

Demiryollarında Fonksiyonel Emniyet ve SIL Sertifikasyonu

TÜV Teknik Kontrol ve Belgelendirme A.Ş.
Ayhan Levent Arslan
(Fonksiyonel Emniyet Uzmanı, EN 15085 Denetçisi)
Levent.arslan@tuv-turkey.com, [+90 536 603 0390](tel:+905366030390)

Demiryollarında Fonksiyonel Emniyet ve SIL Sertifikasyonu

- TÜV NORD; yetkinlik, hizmet ve referanslarımız,
- Avrupa Birliği direktifi, yönetmelikleri, standartları ve emniyet,
- Emniyet, fonksiyonel emniyet,
- SIL Sertifikasyonu; amacı, anlamı, kapsamı,
- SIL sertifikasyon süreçleri,
- ISA rapor ve SIL sertifikasyonu arasındaki ilişki,
- Değerlendirici yetkinliği,

*SIL (*Safety Integrity Level*): Emniyet Bütünlük Seviyesi

**ISA (*Independent Safety Assessor*):Bağımsız Emniyet Değerlendirici



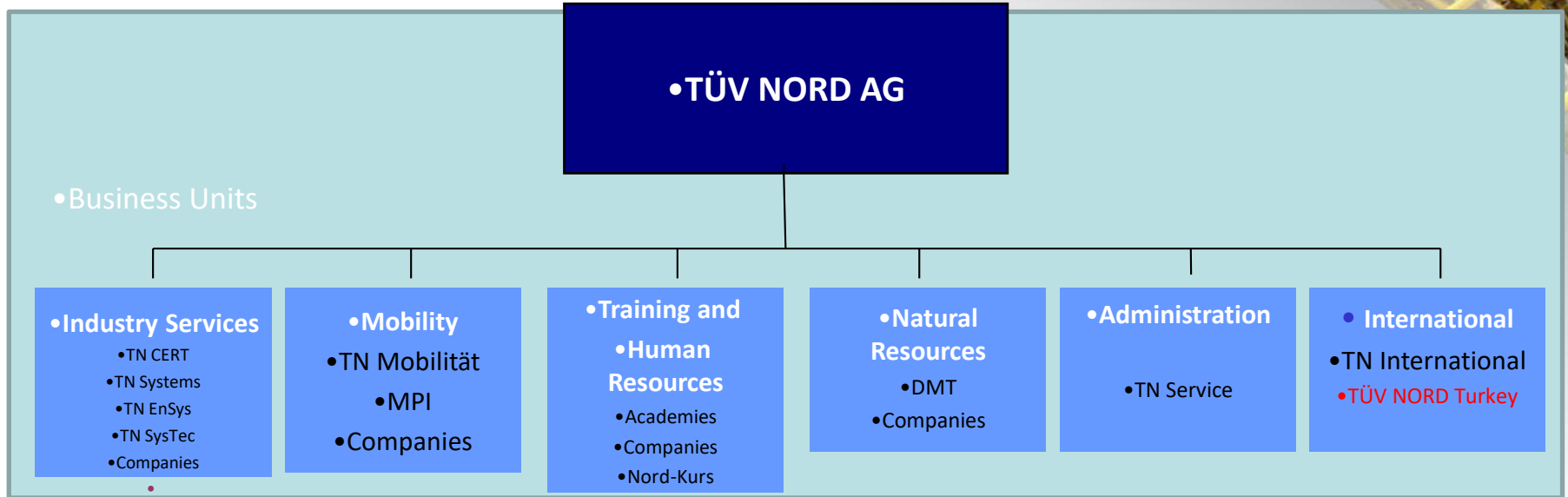
TÜV NORD Group



TÜV NORD

•TÜV NORD Group, 70'i aşkın ülkede ulusal ve uluslararası müşterilerine hizmet vermektedir.

TÜV NORD Group'un Yapısı



- TÜV NORD Türkiye'nin kuruluşu: 1994
- TÜV NORD Çalışan sayısı: 70 ülkede
- 11 binden fazla çalışan

- Birleşme:
- TÜV Nord e.V.: 1869
- RWTÜV e.V.: 1872
- TÜV Hannover/Sachsen-Anhalt e.V.: 1873



TÜV NORD Group'un Hizmet Alanları

- Sertifikasyon
- Malzeme kontrolleri
- Yenilenebilir enerji
- Nükleer enerji santralleri
- **Demiryolu teknolojileri**
- Basınçlı kaplar ve buhar kazanları
- Sağlık sektörü
- Havacılık sektörü
- Hammadde sektörü
- Motorlu taşıtlar
- Madencilik
- Çevresel uyum
- İş sağlığı ve iş güvenliği
- Bilişim teknolojileri



TÜV NORD Demiryolu Departmanı

Akreditasyon ve Yetkinlikleri



- ISO EN 17020 ve ISO 17065 akreditasyonlarına sahip,
 - 2016/797 (*2008/57/EC*) direktifine (TSI) göre *NoBo* (Notified Body: Onaylı Kuruluş),
 - ECWRV *MCB* (Manufacturer Certification Body-EN15085),
 - EBA (Alman Ulusal Emniyet Otoritesi) akreditasyonlu *test laboratuvarı-DeBo*,
 - ERA (Avrupa Birliği Demiryolu Ajansı) tarafından onaylı *ISA* (Bağımsız Emniyet Değerlendirici) – *AsBo* kuruluşudur.
- ❖ EBA, ERA ve ECWRV onaylı demiryolu uzmanları.



TÜV NORD Demiryolu Departmanı

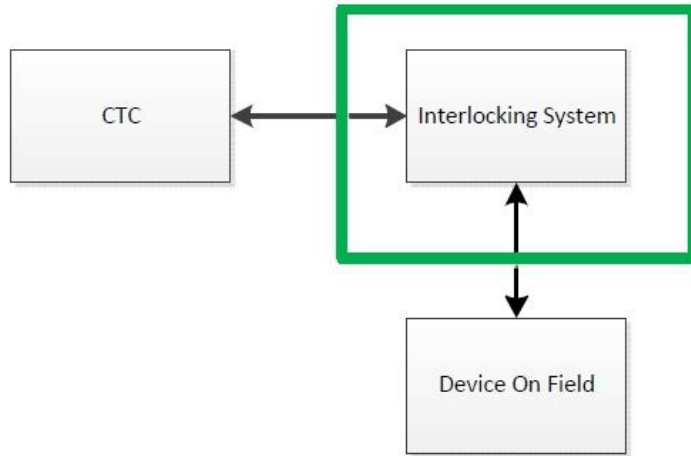
Faaliyet Alanları



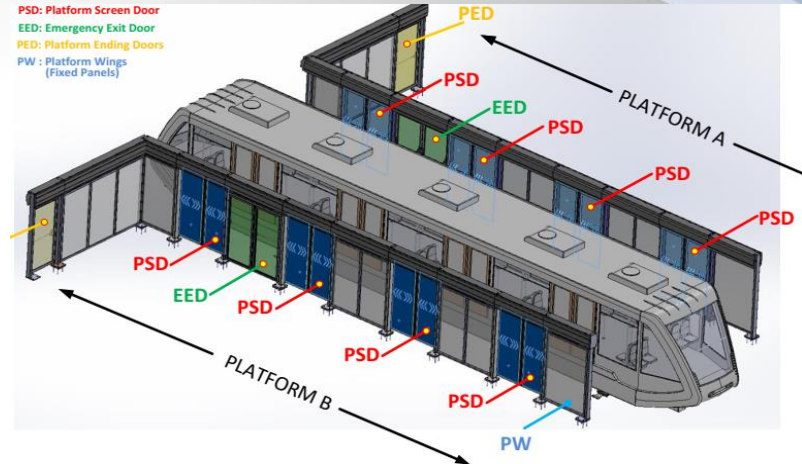
- ❖ TSI (Technical Specification for Interoperability) sertifikasyonu
- ❖ SIL (Safety Integrity Level) sertifikasyonu
- ❖ EN 15085-2, EN 3834-2,3, DIN 27201-6
- ❖ ECM (Entirety of Charge of Maintenance)
- ❖ SPVD (Simple Pressure Vessel Directive)' ye göre CE markalaması.
- ❖ RID (Demiryolu ile tehlikeli madde taşınması)'a göre Pi markalaması.
- ❖ NDT (Non-Destructive Testing) hizmetleri
- ❖ IRIS belgelendirilmesi
- ❖ Eğitim (functional safety) ve teknik destek



TÜV NORD Türkiye SIL/ISA Referans Projeleri



Yerli Anlaşman (Interlocking) Sistemi

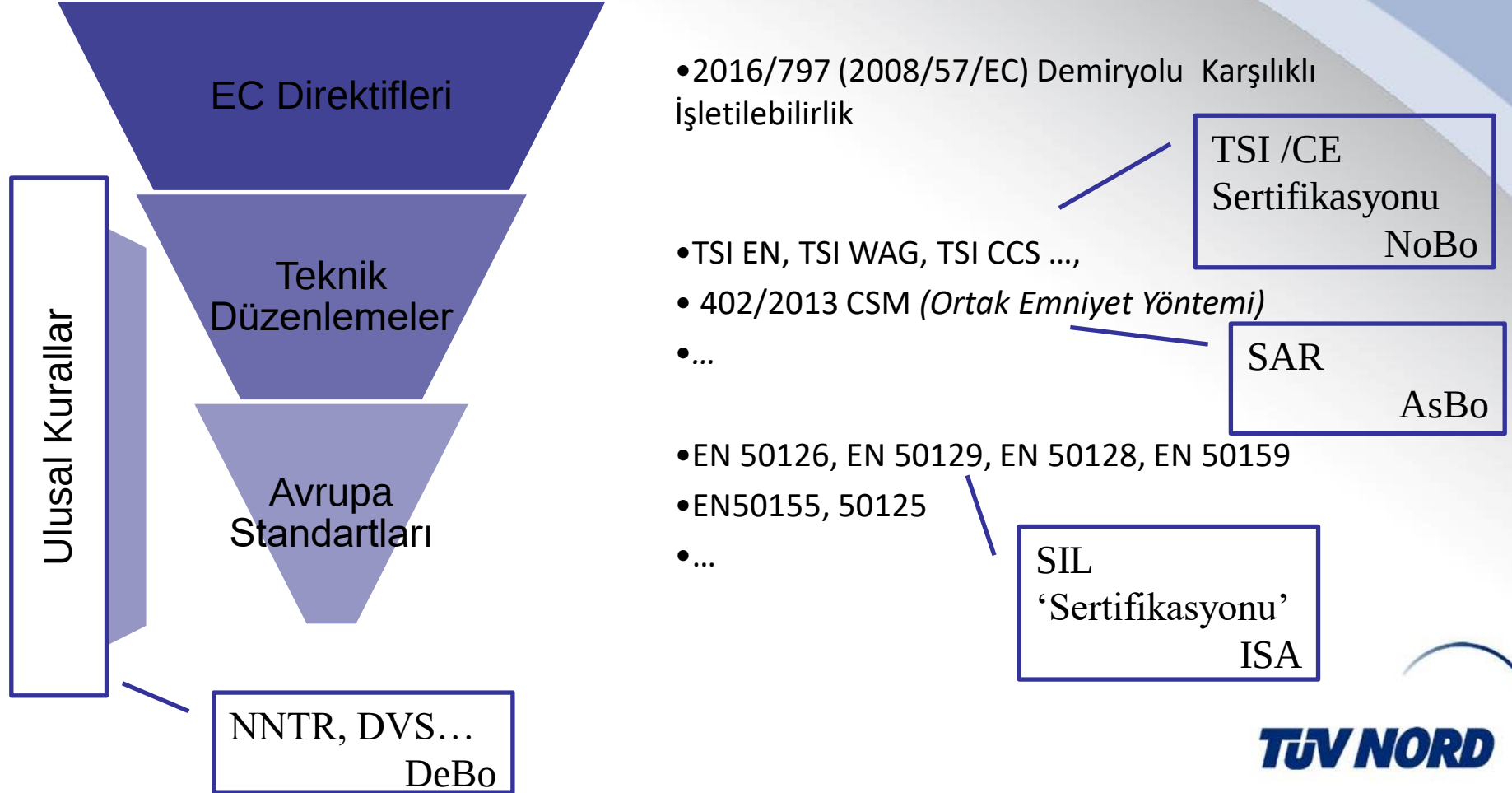


Yerli Peron Ayırıcı Kapı Sistemi (PSD)

- ✓ Kontrol üniteleri ve sürücüler (DCU, ECU...)
- ✓ Sinyalizasyon saha ekipmanları (Ray devresi, sinyal lambası...)
- ✓ Sinyalizasyon sistemleri (Anlaşman, Makas kontrol sistemleri, park alanı kontrol sistemi...)

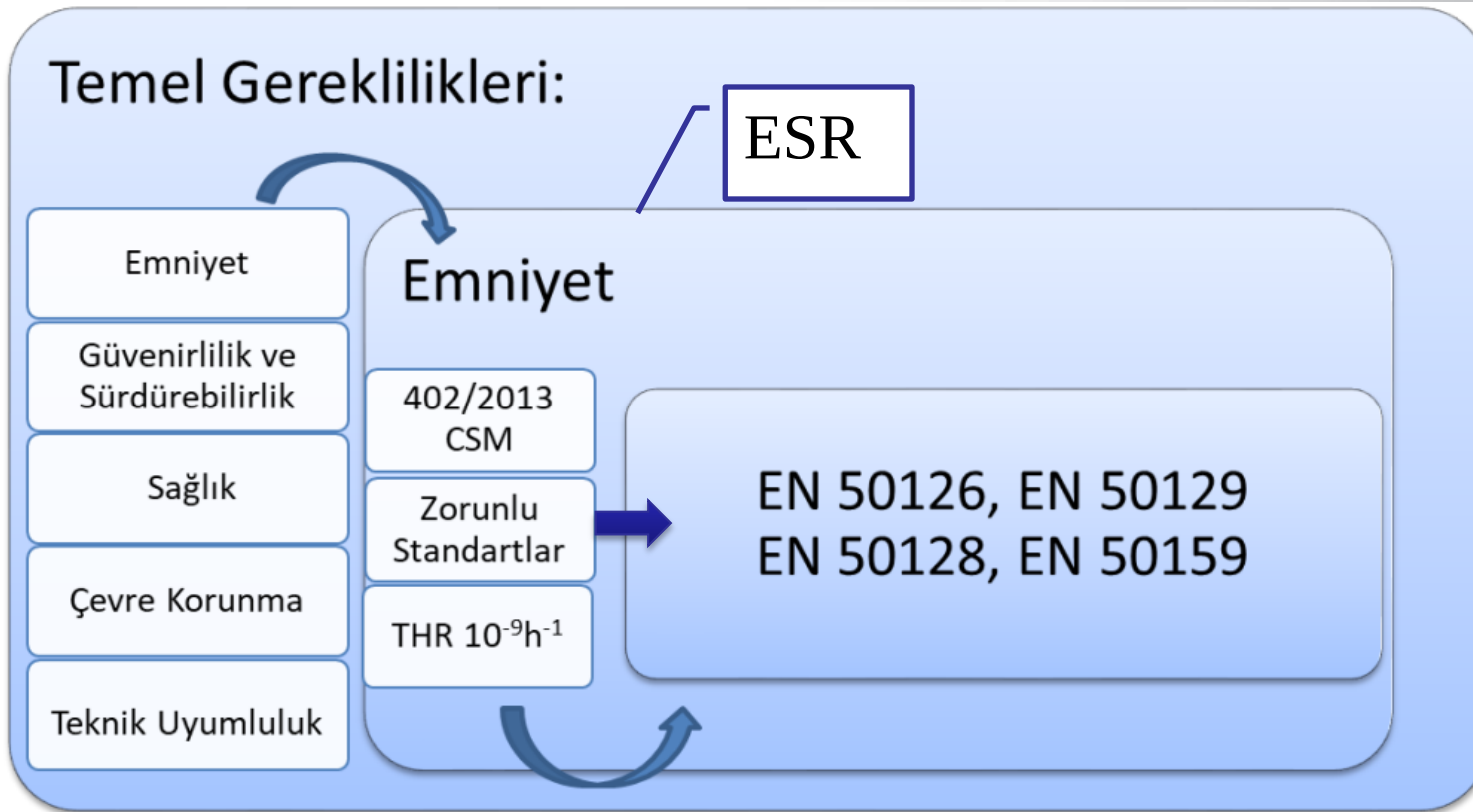
EC(Avrupa Birliği) Hiyerarşisi

Demiryollarının daha güvenli olabilmesi için direktifler, düzenlemeler ve standartlar oluşturulmuş ve temel emniyet gereklilikleri (ESR) belirlenmiştir.



TSI CCS / ESR / THR / EN 5012X

TSI CCS, temel gereklilikleri 5 ana başlık altında sınıflandırır;



*THR: Kabul edilebilir hata oranı *ESR: Temel Emniyet Gereklilikleri

*CSM: Ortak Emniyet Yöntemi *CCS: Kontrol Kumanda Sinyalizasyon

Zorunlu Standartlar / EN 5012X

SIL

No	Reference	Document name and comments	Version	Note
A1	EN 50126	Railway applications — The specification and demonstration of reliability, availability, maintainability and <u>safety</u> (RAMS)	1999	1
A2	EN 50128	Railway applications — Communication, signalling and processing systems — <u>Software</u> for railway control and protection systems	2001 or 2011	
A3	EN 50129	Railway applications — Communication, signalling and processing systems — Safety related <u>electronic systems</u> for signalling	2003	1
A4	EN 50159	Railway applications — <u>Communication</u> , signalling and processing systems	2010	1

2017

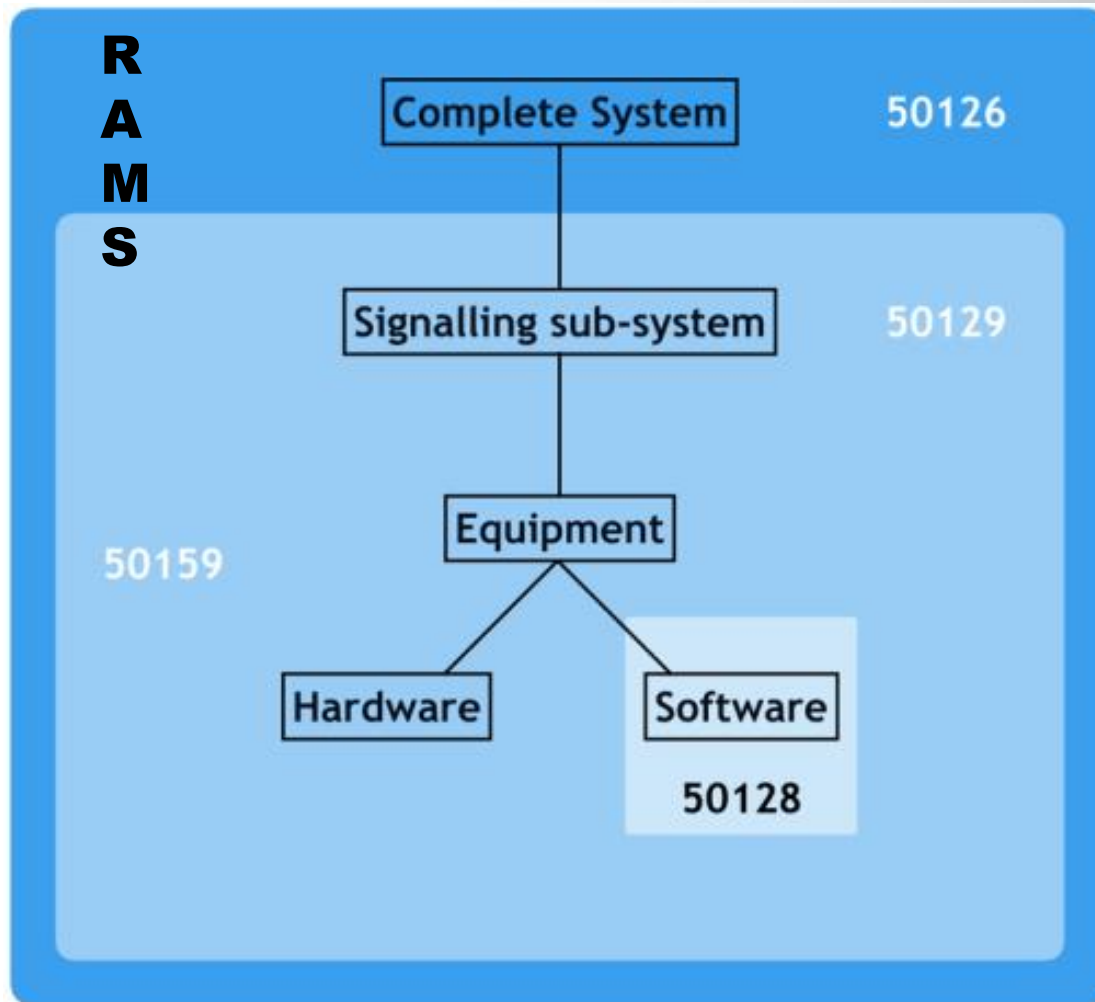
2018

Note 1: this standard is harmonised, see Commission communication in the framework of the implementation of the Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (OJ C 345, 26.11.2013, p. 3), where also published editorial corrigenda are indicated.

*2016/919/EU TSI CCS Tablo A3

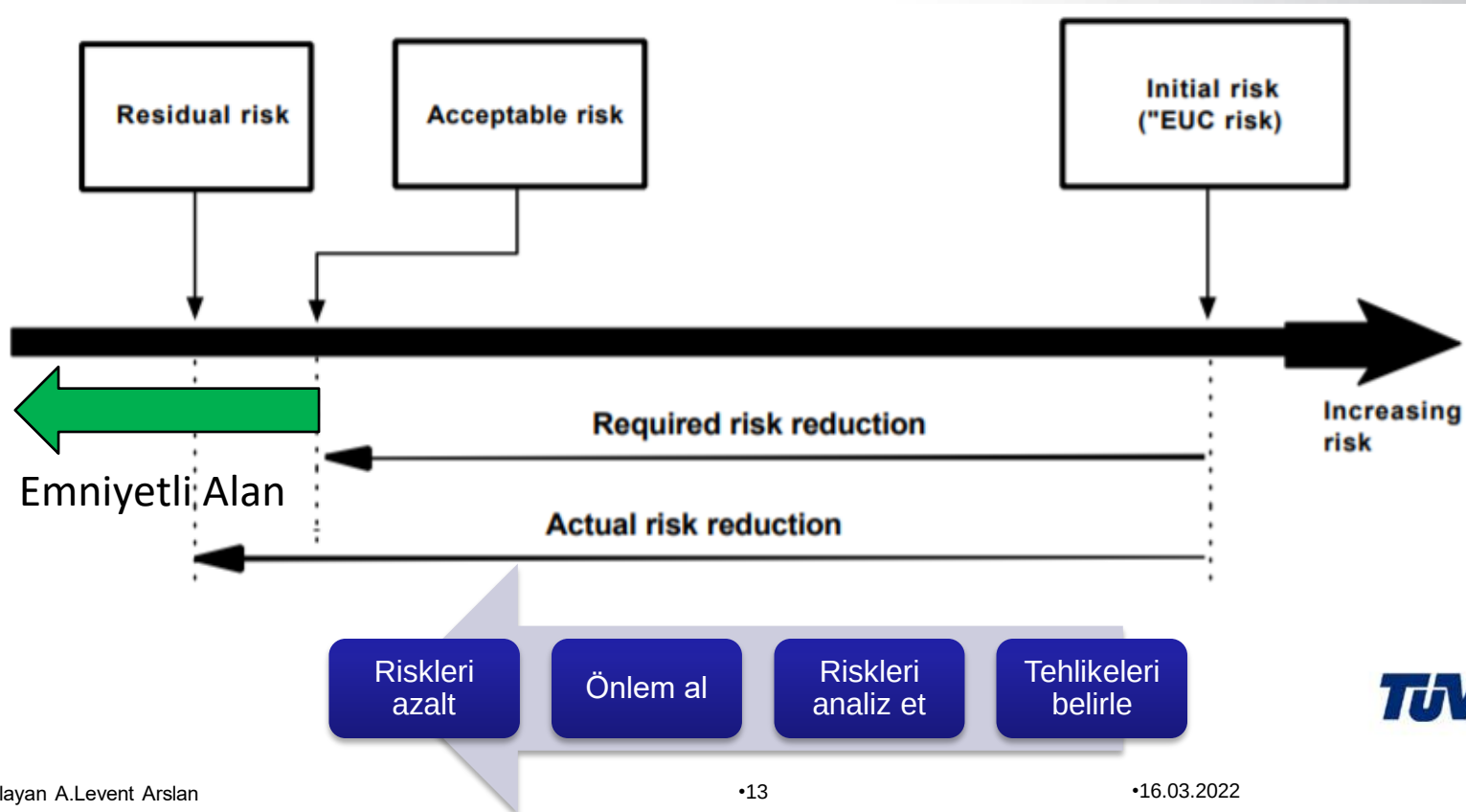


Zorunlu Standartlar / EN 5012X

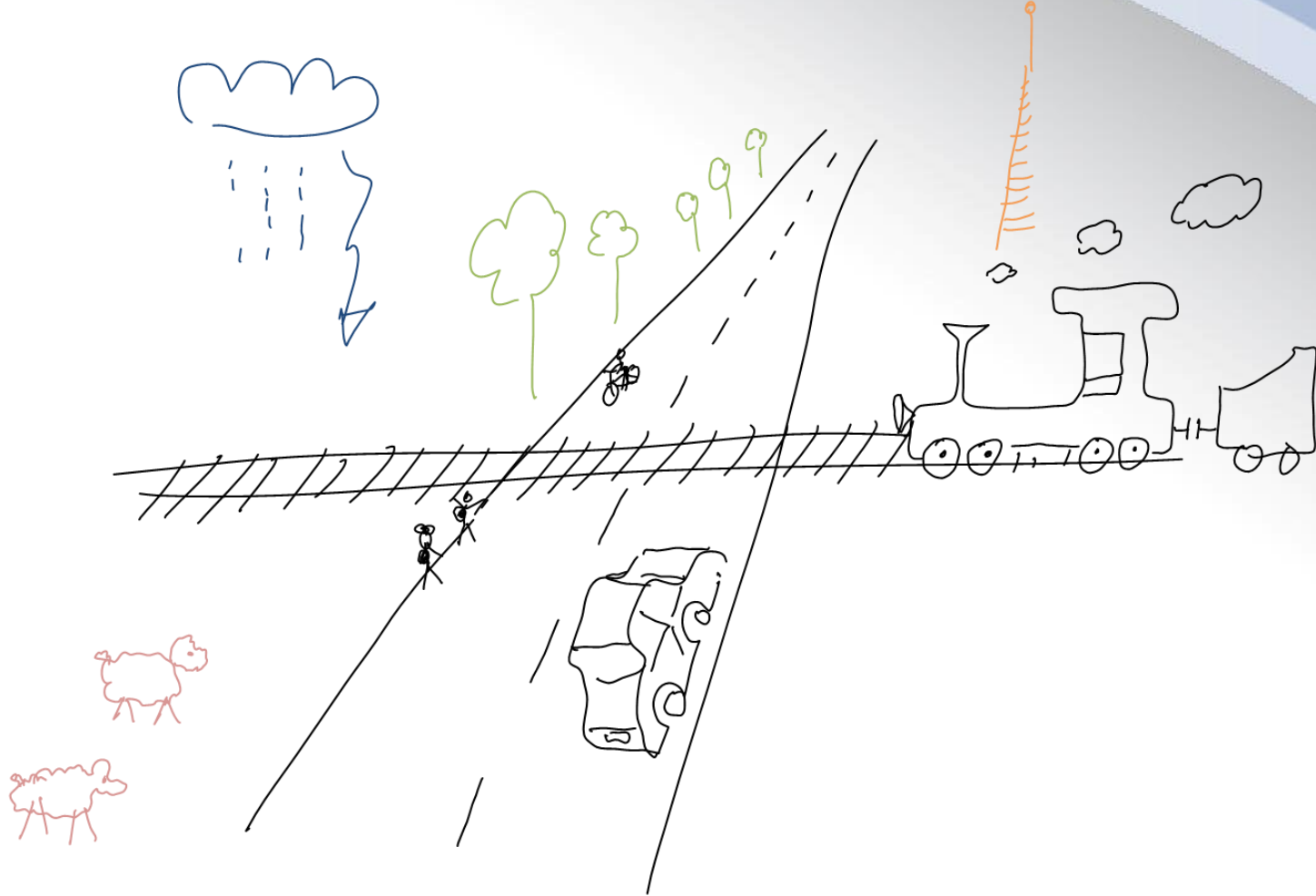


Emniyet, Fonksiyonel Emniyet, SIL?

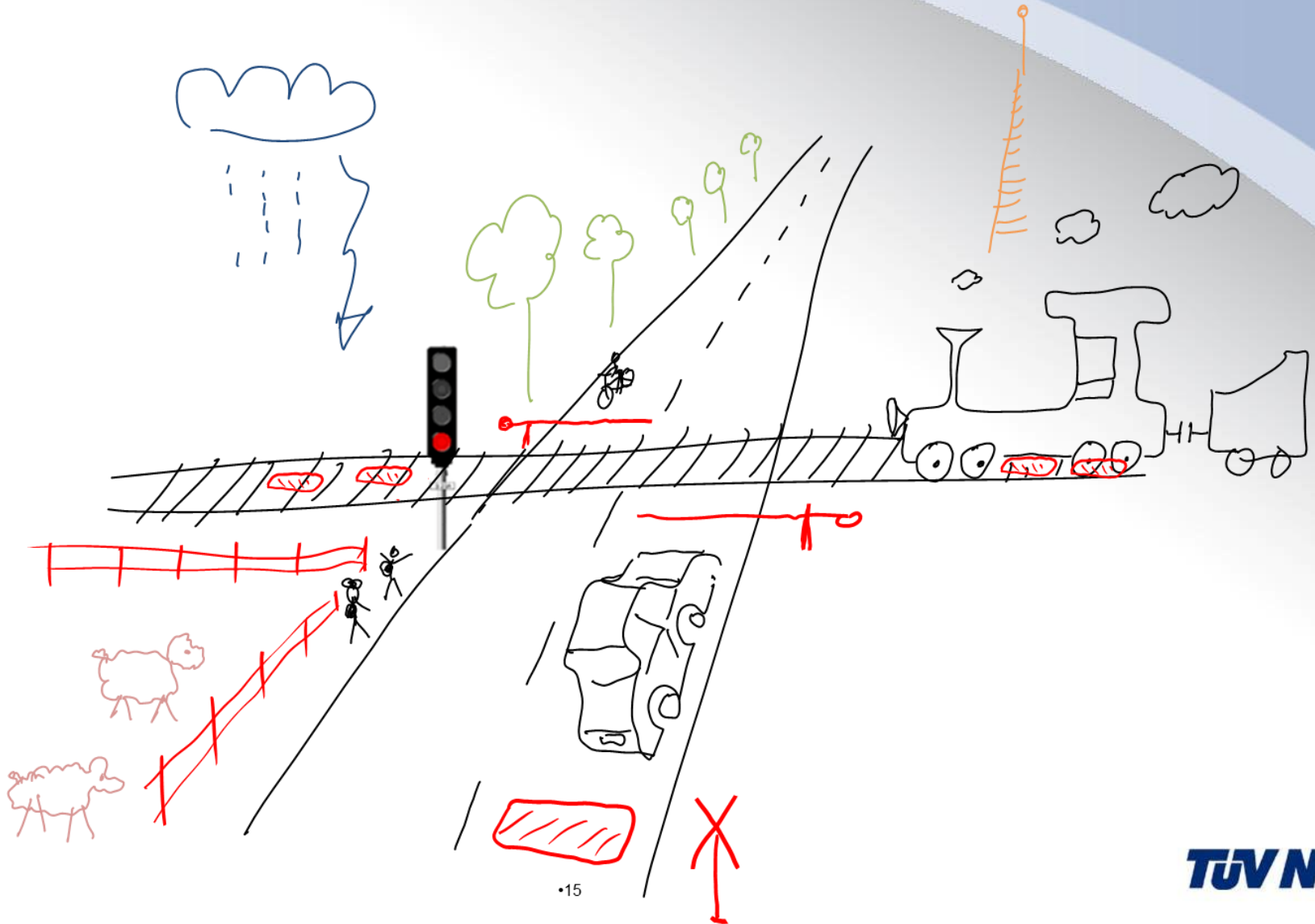
- Emniyet: kabul edilemez bir riskin bulunmaması. (EN50129:2018 3.1.40)



Örnek- Hem Zemin Geçit

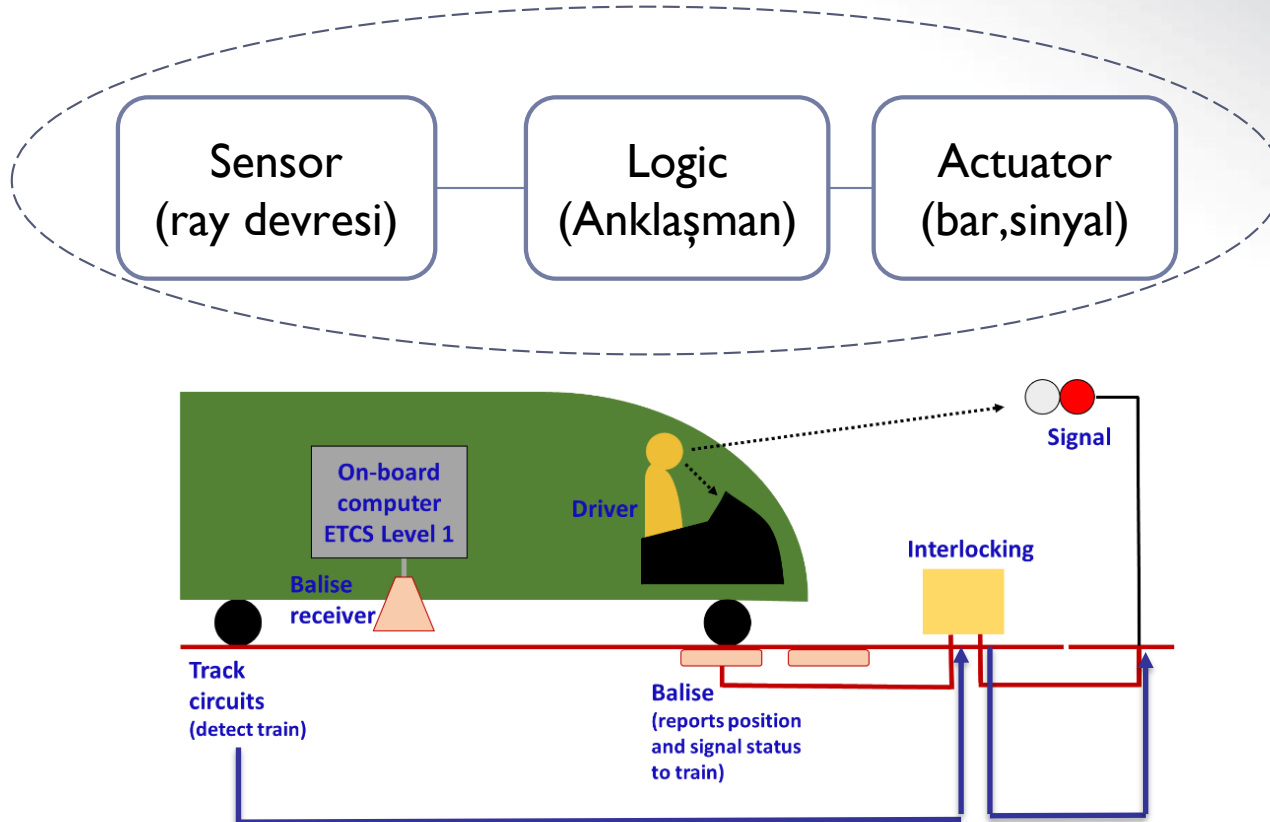


Örnek- Hem Zemin Geçit

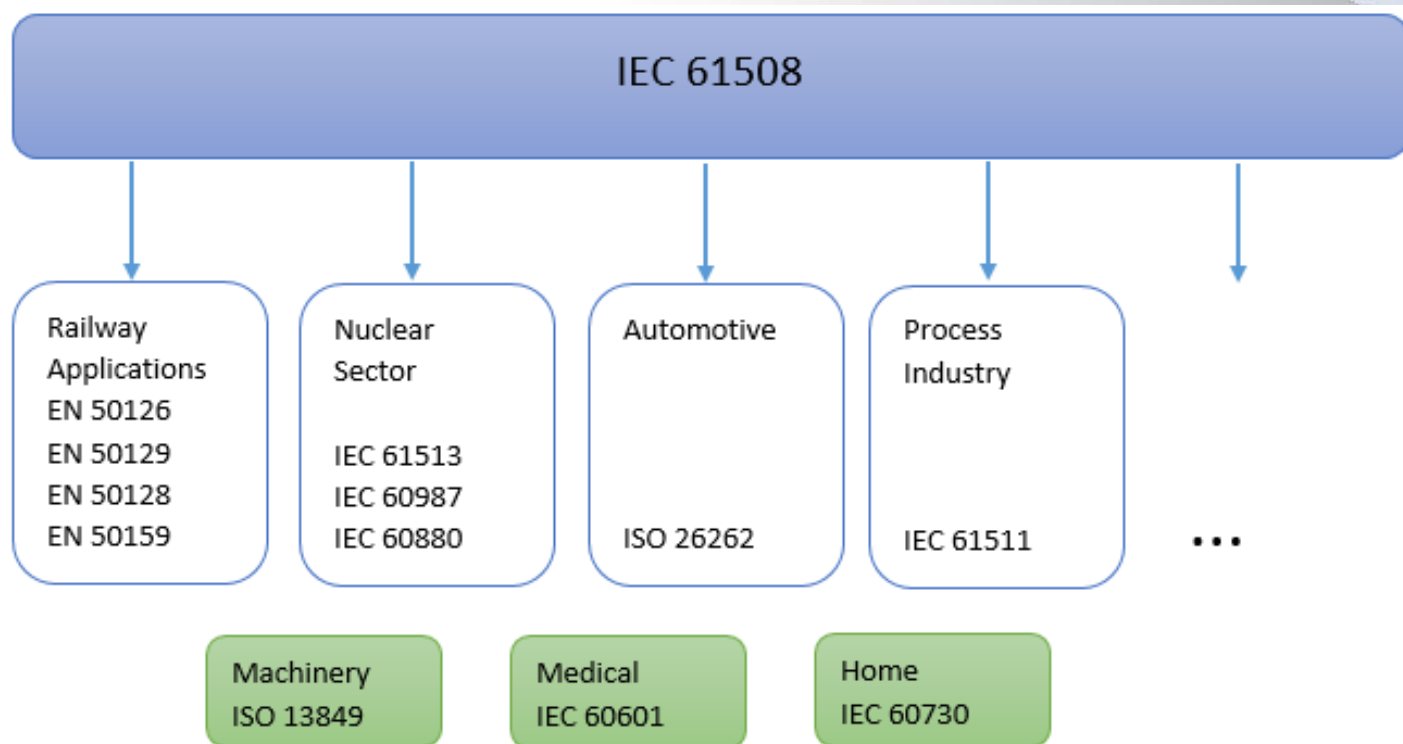


Emniyet, Fonksiyonel Emniyet, SIL?

- Fonksiyonel Emniyet: E/E/PE (Electric/Electronic/Programmable Electronic) sistemlerini kullanarak riski azaltan fonksiyonlar.



Sektörler ve Fonksiyonel Emniyet Standartları



❑ Yeşil kutular IEC 61508'den türetilmemiştir.

Fonksiyonel Emniyet Standartlarının Prensipleri

- Risk odaklı
- Risk azaltma
- Fonksiyonel emniyetin yönetimi
- Yaşam döngüsü (lifecycle) odaklı
- Emniyet ilgili fonksiyonların tanımı
- Emniyet seviyesinin tanımı (SIL, ASIL, PL)
- Nicel (quantitative) gereklilikler (olasılık)
- Niteliksel (qualitative) gereklilikler (arızadan kaçınma)

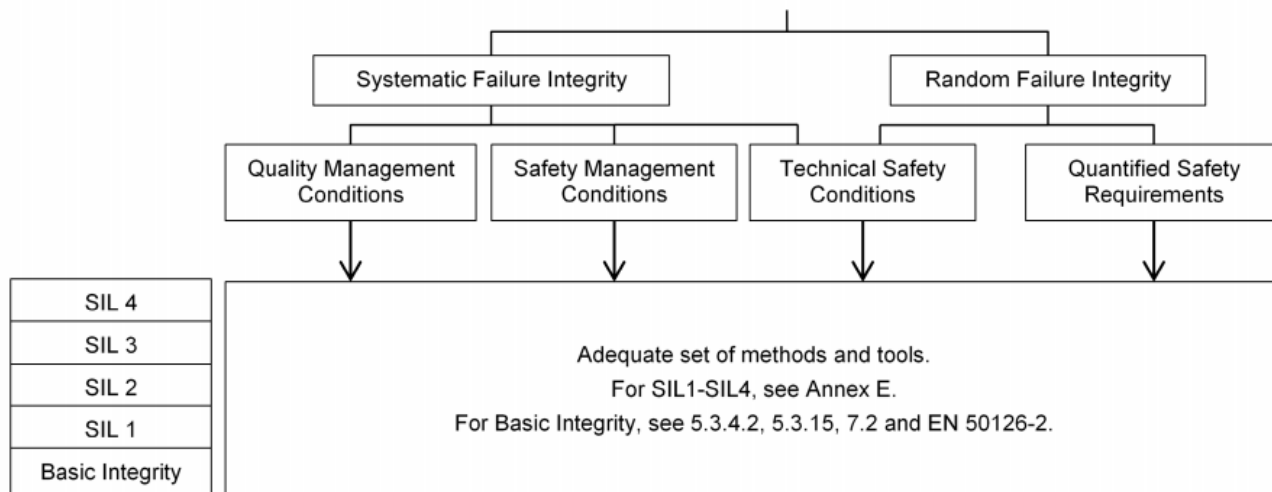
Emniyet, Fonksiyonel Emniyet, SIL?

- Emniyet Bütünlük Seviyesi (SIL: **S**afety **I**ntegrity **L**evel); emniyet fonksiyonlarının **güvenirlilik seviyesini** tanımlar. Bir emniyet fonksiyonu için gerekli en düşük güvenirlilik seviyesi **SIL 1** en yüksek **SIL 4** olarak dört sınıfta tanımlanmıştır.

SIL tanımı;

- sadece* E/E/PE sistem / alt sistem / ekipmanları kapsar,
- sadece emniyet ile ilgili fonksiyonları içindir,
- Sadece bir olasılık hesabı değildir.

Safety Integrity Levels and Basic Integrity



Nice & Niteliksel Gereklilikler Örnek-(EN 50129:2018)

Table A.1 — The SIL table

TFFR per hour and per function	Safety Integrity Level
$10^{-9} \leq \text{TFFR} < 10^{-8}$	4
$10^{-8} \leq \text{TFFR} < 10^{-7}$	3
$10^{-7} \leq \text{TFFR} < 10^{-6}$	2
$10^{-6} \leq \text{TFFR} < 10^{-5}$	1

Nice (quantitative)
gereklilikler (olasılık)
-random

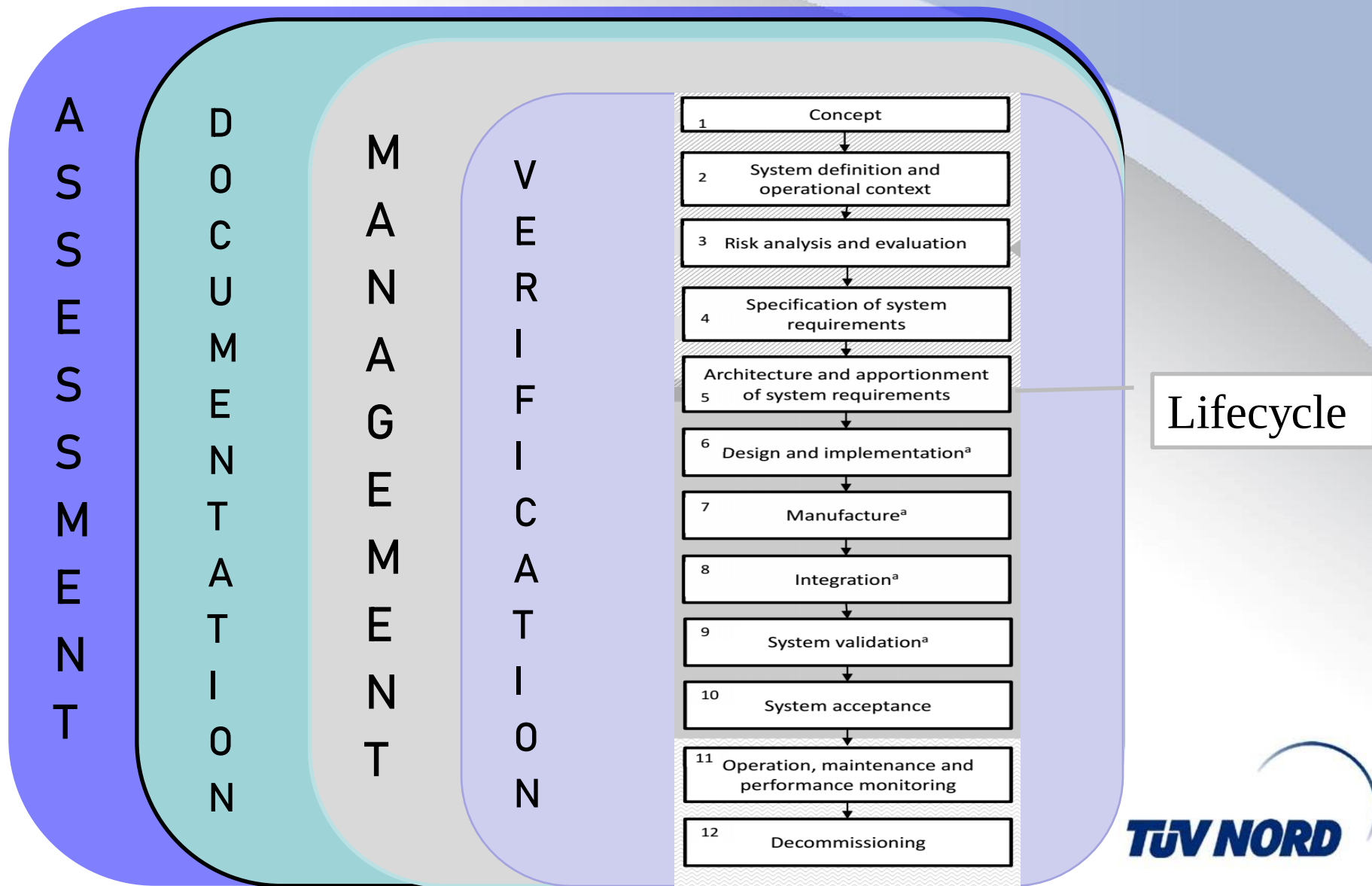
Table E.4 — Architecture of system, subsystem or equipment

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Separation of safety-related functions from non-safety-related functions to prevent unintended influences	See 7.2, "Section 3 of the Technical Safety Report"				
2 single electronic structure with self-tests and supervision	R	R	NR	NR	(a)
3 single electronic structure based on inherent fail-safety	R	R	HR	HR	(b)
4 single electronic structure based on reactive fail-safety	R	R	HR	HR	(c)
5 Dual electronic structure	R	R	NR	NR	(d)
6 Dual electronic structure based on composite fail-safety with fail-safe comparison	R	R	HR	HR	(e)

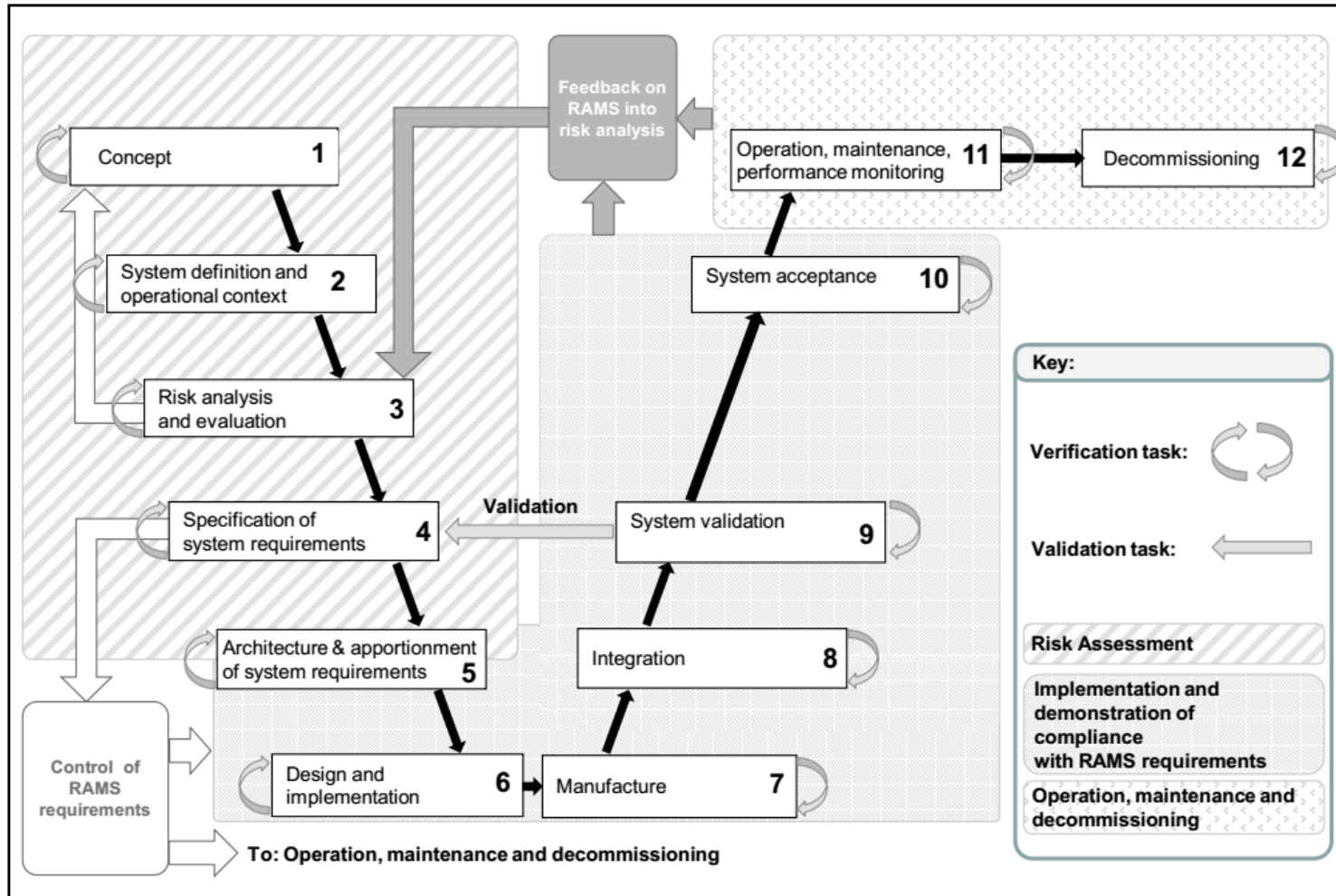
Niteliksel (qualitative)
gereklilikler (arızadan kaçınma)
-systematic

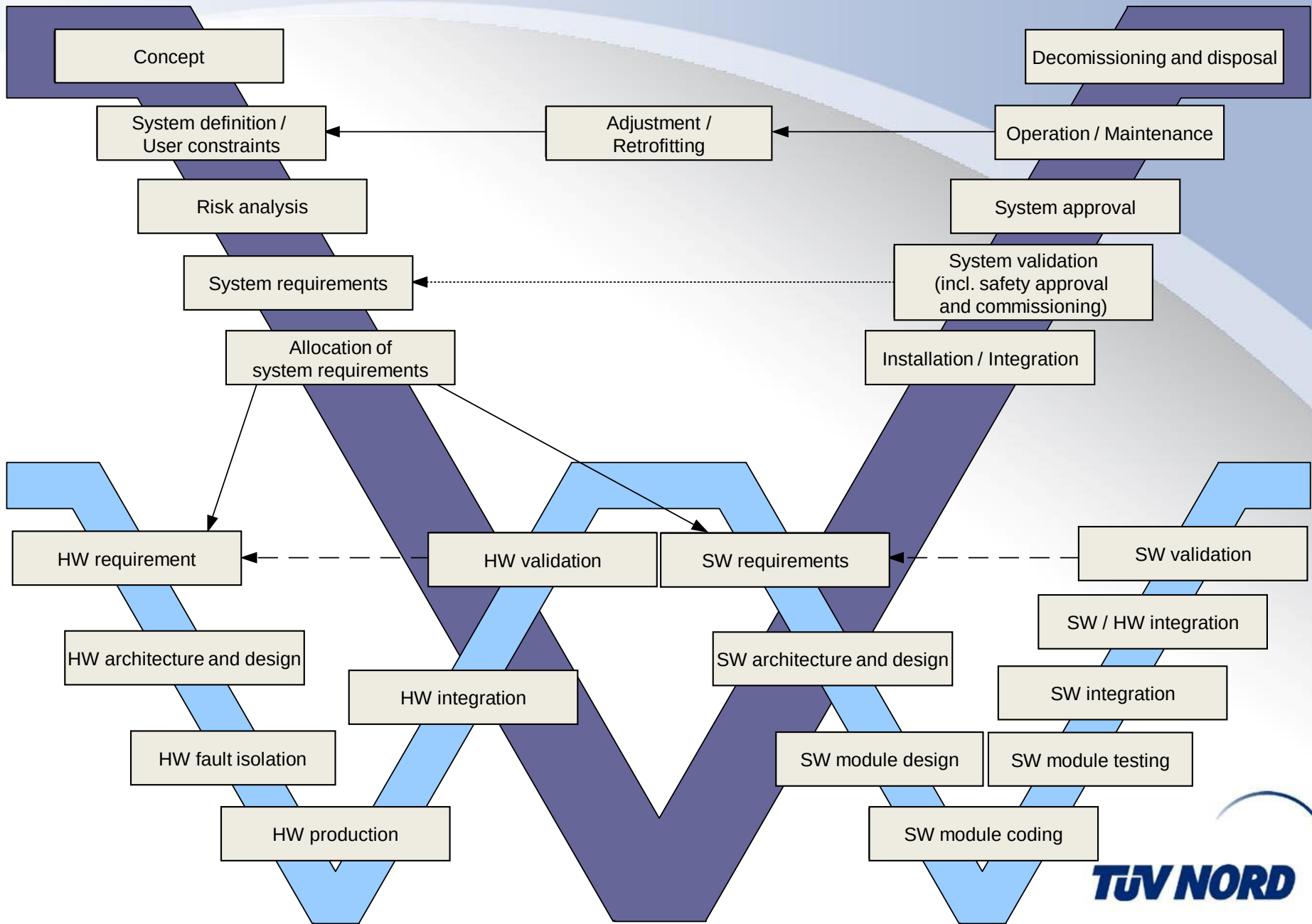


Fonksiyonel Emniyet Standartlarının Prensipleri



Lifecycle / V model –Örnek (EN 50126)





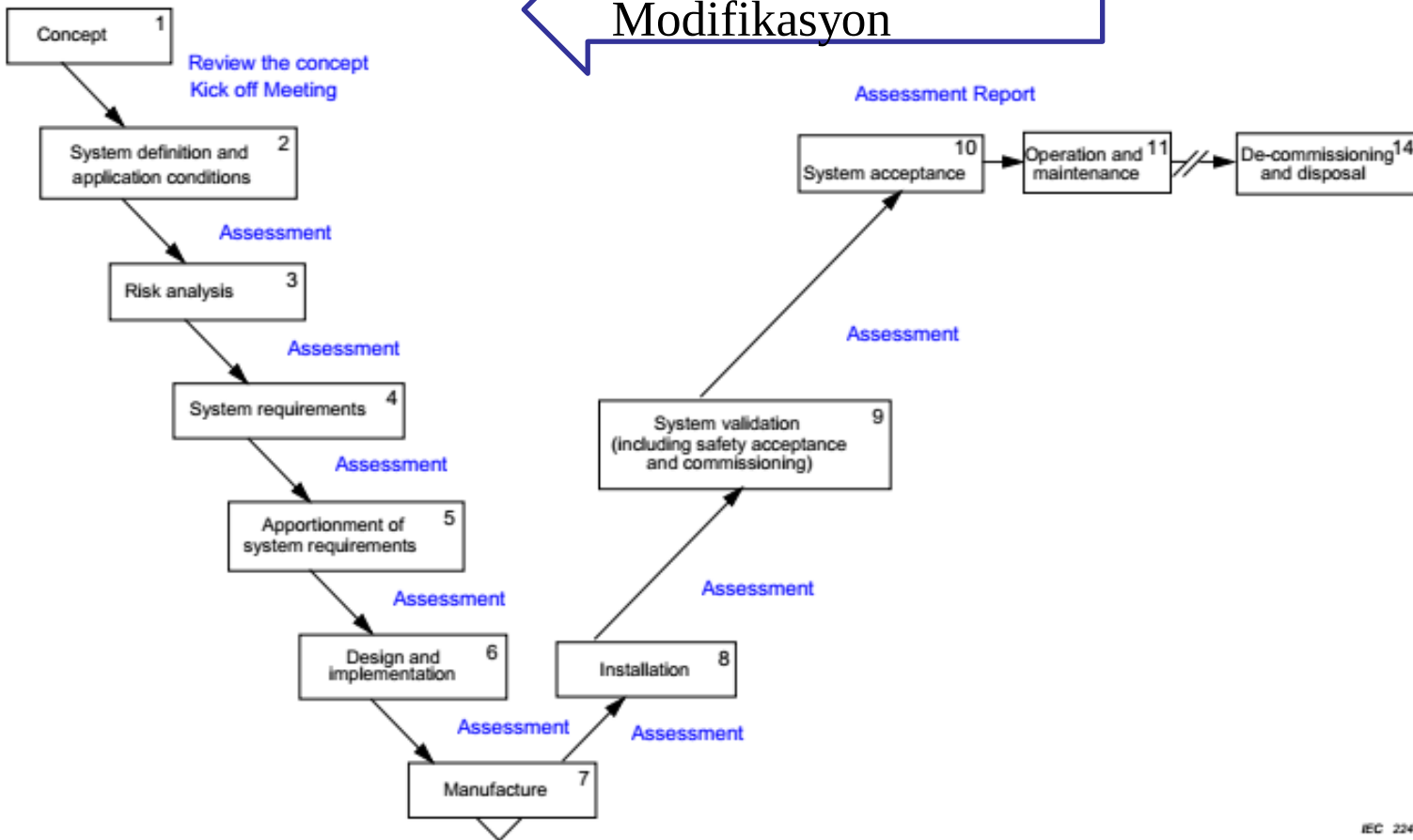
SIL Sertifikasyon Süreci

- i. 'Concept' dokümanını hazırla,
- ii. Bağımsız bir değerlendirme kuruluşuna (ISA) başvur,
- iii. Başlangıç toplantısı ve değerlendirme planını (Assessment Plan),
- iv. Faz , faz değerlendirme (step by step assessment),
- v. Değerlendirme raporu,
- vi. Ve sertifikasyon,
- vii. Sertifikasyon sonrası modifikasyon olursa değerlendiriciye modifikasyon değerlendirmesi için başvur
- viii. Modifikasyon için 'delta assessment'
- ix. Modifikasyon değerlendirme raporu,
- x. Yeni sertifikasyon.



SIL Sertifikasyon Süreci

Modifikasyon

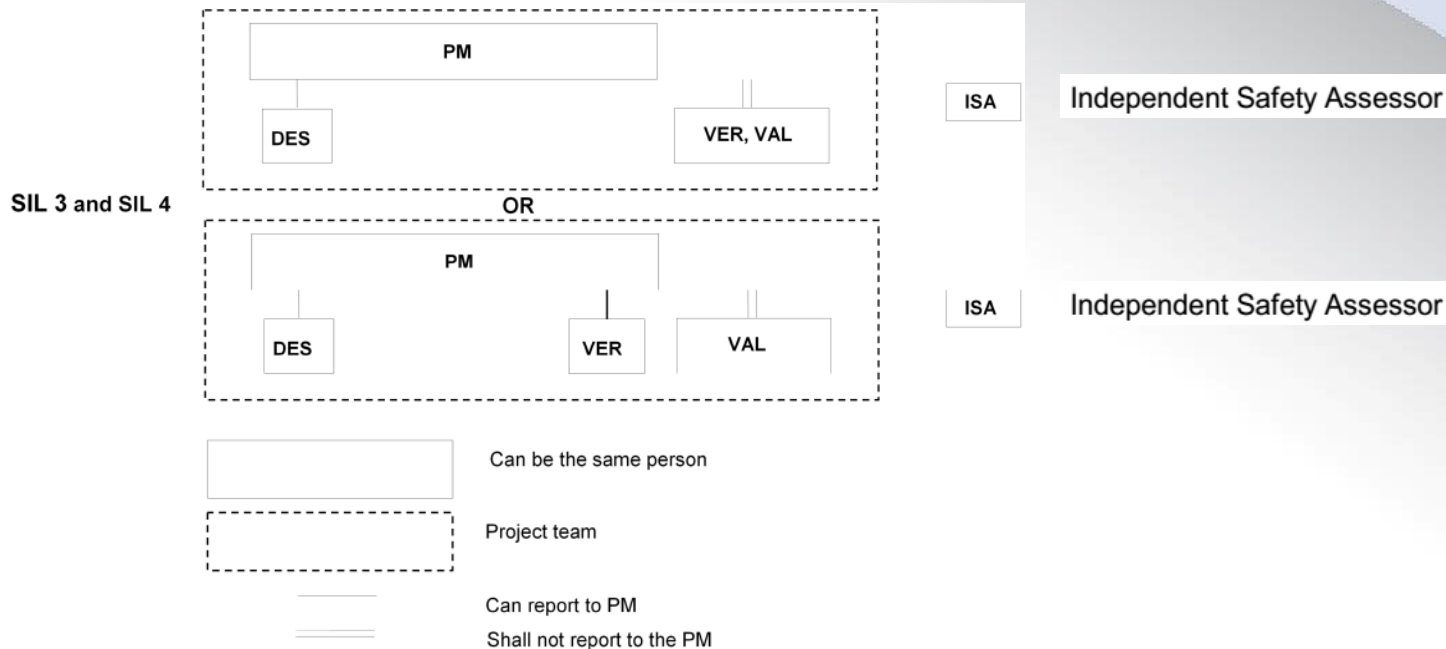


IEC 22440:2020



Değerlendirici Yetkinliği – EN 50129:2018

Figure 5 — Independence of Roles for different SILs



EN 50129:2018 ch. 5.3.15 ISA shall be;

- independent of any system design, development, operational and maintenance personnel.
- accepted by the railway duty holder in accordance with the legal framework.
- ...
- ...
- Results from the independent safety assessment shall be presented in a report.

Değerlendirici Yetkinliği – EN 50128:2011

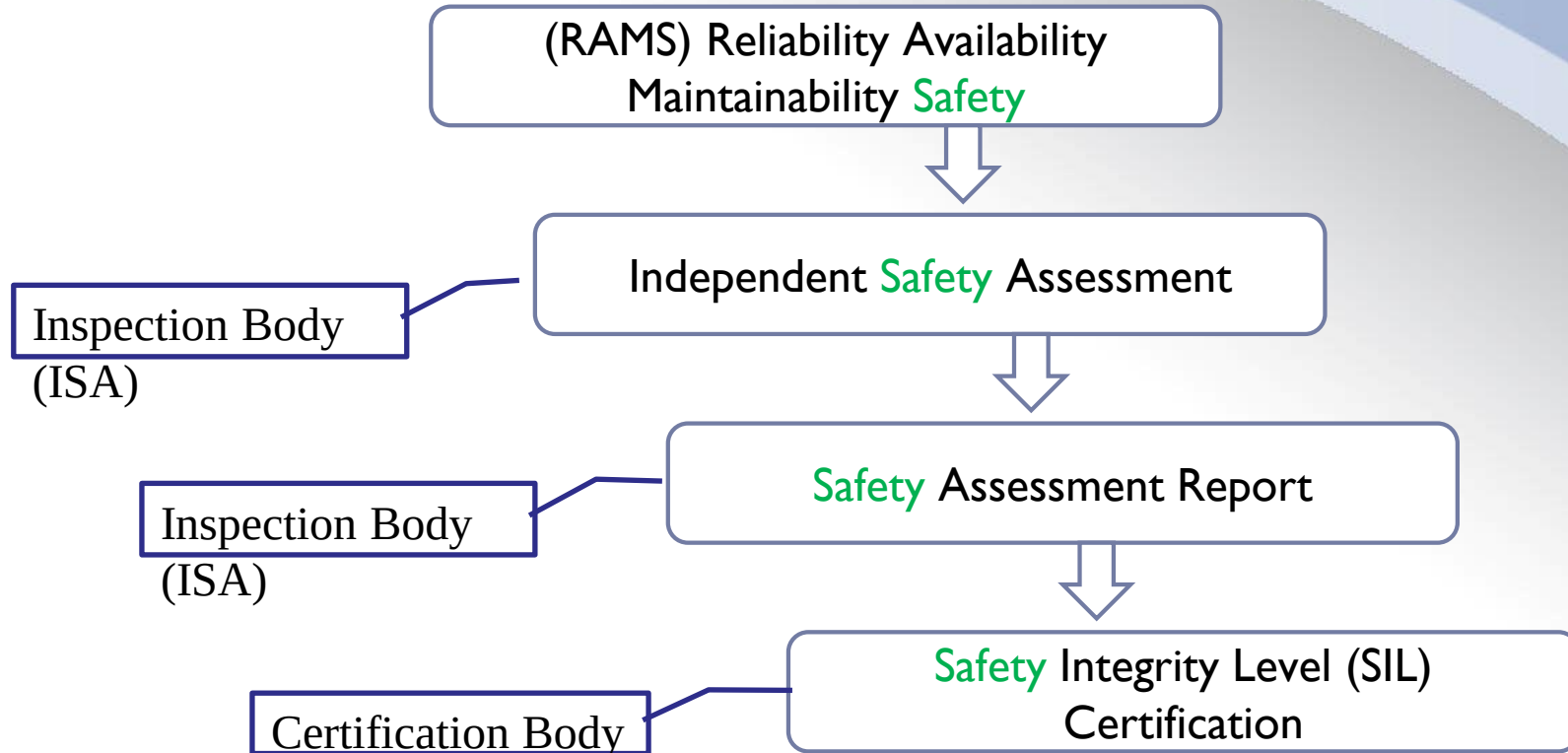
EN 50128 Table B.8 – Assessor Role Specification

Key competencies:

1. shall be competent in the domain/technologies where assessment is carried out
2. shall have acceptance/licence from a recognised safety authority
3. shall have / strive to continually gain sufficient levels of experience in the safety principles and the application of the principles within the application domain
4. shall be competent to check that a suitable method or combination of methods in a given context have been applied
5. shall be competent in understanding the relevant safety, human resource, technical and quality management processes in fulfilling the requirements of EN 50128
6. shall be competent in assessment approaches/methodologies
7. shall have analytical thinking ability and good observation skills
8. shall be capable of combining different sources and types of evidence and synthesise an overall view about fitness for purpose or constraints and limitations on application
9. shall have overall software understanding and perspective including understanding the application environment
10. shall be able to judge the adequacy of all development processes (like quality management, configuration management, validation and verification processes)
11. shall understand the requirements of EN 50128

SIL Sertifikasyon Süreci

TÜV NORD Organizasyonu



Inspection Body: EN 17020 Akreditasyonuna sahip, TÜV NORD Seelab

Certification Body: EN 17065 Akreditasyonuna sahip, TÜV NORD Seecert **TÜV NORD**

10-12.Mayıs.2022 Eskişehir
Demiryolu Fuarı Stant: A-102



Teşekkürler.

Ayhan Levent Arslan

Levent.arslan@tuv-turkey.com

+90 536 603 0390

