ECE 50874/59595: Advanced Software Engineering

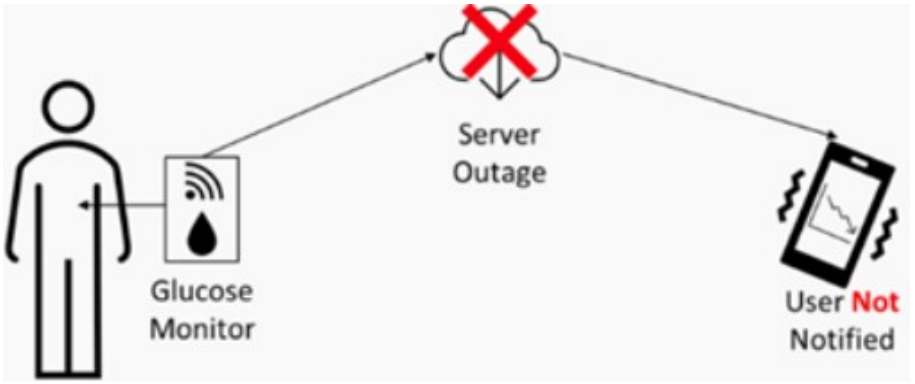
Risk mitigation using standardized processes

Profs Davis & Torres

PURDUE UNIVERSITY | Elmore School of Electrical and Computer Engineering

The case of Dexcom: Who is at fault?

Dexcom glucose monitor

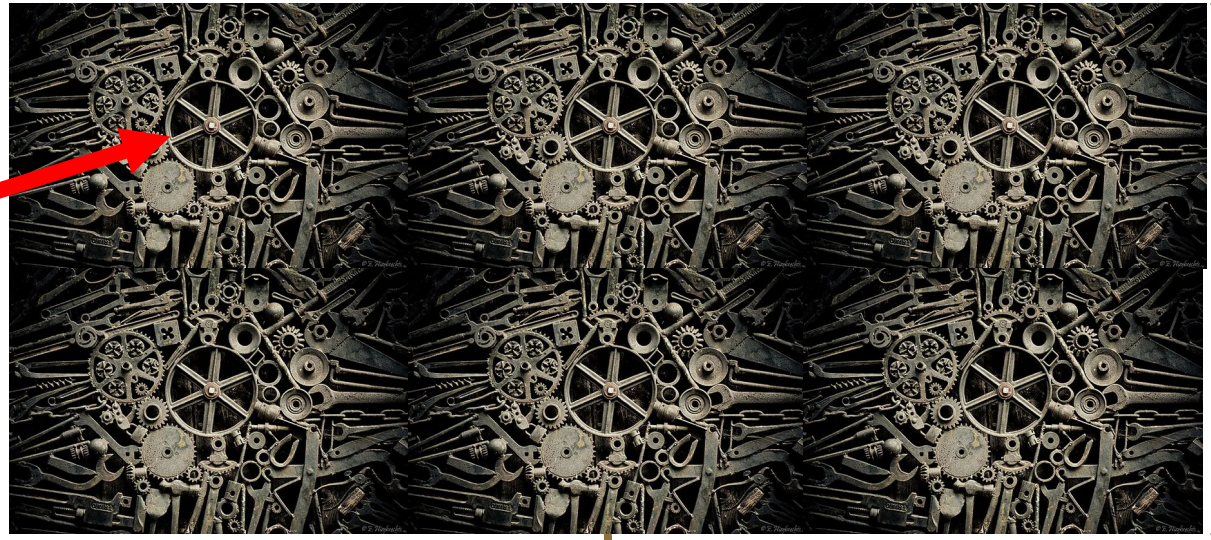


How might the engineers evade a charge of negligence?

Unit outline

- Why process?
- An introduction to “standardized” processes
- What the standards say
- Compliance and Certification

Why process?

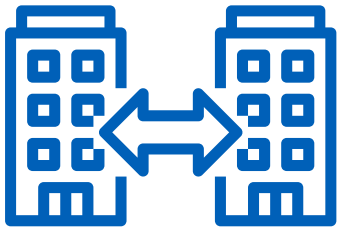


Yo
u

Your
company

Regulation
s

Your
company'
s product



Contractu
al
obligations

X

Consume
r

Sample regulatory language

Title 21 - Food and Drugs > Chapter I - Food and Drug Administration, Department of Health and Human Services > Subchapter H - Medical Devices > Part 820 Quality System Regulation

- Current good manufacturing practice (CGMP) requirements are set forth in this… regulation
- The requirements in this part are intended to ensure that finished devices will be safe and effective…in compliance with the Federal Food, Drug, and Cosmetic Act.
- This part establishes basic requirements applicable to…finished medical devices
  - Each manufacturer shall establish and maintain procedures to ensure that the design requirements relating to a device are appropriate and address the intended use of the device
  - Each manufacturer shall establish and maintain procedures to ensure that the device design is correctly translated into production specifications.
  - Each manufacturer shall establish and maintain a design history file (DHF) for each type of device. The DHF shall contain or reference the records necessary to demonstrate that the design was developed in accordance with the approved design plan and the requirements of this part

IEC 62304: Medical Device Software – Software Life Cycle Processes

Contractual obligations

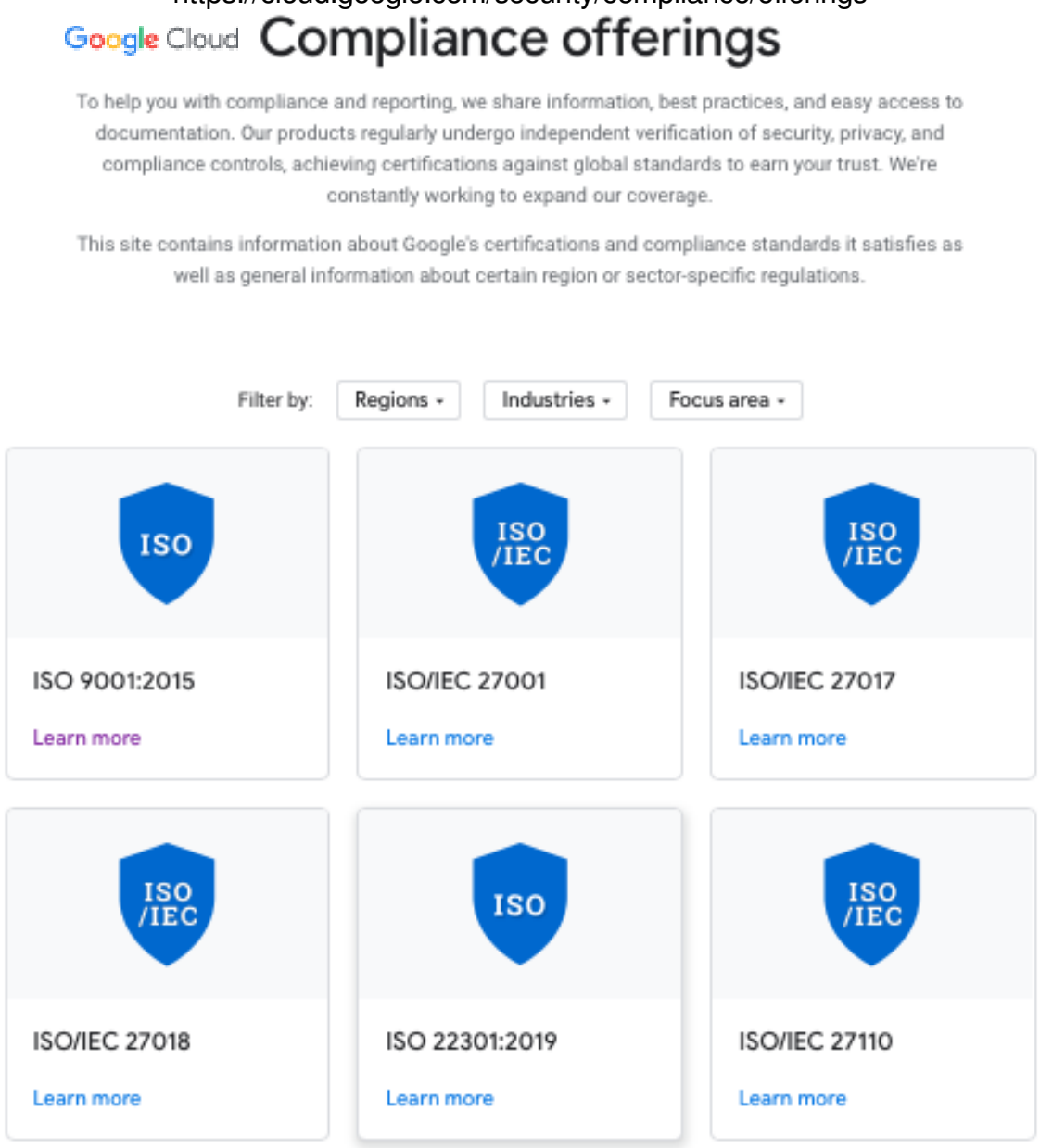
"Company A will purchase a software component from Company B, provided they achieve an ISO 26262 certificate stating that the component is suitable for use in items to be certified to Automotive Safety Integrity Level C"

https://docs.windriver.com/bundle/mbl1526506718501/page/ilk1526508640058.html

WindRiver's VxWorks

"This release adds compliance with IEC and ISO evidence, and an update to DO-178 evidence. There are no software updates for this release"

https://cloud.google.com/security/compliance/offerings

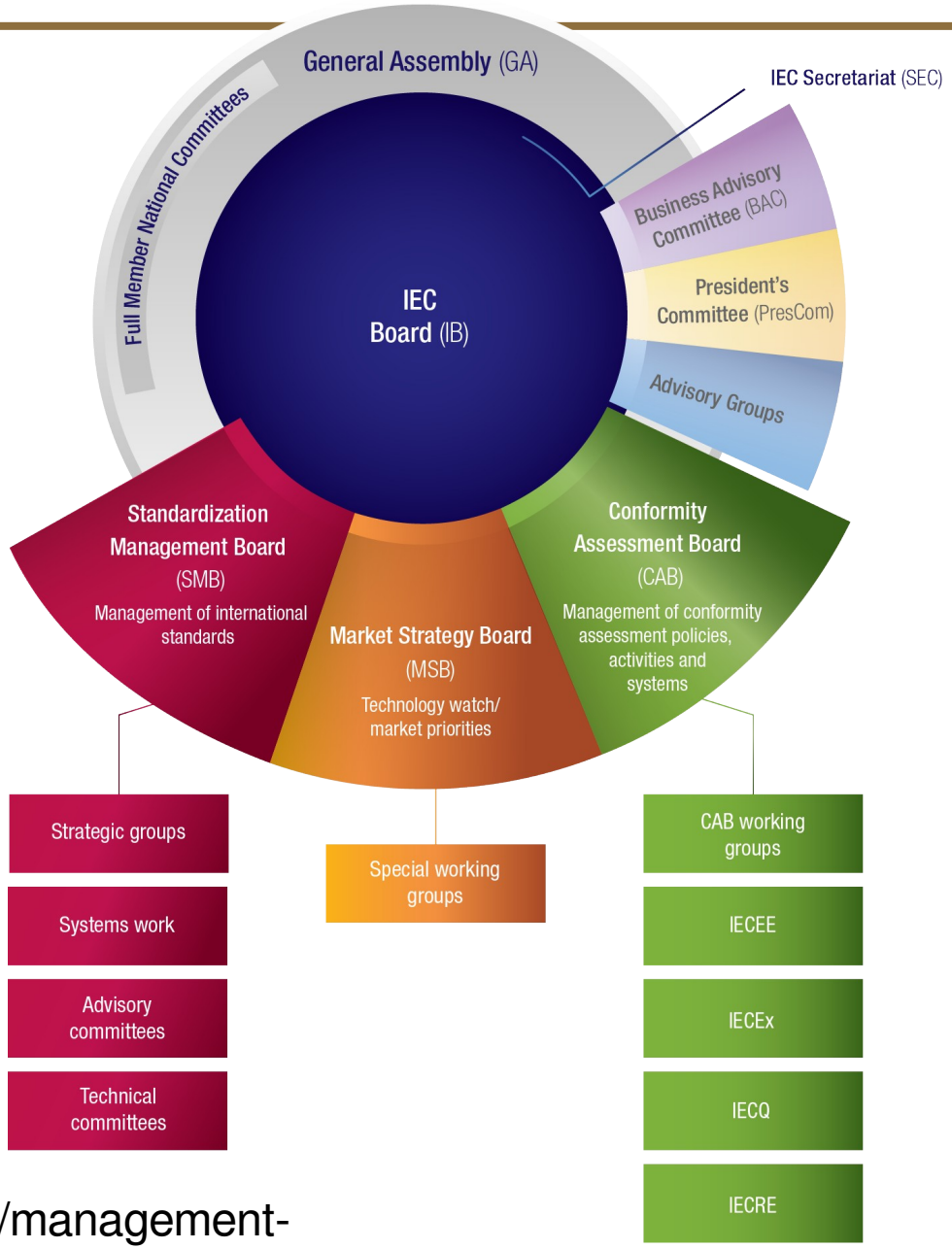


Liability and Negligence

- ”A design which departs substantially from relevant engineering codes is prima facie a faulty design unless it can be demonstrated that it conforms to accepted engineering practice by rational analysis”
  - Ruling in the case of Bevan Investments v Blackhall and Struthers, 1973, New Zealand

The standards

How a standard gets developed



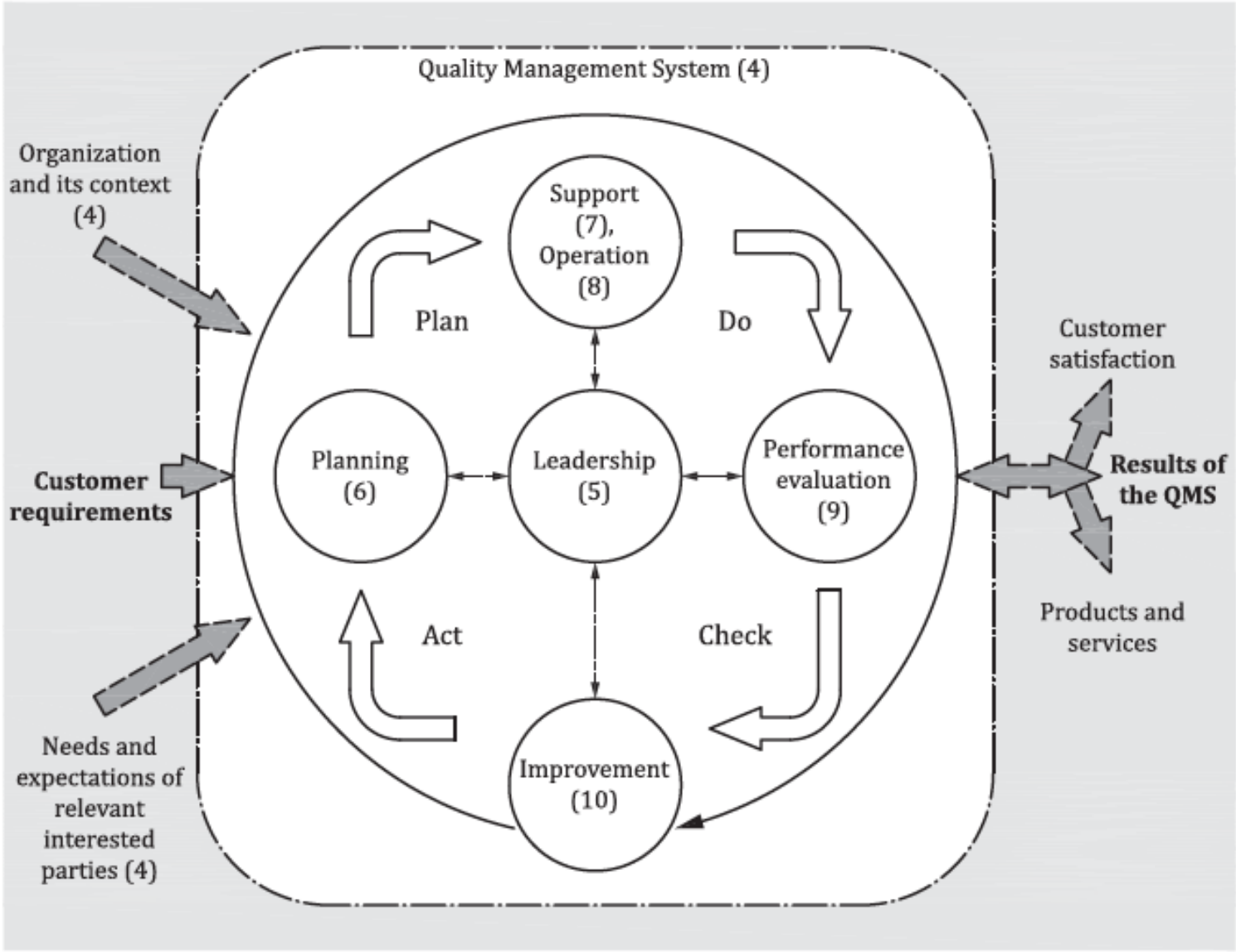
https://www.iec.ch/management-structure

What kinds of standards are there?

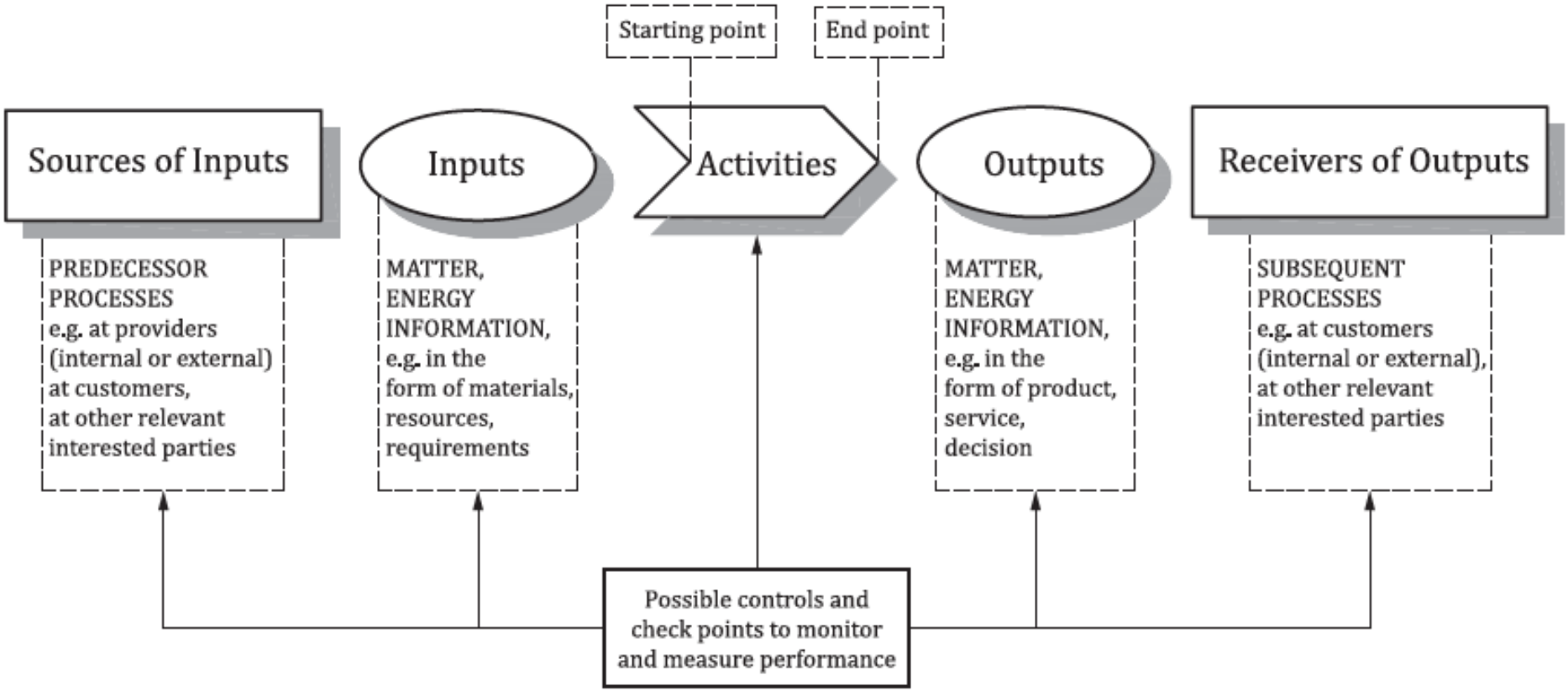
- Prescriptive standards
- Goal-based standards

What the standards say

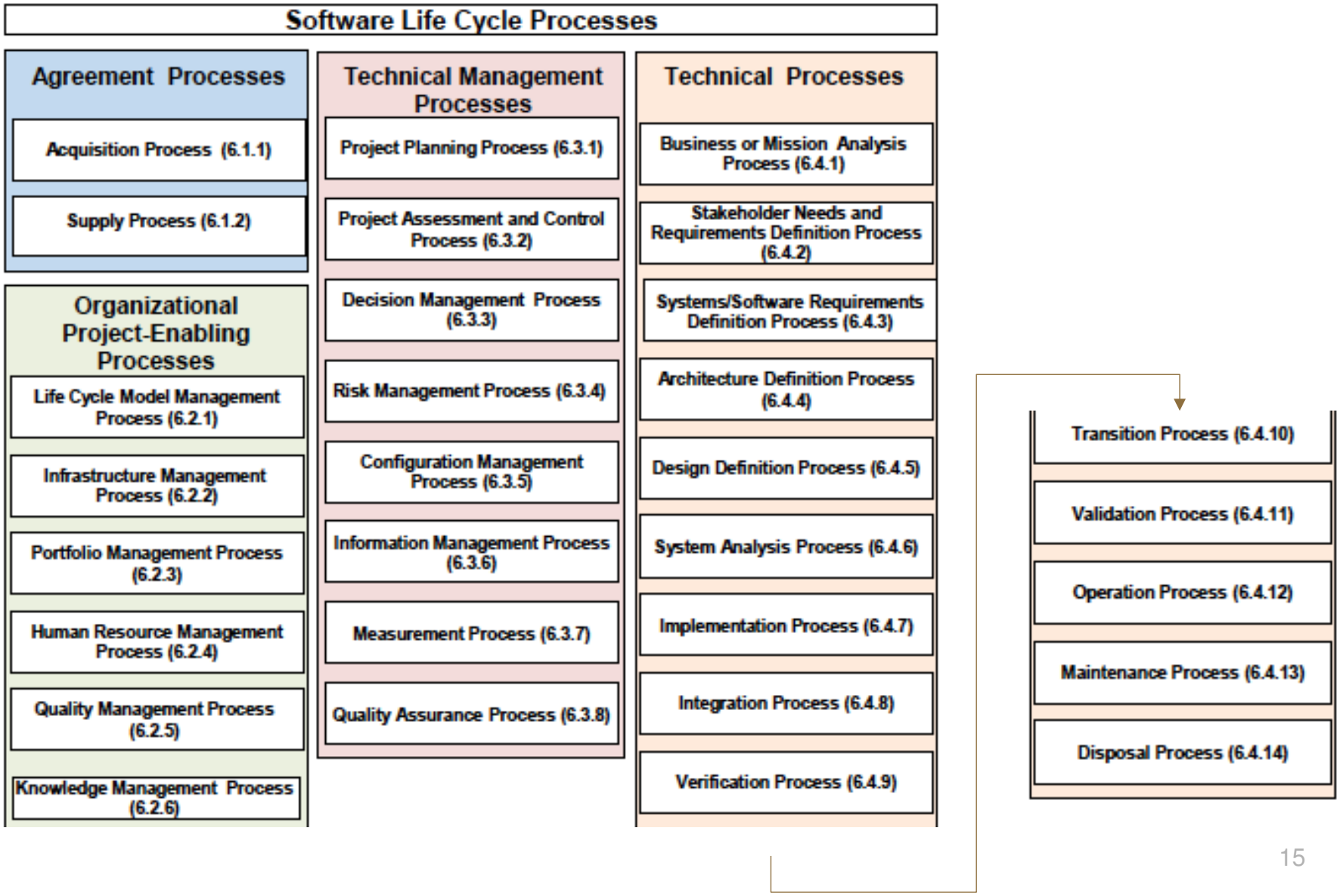
General quality process (ISO 9001/90003)



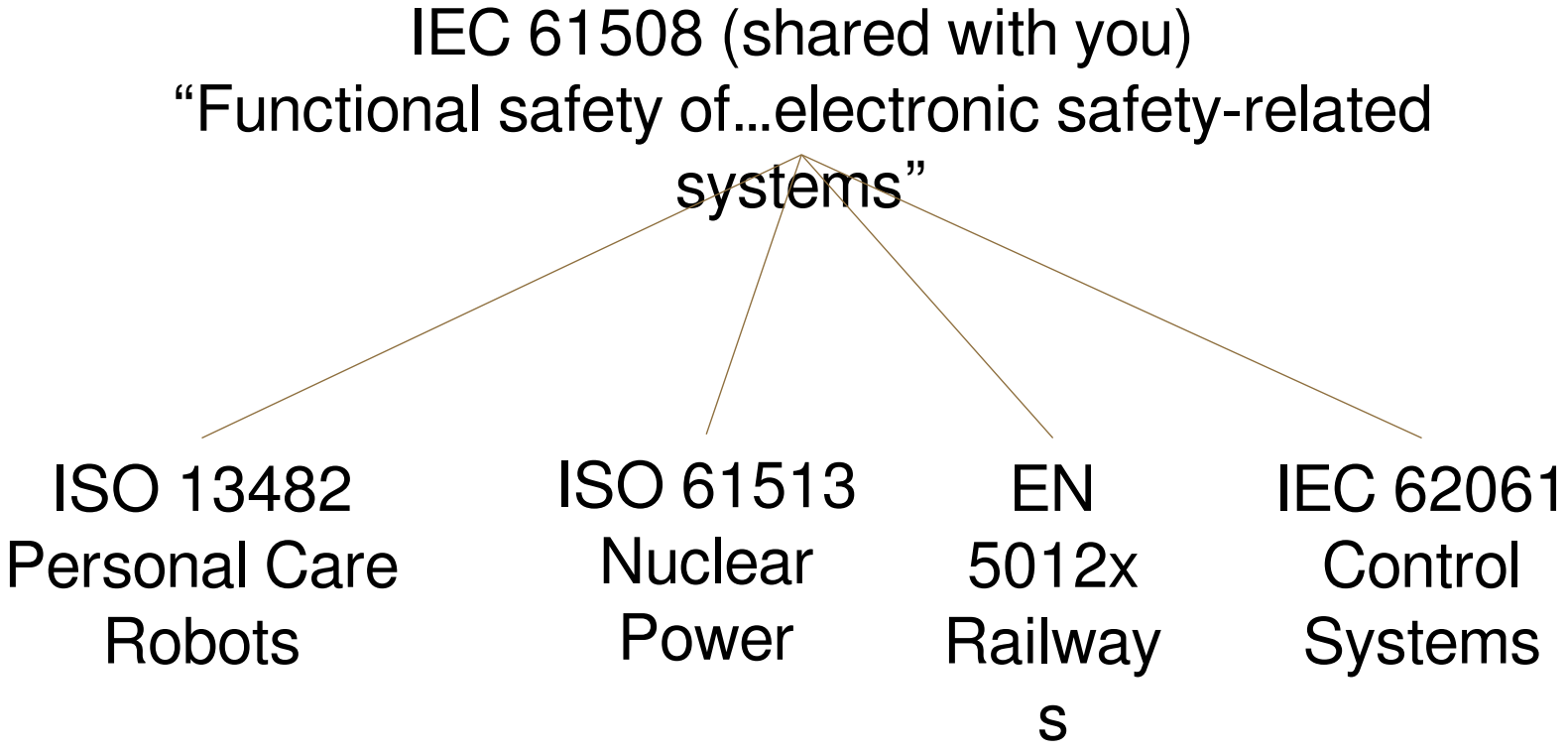
General quality process (ISO 9001/90003)



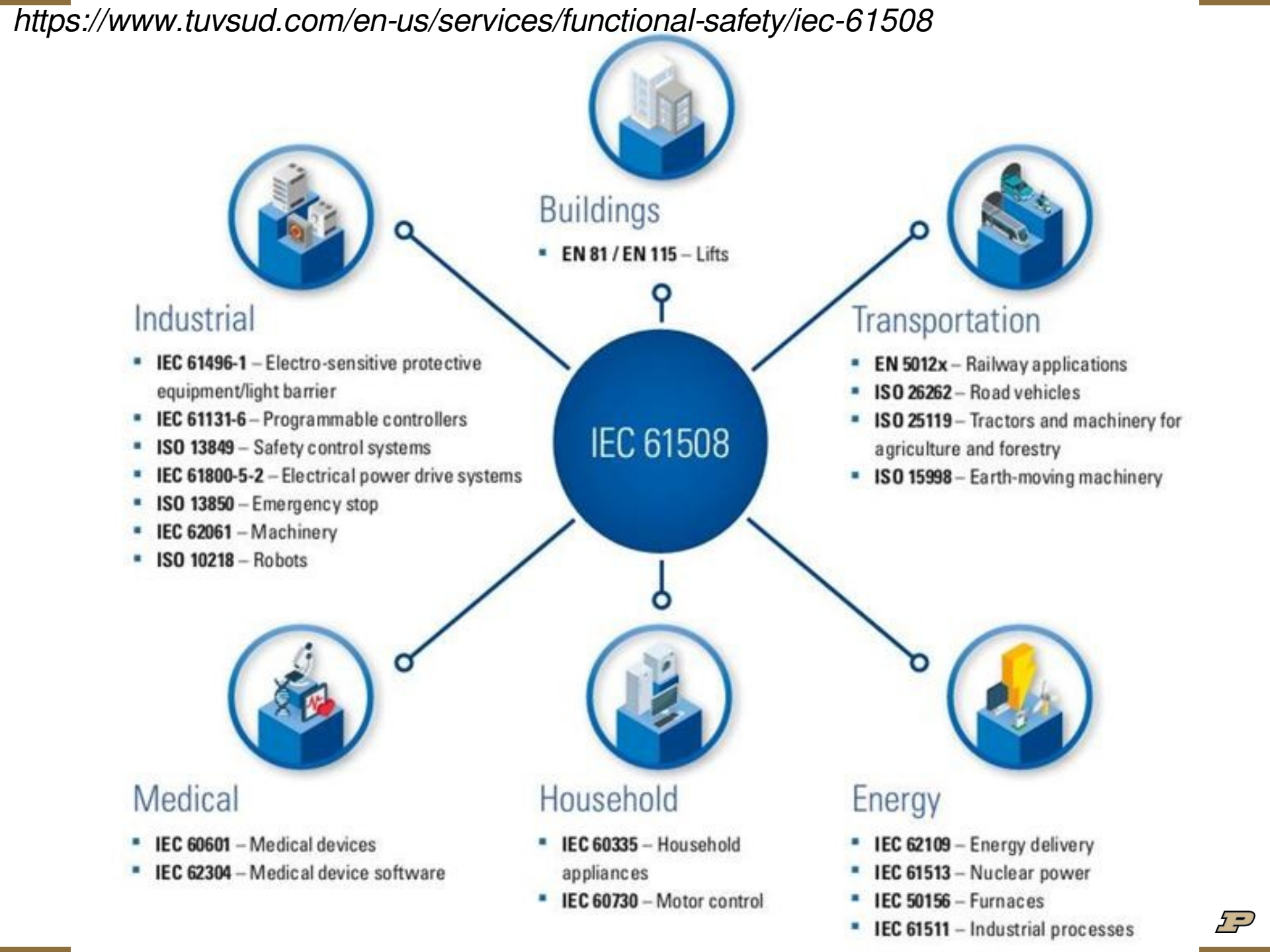
Sub-processes in the software life cycle (IEEE 12207)



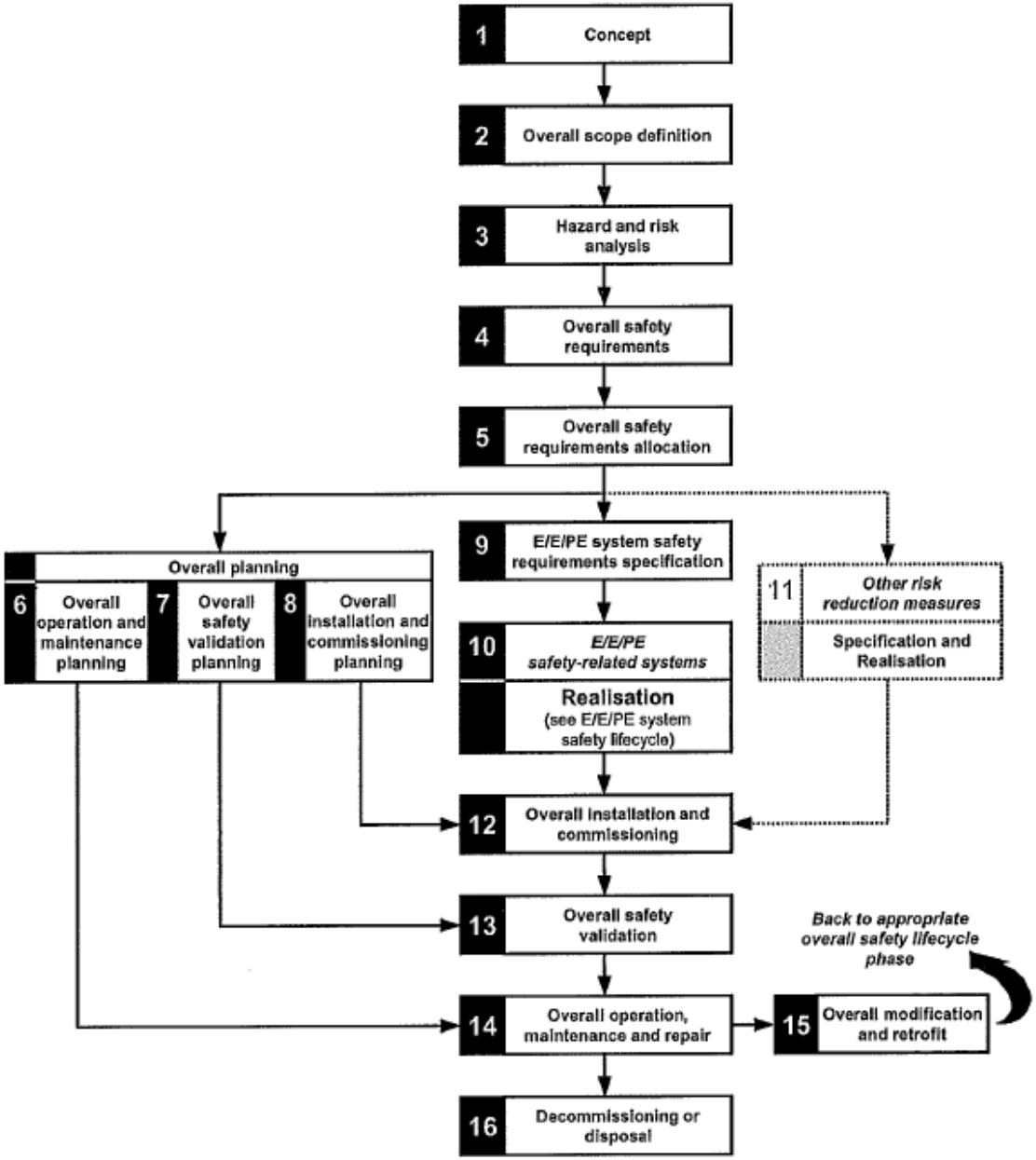
Safety processes (IEC 61508 and friends)



https://www.tuvsud.com/en-us/services/functional-safety/iec-61508



Safety processes (IEC 61508 and friends)



Compliance and Certification

Behold, a certificate https://www.ti.com/lit/fs/szzq188c/szzq188c.pdf?ts=1705628931703

CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Q4B 088989 0008 Rev. 03

Holder of Certificate: **Texas Instruments**
12500 TI Boulevard
Dallas TX 75243
USA

Factory(ies): **Texas Instruments**
12500 TI Boulevard, Dallas TX 75243, USA

Certification Mark:

Scope of Certificate: **Functional Safety Software Development**

Applied Standard(s):
IEC 61508-1:2010
IEC 61508-3:2010
ISO 26262-2:2018
ISO 26262-6:2018
ISO 26262-8:2018

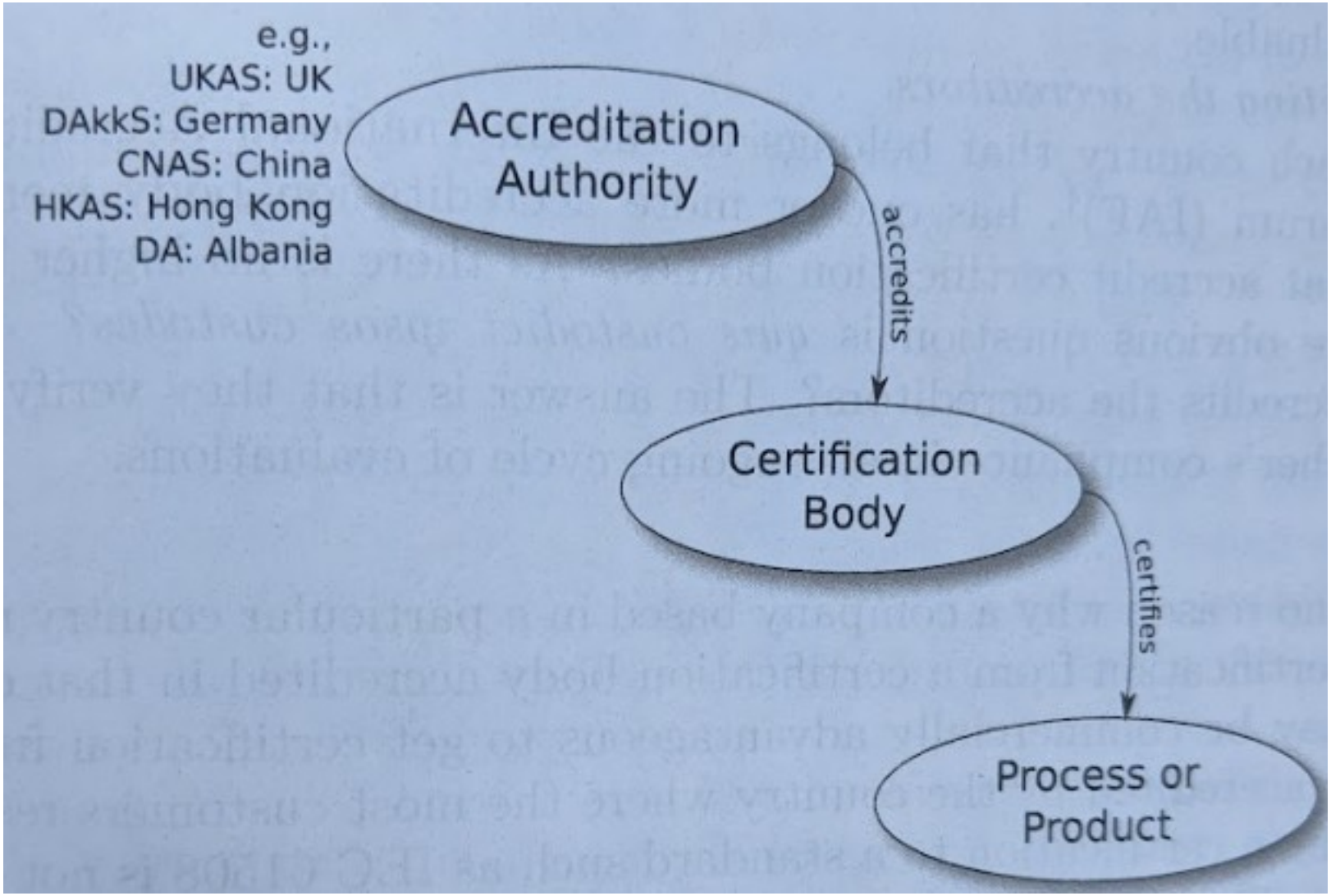
The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. For details see: www.tuvsud.com/ps-cert

Report No.: **TG93754T**

Valid until: 2025-06-23

Date, 2023-08-31

(Peter Weiß)



Hobbs 2019, "Embedded software development for safety-critical

Auditing compliance

Software Lifecycle Phase	% Compl.
A1 Software Requirements Specification	33
A2 Software Architecture Design	25
A3 Software Design and Development - Support Tools and Programming Language	45
A4 Software Detailed Design	25
A5 Software Module Testing and Integration	31
A6 PE Integration (Hardware + Software)	0
A7 Software Validation	17
A8 Modification	20
A9 Software Verification	20
Overall average compliance	24

Lloyd & Reeve, 2008. *IEC 61508 and IEC 61511 Assessments – some Lessons*

Discuss

- What risks does “having a standards-compliant process” mitigate?
- What risks does “having a standards-compliant process” not mitigate?
- How might you measure the value of a standard?
- Is it acceptable for an engineer to ignore organizational quality standards if they deliver working code?