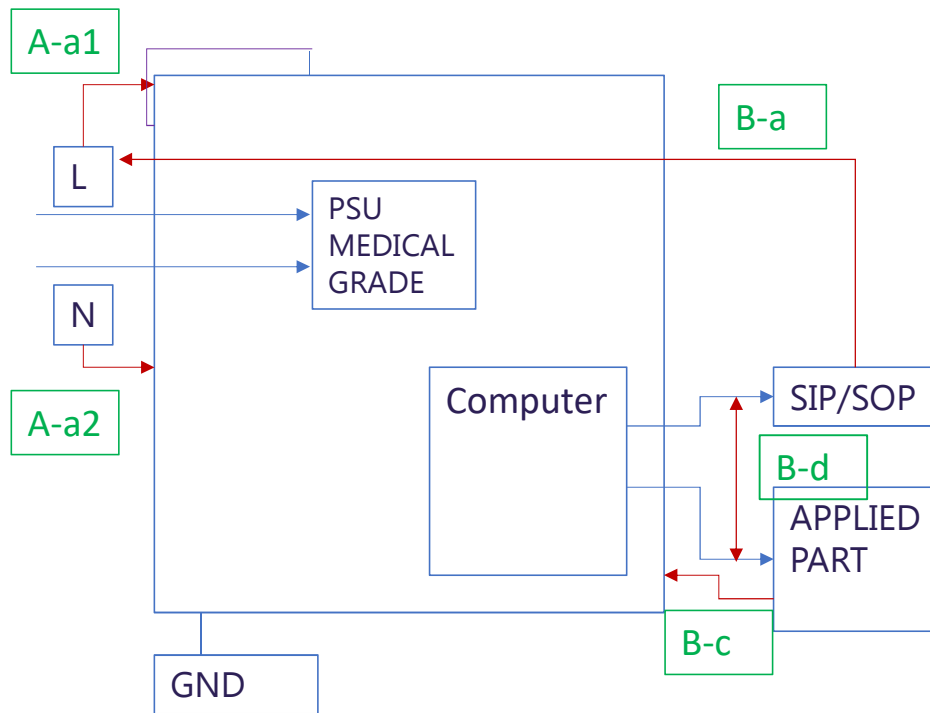
NOTE  $P_1$  is the probability of a HAZARDOUS SITUATION occurring.  
 $P_2$  is the probability of a HAZARDOUS SITUATION leading to a HARM.

# Wishlist for Edition 4

Get involved in standards committees

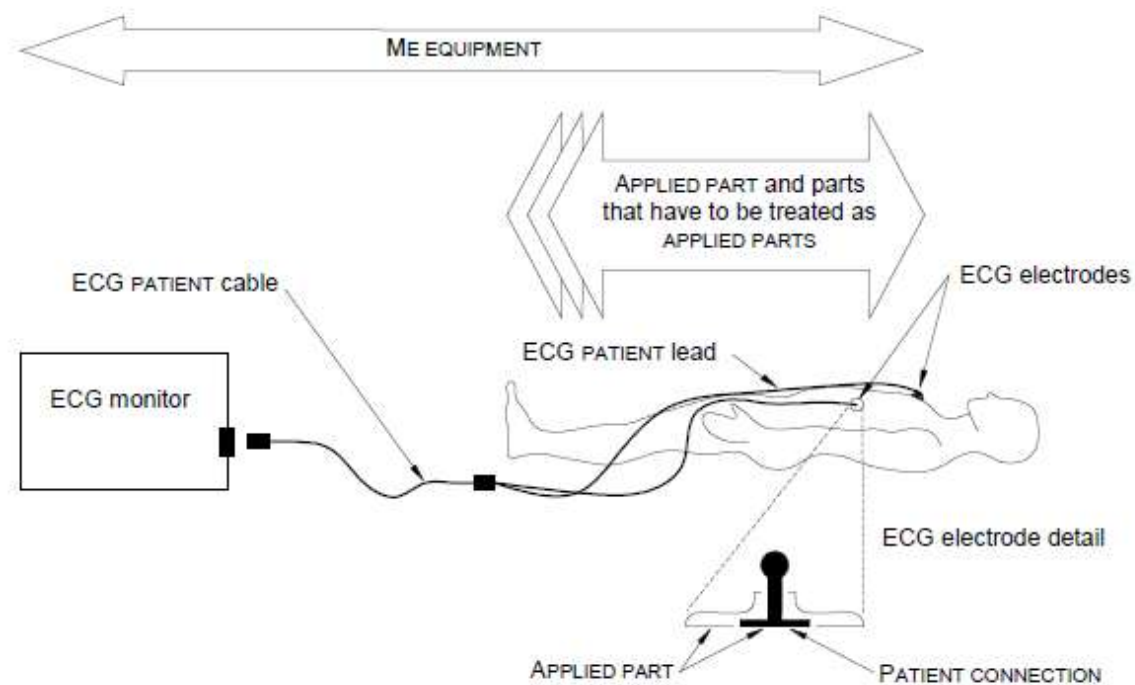


# Wishlist - Insulation diagrams



Insulation Type	Voltage	Required Creepage	Required Clearance	Measured
A-a1 Basic	240	4mm	3mm	>12mm
A-a2 Reinforced	240	8mm	5mm	>12mm
B-a Reinforced	240	8mm	5mm	>12mm
B-c Supplementary	12	1,7mm	0,8mm	>12mm
B-d Basic	12	1,7mm	0,8mm	>12mm

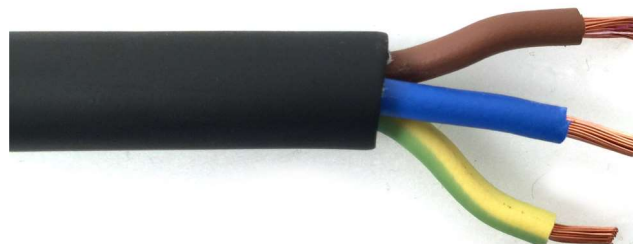
# Wishlist – Insulation Diagrams



## Wishlist - Is there a future for Basic Safety?

BASIC SAFETY relates to a device not resulting in HARM **incidental** to its operation.  
BASIC SAFETY is often a **passive form of protection** (such as radiation shielding or electrical grounding).

Since IEC 60601-1:2012 really a **sub-division** of **RISK CONTROL** mechanism



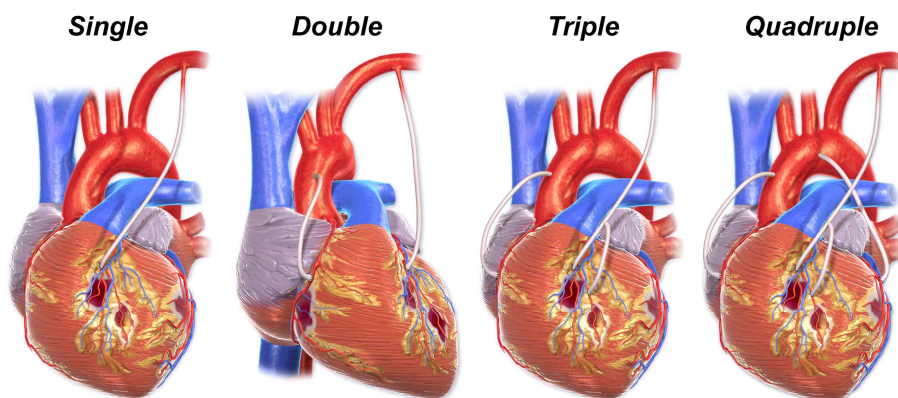
# Wishlist – Reducing the PEMS Bypass

The requirements in 14.2 to 14.12 (inclusive) shall apply to PEMS unless:

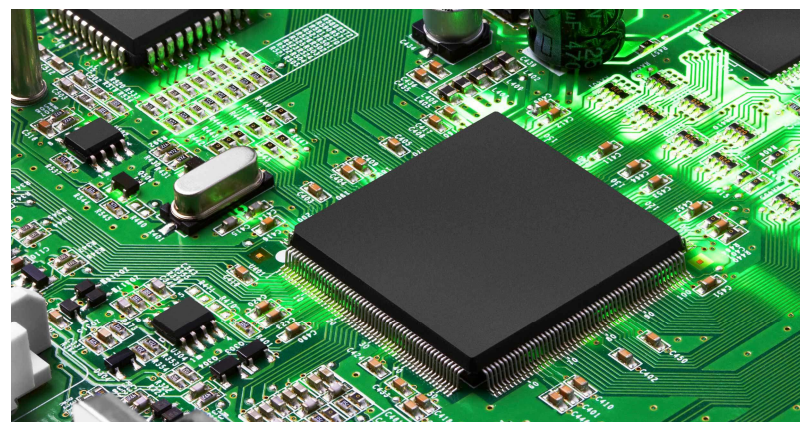
- **none of the** PROGRAMMABLE ELECTRONIC SUBSYSTEM (PESS) provides functionality necessary for BASIC SAFETY or ESSENTIAL PERFORMANCE; or
- the application of RISK MANAGEMENT as described in 4.2 demonstrates that the failure of any PESS **does not lead to an unacceptable RISK**.

## PESS

system based on one or more **central processing units**, including their **software** and interfaces



**Coronary Artery Bypass Graft (CABG)**





# Wishlist – Reducing the PEMS Bypass

## §14.8 PEMS Architecture

Where appropriate, to reduce the RISK to an acceptable level, the **architecture specification** shall make use of:

- a) COMPONENTS WITH HIGH-INTEGRITY CHARACTERISTICS;
- b) **fail-safe functions**;
- c) **redundancy**;
- d) **diversity**;
- e) **partitioning** of functionality;
- f) defensive design, e.g. limits on potentially hazardous effects by restricting the available output power or by introducing means to limit the travel of actuators.

# Wishlist – Reducing the PEMS Bypass

## §14.8 PEMS Architecture

The architecture specification shall take into consideration:

- g) allocation of RISK CONTROL measures to subsystems and components of the PEMS;

NOTE Subsystems and components include sensors, actuators, PESS and interfaces.

- h) **failure modes** of components and their effects;
- i) **common cause failures**;
- j) **systematic failures**;
- k) **test interval** duration and **diagnostic coverage**;
- l) maintainability;
- m) protection from reasonably foreseeable **misuse**;
- n) the NETWORK/DATA COUPLING IT-NETWORK specification, if applicable.

# Wishlist – Reducing the PEMS Bypass

## Architecture

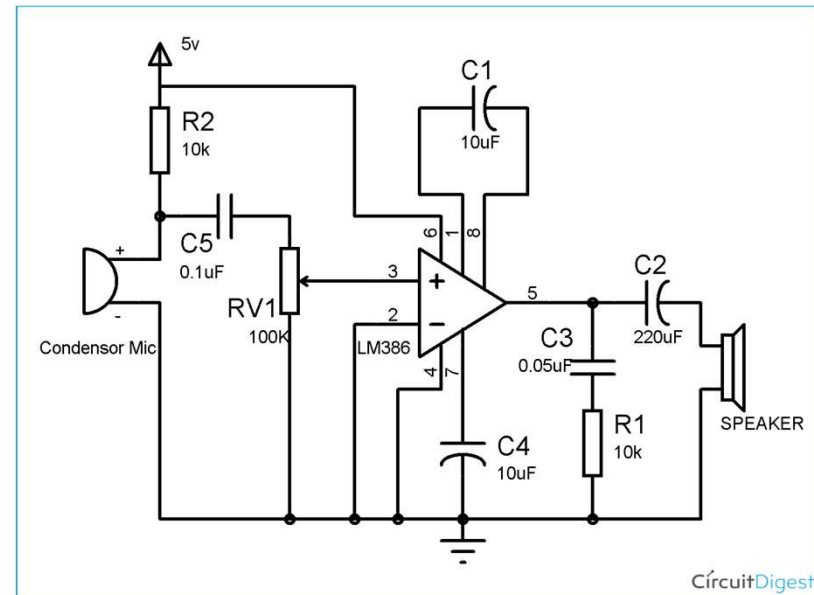
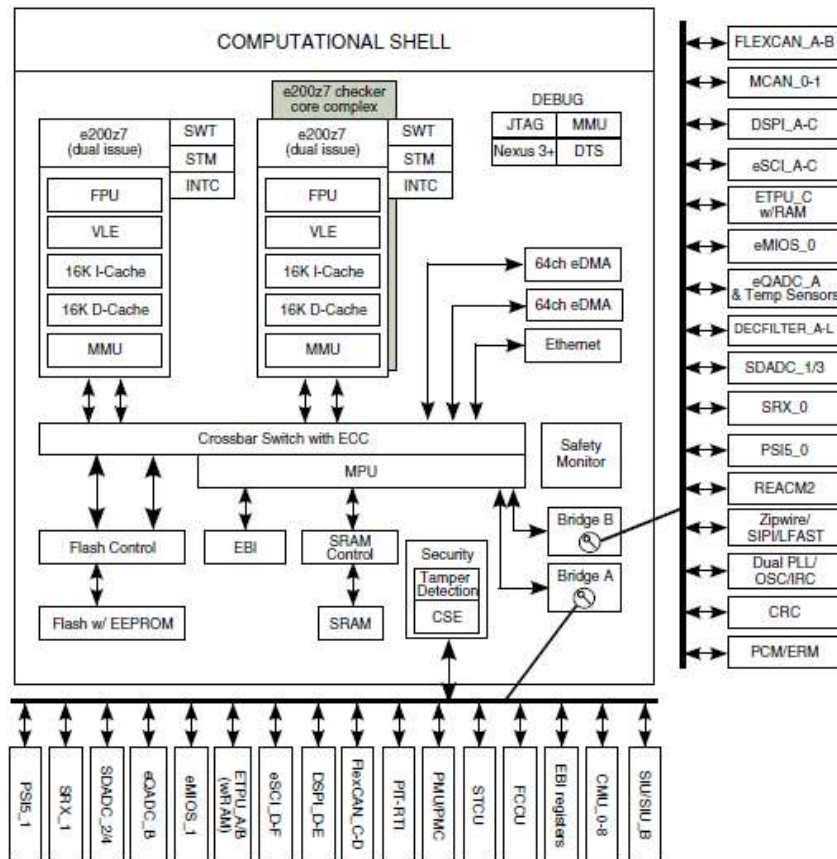
- Fail-safe functions
  - If a function or component fails ensure the failure mode is in a **non-hazardous state**
  - e.g. open circuit resistor does not result in a device switching on when it should be off
  - Microcontroller reset and I/O high impedance does not result in an uncontrolled state
  - Power transistor failing can be detected and handled safely
- Redundancy
  - Techniques redundancy, diversity and **partitioning of functionality** can be found in standards such as IEC 61508 or ISO 26262
- Diversity
  - Ensure if a redundant mechanism is implemented it's functionality is diverse from the original implementation.
  - Avoidance of **common-cause failures** through shared interfaces, power supply rails etc.

## *Good Background Reading*

*Controller Integrity in Automotive Failsafe System Architectures - Padma Sundaram and Joseph G. D'Ambrosio, Delphi Corporation*

# Wishlist – Reducing the PEMS Bypass

PEMS applicability could be based on device class



# Summary

- Don't add to the workload!
- Get involved in the standards committees
- IEC 60601-1 Section 14 (PEMS) could form the basis of system level activities
- Class reduction moved to PEMS only
- Other standards can reference PEMS
- Reference BASIC SAFETY as a subset of RISK CONTROL measures
- Clear strategy for class reduction in IEC 82304-1
- Eliminate PEMS bypass



# Thank you!

Lorit Consultancy – Salzburg & Edinburgh

[www.lorit-consultancy.com](http://www.lorit-consultancy.com)

[info@lorit-consultancy.com](mailto:info@lorit-consultancy.com)

+43 676 338 8884 & +44 7708 360023



18 Sep 19



EuroSPI 2019

26