UPTEC STS 20018
Examensarbete 30 hp
Juni 2020

UPPSALA
UNIVERSITET

Uppdateringen av standarden EN 50129 och dess påverkan på ERTMS-programmets säkerhetsstyrning

En kartläggning av skillnader, påverkan samt åtgärder till följd av uppdateringen

Julia Waltersson

UPPSALA
UNIVERSITET

Teknisk- naturvetenskaplig fakultet
UTH-enheten

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

The effect of the update of the European standard EN 50129

Julia Waltersson

The railway signalling is a system used to control the traffic on the Railway and thereby prevent accidents. The railway signalling in Sweden is a safe system and not a single train passenger has died as a result of an accident since year 2010. However, as railway signalling has been developed nationally and has not always been compatible with each other, a problem has arisen when trains travel between countries. To enable a more compatible signalling system a standardized and digitized system called European Railway Traffic Management System (ERTMS) is now implemented in Europe. Trafikverket (TRV) is responsible for the implementation of ERTMS in Sweden and a ERTMS-programme is established. ERTMS is expected to med implemented in Sweden by 2035.

To maintain a safe railway system in Sweden, the implementation of ERTMS need to be at least as safe as the current system. This can be ensured by following different requirements stated in standards regarding safety. The European standard EN 50129, "Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling", is one of these standards. EN 50129 is updated from an old version to a new version. The purpose of this master thesis is to identify and analyse the effect of the update of the European standard EN 50129 on the implementation process of ERTMS. In addition, this study aims to suggest which actions need to be done at ERTMS-programme to implement the new version of the standard. To investigate this a qualitative method is used which involves a literature study, an analysis of the differences in the standard and semi-structured interviews with persons working at TRV. Theory about safety, safety management and the concept of Safety-I and Safety-II is used in order to analyse and discuss the safety management at ERTMS-programme regarding the update of EN 50129.

The results in this study show that the new version contains some new requirements that need to be implemented in the safety work within the ERTMS-programme, for example IT-security and human factors. Furthermore, the new version also contains additional explanations of subjects which can be helpful in the daily safety work. However, the study also shows that the new version involve already known requirements to a great extent. Therefore, regarding these part, the effect of the update is small. The suggested necessary actions are partly about implement the identified new requirements but also about implementing a more proactive safety approach and share the knowledge about the new version.

Handledare: Åsa Zade
Ämnesgranskare: Anders Arweström Jansson
Examinator: Elísabet Andrésdóttir
ISSN: 1650-8319, UPTEC STS 20018

Populärvetenskaplig sammanfattning

Trafiken på järnvägen har sedan 1990-talet fördubblats och cirka 420 000 personer reser via tåg en vanlig dag i Sverige. Detta gör säkerheten på järnvägen till en viktig aspekt. Järnvägens signalsystem syftar till att kontrollera järnvägens trafik för att undvika olyckor som kollisioner och urspårningar. Signalsystem har tidigare utvecklats på nationell nivå och järnvägen i Sverige är idag ett väldigt säkert system där ingen tågresenär har omkommit till följd av en olycka sedan år 2010. I och med att signalsystem har utvecklats nationellt har dock ett problem uppstått när tåg ska färdas mellan länder. För att lösa detta problem och möjliggöra ett mer kompatibelt system utvecklades det standardiserade och digitaliserade signalsystemet, European Railway Traffic Management System (ERTMS). ERTMS ska införas i Europa enligt EU-direktiv. Till följd av detta är ett teknikskifte för den svenska järnvägen på ingång. I Sverige är det Trafikverket som ansvarar för införande av ERTMS och ett ERTMS-program är tillsatt. ERTMS beräknas vara implementerat i Sverige år 2035.

För att upprätthålla en säker järnväg är det viktigt att ERTMS blir ett minst lika säkert system som det nuvarande signalsystemet. Detta kan säkerställas genom att bland annat följa krav som beskrivs i olika säkerhetsstandarder. En av dessa standarder är den europeiska standarden EN 50129, *Järnvägsanläggningar – Dataöverföring och järnvägsstyrning – Elektroniska signalsystem av betydelse för säkerheten*. Standarden beskriver arbetssätt och villkor för säkerhetsacceptans gällande elektroniska signalsystem. EN 50129 har uppdaterats till en ny version. Idag gäller versionerna, den gamla och den nya, parallellt, men 2021 kommer endast den nya versionen att gälla. ERTMS-programmet har i dagsläget inte koll på vad uppdateringen av standarden kommer att innebära. Hur påverkas säkerhetsarbetet inom järnvägens signalsystem vid uppdatering av en standard?

Syftet med studien är att kartlägga och analysera hur uppdateringen av standarden EN 50129 påverkar ERTMS-programmets säkerhetsstyrning. Studien syftar även till att föreslå åtgärder för ERTMS-programmet vid övergång till den nya versionen av standarden. För att uppfylla studiens syfte har en kvalitativ metod valts, där en litteraturstudie och semi-strukturerade intervjuer har genomförts. Samtliga intervjupersoner som har medverkat i studien arbetar på TRV. För att kartlägga skillnaderna mellan de två versionerna av standarden har även en jämförande analys utförts.

Studiens resultat visar att den nya versionen innehåller en del nya krav som behöver tillämpas i ERTMS-programmets säkerhetsstyrning. Bland annat gällande IT-säkerhet och kvalitetsstyrningen. Vidare innehåller den nya versionen även utökade förklaringar och krav för ämnen som kan vara hjälpsamma vid arbetet kring säkerhet. Resultatet visar dock på att en stor del av det utökade innehållet i den nya standarden redan uppfylls och är kända krav hos ERTMS-programmet. Till följd av detta har uppdateringen av standarden en relativt liten påverkan. De åtgärder som har identifierats för att ERTMS-programmet ska kunna övergå till den nya versionen kopplas dels till specifika krav i

standarden, dels till förändringar på ett mer övergripande plan. Exempelvis föreslås ett mer proaktivt förhållningssätt till uppdateringen av standarden. Ytterligare en väsentlig åtgärd som lyfts fram är att kunskapen om standarden borde öka samt att de identifierade nya delarna som kan vara hjälpande i säkerhetsarbetet borde framhävas på ERTMS-programmet. Detta för att utnyttja standarden på bästa sätt. Slutligen kan ett utökat systemtänk vara en åtgärd som bör vidtas för att väva samman alla delar som tas upp i standarden i syfte att öka säkerheten.

Förord

Detta examensarbete har genomförts som en sista del inom civilingenjörsprogrammet System i Teknik och Samhälle vid Uppsala universitet. Arbetet har utförts i samarbete med ERTMS-programmet på Trafikverket i Solna. Jag vill rikta ett stort tack till mina handledare på ERTMS-programmet, Åsa Zade och Ellinor Olsson, som har bidragit med uppmuntran, feedback och ett stort engagemang. Jag vill även tacka alla involverade på ERTMS-programmet för er hjälpsamhet och er värdefulla tid. Slutligen vill jag tacka min ämnesgranskare Anders Arweström Jansson vid Uppsala universitet som har gett mig värdefullt stöd och återkoppling under hela processen.

Julia Waltersson
Uppsala, juni 2020

Begreppslista

Förkortning	Beskrivning
AsBo	Assessment Body. Oberoende bedömningsorgan.
ATC	Automatic Train Control. Äldre tågskyddssystem som används i Sverige.
ATP	Automatic Train Protection. Internationellt begrepp för tågskyddsystem.
BI	Basic Integrity. Gilitg för en säkerhetsrelaterad funktion med TFFR högre än 10^{-5} per timme. Kan även appliceras på icke-säkerhetsrelaterade funktioner.
CENELEC	European Committee for Electrotechnical Standardization
ERA	European Union Agency for Railways. Koordinerar och harmoniserar regelverk inom järnvägssektorn.
ERTMS	European Railway Traffic Management System. EU-gemensamt signalsystem.
ETCS	European Train Control System. Tågskyddssystem i ERTMS.
GSM-R	Global System for Mobile Communications–Railways
ISA	Independent Safety Assessment eller Independent Safety Assessor. Oberoende granskning/granskare.
ISO	International Organization for Standardization
MTO	Människa, Teknik, Organisaition
PDCA-cykel	Plan, do, check, act – cykel. Beskriver arbetssätt gällande kvalitetsstyrning.
RBC	Radio Block Central. Databaserat system som får och skickar information som tåget efterfrågar.
SC	Subcommittee (sv. Subkommitté)
SEK	Svensk Elstandard
SIL	Safety Integrity Level. En definierad nivå som specificerar krav för säkerhetsrelaterade funktioner.
SIS	Svenska Institutet för Standarder
SRAC	Safety-Related Application Condition. Ett villkor som ska uppfyllas för att minska risker när systemet i fråga blir integrerat med det övriga systemet. En SRAC är alltid kopplad till en risk. SRAC-hantering är en förutsättning för säker integrering.
STM	Specific Transmission Module. Ombordenhet som översätter information från det äldre tågskyddsystemet ATC till ERTMS.
TC	Technical Committee (sv. Teknisk kommitté)
TRV	Trafikverket
WG	Working Groups (sv. Arbetsgrupper)

Begrepp	Beskrivning
ERTMS-programmet	Ett program inom TRV:s verksamhetsområde Stora projekt som ansvarar för införande av ERTMS i Sverige.
IT-säkerhet	Säkerhet med avseende på användningen av informationsteknologi.
Konventionella systemet	Den nuvarande signalanläggningen med tågskyddssystemet ATC.
Livscykel	De aktiviteter som utförs under det givna tidsintervallet som startar när ett system är uppfunnet och som slutar när systemet inte längre är brukbart samt att det är avvecklat och bortskaffat.
Mänskliga fel	En mänsklig handling eller icke-handling som leder till ett oväntat resultat.
Säkerhet (eng.Safety)	I denna studie avser begreppet säkerhet vad som på engelska benämns som safety och innefattar inte engelska security. I resultatdelen samt analysen avser användandet av säkerhet främst trafiksäkerhet.
Säkerhetsstyrning	Organisatorisk kontroll som säkerställer att säkerhetsprocessen implementeras korrekt.
Säkerhetsrapport (eng. Safety Case)	Ett strukturerat säkerhetsdokument som ska bevisa att ett system, delsystem eller komponent är accepterad med avseende på säkerhet.
Sociotekniskt system	Ett system där interaktionen mellan sociala och tekniska faktorer tillsammans skapar både lyckade och misslyckade organisatoriska utföranden.
Systematiskt fel	Inneboende fel i specifikation, design, konstruktion, installation, drift och underhåll för ett system, delsystem eller komponent.
Validering (VAL)	Bekräftelse, genom tillhandahållande av objektiva bevis, att kraven för en applikation eller avsedd användning har uppfyllts. Genomförs oftast vid utvecklingen slutfas men kan utföras i tidigare faser.
Verifiering (VER)	Bekräftelse, genom tillhandahållande av objektiva bevis, att specifika krav har uppfyllts. Genomförs vid flertal tillfällen under utvecklingen.

Innehållsförteckning

1. Inledning

Trafiken på järnvägen har sedan 1990-talet fördubblats och cirka 420 000 personer reser via tåg en vanlig dag i Sverige (Trafikverket, 2019c). Säkerheten på järnvägen är därmed en viktig aspekt och i Sverige implementerades år 1997 *nollvisionen*. Nollvisionen innebär att ingen ska omkomma eller skadas allvarligt till följd av olyckor. Transportsystemets utformning, användning och funktion ska därmed anpassas för att uppfylla visionen, vilket omfattar järnvägen (Regeringskansliet, 2016). Järnvägens signalsystem har som syfte att på ett säkert sätt styra järnvägens trafik så att olyckor, så som urspårningar och kollisioner, förhindras (Åkeson, 2017). Signalsystem har tidigare utvecklats på nationell nivå och Sverige har varit ledande i järnvägsbranschen med att utveckla signalsystem för järnväg som har ökat säkerheten, effektiviserat tågframkomligheten och minskat antalet olyckor (Vinnova, 2013). Järnvägen i Sverige är idag ett väldigt säkert system och senaste dödliga olyckan skedde år 2010. I september år 2010, i Kimstad utanför Norrköping, körde ett tåg in i en grävlastare som arbetade på ett spår intill men som hade halkat ur sitt spår. 20 resenärer skadades och en person omkom till följd av olyckan (SVT, 2016). Sedan dess har dock ingen tågresenär omkommit till följd av en olycka i Sverige.

I och med att signalsystem har utvecklats nationellt har dock en problematik uppstått när tåg ska åka mellan länder. Signalsystemen som har funnits har inte alltid varit kompatibla med varandra och tågen har tvingats varit utrustande med flera olika system för att kunna övergå från ett signalsystem till ett annat. För att möjliggöra ett enklare och mer kompatibelt system började Europeiska kommissionen år 1989 att studera möjligheten till ett gemensamt och framförallt mer standardiserat signalsystem i Europa (Smith, et al., 2012). Detta gemensamma digitaliserade och standardiserade signalsystem har fått namnet European Railway Traffic Management System (ERTMS). ERTMS implementeras i Europa med syfte att höja säkerheten för järnvägstransport och samtidigt öka järnvägens konkurrenskraft (European Commission, 2020). Enligt EU-direktiv ska ERTMS införas i Europa.

Ett teknikskifte för den svenska järnvägen är därmed på ingång. Det nuvarande konventionella signalsystemet ska bytas ut mot det digitaliserade och EU-standardiserade systemet ERTMS. Trafikverket (TRV) är ansvarig för införandet av ERTMS i Sverige och har tillsatt ett program för detta, ERTMS-programmet. Senast 2035 beräknas implementeringen av ERTMS vara klar i Sverige (Trafikverket, 2019a). Det är viktigt att det nya signalsystemet ERTMS, och alla tillkommande säkerhetsföreskrifter, blir ett minst lika säkert system som tidigare. Att bibehålla eller öka säkerheten är dock inte enkelt då system blir allt mer komplexa och bland annat Hollnagel (2014) belyser att säkerheten är en central fråga i dagens socio-tekniska system.

Vid utveckling av ett nytt signalsystem finns det standarder från EU som bör följas. TRV har dessutom satt krav på användandet av olika standarder, vilket gör de obligatoriska att följa (Trafikverket, 2020). Bland annat finns det standarder som beskriver arbetssätt och

villkor för säkerhetsarbetet vid utveckling av signalsystem. Dessa säkerhetsstandarder uppdateras med jämna mellanrum och kan då innehålla nya krav gällande säkerheten. Vid uppdatering av en standard är det därmed viktigt att veta vad uppdateringen kommer att innebära. En fråga som då uppstår och som utgör denna studies övergripande forskningsfråga är; Hur påverkas säkerhetsarbetet inom järnvägens signalsystem vid uppdatering av en standard?

1.1 Syfte

För att upprätthålla den säkra järnvägstrafiken som Sverige har idag, krävs att införandet av ERTMS blir ett minst lika säkert system. Detta säkerställs bland annat genom att följa säkerhetsstandarder som berör utvecklingen av järnvägens signalsystem, där den europeiska standarden EN 50129 utgör en av dessa. EN 50129, *Järnvägsanläggningar - Dataöverföring och järnvägsstyrning - Elektroniska signalsystem av betydelse för säkerheten* har uppdaterats från version EN 50129:2003 till EN 50129:2018, vidare nämnda som den gamla versionen respektive den nya versionen. ERTMS-programmet följer i dagsläget den gamla versionen men måste senast år 2021 övergå till den nya versionen. Syftet med examensarbetet är således att kartlägga och analysera hur uppdateringen av standarden EN 50129 påverkar ERTMS-programmets säkerhetsstyrning.

1.2 Mål

Målet, vilket examensarbetet syftar till att uppfylla, är att föreslå åtgärder vid övergång till den nya versionen av standarden. Med andra ord är målet att studera vilka åtgärder som krävs för att ERTMS-programmet ska kunna övergå till den nya versionen.

1.3 Frågeställningar

Följande frågeställningar har formulerats och undersökts för att uppfylla målet och syftet med examensarbetet:

- *Vilka skillnader finns det mellan de två versionerna av standarden EN 50129?*
- *Hur påverkar dessa skillnader ERTMS-programmet?*
- *Vilka åtgärder krävs för att övergå till den nya versionen av standarden?*

1.4 Avgränsningar

Standarden EN 50129 innehåller säkerhetsrelaterade krav för utvecklingen av signalsystem och berör således en mängd olika aktörer. Eftersom denna studie syftar till att studera hur uppdateringen påverkar ERTMS-programmet har studien begränsats till de delar i standarden som är kopplade till ERTMS-programmets arbete. Den empiriska datainsamlingen har således avgränsats till att beröra endast representanter från TRV och främst ERTMS-programmet. Exempelvis tas inte ERTMS-programmets leverantörers perspektiv upp.

2. Bakgrund

För att undersöka hur uppdateringen av standarden EN 50129 påverkar ERTMS-programmet krävs förståelse för signalsystem, ERTMS, TRV och ERTMS-programmet, standardiseringsarbetet samt EN 50129:s innehåll. Följande avsnitt inleds därför med bakgrundsfakta om järnvägens signalsystem, med fokus på ERTMS. Därefter introduceras TRV. Vidare beskrivs standarder och standardiseringsorgan. Slutligen presenteras standarden EN 50129, dess relation till andra standarder gällande signalsystem samt en introduktion till dess generella innehåll.

2.1 Järnvägens signalsystem

Signalsystem har som syfte att styra järnvägens trafik på ett säkert sätt och förhindra urspårningar samt kollisioner (Åkeson, 2017). Signalsystemet består av en signalanläggning och ett tågskyddssystem. Tabell 2 och 3 beskriver dessa två delar och Tabell 1 presenterar övriga viktiga begrepp gällande järnvägens signalsystem.

Tabell 1. Beskrivning av begrepp i järnvägens signalsystem.

Begrepp	**Beskrivning**
Balis	En överföringsenhet som är placerad på spåret som sänder ut information till spårfordon (ERA, 2016).
Driftplats	Ett avgränsat område av banan som kan övervakas i detalj (Klawitter, 2019).
Interoperabelt signalsystem	Ett signalsystem som möjliggör enkel färd med tåg mellan länder som infört samma system (Åkesson, 2017).
Optiska signaler	Fysiska signaler längs tågväg som visar olika körbesked. Det finns ett flertal olika signaler bland annat huvudljussignal, stopplykta, försignal mer flera (Trafikskolan, 2017).
Spåravsnitt	Ett spåravsnitt är den minsta del av ett spår som behandlas i RBC/signalställverk (Trafikskolan, 2017).
Trafikledningscentral	I de åtta trafikledningscentraler som finns i Sverige jobbar tågklarerare med att övervaka, organisera och styra trafiken på järnvägarna (Klawitter, 2019).
Tågväg	En tågväg utgörs av en bestämd börjanpunkt och en slutpunkt och är ett spåravsnitt avsett för framförande av tågfärd. Tågvägen kontrolleras av signalställverk (Trafikskolan, 2017).

Tabell 2. Beskrivning av järnvägens signalanläggning.

Signalanläggningen är en del av signalsystemet och utgörs, i det nuvarande konventionella systemet, i huvudsak av följande komponenter: Ställverk, Utdelningssystem, Teknikhus, Spårledningar och Signalskåp.

Ställverk är väsentliga komponenter i en signalanläggning. De har till uppgift att reglera trafiken på driftplatser och kan bland annat låsa tågväg och spärra spåravsnitt automatiskt. Ställverk ser därmed till att tågvägen är fri från övrig trafik. (Trafikverksskolan, 2017).

Utdelningssystem krävs för att ställverkens kommando ska kunna styra signalobjekt som växlar, spårledningar med mera (Klawitter, 2019).

Teknikhus förser komponenter i signalsystemet med elkraft samt skyddar och förvarar utrustning i signalsystemet som möjliggör kommunikation mellan olika komponenter (Klawitter, 2019).

Spårledning har som syfte att säkerställa om ett spåravsnitt är fri från fordon. Detta sker genom att spårledningar utgör en strömkrets mellan rälerna som kortsluts när ett spårfordon passerar. Ställverket blir då informerad om att det befinner sig ett tåg på spåret. I Sverige är avståndet mellan spårledningar i snitt ungefär 1,5 km. (Klawitter, 2019).

Signalskåp krävs för varje teknikhus och är det gemensamma namnet för kopplingskåp, tranformatorskåp och kraftmatning för spårledningar. Skåpen utgör en förbindelse mellan signalobjekt och utdelningssystem i teknikhus (Klawitter, 2019).

Tabell 3. Beskrivning av järnvägens tågskyddsystem.

Tågskyddssystem är den andra delen i signalsystemet som används för att hålla hastighetsgränser och stoppunkter. Systemet utgör ett stöd för lokföraren då det automatiskt kan sänka tågets hastighet samt nödbromsa. Automatic Train Protection (ATP) är det internationella begreppet för tågskyddsystem (Klawitter, 2019).

Idag är det tågskyddssystemet Automatic Train Control (ATC) som är i drift i Sverige. ATCs funktion är att överföra baninformation till spårfordon, lagra information och förmedla den vidare till lokföraren, övervaka åtgärder samt vid vissa situationer bromsa automatiskt eller sänka hastigheten. Information från signalsystemet om hastighet, avstånd och lutning överförs via baliser. När ett tåg passerar en balis skickas information från balisen till tåget via en antenn under loket. På så sätt fungerar ATC och lokföraren tillhandahålls med relevant information. Den fysiska placeringen av baliser är därmed en viktig aspekt. ATC-systemet ska fungera som ett extra skydd,

framför allt för tåg som kör i höga hastigheter, då det optiska signalsystemet inte alltid är tillräckligt (Trafikverksskolan, 2017).

ATC-systemet i Sverige har varit och är fortfarande ett väldigt säkert system där inga olyckor med dödsfall har skett sedan 2010, bortsett från järnvägsövergångar, självmord och arbete i spår (Regeringskansliet, 2016).

Tidigare har signalsystem ofta utvecklats på nationell nivå och det har funnits över 20 olika tågskyddssystem för järnväg i Europa (Smith, et al., 2012). Dessa olika system har inte alltid varit kompatibla med varandra vilket har inneburit att flera system har krävts för att tågen ska kunna passera gränser mellan länder, det vill säga för att kunna övergå från ett signalsystem till ett annat. På grund av detta började Europeiska kommissionen år 1989 att studera möjligheten till ett interoperabelt signalsystem i Europa. För att möjliggöra en ökad interoperabilitet rekommenderades att konventionella signalsystem förnyades till mer kompatibla och standardiserade system (Smith, et al., 2012).

Till följd av detta är ett teknikskifte på den svenska järnvägen på ingång. Signalsystemet för järnväg i Sverige är dessutom slitet och orsakar ofta förseningar vilket påverkar både persontrafik och godståg. Signalsystemet uppdateras och ersätts därför nu med det nya europeiska standardiserade systemet European Rail Traffic Management System (ERTMS) (Trafikverket, 2019a).

2.2 ERTMS

ERTMS är ett EU-gemensamt signalsystem som möjliggör ett driftkompatibelt järnvägssystem inom Europa. ERTMS implementeras i Europa med syfte att höja säkerheten för järnvägstransport och samtidigt öka järnvägens konkurrenskraft (European Commission, 2020). Syftet med ERTMS är enligt Internationella järnvägsunionen (Smith et al., 2012, s.80):

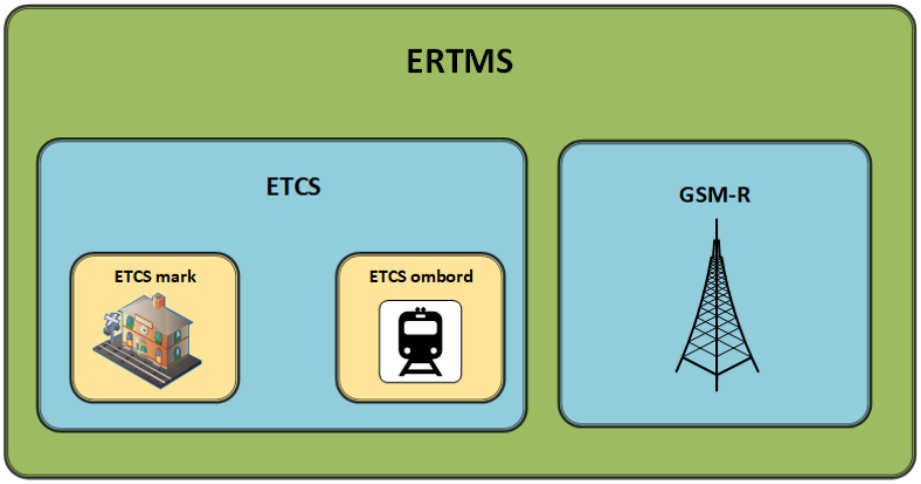
"Att förbättra gränsöverskridande interoperabilitet genom att skapa en Europeisk standard för järnvägens signalsystem med det slutliga målet att förbättra järnvägssektorns konkurrenskraft"

ERTMS bidrar bland annat till optimerad användning av energi- och nätverksresurser, ökad kapacitet och förbättrad trafikledning (Smith, et al., 2012). Andra fördelar som ERTMS förväntas ge är en likvärdig eller ökad säkerhet, möjlighet till högre hastighet, potentiellt minskade kostnader för underhåll, ökad flexibilitet och större tillgänglighet (European Commission, 2020). ERTMS införs enligt lagkrav från EU och den europeiska standarden för driftskompabilitet som innebär att alla nya investeringar av järnväg ska utrustas med ERTMS. Samtliga länder i EU samt Norge och Schweiz agerar för att införa ERTMS (Trafikverket, 2015). Vidare i denna studie beskrivs de delsystem som ingår i ERTMS.

2.2.1 Delsystem

Det finns två tekniska delsystem inom ERTMS; Global System for Mobile Communications - Railway (GSM-R) och European Train Control System (ETCS) vilka beskrivs mer ingående nedan. Se Figur 1 för en illustration av ERTMS:s delsystem.

- GSM-R är ett radiokommunikationssystem som ger lokföraren kontinuerlig information via en skärm. Information går i båda riktningarna och passerar ställverk, RBC och trafikledningscentral (ERA, 2016).
- ETCS är tågskyddsystemet som övervakar tågets rörelse och lokförarens respons. ETCS består både av markutrustning och ombordutrustning, vilka förklaras mer ingående nedan (ERA, 2016).



Figur 1. Delsystem i ERTMS (Klawitter, 2019).

ETCS markutrustning består av följande delar:

- Radio Block Central (RBC) är ett databaserat system. RBC får information om tågets position och skickar ut körtillstånd och övrig information som tåget efterfrågar. RBC hanterar även överföring av markdata och kommunicerar med närliggande RBC:er (ERA, 2016). RBC integrerar även med signalställverk för att dela signalrelaterad information.
- Eurobalise är en passiv överförningsenhet som placeras på järnvägsspåret. Dess funktion är att samla och skicka data från markutrustning till ombordutrustning. Data berör bland annat tågets position och hastighet (ERA, 2016). Enheten är passiv eftersom den inte behöver någon elektrisk försörjning.
- Lineside Electronic Unit (LEU) utgör kopplingen mellan baliser och ställverk (European Commission, 2020).
- Key Management Center (KMC) är ett datorbaserat system som skyddar information mellan RBC och tåg. Det sker genom att systemet genererar och skickar krypteringsnycklar till RBC och tågets ombordutrustning (Klawitter, 2019).
- Signalpunktstavlor ersätter dagens optiska signaler och har som syfte att visa start och slut samt att sträckan är utrustad med ERTMS (Klawitter, 2019).

ETCS ombordutrustning består av följande delar:

- Odometer är en enhet som beräknar tågets körsträcka.
- Balise Transmission Module (BTM) bearbetar signaler från en antenn ombord och upptar information från baliser (European Commission, 2020).
- Driver Machine Interface (DMI) är gränssnittet mellan lokföraren och ETCS. Det är förarpanelen där information om hastighet, avstånd, larm med mera presenteras för lokföraren (Trafikverksskolan, 2017).
- Euro Vital Computer (EVC) hanterar data från andra enheter och ligger till grund för informationen som visas på förarpanelen. EVC säkerställer att givna hastigheter och angivna körbesked följs (Klawitter, 2019).
- Specific Transmission Module (STM) är en ombordenhet som översätter information från det äldre tågskyddsystemet ATC till ERTMS (Trafikverket, 2019a)

Förutom byte från tågskyddsystemet ATC till ETCS pågår även en stor restaurering av signalanläggningen i Sverige då många av ställverken är över 50 år gamla. Ställverken ska ersättas med nya standardiserade och digitaliserade ställverk. Uppdateringen kommer förutom att underlätta underhåll även leda till ett minskat behov av antal ställverk. Detta beror på att de nya ställverken kan styra större områden, så kallade styrområden, än tidigare (Trafikverket, 2019a). Nedan beskrivs de fem olika systemnivåerna av ERTMS som kan väljas att implementeras.

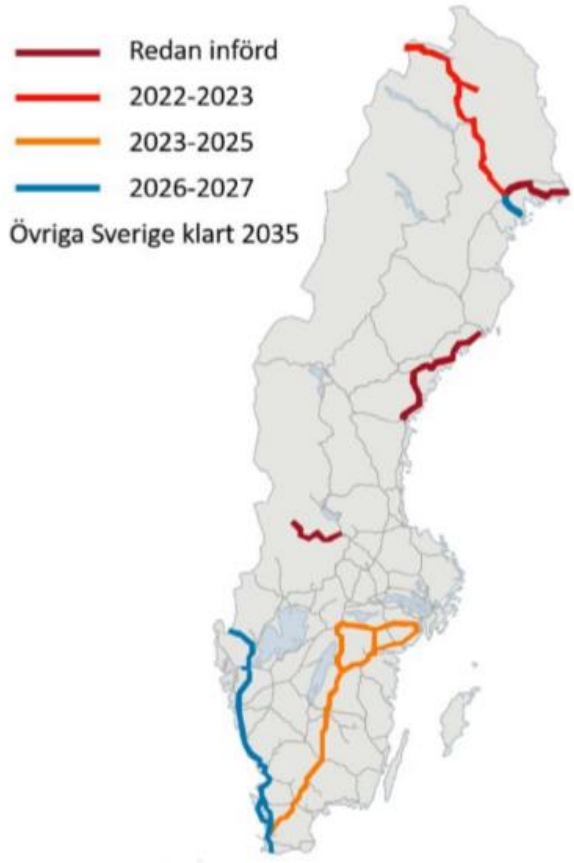
2.2.2 Systemnivåer

Det finns fem nivåer av ERTMS som skiljer sig med avseende på funktionalitet, sättet föraren får information och markutrustning (Trafikverksskolan, 2017).

- Nivå STM används för både ERTMS och andra system. STM möjliggör trafik för tåg utrustade med ERTMS/ETCS ombord men med nationell markutrustning (Trafikverksskolan, 2017).
- Nivå 0 använder enbart optiska signaler och är applicerbar på linjer utan ERTMS (Trafikverksskolan, 2017).
- Nivå 1 använder optiska signaler, spårledningar och motsvarar till stor del dagens ATC-system. Baliser används för kommunikationen mellan RBC och fordon (Åkeson, 2017).
- Nivå 2 har inga optiska signaler och baseras på GSM-R för kommunikation mellan RBC och fordon. Baliser används endast för information om tågets position. Spårledningar eller axelräknare krävs för detektering av tåg. Axelräknare är en enhet placerad på insidan av rälsen som räknar antalet axlar som passerar. Syftet är att avgöra om spåravsnittet är fri från fordon eller inte. Axelräknare kan ersätta eller komplettera spårledningar (Trafikskolan, 2017).
- Nivå 3 har varken optiska signaler, spårledningar eller axelräknare. Kommunikation och detektering av tåg sker via GSM-R (Trafikverksskolan, 2017).

2.2.3 ERTMS införande i Sverige

Reinvesteringen av signalanläggningen och bytet från tågskyddssystemet ATC till ETCS är beräknat att kosta cirka 30 miljarder kronor och ska vara implementerat i Sverige år 2035 (Åkeson, 2017). TRV är ansvarig för införandet av ERTMS i Sverige. I dagsläget finns det fyra pilotbanor; Botniabanan, Ådalsbanan, Haparandabanan och Västerdalsbanan, som är driftsatta med ERTMS i Sverige, se ”Redan införd” i Figur 2. Det finns även två testbanor, Katrineholm-Åby och Mertainen, där markutrustning och ombordutrustning testas efter att systemutvecklingen är klar från leverantörens testlabb. TRV har valt att implementera ERTMS nivå 2 på samtliga linjer i Sverige. Figur 2 visar hur ERTMS har införts och planeras att införas i Sverige från år 2010-2035 (Trafikverket, 2019a).



Figur 2. Karta över införandeplan av ERTMS i Sverige. Banorna Scandinavia-Mediterran väst (blå färg), Scandinavia-Mediterran öst (orange färg) och Malmbanan (ljusröd och blå färg) visas (Klawitter, 2019).

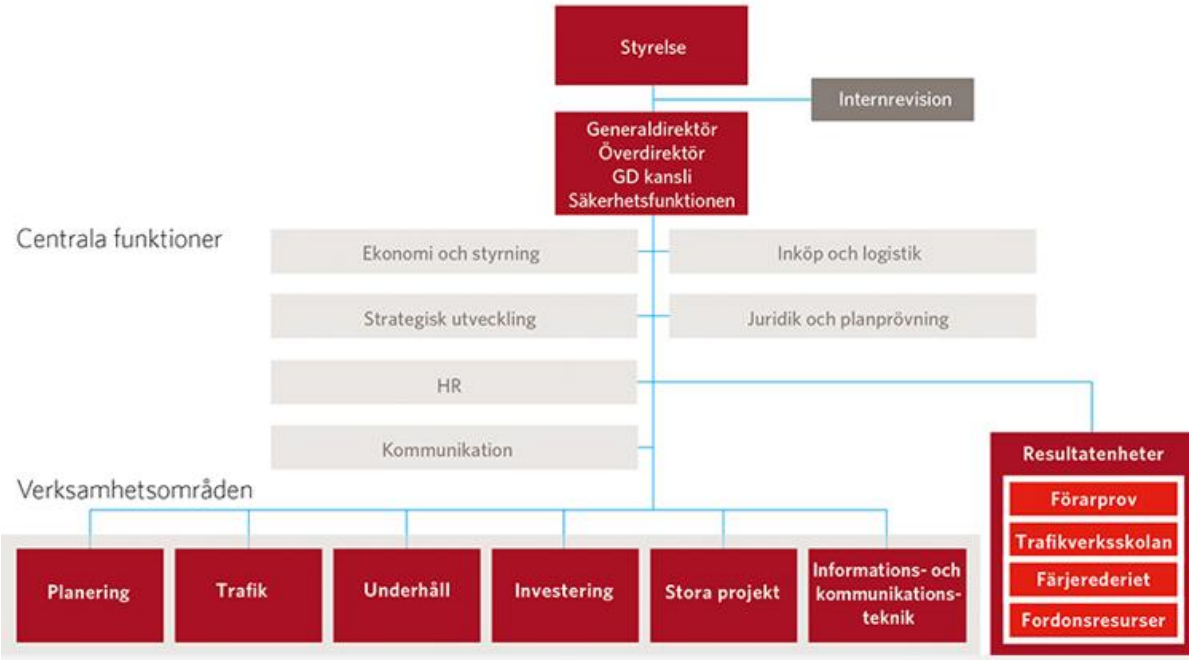
2.3 Trafikverket

TRV är en svensk myndighet som på uppdrag av regeringen ansvarar för långsiktig infrastrukturplanering gällande vägtrafik, luftfart, sjöfart samt järnvägstrafik. TRV ansvarar även för att utveckla och förvalta statliga vägar och järnvägar i Sverige (Trafikverket, 2019b). Med utgångspunkt i de transportpolitiska målen har TRV följande vision:

"Alla kommer fram smidigt, grönt och tryggt"

Visionen innebär att resor och transporter av varor ska vara enkelt för både människor och företag. Detta ska även ske med minimal påverkan på klimatet och på ett säkert sätt, där ingen ska skadas allvarligt eller dö i trafiken. TRV prioriterar säkerheten och strävar efter att transportsystemet ska vara tillgängligt och tillförlitligt i syfte att samhället ska fungera (Trafikverket, 2019b). TRV är därmed en bidragande aktör till samhällsutvecklingen.

TRV bildades i april år 2010 i samband med att Banverket, Vägverket och Statens institut för kommunikationsanalys (SIKA) avvecklades. Idag har TRV cirka 9000 anställda med huvudkontor placerat i Borlänge. Organisationen består av en styrelse, generaldirektör med flera, en internrevision, sex olika centrala funktioner, fyra resultatenheter samt sex verksamhetsområden, se Figur 3. Stora projekt är ett verksamhetsområde där bland annat ERTMS-programmet ingår, vilket är det program som ansvarar för införande av ERTMS i Sverige (Trafikverket, 2019b).



Figur 3. Trafikverkets organisationsstruktur (Trafikverket, 2019b).

2.4 Standarder

"En standard är en gemensam lösning på ett återkommande problem" (Boverket, 2018)

En standard syftar till att bygga upp gemensamma rutiner för att möjliggöra en fri och effektiv marknad, minskade kostnader samt ökad kvalitet och säkerhet. Standarder kan i vissa fall vara obligatoriska men är oftast frivilliga att använda. Det finns många olika typer av standarder inom flera olika områden, allt från energi och hållbarhet till sjukvård och informationsteknologi. Exempel på standardtyper är bland annat tjänstestandard, metodstandard, kompetensstandard, informationsstandard, materialstandard, klassningsstandard och processtandard (Boverket, 2018).

Standardiseringsorgan finns på både global, europeisk och nationell nivå, se Tabell 4. De globala standardiseringsorganisationerna utgörs av International Electrotechnical Commission (IEC), International Organization for Standardization (ISO) och International Telecommunication Union (ITU). Beteckningen för globala standarder är ISO eller IEC. The European Committee for Electrotechnical Standardization (CENELEC), European Committee for Standardization (CEN) och European Telecommunications Standards Institute (ETSI) är de tre europeiska standardiseringsorganisationerna som har mandat att utveckla standarder. Beteckningen för standarder på europeisk nivå är EN. I Sverige betecknas standarder med SS och följande tre standardiseringsorganisationer finns: Svensk Elstandard (SEK), Svenska Institutet för Standarder (SIS) och Svenska Informations- och Telekommunikations-Standardiseringen (ITS) (Boverket, 2018).

Tabell 4. Standardiseringsorgan globalt, i Europa och i Sverige.

Globalt	Europa	Sverige
IEC	CENELEC	SEK
ISO	CEN	SIS
ITU	ETSI	ITS

Utveckling av standarder sker genom tekniska kommittéer. Dessa kommittéer kan bestå av representanter från myndigheter, företag, kommuner, branschorganisationer, ideella föreningar, universitet med flera. Tekniska kommittéer inom SIS och SEK betecknas TK medan ITS istället har så kallade arbetsgrupper. Liknande system gäller på europeisk och global nivå då en teknisk kommitté (TC) ansvarar för framtagandet av standarder men där det faktiska arbetet utförs av så kallade arbetsgrupper (WG) (Boverket, 2018). Standardiseringsarbetet bedrivs ideellt och innefattar många olika parter. Efter att en standard har fastställts ses den över regelbundet, cirka vart femte år, och kommittéerna kontrollerar om standarden behöver revideras eller uppdateras. En uppdatering av en standard är ett tidskrävande arbete då kommitténs representanter kommer från olika

företag och myndigheter som har olika åsikter. Dessutom måste kommentarer från hela Europa tas hänsyn till innan uppdateringen kan fastställas.

Deltagande i standardiseringsarbete ger möjlighet till att dels tillgodose företags, organisationers och myndigheters behov, dels påverka resultatet av standarder. Standarder påverkar export av varor, utvecklingen av ny teknik och global spridning av innovationer vilket gör deltagande i processen väsentlig (SEK, 2019). Det finns representanter från TRV och även inom ERTMS-programmet som deltar i standardiseringsarbete.

2.4.1 CENELEC

Tekniska regler och säkerhet inom det elektrotekniska området har diskuterats i samarbete mellan länder i Europa sedan 1920-talet. CENELEC, som är en av de tre nuvarande standardiseringsorganisationerna i Europa, bildades 1973 och ansvarar för standarder inom det elektrotekniska området i Europa. Organisationen har som syfte att avlägsna tekniska handelshinder för att förenkla handel med elektriska produkter. CENELEC har 34 europeiska länder som medlemmar och 10 nationella standardiseringspartners, bland annat Egypten, Israel och Ukraina (SEK, 2019).

Inom CENELEC finns ett flertal olika TC:s. TC 9X - *Electrical and electronic applications for railways* omfattar standardisering av elektriska och elektroniska system, utrustning och relaterad mjukvara för användning i alla järnvägsapplikationer, både på fordon och i fasta installationer. TC 9X har följande tre subkommittéer (SC) (SEK, 2019);

- SC 9XA - *Communication, signalling and processing systems.*
- SC 9XB - *Electrical, electronic and electromechanical material on board rolling stock.*
- SC 9XC - *Electric supply and earthing systems for public transport equipment and ancillary apparatus (Fixed installations)*

SC 9XA omfattar standardisering av järnvägskommunikation, signalsystem och process med hänsyn till relevanta säkerhetskrav. Inom denna subkommitté omfattas bland annat den europeiska standarden EN 50129. I Sverige är SEK ansvariga för alla elektrotekniska standarder (SEK, 2019).

2.4.2 CENELEC-standarder för signalsystem

Det finns många standarder som berör olika delar av järnvägen. Följande tre CENELEC-standarder är de standarder som huvudsakligen styr arbetssätt för signalsystem (CENELEC, 2018):

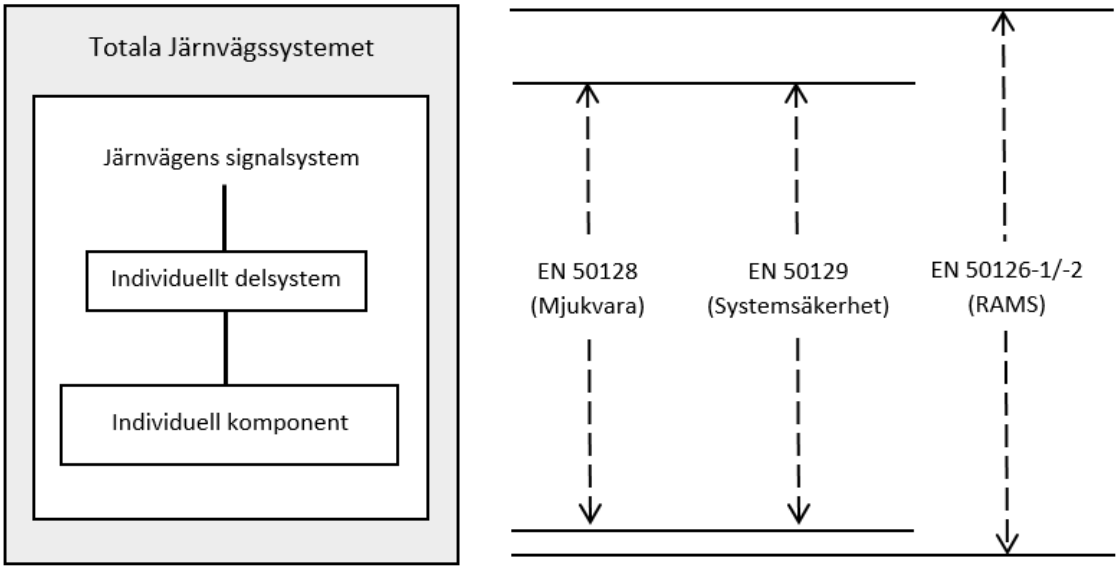
- EN 50126, *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process* och *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems*

Approach to Safety, beskriver säkerhetshantering av system med avseende på tillförlitlighet, tillgänglighet, underhåll och säkerhet (RAMS) i förhållande till systemets livscykel (CENELEC, 2017a; 2017b).

- EN 50128, *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*, beskriver tekniska krav och metoder för utvecklingen av programmerbara elektroniska kontroll- och säkerhetsrelaterade system gällande järnväg (CENELEC, 2011).

- EN 50129, *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*, beskriver krav för acceptans och godkännande av säkerhetsrelaterade elektroniska system gällande järnvägens signalsystem (CENELEC, 2018).

Figur 4 visar vad respektive ovannämnd standard omfattar och standardernas relation till varandra.



Figur 4. CENELEC-standarderna EN 50126, EN 50128 och EN 50129 roll och relation till varandra.

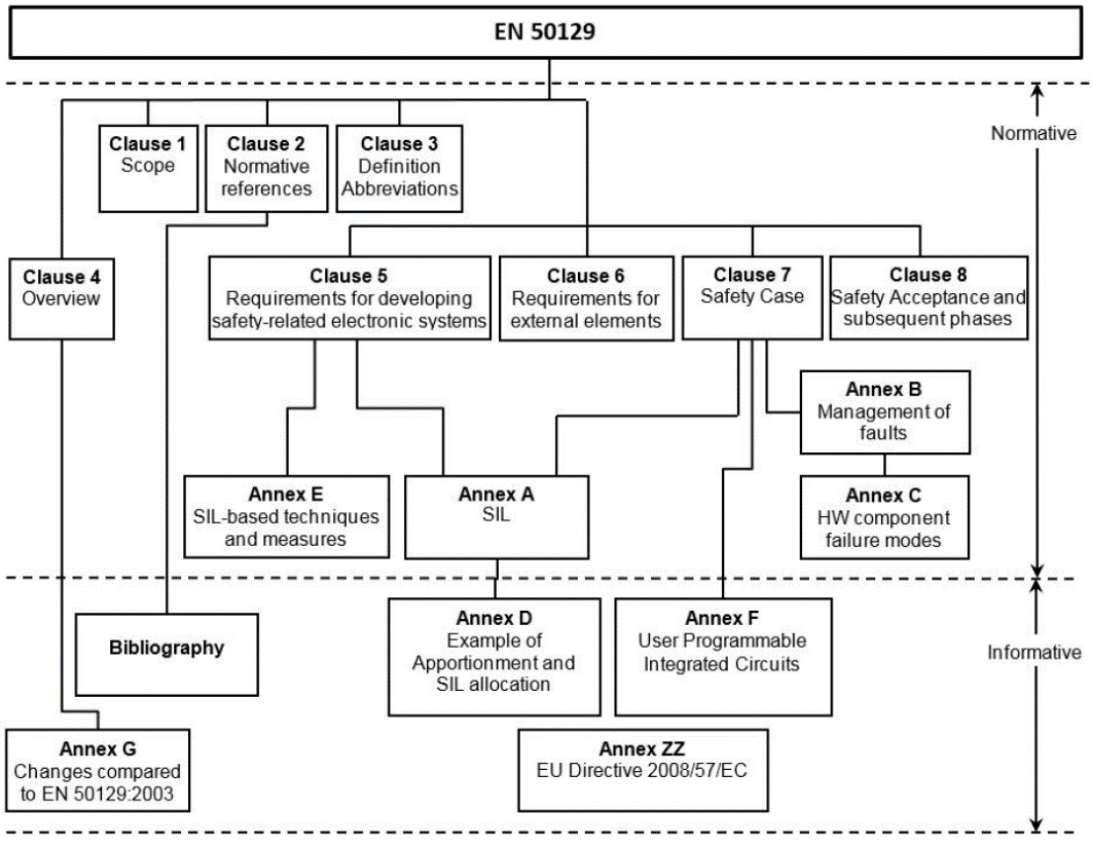
2.4.3 EN 50129

Den europeiska standarden EN 50129, *Järnvägsanläggningar - Dataöverföring och järnvägsstyrning - Elektroniska signalsystem av betydelse för säkerheten* (eng. *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*) är tillämpbar för säkerhetsrelaterade produkter inom järnvägens signalsystem. Den senaste uppdateringen av EN 50129 startade i januari 2015 och pågick till hösten 2017. Uppdateringen blev aktuell i samband med att EN 50126 uppdaterades. Den nya versionen blev godkänd av CENELEC 2018-06-07 och fastställdes 2019-01-23. Fram till 2021-11-23 gäller versionerna parallellt då den gamla

versionen utgår (CENELEC, 2018). WG 15 är den arbetsgrupp inom CENELEC SC 9XA som arbetade med uppdateringen och som ansvarar för underhåll av EN 50129.

EN 50129 beskriver villkor för säkerhetsacceptans gällande säkerhetsrelaterade elektroniska signalsystem. Huvudsakligen innehåller standarden hur en säkerhetsrapport (eng. Safety Case) ska vara uppbyggd samt övriga säkerhetskrav för systemet, delsystemet och komponenter (CENELEC, 2018). Figur 5 visar strukturen och innehållet för den nya versionen. Pilarna till höger i bilden visar vilka delar i standarden som klassas som normativa respektive informativa. De normativa delarna står för kravställande delar, det vill säga de avsnitt som innehåller krav på systemet, delsystemet eller komponenten. De informativa delarna är inte kravställande utan består av kompletterande material som delvis avser att öka förståelsen för de övriga delarna i standarden. Bestämmelser i standarden beskrivs med följande tre uttryck (Ciancabilla, 2019):

- Ska/Ska inte, för krav.
- Bör/Bör inte, för rekommendationer.
- Kan/Behöver inte, för medgivande/tillstånd.



Figur 5. Strukturen för den nya versionen(CENELEC, 2018).

En utgörande del av EN 50129 innehåller, som tidigare nämnt, krav gällande en så kallad säkerhetsrapport. För att öka förståelsen för denna studie beskrivs detta begrepp mer utförligt nedan.

Säkerhetsrapport

Säkerhetsrapport har använts sedan en lång tid tillbaka inom säkerhetskritiska system som bilindustrin, kärnkraft och järnväg. En säkerhetsrapport är ett strukturerat säkerhetsdokument som ska bevisa att systemet, delsystemet eller komponenten är accepterad med avseende på säkerhet (CENELEC, 2018). Författarna Stålhane och Myklebust (2016) redogör för att en säkerhetsrapport är en effektiv metod för att hjälpa företag inom systemutveckling att säkerställa att systemet är säkert nog. Syftet med att använda säkerhetsrapport är att framföra säkerhetsbevisning och att argumentera för säkerheten i systemet snarare än att bevisa det statistisk eller matematiskt. Enligt Stålhane och Myklebust (2016) är det mer ekonomiskt och effektivt att arbeta med säkerhetsrapporten under hela utvecklingsprocessen istället för att endast skriva den i utvecklingens slutfas. Författarna menar vidare att ett kontinuerligt arbete med säkerhetsbevisning under hela utvecklingen leder till en ökad förståelse för, och medvetenhet om säkerhet.

EN 50129 (både version 2003 och 2018) beskriver att följande sex delar ska ingå i en säkerhetsrapport (CENELEC, 2018):

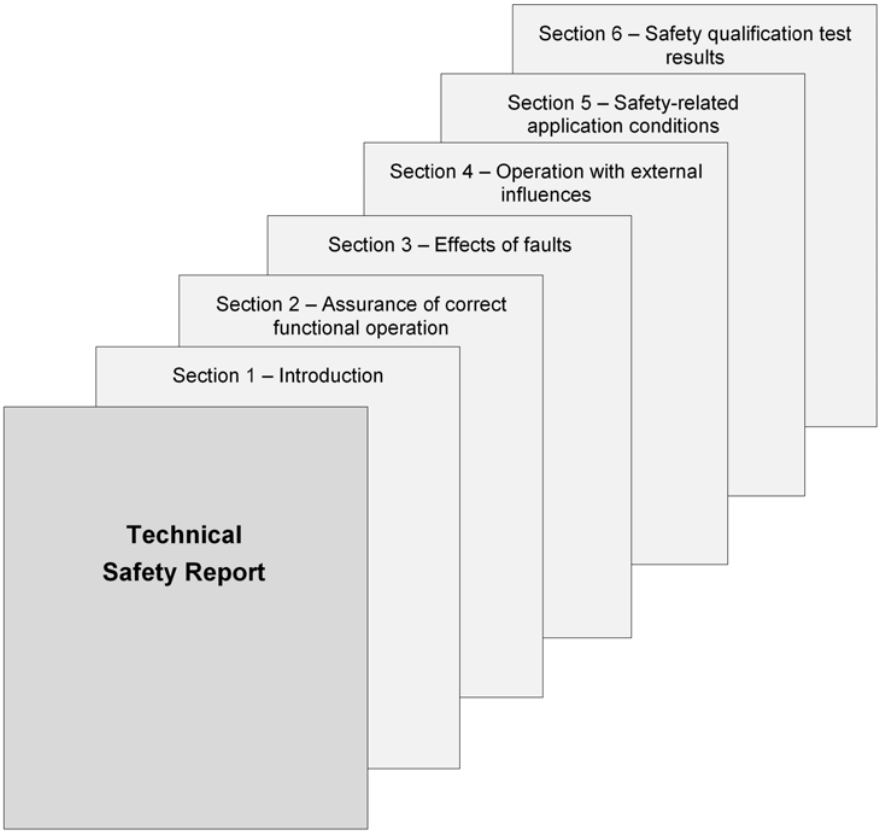
1) Systemdefinition (eng. Definition of System), ska specifikt definiera eller referera till systemet, delsystemet eller komponenten som den enskilda säkerhetsrapporten avser. Detta ska inkludera status för ändringen gällande samtliga krav samt dokumentation om tillämpning och design.

2) Kvalitetsledningsrapport (eng. Quality Management Report), ska redogöra bevis för ett effektivt kvalitetsarbete. Syftet med kvalitetsarbetet är att förbättra utförandet vid varje steg i livscykeln och att minska antal mänskliga fel för att totalt minska risken för systematiska fel. Organisationsstruktur, kvalitetsplanering, specifikation av kvalitetskrav, kompetens och erfarenheter, samt kvalitetsgranskning är exempel på delar som bör inkluderas i en kvalitetsledningsrapport.

3) Säkerhetsledningsrapport (eng. Safety Management Report), ska redogöra bevis för att alla delar inom processen för säkerhethantering utförs genom hela livscykeln. Processen av säkerhetshanteringen syftar till att minimera resterande risker som uppkommer från säkerhetsrelaterade systematiska fel och andra hot mot säkerheten. Rollfördelning och bevis för oberoende, säkerhetsplan, hantering av risker, specifikation av säkerhetskrav, systemdesign med avseende på säkerhet, drift- och underhållsplan samt validering och verifiering är delar som ingår ska ingå i en säkerhetsaledningsrapport.

4) Teknisk säkerhetsrapport (eng. Technical Safety Report), ska redogöra tekniska bevis för systemets, delsystemets eller komponentens design med avseende på säkerhet. I EN 50129 (både version 2003 och 2018) beskrivs hur strukturen för

en sådan rapport ska se ut vilket visas i Figur 6. Tekniska principer och alla tillhörande bevis som intygar säkerheten gällande design ska förklaras i denna del. Tillhörande bevis kan till exempel bestå av beräkningar, säkerhetsanalyser, designprinciper och testspecifikationer med tillhörande resultat.



Figur 6. Strukturen för den tekniska säkerhetsrapporten (CENELEC, 2018).

5) Relaterade säkerhetsbevis (eng. Related Safety Case), ska referera till övriga säkerhetsrapporter som systemet, delsystemet eller komponenten beror på.

6) Slutsats (eng. Conclusion), ska Slutsats sammanfatta samtliga säkerhetsbevis som dokumenterats i säkerhetsrapporten. Argument för att det gällande systemet, delsystemet eller komponenten är tillräckligt säker, givet att de angivna villkoren uppfylls, ska även redogöras för.

3. Teori

Teoriavsnittet beskriver inledningsvis begreppet säkerhet och synen på risker. Därefter redogörs för säkerhetsstyrning (eng. safety management) i organisationer och de två säkerhetsrelaterade perspektiven Safety-I och Safety-II. Avsnittet avslutas med den beskrivna teorins koppling till bakgrunden och studiens omfattning. Syftet med teorins delar är att sätta arbetet i en teoretisk kontext. Teorin utgör också en grund angående synen på säkerhet och säkerhetsstyrning som arbete hos ERTMS-programmet, gällande uppdateringen av EN 50129, kan jämföras med. Utifrån denna grund kan även eventuella åtgärder utmärkas vilket är en del av studiens mål.

3.1 Säkerhet

Begreppet säkerhet (eng. safety) är välkänt, används frekvent och förekommer i många olika typer av sammanhang. Till följd av att begreppet är så pass etablerat i samhället och att det har en betydelse för i princip alla menar Hollnagel (2014) att vi antar att säkerhet även har samma innebörd för alla individer. Det är till exempel ganska ofta som säkerhet inte ens definieras i olika dokument, doktorsavhandlingar, standarder med mera på grund av antagandet att alla redan vet vad säkerhet innebär. En förekommande beskrivning som finns är att säkerhet är frånvaro av oönskade utfall som exempelvis incidenter eller olyckor. Hollnagel (2014, s.2) nämner även följande mer detaljerade definition av säkerhet;

"Safety is the system property or quality that is necessary and sufficient to ensure that the number of events that could be harmful to workers, the public or the environment is acceptably low"

Trots att definitionen innehåller en del vagt uttryckta begrepp som inte direkt går att mäta är det en definition som är allmänt accepterad (Hollnagel, 2014). Även Leveson (2011) framhäver att säkerhet inte är en egenskap hos komponenter utan hos ett system. Säkerhet bör därför hanteras på systemnivå och inte på komponentnivå (Leveson, 2011). I den europeiska CENELEC-standarden EN 50129 definieras säkerhet som (CENELEC, 2018, s.16):

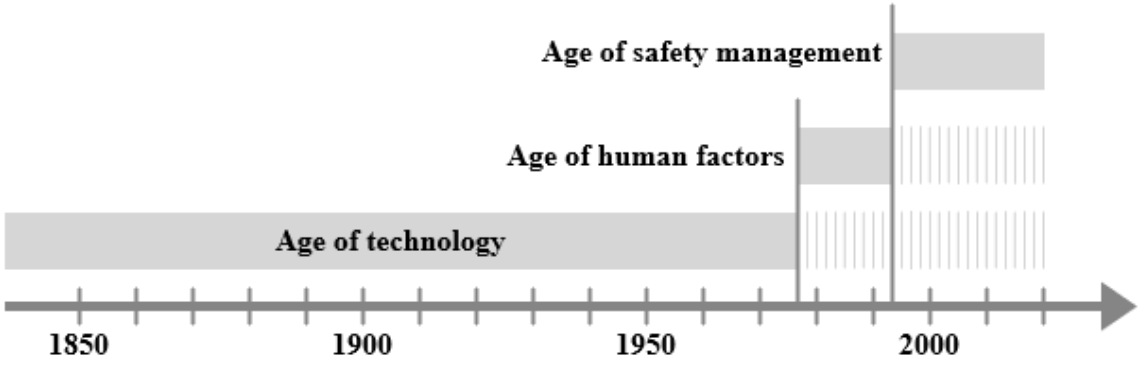
"Freedom from unacceptable risk"

I enighet med denna definition belyser Hollnagel (2014) beskrivningen av säkerhet som ett dynamiskt icke-event där fokus ligger på vad som inte händer. Båda definitionerna antyder att ett system är säkert när ingenting går fel. Innebörden av termen dynamisk är att det inte går att säkerställa att systemet fungerar felfritt. Därmed bör systemet regelbundet bevakas och hanteras (Hollnagel, 2014).

3.1.1 Historiskt perspektiv på säkerhet och risker

Förståelse för risker och att saker kan gå fel har funnits från början av den mänskliga civilisationen (Hollnagel, 2014). I och med den industriella revolutionen introducerades dock nya risker och till följd av detta även en ny förståelse för risk och säkerhet i samhället. Historiskt sett har tekniska komponenter setts som den primära orsaken till fel. I dagens samhälle, i takt med teknikens utveckling, har emellertid andra aspekter tagit mer plats. Hollnagel (2014) belyser exempelvis att en viss situation eller ett specifikt tillstånd kan analyseras som en orsak till en händelse idag till skillnad från tidigare då man endast studerade felfunktioner hos en eller flera komponenter.

Utvecklingen av synen på risk och säkerhet har beskrivits av bland annat Hale och Hovden (1998). De delar upp utvecklingen i tre olika faser; *the age of technology*, *the age of human factor* och *the age of the safety management*, se Figur 7. I den första fasen, *the age of technology*, sågs tekniken som det största hotet mot säkerhet. Detta berodde till stor del på att tekniken var opålitlig och att människan inte hade lärt sig att hantera och skydda sig från de olika risker som tekniken utgjorde. Vid tidigt 1950-tal utvecklades ett nytt ingenjörsområde inom pålitlighet och riskanalyser samt säkerhetsbedömningar baserade på sannolikhetsteorier etablerades i samhället. I takt med att tekniken växte utvecklades även olika metoder för att säkerställa och analysera risker med tekniken så som felträdsanalys. Under denna period fanns dock inget större fokus på mänskliga eller organisatoriska aspekter utan tekniken stod i centrum (Hale och Hovden, 1998).



Figur 7. Tre faser av säkerhet

I den andra fasen, *the age of human factor*, upptäcktes dock vikten av den mänskliga faktorn och människan började ses som en opålitlig och felande länk i systemet. Metoder för att involvera och utvärdera den mänskliga faktorn utvecklades därefter och blev en del av riskanalyser. Hale och Hovden (1998) menar vidare att i den tredje fasen, *the age of the safety management*, klargjordes även att den organisatoriska aspekten var en avgörande del gällande systemsäkerhet och fokus skiftade till systemet bakom säkerhetsstyrning (eng. safety management). Att inkludera denna aspekt krävde dock nya sätt att tänka angående säkerhet, exempelvis med avseende på organisationskultur (Hale och Hovden, 1998). Hollnagel (2014) menar på att varken mänskliga eller organisatoriska faktorer kan hanteras på samma sätt som tekniska komponenter. Synen på att säkerheten

ökar genom att minimera orsakerna till incidenter och olyckor har dock varit konstant under samtliga faser.

3.2 Säkerhetsstyrning

Det krävs något sätt att bevisa säkerhet för att veta att system är säkra i praktiken. Säkerhetsstyrning handlar enligt Hollnagel (2014) om att kontrollera och agera på ett sådant sätt som stärker säkerheten. Genom noggrann planering, utbildning av personal och detaljerade instruktioner kan säkerheten höjas (Hollnagel, 2014). Vid fall där det inte finns någon återkoppling för det agerandet, eller om återkopplingen är långsam och fördröjd, är konsekvensen av agerandet svår att avgöra. Detta gör det problematiskt att veta om säkerhetsarbetet uppfyller dess tänkta effekt. Hollnagel (2014) menar dessutom att en minskad aktivitet i säkerhetsarbetet kan ske till följd av att få fel inträffar i ett system, det vill säga när säkerhetsnivån anses vara hög. Enligt Wallström och Rollenhagen (2014) kan säkerhetsstyrning generellt ses som organisatorisk kontroll som är väsentlig för säkerheten. Författarna belyser även vikten av att hantera säkerhet ur ett MTO-perspektiv, det vill säga att ta hänsyn till alla delsystem gällande människa, teknik och organisation (MTO). Information bestående av dokumentation, databaser och instruktioner beskrivs vidare av Wallström och Rollenhagen (2014) som ett fjärde element som utgör en viktig del inom säkerhetstyrning. I standarden EN 50129 definieras säkerhetsstyrning (eng. Safety management) enligt följande:

”The management structure which ensures that the safety process is properly implemented” (CENELEC, 2003, s.12)

Lucic (2015) anser att detaljerade riskanalyser är fördelaktigt för systemets utförande avseende säkerhet samtidigt som en utförlig säkerhetsstyrning både är kostnads- och tidseffektiv. Vidare beskriver Lucic (2015) tre principer inom riskanalys som bör beaktas för att säkerställa analysens fullständighet och för att skapa försvarbara argument om systemets säkerhet. Systematiskt tillvägagångsätt är den första principen där dokumentering och planering av säkerhetsrelaterat arbete är av största betydelse. Vidare beskrivs vikten av ett holistiskt perspektiv. Då säkerheten i ett system påverkas av alla komponenter, från hårdvara och mjukvara till mänskliga samt miljömässiga faktorer, bör dessa tas hänsyn till genom hela systemets livscykel. Den tredje principen är användandet av ämnesspecifik expertis. Dagens system är ofta komplexa och består av många olika delsystem vilket ökar relevansen av kunskap från experter på dessa delsystem (Lucic, 2015).

Enligt Hollnagel (2014) fokuserar säkerhetsstyrning ofta på att undvika eller förebygga att något går fel snarare än att säkerställa att det går rätt till. Anledningen till detta menar Hollnagel (2014) grundar sig i både praktiska och psykologiska faktorer. Människor vill både säkerställa att aktiviteter och planer är fria från fel samtidigt som det finns ett kunskapsbehov av att veta vad som har hänt eller vad som kan hända och att det är hanterbart. Dessutom finns det krav från regeringar och auktoriteter världen över på rapportering av incidenter, oavsiktliga händelser och olyckor. Stort fokus läggs därmed

på vad som går fel vid hantering av systemsäkerhet. Hollnagel (2014) belyser dock det faktum att ingen lägger energi på att analysera eller uppmärksamma det som går rätt till.

3.3 Safety-I och Safety-II

Hollnagel (2014; 2019) beskriver två perspektiv av säkerhet, vilka benämns som Safety-I och Safety-II. Safety-I representerar ett mer traditionellt säkerhetstänk medan Safety-II är ett nytt kompletterande sätt att se på säkerhet. Båda perspektiven och deras relation till varandra presenteras i detta avsnitt.

Inom Safety-I definieras säkerhet som ett tillstånd där antalet negativa händelser, som incidenter och olyckor, är så lågt som möjligt. Syftet med säkerhetsstyrning inom Safety-I är således att minska antalet negativa händelser till en viss acceptabel nivå, med andra ord att upprätthålla det säkra tillståndet. Vidare menar Hollnagel (2014) att perspektivet innehåller två tillstånd; när något går fel och när allt fungerar som det ska. Ur ett Safety-I perspektiv antas fel bero på felfunktion hos systemets olika komponenter så som teknik, arbetare, processer och organisationen. Eftersom människan är den mest varierande komponenten ses den mänskliga faktorn som en stor riskfaktor (Hollnagel et al., 2015). De fel som orsakar negativa händelser kan minskas genom att avlägsna faror och risker samt genom att se till att arbetet utförs som planerat. Felen kan även minskas genom olika typer av barriärer som regler, standarder, procedurer med mera. Inom Safety-I anses det alltid finnas en eller flera identifierbara orsaker bakom varje negativ händelse, ett så kallat orsakssamband. Detta innebär i sin tur att alla olyckor kan förhindras (Hollnagel, 2019). Enligt Hollnagel et al (2015) blev denna syn på säkerhet väl etablerad inom säkerhetskritiska industrier redan vid 1960-talet.

I takt med att system i samhället blir mer och mer komplicerade anser dock Hollnagel (2014) att orsakssambandet mellan händelser och utfall blir svårare att förstå. En enkel orsak för varje händelse går således inte att finna på samma sätt som tidigare. Traditionella tankesätt kring säkerhet, som Safety-I perspektivet, går därmed inte längre att applicera i alla sammanhang. Till följd av detta menar Hollnagel (2014) att metoder och modeller gällande säkerhet bör spegla dagens förändrade och mer komplexa sociotekniska system. Det är exempelvis relevant att granska systemet under ett längre tidsspann, det vill säga både tidigare och senare under systemets livscykel. Det är även relevant att ta in både vad som händer i det dagliga arbetet och hur organisationen som styr det fungerar. Ytterligare faktorer som påverkar säkerheten och som bör tas hänsyn till är hur system interagerar med och påverkar andra system samt gränssnitten där emellan (Hollnagel, 2014). På grund av systemens ökade komplexitet föddes Safety-II.

Safety-II beskrivs av Hollnagel (2014) som ett komplement till Safety-I för att få ett bredare perspektiv och nytt synsätt i relation till risker och säkerhet. Inom Safety-II definieras säkerhet som ett tillstånd där antalet positiva händelser, det vill säga antalet planerade och acceptabla utfall, är så högt som möjligt. Safety-II strävar inte efter att identifiera orsakssamband utan koncentrerar sig på ett sätt att beskriva det arbete som utförs. I Safety-II analyseras händelser utifrån antagandet att händelserna har skett

tidigare och kommer att ske igen. Händelsen ses som en del i det dagliga arbete och analyseras därefter. Genom denna analys breddas perspektiven av händelsen och den först funna rimliga orsaken fastställs inte som den enda möjliga orsaken (Hollnagel, 2019). Sociotekniska system är mer komplexa och svårhanterliga vilket bidrar till att arbetsförhållanden ofta förändras från det som blivit beskrivet och specificerat. Både uppgifter och verktyg måste därmed anpassas till situationen. Safety-II främjar snarare flexibilitet och variabilitet än att se det som en begränsning. Enligt Hollnagel et al (2015) ligger förändringar och justeringar i arbetet till grund för ett lyckat utförande och är svaret på frågan varför och hur saker går rätt till. Vidare ses frånvaro av fel som ett resultat av aktivt arbete inom Safety-II och säkerhet ses inte som ett icke-event då det varken kan bli uppmätt eller observerat. Säkerhet är istället något som sker kontinuerligt och kan därmed hanteras och mätas (Hollnagel, 2019). Tabell 5 beskriver de två perspektiven.

Tabell 5. Tabellen beskriver skillnader mellan Safety-I och Safety-II (Hollnagel, 2014).

	Safety-I	**Safety-II**
Definition av säkerhet	Antalet negativa händelser, som incidenter och olyckor, är så lågt som möjligt.	Antalet positiva händelser, det vill säga planerade och acceptabla utfall, är så högt som möjligt.
Princip för säkerhetsstyrning	Reaktiv. Reagerar när en olycka skett eller en risk klassas som oacceptabel.	Proaktiv. Arbetar kontinuerligt med att förutse händelser och utveckla arbetssätt samt system som fungerar.
Orsaker till olyckor	Olyckor orsakas av misslyckanden och felfunktioner. Syftet med en utredning är att finna orsaker och medverkande faktorer.	Saker sker på samma sätt oavsett utfall. Syftet med en utredning är att förstå hur det vanligtvis går rätt till för att förklara hur och varför saker ibland går fel.
Attityd till den mänskliga faktorn	Människan ses främst som en belastning eller en riskfaktor.	Människan ses som en nödvändig resurs för systemets flexibilitet.
Variabilitet gällande prestation	Skadlig. Bör förhindras till så stor grad som möjligt.	Både oundviklig och användbar. Bör övervakas och hanteras.

Det Hollnagel (2014;2019) framför med dessa två perspektiv är att det bör vara viktigare inom säkerhetsstyrning att fokusera på att det ska gå rätt till än att det inte ska gå fel. Safety-I perspektivet fokuserar på att undvika samt förhindra fel och därmed på förmodade orsaker. Genom att identifiera och eliminera fel kan en attityd av att allt är under kontroll skapas. Safety-II motverkar denna effekt genom att arbeta kontinuerligt

och proaktivt. Inom Safety-II ligger framgång i fokus och arbete för att skapa de bästa möjligheterna för att systemet fortsättningsvis ska kunna prestera som tänkt. Orsaken till varför system fungerar som de ska beror på en förståelse för systemet som helhet. Ju mer som går rätt till desto säkrare är systemet (Hollnagel, 2014).

Både Safety-I och Safety-II resulterar i ett minskat antal oönskade utfall om än genom olika metoder. Safety-II handlar om proaktivt säkerhetsarbete vilket är fördelaktigt då det kräver mindre ansträngning i jämförelse med när händelsen har haft tid att utvecklas (Hollnagel, 2019). Tidiga åtgärder sparar således både tid och resurser. En förståelse för systemet som helhet, dess klimat, komponenter och olika gränssnitt är väsentliga delar för att ett proaktivt arbetssätt ska fungera. Istället för att hitta orsaker till enskilda event bör fokus ligga på att identifiera samband för händelser. Hollnagel (2014) menar dock att det krävs en del ansträngning och motivation för att övergå till ett mer proaktivt arbetssätt varför det ofta ses som för resurskrävande i ett kortsiktigt perspektiv. Effektivitet hamnar ofta högre upp än noggrannhet i pressade arbetssituationer vilket gör det svårare att arbeta proaktivt. Även organisationer som har applicerat en proaktiv säkerhetsstyrning kan mötas av svårigheter i att arbeta proaktivt gällande småskaliga händelser som berör dagliga aktiviteter. Hollnagel (2014) anser dock att investeringen bör vara värt det ur ett långsiktigt perspektiv.

Enligt Hollnagel (2014) har företagsledningar ofta svårt att förstå vikten av investeringar kring säkerhet, framförallt om verksamheten har varit fri från olyckor under en längre period. Två exempel på detta är Forsmarkincidenten år 2006 och Boeing 737 Max-olyckorna år 2018 och 2019. I kärnkraftsanläggningen Forsmark snabbstoppades en reaktor år 2006 till följd av kraftiga spänningsvariationer i elnätet (Analysgruppen, 2006). Vid inträffandet blev säkerheten hotad då de barriärer och försvar som skulle förhindra att en riskfylld situation uppstod inte fungerade. Incidenten visade på en bristande säkerhetskultur, det vill säga säkerhetens betydelse i organisationen och bland medarbetare, då man prioriterat produktionsaspekter framför säkerhetsaspekter under en längre tid. Olyckorna med Boeing 737 Max är ett annat exempel på ett bristande säkerhetsperspektiv. Flygplansmodellen Boeing 737 Max sattes i bruk år 2017 (Palmer, 2019). Den nya modellen utvecklades så pass lik tidigare Boeing-modeller att man inte behövde certifiera om 737 Max-modellen, vilket sparade både resurser och tid. Tidigare modeller hade dessutom fungerat olycksfritt under en lång period. En skillnad mot föregående modeller var dock att Boeing 737 Max installerades med mer bränsleeffektiva motorer. Motorerna positionerades även längre fram och ut på vingarna i jämförelse med tidigare modeller vilket påverkade hur planet flög. För att få planet att likna tidigare modeller och motverka den effekt som positionen av motorerna orsakade installerades ett nytt automatiskt mjukvarusystem. Detta mjukvarusystem skulle fungera automatiskt vid behov och nämndes därför inte i några manualer (Palmer, 2019). Två år efter att modellen sattes i bruk hade två av planen kraschat vilket skedde till följd av den nya tekniken och det automatiska mjukvarusystemet i kombination med en bristande säkerhetskultur.

Det finns således en konflikt mellan säkerhet och produktivitet. I Safety-I utförs säkerhetsarbete, som tidigare nämnt, för att minska antal negativa händelser (Hollnagel, 2014). Investering i säkerhet införs därmed för att förhindra negativa händelser. Till följd av detta ses investeringen som försvarbar endast när en olycka skett. I Safety-II ses en investering i säkerhet istället som en investering i produktivitet då säkerhetsarbete utförs för att försäkra att systemet fungerar som det ska. Detta leder till att säkerhetsarbetet är försvarbart oavsett om det sker en olycka eller inte (Hollnagel, 2014). Tanken med Safety-II är således att fokus bör ligga på att studera och utveckla kunskap både om positiva och negativa händelser. Med andra ord att skapa sig en förståelse för systemet och inte bara utföra åtgärder när systemet inte agerar som tänkt (Hollnagel, 2019).

3.4 Användningsområde

Enligt Hollnagel (2014) var järnvägen en av de första systemen där säker teknik i kombination med kontroll från regeringen efterfrågades då det fanns en oro för säkerheten. Järnvägen är även ett tidigt exempel på ett sociotekniskt system som inkluderar allt ifrån att producera material och verktyg, utbilda personal, planera aktiviteter till att underhålla utrustning och att dagligen övervaka samt kontrollera procedurer. Det krävs därför tydliga beskrivningar och specifikationer för systemet och dess funktioner för att systemet som helhet ska vara kontrollerbart (Hollnagel, 2014). Säkerhet är även en viktig aspekt i arbetet mot en standardiserad och interoperabel järnväg i Europa som ERTMS syftar till att vara. Smith et al (2012) anser att säkerhetsaspekter gällande både ombord och markutrustning, rutiner och mänskliga faktorer måste tas hänsyn till vid utvecklingen av ett sådant system. Införandet av ERTMS kräver därför en gemensam förståelse och uppfyllelse av de säkerhetskrav som tillkommer med systemet.

Vid uppdatering av en standard, som denna studie avser att studera, kan nya krav tillkomma. Den studerade standarden EN 50129 innehåller som tidigare nämnt säkerhetskrav gällande elektroniska signalsystem. Mer specifikt innehåller EN 50129 krav på säkerhetsacceptans genom utformningen av säkerhetsrapporter samt övriga säkerhetsrelaterade krav för systemet. De säkerhetsaspekter i form av ett sociotekniskt system innehållandes människor och kultur som belysts av Hollnagel (2014;2019) påverkas således också av den nya standarden. Den nya versionen av standarden kan därmed påverka aktiviteter kring säkerhetsstyrningen och till följd av det även säkerheten för ERTMS införande i Sverige. Införandet av ERTMS kan ses som en risk då det är en förändring av samma natur som i Boeing-fallet. Uppdateringen av standarden, även om den i sig handlar om säkerhet, måste därför ses som en förändring som ska prövas som vilken annan förändring som helst. Som beskrivet i det inledande avsnittet syftar studien till att kartlägga och analysera hur uppdateringen av standarden EN 50129 påverkar ERTMS-programmet. Detta kan endast undersökas genom kvalitativ metod där intervjuer med experter inom området får möjlighet att problematisera införandet av den uppdaterade versionen av EN 50129 ur ett övergripande säkerhetsperspektiv, med andra ord ur ett sociotekniskt perspektiv.

4. Metodologisk ansats

I detta avsnitt presenteras den metodologiska ansats som har använts i studien. Avsnittet inleds med en beskrivning och motivering för valet av studiens metoder. Vidare beskrivs varje del av studiens genomförande.

4.1 Kvalitativ metod

Denna studies insamling av data bygger på kvalitativa metoder. Kvale och Brinkmann (2014) beskriver att en kvalitativ metod är lämplig då syftet ska besvara *hur* någonting är eller sker. Enligt Alvehus (2013) inriktar sig kvalitativ metod på innebörden av ett fenomen till skillnad från kvantitativ metod som berör statistiskt verifierbara samband. Kvalitativa metoder syftar inte till att begränsa olika fenomens komplexitet för att kunna anpassas till olika samband utan snarare att belysa komplexiteten och den variation som finns. Alvehus (2013) uttrycker även att kvalitativ metod är en tolkande forskning. Begreppet tolkning kan verka vagt och som en godtycklig handling i kontext till forskning. Syftet med kvalitativ metod och den tolkande forskningen är dock att skapa en generell förståelse för de fenomen som studeras, att utveckla förståelse och att medverka till ett mer nyanserat synsätt. Tolkningen utformas inom en viss kontext i förhållande till teorier vilket höjer kvaliteten och tolkningens relevans (Alvehus, 2013).

Eftersom denna studie syftar till att förstå ett fenomen, uppdateringen av en standard, samt att besvara *hur* denna uppdatering påverkar ERTMS-programmet valdes en kvalitativ metod. Valet av metod kan även stärkas i det faktum att studien bidrar till att belysa komplexitet samt utveckla kunskap och synsätt kring det studerade ämnet.

Kvalitativ analys kan enligt Fejes och Thornberg (2015) ha flera olika syften. Bland annat kan ett syfte i en kvalitativ analys vara att utveckla en teori, beskriva ett fenomen eller att identifiera förklaringar till skillnader mellan olika fall som har studerats. Då denna studies syfte är att kartlägga skillnader mellan den gamla och den nya versionen av EN 50129 samt att studera dess påverkan på ERTMS-programmet, är det ett fenomen som beskrivs snarare än att en teori som utvecklas.

4.2 Insamling av data

Insamling av data har skett kvalitativt dels genom en litteraturstudie, dels via intervjuer. En del bakgrundsfakta och förståelse för ämnets kontext har även intagits vid en intern introduktionsutbildning på TRV som genomfördes den 27 och 28 januari. Ytterligare datainsamling har skett i form av mail som har skickats för att täcka kompletterande frågor som uppkommit efter intervjuer och under studiens arbetsgång.

4.2.1 Litteraturstudie

En litteraturstudie har genomförts både med syfte att få en fördjupad kunskap om det valda ämnet och att skapa en grund för den empiriska datainsamlingen. Den första delen

av litteraturstudien bestod av att söka bakgrundsfakta och utveckla kunskap angående signalsystem, ERTMS, standarder och TRV:s ERTMS-program. Även tidigare studier kring standarder, framförallt EN 50129, har studerats. Därefter söktes efter ett teoretiskt sammanhang kopplat till standardens innehåll och kontext vilket ledde till områdena säkerhet, risk, säkerhetsstyrning samt begreppen Safety-I och Safety-II. Val av teoretiskt område samt studiens metodologiska angreppsätt diskuteras vidare i diskussionsavsnittet, se avsnitt 7.1 och 7.2.

4.2.2 Intervjuer

Kvalitativ forskning innehåller ofta intervjuer som metod till empirisk datainsamling. Enligt Alvehus (2013) är intervjuer passande att genomföra om en persons tankar, erfarenheter och åsikter angående ett visst fenomen ska studeras. Även Lantz (2013) uttrycker att ställa frågor via intervjuer är det enklaste sättet att få information kring en persons idéer och uppfattningar. Eftersom studien primärt syftar till att studera hur uppdateringen av EN 50129 påverkar ERTMS-programmet, krävs information från berörda parter. Studiens metod och den empiriska datainsamlingen valdes därmed till att bestå av intervjuer.

Intervjuer kan utformas och genomföras på olika sätt, ostrukturerat, semistrukturerat eller strukturerat. Bryman och Bell (2013) anser att semistrukturerade intervjuer är att föredra vid granskning av mer detaljerade fall. Alvesson (2013) beskriver att en semistrukturerad intervju utgår ifrån några identifierade teman eller ett par öppna frågor som har formulerats inför intervjun. Inom denna intervjuform finns det rum för följdfrågor och även utrymme för respondenten att påverka intervjuns innehåll. Samtliga intervjuer i denna studie har varit av semistrukturerad karaktär. Enligt Kvale och Brinkmann (2014) innehåller semistrukturerade intervjuer en kombination av struktur och flexibilitet vilket bidrar till en bred och nyanserad insamling av data.

4.2.3 Val av respondenter

Hollnagel (2014) skriver att den mest relevanta källan för hur ett arbete utförs är de personer som faktiskt utför arbetet i praktiken. Urvalet av intervjupersoner har utgått från de personer inom ERTMS-programmet som arbetar med och berörs av EN 50129. Ett medvetet urval av respondenter har används i kombination med ett snöbollsurval vilket innebär att identifierade intervjupersoner i sin tur rekommenderade nya personer att intervjua (Bryman och Bell, 2013). Samtliga personer som har medverkat i studiens intervjuer arbetar på TRV, till största del inom ERTMS-programmet men även inom andra organisationer på TRV. Respondenterna har varierat både i kön, ålder, erfarenhet och befattning. Tabell 6 visar de olika befattningar som de valda respondenterna har. Studien har anonymiserats då respondenternas namn inte anses vara relevant för studiens resultat. Anonymisering valdes också för att respondenterna skulle känna sig så fria som möjligt i sina uttalande om verksamheten.

Tabell 6. Tabell över befattning hos de som har intervjuats.

Befattning	Respondent
MTO-specialist	A
Kvalitetsspecialist	B
Säkerhetskoordinator	C, D, E, F, K
GOP-handläggare/säkerhetskoordinator	G
Validering och Verifierings - koordinator	H
Systemspecialist - IT	I
Medlem i CENELEC SC 9XA WG15	J

Totalt har 10 intervjuer genomförts. Tre av intervjuerna var fysiska möten som hölls på TRV:s kontor i Solna. Resterande intervjuer genomfördes via Skype. Intervjuerna pågick mellan 30 – 120 minuter. En grundregel som bör följas i intervjusammanhang är att intervjuaren ska börja med att presentera ramarna för arbetet och intervjuns sammanhang (Lantz, 2013). På så sätt skapas en gemensam förståelse för vad som ska åstadkommas och intervjun blir effektivare. Inför varje intervju informerades därför respondenterna om både syftet med studien och den specifika intervjun. Respondenterna informerades dessutom om att deltagande var frivilligt och att alla resultatet i studien skulle anonymiseras. Enligt Bryman och Bell (2013) kan anteckningar vid intervjuer distrahera intervjuaren. För att upprätthålla ett fullständigt fokus på intervjun och eventuella följdfrågor togs därmed inga anteckningar under intervjuerna. Samtliga intervjuer spelades istället in efter godkännande från de medverkande.

I studiens tidiga stadie hölls en intervju med en medlem i CENELEC SC 9XA WG15, den arbetsgrupp som genomförde uppdateringen av EN 50129. Denna intervju bidrog till utökad generell kunskap om och förståelse för arbetet kring standarder samt bakgrundsfakta till EN 50129 och övriga standarder. Intervjun rymde även specifika frågor om skillnader mellan de två versionerna av standarden samt dess betydelse. Intervjun var av semistrukturerad karaktär och pågick i 90 minuter.

Hollnagel (2014) nämner fördelen av att intervjua fler personer samtidigt då det kan leda till en upptäckt om att arbetet utförs på olika sätt. För att samla in fler perspektiv samtidigt och för att möjliggöra diskussioner mellan berörda personer hölls en semistrukturerad gruppintervju. 7 respondenter (A, C, D, E, F, G, H) medverkade vid gruppintervjun som pågick i 120 minuter. Syftet med de resterande intervjuerna var att få ytterligare information om och hur uppdateringen av standarden påverkar ERTMS-programmet. Intervjuerna syftade även till att studera om de nya kraven som specificeras i EN 50129 följs i dagsläget samt hur säkerhetsarbetet går till. Intervjuernas innehåll och fokus

vinklades efter respondentens arbetsområde och befattning. De flesta ämnen och frågor togs dock upp med fler respondenter. Detta för att få fler perspektiv inom samma område. Då intervjuerna har varit av semistrukturerad karaktär har intervjufrågorna varierat och därmed även ramen för intervjuerna. Till följd av detta presenteras inte samtliga intervjufrågor i denna studie. I Appendix A finns däremot en förenklad intervjuguide som har används under studiens intervjuer. Informationen från intervjuerna har även kompletterats med löpande granskning av säkerhetsrelaterad intern dokumentation hos TRV som bland annat beskriver hur säkerhetsarbetet ska fungera på TRV.

4.3 Bearbetning av insamlad data

Inom kvalitativ forskning är bearbetning och analys av data en process där forskaren arbetar och organiserar datamaterial, som exempelvis transkriptioner från intervjuer eller observationer. Fejes och Thornberg (2015) påpekar att varje analys av data vid en kvalitativ studie är unik. Däremot, för att analysen ska landa i ett resultat, är det enligt Fejes och Thornberg (2015) viktigt att bryta ner data, identifiera mönster och urskilja det som är västenligt från mängden av data. Eriksson och Widersheim-Paul (2006) anser att bearbetning av insamlad data bör utföras fortlöpande då det är fördelaktigt för arbetet framåt. De inspelade intervjuerna transkriberades således i nära anslutning efter varje intervju. Transkriberingen utfördes ordagrant och kontrollerades flertal gånger för att möjliggöra korrekta citeringar och för att inte förbise något.

Lantz (2013) beskriver att ett första steg i bearbetning av data och den kvalitativa analysen är att reducera data, det vill säga att både välja och välja bort insamlad data. Efter transkriberingen identifierades således de främst förekommande ämnena och de respondenterna uttryckte som mest väsentligt med avseende på studiens syfte. Dessa ämnen utgjorde sedan grunden och strukturen för studiens resultat samt analys. Enligt Lantz (2013) innehåller en kvalitativ analys inledningsvis en beskrivning av resultaten, till exempel vad respondenterna har sagt, som sedan följs av en analys. I denna studie beskrivs först det insamlade materialet både från EN 50129 samt från intervjuerna i resultatavsnittet, avsnitt 5. Detta material diskuteras därefter i det efterföljande analysavsnittet, avsnitt 6.

4.4 Gap-analys

En utgörande del av studiens genomförande har varit att kartlägga och jämföra skillnader mellan de två versionerna av standarden EN 50129. En gap-analys av dessa två dokument har därmed genomförts. En gap-analys syftar till att identifiera och bedöma skillnader för att på ett effektivt sätt kunna genomföra ett förändringsarbete. En förutsättning för ett genomföra en gap-analys är att det finns ett nuläge och ett önskat framtida läge som går att jämföra. I denna studie utgör nuläget den gamla versionen av standarden och det önskade framtida läget den nya uppdaterade versionen. Genom att utföra en gap-analys kan skillnader framhävas samt vilka åtgärder som krävs för att nå det önskande framtida läget och vilka effekter det kan få.

Den utförda gap-analysen i denna studie består av en sammanfattning över de främsta identifierade skillnaderna samt en detaljerad kravanalys, det vill säga en analys av de krav som finns i de båda versionerna av standarden. I gap-analysen presenteras den detaljerade kravanalysen i tabellform och innehåller samtliga krav från den nya och gamla versionen av EN 50129. Tabellen innehåller även kommentarer och sammanfattningar av versionsskillnaderna. Kommentarerna som har använts för att beskriva förändringen i gap-analysen visas i Tabell 7.

Tabell 7. Kommentarer som har använts för att beskriva förändringen i gap-analysen.

Kommentarer använda i gap-analysen	**Förklaring**
-	Ingen förändring. Samma eller till största del samma innebörd
Borttaget	Borttaget krav/ borttagen del i EN50129:2018
Nytt	Nytt krav/ny del i EN 50129:2018
Anpassat (med avseende på EN 50126 och/eller SIL-klassning)	Kravet har anpassats till de nya referenserna EN 50126-1 och EN 50126-2 och/eller till ny SIL-klassning, dvs Basic Integrity istället för SIL 0.
Uppdelat	Flera krav i EN 50129:2003 har delats upp i EN 50129:2018
Sammanslaget	Flera krav i EN 50129:2003 har slagits ihop i EN 50129:2018
Striktare	Tydligare eller striktare krav i EN 50129:2018.
Mindre strikt	Mindre specifikt eller mindre strikt krav i EN 50129:2018.
Mer detaljerad bild/tabell	Bilden/tabellen i EN 50129:2018 är mer detaljerad
Flyttat	Krav i EN 50129:2003 har flyttat till ny del i EN 50129:2018

Gap-analysen utgjorde en grund för en del av resultatet samt de intervjuer som har genomförts. Detta arbete utfördes främst i början av studien, parallellt med litteraturstudien, men även löpande i samband med studiens empiriska datainsamling. Det material som denna del av studien bygger på är refererad till i referenslistan, under rubriken standarder, men finns inte direkt tillgänglig för externa parter.

5. Resultat

I resultatavsnittet presenteras studiens resultat vilket består av insamlad data dels från den utförda gap-analysen, dels från intervjuerna. De resultat som presenteras från intervjuerna kommer både från gruppintervjun samt de individuella intervjuerna, ingen specifik uppdelning mellan dessa har gjorts. Avsnittet inleds med en allmän beskrivning av säkerhetsstyrningen på ERTMS-programmet. Denna del avser inte att specifikt besvara någon av studiens frågeställningar utan är en allmän beskrivning av säkerhetsstyrningen på ERTMS-programmet. Delen är dock ett resultat från intervjustudien och är relevant inför den kommande analysen kring åtgärder samt den efterföljande diskussionen, vilket är anledningen till att den informationen introduceras i resultatet. Vidare beskrivs uppdateringen av EN 50129 som inleds med att presentera generella skillnader mellan den gamla och den nya versionen av standarden. Därefter presenteras ett antal identifierade förändringar och deras påverkan på TRV:s ERTMS-program. Dessa identifierade förändringar gäller följande områden; SIL, Kvalitetsstyrning, Dokumentation, Organisation, Roller och Granskning, Verifiering och Validering, Ansvarsfördelning, Safety Related Applicaion Condition (SRAC), IT-säkerhet och Människa, Teknik, Organisation (MTO). Urvalet av de identifierade områdena baserar sig på gap-analysen samt den bearbetning av insamlad data som beskrivs i avsnitt 4.3 och 4.4 i metodavsnittet. Då studien har anonymiserats har respondenterna istället för namn benämnts med en bokstav (A, B, C, D, E, F, G, H, I, J och K), se Tabell 6 för befattningar.

5.1 Säkerhetstyrning på ERTMS-programmet

> *Det här med säkerhetsfrågan i grunden, det är för mig en ja eller nej fråga. Finns det en koppling till säkerhet? Ja eller nej, och finns det de så måste det beaktas i säkerhetsarbetet."* (Respondent F)

Att veta att systemet blir helt säkert är svårt att konstatera. Respondent F beskriver att säkerhet bygger på att man har drivit systemet under en lång tid och vet vad som fungerar och inte i kombination med organisationen och hur allt samverkar. Det som formar säkerheten är en blandning av erfarenhet, krav från regler och standarder samt kunskapen hos experter och personer i organisationen som har den kunskapen (Respondent C, E, F). Det beskrivs även att arbetet kring säkerhet utförs mer proaktivt nu, i och med att man till exempel arbetar efter standarder, jämfört med hur man arbetat tidigare. Säkerhetsstyrningen framställs vara under ständig utveckling vilket Respondent F beskriver är viktigt; *"så fort man hittar någon förbättringspotential så jobbar vi ju på det och det är ju en väldigt viktig aspekt i det hela. För det kommer inte vara perfekt i praktiken och det viktiga där är att man har inställningen att man får lyfta saker och att man kommer ta det på allvar och kommer reagera på det"* (Respondent F). Respondent E anser att säkerhet är mer komplext än att endast se det som frånvaro av oacceptabla risker och menar på att *"det grundar sig i en tanke att man ska förstå sig på vilken risknivå man har och kunna bekräfta att den är acceptabel på ett informerat, medvetet,*

genomtänkt och förankrat sätt". Man strävar hela tiden efter ett säkrare system. Samtidigt sätts säkerheten alltid i relation till driftmål och övriga faktorer. Respondent E menar att det absolut säkraste sättet för att inte få några olyckor skulle vara att man till exempel aldrig kör snabbare än gånghastighet vilket motstrider det man vill ha ut av systemet. Systemets säkerhet får inte överskattas men kan underskattas och ju mer man underskattar systemet desto dyrare blir det (Respondent F).

I de säkerhetsplaner som finns, som beskriver hur säkerhetsarbetet ska gå till på ERTMS-programmet, relaterar man till CENELEC-standarderna vilket styr hur standarderna ska användas. Respondent E belyser att det även måste finnas en förståelse för standardernas innebörd och hur de uppfylls hos säkerhetskoordinatorer. För att säkerställa att standarderna följs sker en tredjepartsgranskning. Gällande standarden EN 50129 har samtliga respondenter som medverkat i studien vetskap om att den finns. Däremot finns det skillnader i kunskapen kring innehållet samt hur och om den används i arbetet.

> *"Jag kommer i kontakt med alla CENELEC-normerna och inte minst med det här arbetet som jag har inom ERTMS-projektet med att både granska leverantörens dokumentation och sen så skriver jag själv säkerhetsakter som också måste uppfylla kraven i CENELEC-normerna och inte minst just den här EN 50129, så jag är väl bekant med det."* (Respondent D)

Respondent A, B och H uttrycker att deras roller mer kommer i kontakt med EN 50126 och även EN 50128 för Respondent H. Respondent C anser sig vara ganska insatt i standarden men uttrycker att det inte är helt självklart var i arbetet man kommer i kontakt med EN 50129; *"för jag tycker mig höra lite överallt att man inte berörs av den eller inte kommer i kontakt med den men den är alltid med överallt."*. EN 50129 används i huvudsak vid granskning av leverantörernas dokumentation samt vid utformningen av säkerhetsrapporter (Respondent C, D, E, F, G, H). Eftersom den nya versionen inte tillämpats uttrycks en viss okunskap om den nya versionen av standarden och dess påverkan på ERTMS-programmet.

5.2 Uppdateringen av EN 50129

5.2.1 Generella skillnader

Den nya versionen har en helt ny struktur och har totalt sett utökat innehåll med 157 sidor i förhållande till den gamla versionen som består av 96 sidor. Dock beror en stor del av utökningen på förtydliganden av de redan etablerade kraven. Exempelvis innehåller den nya versionen tydligare beskrivningar av hantering av olika säkerhetsaspekter och tabeller samt figurer är mer detaljerade. Tabeller och figurer förklaras även i textformat i en större utsträckning än i den gamla versionen. Det finns också fler exempel på vad som ska och bör göras och vilka roller som borde göra vad. Standardens utökning beror vidare på de två nya informativa kapitlen, Annex D och Annex F. Dessa berörs inte vidare i denna studie då informativa delar inte är kravställande utan endast innehåller ytterligare information som bidrar till ökad förståelse av standarden. Därmed utgör de inte en

avgörande påverkan på ERTMS-programmet. Den nya versionen är även till stor del anpassad efter den nyaste versionen av EN 50126. I avsnitt 5.2.2 till 5.2.10 presenteras de främsta identifierade skillnaderna och dess påverkan som framkommit genom gap-analysen samt under de genomförda intervjuerna.

5.2.2 SIL

Safety Integrity Level (SIL), som EN 50129 i stora delar utgår ifrån, beskriver systemets, delsystemets eller komponentens säkerhetsnivå. SIL definieras i fyra nivåer, från SIL 1 till SIL 4. SIL-klassning hänger samman med en funktions accepterade felfrekvens, så kallad Tolerable Functional Failure Rate (TFFR), se Tabell 8. Ju färre antal fel per timme som accepteras desto högre klassas SIL. SIL-klassning handlar således om hur många fel man tillåter systemet att ha vilket resulterar i olika krav på hur man jobbar med och utvecklar system (Respondent K). I ERTMS-programmet kravställs ett SIL 4-signalsystem.

Tabell 8. SIL-klassning från den nya versionen

TFFR per timme och per funktion	**SIL**
$10^{-9} \leq TFFR < 10^{-8}$	4
$10^{-8} \leq TFFR < 10^{-7}$	3
$10^{-7} \leq TFFR < 10^{-6}$	2
$10^{-6} \leq TFFR < 10^{-5}$	1

I den gamla versionen av standarden fanns även termen SIL 0. SIL 0 introducerades för att indikera icke säkerhetsrelaterade funktioner. Både Respondent J och C menar på att införandet av SIL 0 skapade förvirring och tolkades olika då termen inte definierades tydligt nog i CENELEC-standarderna. Dessutom uppstod ett gap för en TFFR större än 10^{-5} där SIL-klassningen inte var tillämpbar. Detta skapade i sin tur ett tolkningsutrymme gällande huruvida det gapet klassades som säkerhetsrelaterat eller om det låg utanför SIL-klassningen. Termen SIL 0 används därför inte i den uppdaterade versionen an EN 50129 utan man har istället infört begreppet Basic Integrity (BI), vilket beskrivs i följande text:

> EN 50129:2018, kap.3.1.2:
>
> Basic Integrity: Integrity attribute for safety-related functions with a TFFR higher than (less demanding) 10−5 h−1 or for non-safety-related functions
>
> Note 1 to entry: In this document Basic Integrity requirements relate only to safety-related functions. If a non-safety-related function has been given basic-integrity

requirements on the basis of the process described in EN 50126-2:2017, no additional requirements are defined in this document.

BI gäller alltså när en säkerhetsrelaterad funktion har ett kvantitativt krav, TFFR, högre än 10^{-5} per timme, det vill säga när den accepterade felfrekvensen är mindre krävande än 10^{-5} per timme. BI kan även appliceras på icke-säkerhetsrelaterade funktioner, så som SIL 0 ämnade att göra i den gamla versionen. I EN 50129 tas dock endast säkerhetsrelaterade krav upp och därmed syftar BI i den nya versionen till krav för säkerhetsrelaterade funktioner. Enligt Respondent J är förändringen gällande SIL en av de största skillnaderna mellan den gamla och den nya versionen, eftersom det är ganska stora skillnader i standarden i hur ett projekt ska utföras beroende på SIL-klassning. Om något ligger utanför SIL-klassningen finns det inte lika definierade krav. Ju högre SIL desto hårdare krav finns det på systemet vilket både är tids- och kostandskrävande (Respondent J och K).

> *”Många av direktiven pekar på standarderna och de blir i praktiken lagstiftningstext. Därför blir det här med SIL så viktigt, inte bara gällande säkerhet utan även ekonomiskt.”* (Respondent J)

Respondent J beskriver exempelvis att rollen för verifiering och validering i en lägre SIL-klassning kan innehas av samma person medan det i högre SIL-klassning kan vara helt uteslutet. Detta kan göra så att fler personer behöver vara involverade i projekt som har en högre SIL-klassning vilket ökar kostnaderna (Respondent J). Respondent C åskådliggör dock att detta inte alltid är fallet. Ibland sätts en högre SIL än nödvändigt på ett delsystem för att få samma krav som ett annat integrerande delsystem vilket i sin tur kan minska krångel och därmed bli billigare. Emellertid kan förändringar i SIL-klassning påverka säkerhetstyrningen. Respondent C anser dock att bytet från SIL 0 till BI i just EN 50129 blir mer informativ och inget som direkt påverkar ERTMS-programmet i och med uppdateringen av EN 50129. BI är dessutom ett begrepp som är känt sedan tidigare då den uppdaterade versionen av EN 50126, som ERTMS-programmet håller på att övergå till, även den innehåller definitionen BI. Införandet av BI kan däremot förtydliga definitionen och kommunikationen mellan ERTMS-programmet och dess leverantörer. Respondent C belyser att *”Allting får alltid mest påverkan om något ändras i EN 50128 eftersom det är den som styr hela leverantörernas arbetssätt”*. En rättning av standarden EN 50128, med SIL 0 utbytt mot BI, kommer ut i år. Bytet är dock något som Respondent C och F belyser att ERTMS-programmets leverantörer inte verkar vara insatta i.

5.2.3 Kvalitetsstyrning

En del i säkerhetsrapporten är kvalitetsledningsrapporten, se avsnitt 2.4.3. Den ska redogöra bevis för ett effektivt kvalitetsarbete. I EN 50129 beskrivs att det första kravet för säkerhetsacceptans är att systemets, delsystemets eller komponentens kvalitet, genom hela systemets livscykel, ska kontrolleras av en effektiv kvalitetsstyrning. Respondent B

beskriver kvalitetsarbetet på ERTMS-programmet som ett systematiskt förbättringsarbete.

> *”Kvalitet handlar egentligen om att vi ska arbeta på ett systematiskt sätt i allt vi gör, vilket innebär att kvalitet påverkar säkerhetsarbetet.”*
>
> *”Jag skulle nog säga att det handlar om att vi ska försöka hitta ett överenskommet bästa arbetssätt som alla följer och att man gör det på ett systematiskt sätt så alla vet vad som gäller” (Respondent B)*

I den nya versionen av standarden beskrivs att kvalitetsstyrningen bör följa EN ISO 9001 vilket inte beskrevs förut, se följande kravtext:

EN 50129:2018, kap.5.2: The quality management system should be compliant to EN ISO 9001

ISO 9001 beskriver och innehåller krav på ledningssystem för kvalitet som syftar till att effektivisera och kvalitetssäkra organisationers arbete. I ISO 9001 tillämpas en processinriktning där PDCA-cykeln (Plan, Do, Check, Act) och riskbaserat tänkande ingår. En processinriktning möjliggör identifiering och kartläggning av processer inom en organisation vilket i sin tur, genom en PDCA-cykel, kan bidra till att förbättringsmöjligheter identifieras. Genom att ha ett riskbaserat tänkande kan även organisationen urskilja orsaker till avvikelser i processerna (SIS, 2015).

Respondent B, som har arbetat mycket med ISO 9001, anser att denna förändring i den nya versionen är positiv. Enligt Respondent B är det viktigt att ha kontroll på dokumentation och att ha en systematisk hantering av avvikelser, uppföljning och ansvar, vilket beskrivs i ISO 9001. Respondent B beskriver att i ISO 9001 är det även tydligt att allt arbete under PDCA-cykeln ska utgå ifrån ledarskapet och att det yttersta ansvaret ligger på ledningen. I TRV:s ledningssystem har man skrivit att arbetet ska ske enligt ISO 9001. På ERTMS-programmet jobbar man dock inte enligt ISO 9001 idag men det är något man går emot. Respondent B anser att; ”*Folk behöver bli medvetna om att vi jobbar enligt ISO och att det finns vissa förutsättningar som vi måste leva upp till”*. Den nya versionen av EN 50126 är även den uppdaterad med kravet att ISO 9001 bör följas. Respondent B belyser att det faktum att det även finns med i EN 50129 innebär att TRV måste lägga ännu mer tryck på det. Ledningen har även informerats om att ett ISO 9001-tänk måste implementeras i arbetssätten. Vidare beskriver Respondent B att arbetet är på gång men att en tydligare analys av var ERTMS-programmet står i de olika delarna som ISO 9001 beskriver behöver genomföras, något som planeras ske under 2020.

Följande text är ytterligare ett nytt krav i den nya versionen som berör kvalitetsstyrning:

EN 50129:2018, kap.5.3.4.1:

A record shall be maintained of the personnel assigned to the roles involved in the development or modification of the system, subsystem or equipment.

Den nya texten kravställer att det ska finnas dokumenterat vem i programmet som utför vad samt rollbeskrivningar. SH1 revision är en granskning av kvalitetsstyrningssystemet som utförs av utomstående organ regelbundet på ERTMS-programmet. Under en SH1 revision som utfördes i februari poängterades att detta saknades hos ERTMS-programmet (Respondent B). Respondent B klarlägger även att arbetet som utförs inom kvalitet och säkerhet borde vävas ihop mer än vad de gör i dagsläget.

5.2.4 Dokumentation

En del av säkerhetsarbete på ERTMS-programmet är att granska leverantörernas säkerhetsrelaterade dokumentation. I den nya versionen finns en ny kravtext som beskriver riktlinjer angående strukturering och hantering av dokumentation:

EN 50129:2018, kap.5.3.2:

Accurate, clear and complete documentation is essential to ensuring the verification of safety evidence. It is important to ensure that generic guidelines for documentation are defined, covering the following aspects:
— specification of a documentation plan;
— checklists for the contents of documents;
— determination of the form of the document;
— management of the documentation, e.g. with the help of a computer-aided and organized project library.
…
All safety-related documents, including design documents, shall be classified in accordance with their confidentiality requirements including document storage, access conditions and modification traceability.

Både Respondent C, E och F menar på att den utökade delen är hjälpsam i relation till leverantörerna och deras dokumentationshantering. Leverantörernas struktur på dokumentationen beskrivs i vissa fall som bristfällig och processen kring hanteringen fungerar inte så bra som önskat. Respondent C och E belyser båda en önskan om en dokumentationsplan där innehållet av dokumenten beskrivs. Det faktum att detta tas upp i den nya versionen upplevs som positivt. I och med att det står i den nya versionen går det att trycka på vikten av en strukturerad dokumentation till leverantörerna. Dock uttrycker Respondent C att standarden skulle kunna få vara mer detaljerad i det avseendet.

5.2.5 Organisation, Roller och Granskning

Organisatoriska krav för att stärka säkerheten är ett ämne som tas upp i båda versionerna. Det beskrivs att en lämplig grad av oberoende mellan olika roller ska finnas. I den nya versionen beskrivs detta tydligare i en ny kravtext, se text nedan.

EN 50129:2018, kap.5.3.4.2:

For any SIL from 1 to 4 and for Basic Integrity, the organizational structure of the project team shall comply with the following requirements:

a) A person who is Designer shall not be Verifier for the same system, subsystem or equipment.

b) A person who is Designer shall not be Validator.

c) The Validator shall be given sufficient autonomy and responsibility to reach an independent judgement of the completeness, adequacy and fulfilment of the safety requirements. The Validator shall inform the Project Manager about this judgment.

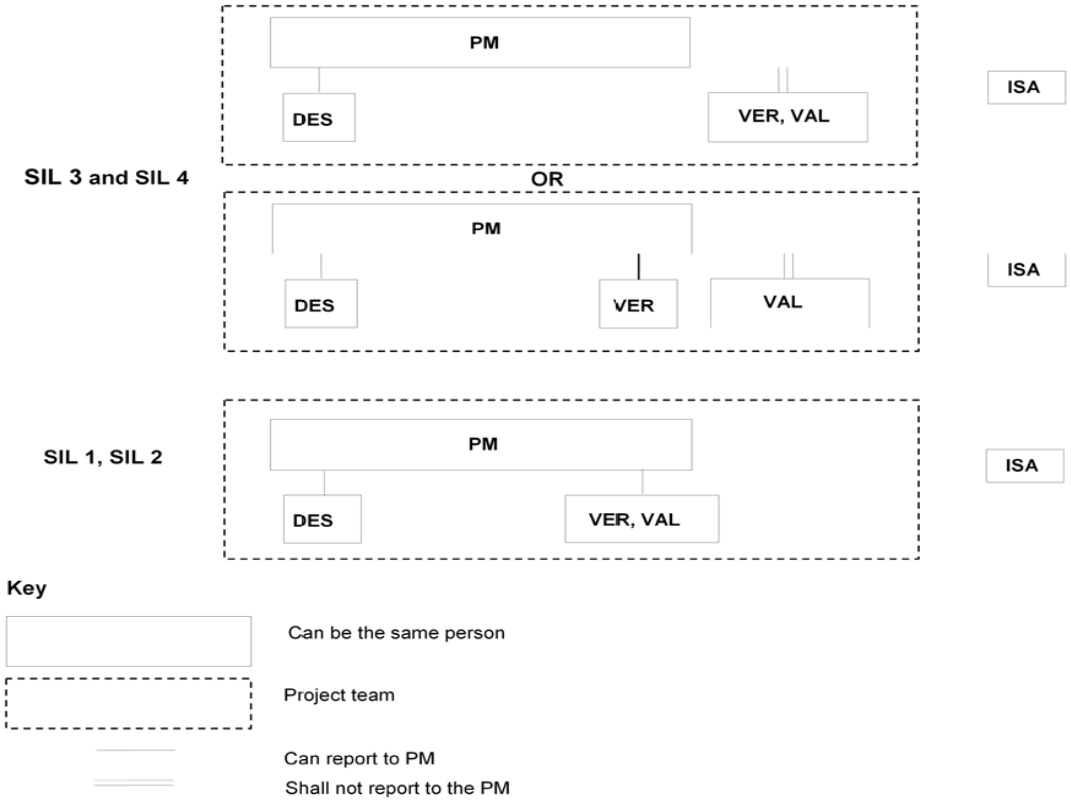
d) A person who is Validator may also perform the role of Verifier. In this case, as for all other development activities, the safety verification and safety validation outputs shall be reviewed by another competent person.

In addition, for SIL 3 and SIL 4, the organizational structure of the project team shall comply with the following requirement:

e) The Validator shall not report to the Project Manager.

En tillhörande figur som visualiserar kraven på roller och deras förhållanden har uppdaterats och några förhållanden mellan rollerna har förändrats från den gamla versionen, se Figur 8 som visar den nya versionen. Det som har uppdaterats i figuren är att det nu finns beskrivet huruvida olika roller kan eller inte bör rapportera till projektledaren (i figur kallad PM). Dessutom är strukturen för SIL 0 är borttagen.

Respondent C, F och G uttrycker att det är lite konstigt beskrivet att en validator inte ska rapportera till projektledaren (PM) för SIL 3 och SIL 4 projekt. *”Om PM beställer ett jobb så måste den ju veta vad som händer”* (Respondent C). Respondenterna belyser dock att ”Report” förmodligen innebär att validatorn inte ska vara underställd PM, det vill säga att den ska vara en oberoende part, men att den kan informera PM. Denna syn på organisationsstrukturen som presenteras i den nya versionen harmoniserar med de nyaste versionerna av både EN 50128 och EN 50126. Det är nytt i EN 50129 men något som inte påverkar ERTMS-programmet eftersom den redan är implementerat (Respondent, C, F, G, H).



Figur 8. Krav på organisationsstruktur. DES = designer, PM = project manager, VER = verifier, VAL =validator och ISA = Independent safety assesor (CENELEC, 2018).

Independent Safety Assesment (ISA) är en granskning som ska utföras oberoende för att bedöma huruvida systemet har utvecklats efter de krav som finns. I den nya versionen av standarden finns det kravställt vad en ISA ska innehålla, vilket inte funnits lika tydliga krav på tidigare:

EN 50129:2018, kap.5.3.15: The independent safety assessment shall assess whether: 1) the requirements given in the present document have been complied with; 2) the safety process has been adequately implemented; 3) the system under consideration is fit, from the point of view of safety, for its intended purpose.

Kraven är något som följs i dagsläget på ERTMS-programmet. Respondent G belyser det faktum att det inte står något i standarden om huruvida en person som utför ISA, även den kallad ISA (Independent Safety Assesor), får vara anställd av det företag som är leverantör till systemet.

”Det som vi försöker strida emot är till exempel att det står ju egentligen här att man tillåter att ISA är anställd av samma leverantör som levererar. Det godkänner man här och det vill inte TRV gärna ha. Vi har fått bort att våra leverantörer har interna ISA och att det istället ska vara utanför bolaget. Men man tillåter ju det här vilket är ganska svagt.” (Respondent G)

Respondent F påpekar att man inte jobbar så i Sverige och att det fortfarande finns krav på oberoende men, som även Respondent E påpekar, är det svårt med ett oberoende förhållande om man tillhör samma organisation.

Något som däremot är under diskussion är huruvida rollen som ISA kommer att övertas av en så kallad AsBo (oberoende bedömningsorgan). En AsBo är någon som är ackrediterad mot CSM-RA, vilket är en förordning inom riskanalys som kompletterar CENELEC-standarderna. Skillnaden på ISA och AsBo är att ISA inte behöver vara ackrediterad medan AsBo har krav på sig att organisationen den tillhör ska ha ackreditering (Respondent G). AsBo granskar alltså mot CSM-RA-förordningen medan ISA granskar mot CENELEC-standarderna (Respondent, C, E, F, G). Att ha två olika roller som granskar beskrivs som onödigt då en ISA och en AsBo kan vara samma person men att företaget får större omfattning om man både ska granska för CENELEC och CSM-RA. Respondent F uttrycker att: *”kunskapsmässigt antar jag att det blir samma, men titeln ISA kommer väl mer och mer utgå och övertas av AsBo istället”.* Hur detta kommer kravställas, appliceras och följas i framtiden finns det skilda meningar om och Respondent G uttrycker att *”i ERTMS-projektet kommer det påverka hur vi upphandlar oberoende bedömningsorgan i framtiden, tror jag.”*. I dagsläget följs dock den anvisning om ISA som beskrivs i den nya versionen.

5.2.6 Verifiering och Validering

Verifiering och validering utförs av både leverantörerna och ERTMS-programmet. Båda delarna beskrivs mer utförligt i den nya versionen. Respondent H anser att den nya kravtexten om verifiering genomförs men att den är beskriven på en allmän nivå och att den verifiering som ska utföras av leverantörerna beskrivs mycket mer detaljerat i EN 50128. Definitionerna för verifiering och validering har ändrats i den nya versionen, se följande definitioner:

EN50129:2003

Validation: The activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements

EN50129:2018

Validation: Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: The term "validated" is used to designate the corresponding status.

Note 2 to entry: The use conditions for validation can be real or simulated.

Note 3 to entry: In design and development, validation concerns the process of examining an item to determine conformity with user needs.

Note 4 to entry: Validation is normally performed during the final stage of development, under defined operating conditions, although it can also be performed in earlier stages.

Note 5 to entry: Multiple validations can be carried out if there are different intended uses.

EN 50129:2003

Verification: The activity of determination, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements

EN 50129:2018

Verification: Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The term "verified" is used to designate the corresponding status.

Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the specified requirement.

Note 3 to entry: Verification is conducted at various stages of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that stage.

Respondent H anser att definitionerna är tydligare nu. Enligt de nya definitionerna handlar verifiering om att specificerade krav ska uppfyllas inför varje fas i utvecklingen. Validering handlar om att kraven för den specifika användningen ska uppfyllas. Det omfattar därmed hela systemet och själva användningen av det vilket den tidigare definitionen inte gör (Respondent H). I och med detta menar Respondent H att *”där har vi ju en viktigare roll som beställare”.* Det finns således ett större fokus på den som skriver kraven.

5.2.7 Ansvarsfördelning

I definitionslistan i standarden har namnet Railway authority i den gamla versionen bytt namn till Railway duty holder i den nya versionen. Båda definieras på liknande sätt och det är TRV som utgör denna roll i Sverige. Safety authority, som gäller i båda versionerna, utgörs av Transportstyrelsen.

Safety qualification tests (SQT) är en del av säkerhetsstyrningen som kravställs både i den gamla och nya versionen. SQT syftar till att öka förtroende att systemet uppfyller kraven och att uppsatt säkerhetsnivå nås. En omfördelning av ansvar och roller har dock skett i och med uppdateringen vilket följande text visar på:

EN 50129:2018, kap.5.3.12: The extent and duration of the safety qualification tests shall be agreed between the railway duty holder and the supplier, and shall be justified having regard to the degree of novelty and complexity associated with the system, subsystem or equipment. EN 50129:2003, kap.B.6.1: The extent and duration of the Safety Qualification Tests shall be agreed between the railway authority and the safety authority, and shall be justified having regard to the degree of novelty and complexity associated with the system/sub-system/equipment.

Respondent G menar att detta är en ganska påtaglig förändring då det påverkar TRV:s förhållande gentemot transportstyrelsen. Förut har ERTMS-programmet redovisat för transportstyrelsen hur SQT planeras att utföras vilket inte längre krävs när den nya versionen införs. En förändring som upplevs relevant då kommunikationen inte anses nödvändig (Respondent G, H).

> *”Det kommer att i den detaljen förändra vår relation till transportstyrelse. För nu så till exempel måste jag skicka in underlag för hur vi tänker på SQT för nästan varje driftsättning till transportstyrelsen och det behöver vi inte så fort vi går över till 2018:s version”* (Respondent G)

5.2.8 Safety Related Application Condition (SRAC)

Hanteringen av Safety Related Application Condition (SRAC) är ytterligare en del inom säkerhetsstyrningen som kravställs i standarden. SRAC:ar beskriver villkor som ska uppfyllas i syfte att motverka risker. Varje SRAC är kopplad till minst en fara/risksituation vilket innebär att om en SRAC inte uppfylls ökar sannolikheten för att en fara inträffar och en riskfylld situation kan uppstå. Korrekt hantering av SRAC:ar är ett krav för säker implementering av ett system och ska därmed även behandlas i säkerhetsrapporten. Hanteringen av SRAC:ar har fått ett nytt stycke i den nya versionen som beskriver SRAC:arnas syfte samt krav på vad de ska och bör vara/innehålla, se följande text:

EN 50129:2018, kap.5.3.13:

The SRACs shall:
— be uniquely identifiable (at least within an organization) both in records/documents and support tools used in the project;
— have an identified receiver or class of receivers or entity (e.g. application engineer, operator, maintainer);
— be self-evident (e.g. understandable without access to other documents), unambiguous, complete, suitable for auditing;
— not contain references that the receivers of the SRACs are not able to access;
— be consistent in all languages in which they are written.

The SRACs should:
— have a short title so to support sorting and analysis of contents;
— be kept to the minimum necessary list, eliminating redundancies among them;
— be available in a language known by the user who is asked to comply with them;
— be compiled within a single separate document;
— be provided with examples of how it might be possible to comply with them or, where known, how compliance has been handled in previous projects.

Within SRAC management, SRACs imported from related Safety Cases shall be shown to have been either closed, with relevant evidence being provided, or re-exported (completely or partially) to subsequent users.

På ERTMS-programmet genomförs samtliga punkter (Respondent C och E). Respondent C belyser att det är fördelaktigt att det nu står att SRAC:ar borde vara sammanställda i ett separat dokument. Detta beskrivs som fördelaktigt eftersom assessorer har påpekat att SRAC:ar ska införas i säkerhetsrapporten medan säkerhetskoordinatorerna istället vill referera till ett separat dokument. Just nu genomförs det på båda sätt men i och med uppdateringen behöver man inte längre utföra det.

5.2.9 IT-säkerhet

I den nya versionen finns ett nytt kapitel, Clause 6, som bland annat behandlar IT-säkerhet. I och med utvecklingen av system för modern IT-kommunikation skapas även ett behov av att skydda dessa system från yttre påverkan. Den nya texten i standarden lyfter därför relevansen kring IT-säkerhet vilket är en ny aspekt som inte tagits upp alls i den gamla versionen. I standarden konstateras att IT-säkerhet är ett framväxande område som kan påverka både trafiken och den funktionella säkerheten gällande signalsystem. Dock finns det inga konkreta säkerhetskrav formulerade i den nya versionen som beskriver hanteringen av IT-säkerhet utan för detta hänvisas till andra standarder. Däremot beskrivs i kapitel 6.4 att hot mot IT-säkerhet ska hanteras under riskanalysen och vid hanteringen av potentiella risker, se kravtext nedan.

EN 50129:2018, kap.6.4:

IT-Security threats shall be managed during the Risk Assessment and Hazard Control (or existing analyses shall be referenced), if an impact of IT-Security issues on functional safety is reasonably foreseeable and cannot be excluded by simple arguments (e.g. a system having no connection to untrusted networks). Measures addressing security shall be recorded or referenced in the Safety Case (section 4.5 of the Technical Safety Report, as described in 7.2).

I kravtexten beskrivs att IT-säkerhet ska vara en del av den tekniska säkerhetsrapporten i säkerhetsrapporten under sektion 4.5 skydd mot obehörig tillgång. I denna del beskrivs följande:

EN 50129:2018, kap.7.2 sektion 4.5:

2) IT-Security
This section shall describe how IT-Security threats which have the potential to affect safety-related functions have been evaluated and how protection against them has been achieved.

Till vilken grad detta efterföljs på ERTMS-programmet finns det något skilda meningar om. Respondent I anser att IT-säkerhet generellt är ett ganska omoget område då man tidigare inom signalsystem främst har fokuserat på säkerhet. Respondent I menar att signalsystem allmänt inte har varit kopplat till nätet tidigare och att man då inte heller har haft ett behov av att arbeta med IT-säkerhet. I och med en ökad digitalisering av signalsystemet krävs det att systemet kopplas upp till nätet. Till följd av detta har IT-krav tillkommit. Idag är därför IT-säkerhet något man arbetar med och det pågår ett arbete för att komma till rätta inom området för att minska signalsystemets utsatthet. Till exempel ställs krav på att leverantörerna ska göra sina system mer IT-säkra (Respondent I). Respondenterna anser delvis att aspekter kring IT-säkerhet tas upp men att det inte involveras i säkerhetsrapporten på det sätt som det nya kravet beskriver.

> *”Det finns fragment av det men jag vet inte om man kan säga att vi gör det på djupet”* (Respondent E).

> *”Ja det gör vi, vi har SRAC:ar och annat från leverantörerna som pratar om det här till exempel”* (Respondent G).

> *”Jag tycker inte vi kan säga att vi gör det”* (Respondent C)

I dagsläget hanteras områdena säkerhet och IT-säkerhet relativt separat. Det nya kravet medför att IT-säkerheten behöver kopplas in i säkerhetsarbetet och framförallt säkerhetsrapporten. Respondent E menar på att detta kan leda till att mer behöver göras på området och det beskrivs som ett område som bör ses över (Respondent C, D, E, F och G).

5.2.10 Människa, Teknik och Organisation (MTO)

MTO-arbetet på ERTMS-programmet är inte ett väletablerat område. Respondent A menar att MTO är mer etablerat inom exempelvis kärnkraft och flygbranschen. Även inom järnvägen i bland annat England utgör MTO och den mänskliga faktorn (eng. human factor) en stor del av arbetet. I Sverige finns inte den traditionen lika starkt.

> *”Historiskt har det väl inte funnits så mycket här krasst sätt. I Sverige har det inte skett så mycket järnvägsolyckor vilket är väldigt bra men då har heller inte det här området MTO eller human factors gått framåt så mycket inom järnväg”* (Respondent A)

Respondent A menar vidare att man såklart inte vill att det ska ske olyckor men att när det sker olyckor kan det leda till en ökad förståelse för påverkan av den mänskliga faktorn. ATC-systemet har varit väldigt stabilt och man har kunnat lita mycket på systemet. Respondent A belyser dock att MTO börjar bli mer accepterat och är på väg mot att bli en större del av ERTMS-programmet. Dessutom börjar det komma krav från Europeiska unionens järnvägsbyrå (ERA), som koordinerar och harmoniserar regelverk inom järnvägssektorn, att man bör ta hänsyn och arbeta med MTO-aspekter (Respondent A).

I den nya versionen av standarden har ett större fokus på användarvänlighet införts och vikten av att studera faktorer som funktion i drift och interaktionen mellan systemet och användaren. Detta benämns bland annat i följande utökade del om drift och underhåll:

EN 50129:2018, kap.5.3.9:
The operational and maintenance activities necessary to ensure continued safe and correct functioning of the system, subsystem or equipment within the specified environmental conditions shall be planned in the form of an Operation and Maintenance Plan. Rules, conditions and constraints for operational safety monitoring shall be documented.

På ERTMS-programmet skapas MTO-relaterade SRAC som beskriver förhållanden för bland annat personer i drift att förhålla sig till. Det finns även utformade driftregler som reglerar hur systemet ska användas samt specificerade styrande dokument som reglerar hur projektering ska utföras säkert. Underhållsplaner och manualer tas fram av leverantörerna eftersom det är de som kan reglera hur deras system ska hanteras och underhållas (Respondent C). Det finns MTO-aspekter som tas hänsyn till även i dessa planer men Respondent A beskriver att det är viktigt att leverantörerna säkerställer att användarna och de som ska utföra underhållet förstår vad som menas i dessa dokument. Vidare menar respondent A på att införandet av ERTMS är ett ingenjörs- och tekniktungt område där man inte alla gånger har användbarhet som främsta fokus. Respondent A belyser dock *”att mycket handlar om användarna och då måste man faktiskt prata med dom också och förstå hur dom har det”*. Enligt Respondent A har emellertid MTO-aspekter och mänskliga fel blivit en mer given del vilket bland annat tas hänsyn till i

specifikationsarbetet, det vill säga där man ställer kraven. Respondent H beskriver också att när man utför verifiering av systemet och detta visar på avvikelser av någon form bedöms även MTO-aspekten på nytt.

I Figur 9 visas en del ur standarden som funnits tidigare men som har förtydligats och ändrats från en informativ del till en normativ del. I figuren står det att det är högt rekommenderat (HR, vilket är den högsta nivån av rekommendationer) att system ska utformas användarvänligt så att risken för mänskliga fel minskar. Respondent A anser att det är positivt att standarden tydligare involverar MTO-aspekter då det visar på att dessa aspekter ska finnas med när man följer standarden.

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Protection against operating / maintenance errors	R	R	HR	HR	(a)
2 Operator / maintainer friendliness to reduce the probability of human errors	HR	HR	HR	HR	(b)

(a) Wrong inputs (value range, electrical characteristics, time, consistency) should be detected via plausibility or consistency checks.

(b) Reduce the risk of human errors related to the interaction between the human (operator or maintainer) and the system by:

- limiting human intervention and
- avoiding unnecessary complexity.

Figur 9, Tabell från den nya versionen angående design. HR = Highly recommended

I definitionen av den engelska termen ”Reliability” har man involverat och tydliggjort begreppets innebörd, se följande jämförande text:

EN50129:2003

Reliability: The ability of an item to perform a required function under given conditions for a given period of time

EN50129:2018

Reliability, <of an item> : Ability to perform as required, without failure, for a given time interval, under given conditions

…Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Det som förtydligas är att begreppet innebär att en komponents förmåga att fungera som tänkt ska studeras med hänsyn till driftläge, stress-nivåer, olika miljöförhållanden samt underhåll. Aspekter som kan kopplas till MTO-perspektivet. SQT, som beskrivits tidigare, syftar bland annat att “increase confidence that the specified reliability and safety targets will be achieved”. Därmed ska även MTO-aspekter tas hänsyn i SQT. SQT anses generellt hos respondenterna som ett ganska otydligt formulerat och vagt beskrivet

begrepp som är svårt att förhålla sig till. Respondent F menar bland annat på att *”När det gäller säkerhet är det svårt att testa sig fram”*. ERTMS-programmet genomför dock mer väldefinierade aktiviteter som anses täcka behovet av SQT (Respondent D, E, F, G). De aspekter som beskrivs i den nya definitionen av ”reliability” utförs enligt Respondent G vid den erfarenhetsdrift som görs. *”Vi ställer upp förutsättning att vi har uppfyllt alla säkerhetskrav och sen gör vi då en övervakning som säger att vi faktiskt uppfyller det som vi trodde”* (Respondent G). Vidare uttrycker Respondent G att man tar hänsyn till de delarna men att man inte dokumenterar SQT aktiviteter i säkerhetsrapporten så som standarden avser.

6. Analys

I analysavsnittet sammanfattas och analyseras studiens presenterade resultat. Avsnittet grundar sig i studiens frågeställningar samt analyserar med avseende på studiens mål vilket är att identifiera åtgärder för ERTMS-programmet vid övergång till den nya versionen av EN 50129.

6.1 Skillnader

Vilka skillnader finns det mellan de två versionerna av standarden EN 50129?

Det presenterade resultatet och den gap-analys som har genomförts i denna studie visar på en del skillnader mellan de två versionerna av standarden. Vid en första anblick kan uppdateringen av standarden EN 50129 verka väldigt omfattande då den nya versionen innehåller mer text än tidigare och är betydligt längre. Däremot, vilket är beskrivet i resultatet, består en stor del av utökningen av nya informativa kapitel vilket bidrar med förståelse men som inte är kravställande text. Därutöver är det fler delar i den gamla versionen som har förtydligats och förbättrats genom att tabeller, figurer och kravtext har blivit mer detaljerade och exemplifierade. Strukturen och uppbyggnaden av standarden har även förändrats och anpassats till de nya delarna. Generellt sätt, vilket framkommit i studiens resultat, är skillnaderna inte så pass omfattande som den nya versionen först ger antydan till. I varje fall inte i relation till ERTMS-programmets applicering av standarden. Med det sagt finns det dock en hel del förändringar och nya aspekter som tas upp i den nya versionen som inte har belysts i den gamla versionen.

I och med att CENELEC-standarderna EN 50126, EN 50128 och EN 50129 hör ihop är även innehållet i dessa tre standarder relaterat till varandra. Hur gränsen dras mellan vilka områden som behandlas i respektive standard är en fråga som det inte verkar finnas något uppenbart svar på. Eftersom de alla beror på varandra påverkar en uppdatering även de övrigas uppdateringar. Mycket av det som har förändrats i den nya versionen av EN 50129 beror därmed på den tidigare uppdateringen av EN 50126. Ett exempel på detta är förändringen från SIL 0 som övergår till BI.

Övriga skillnader som har identifierats i resultatet är bland annat kvalitetsaspekten och det nya kravet att kvalitetsstyrningen och kvalitetsledningsrapporten bör följa ISO 9001. Den nya versionen innehåller även nya krav på organisation, roller och granskning samt ändring i ansvarsfördelning gällande SQT, där den nya versionen inte längre kravställer att utförandet av SQT ska rapporteras till transportstyrelsen. Resultatet visar även ett tydligare fokus på säkerhetsstyrningen i form av SRAC-hantering och dokumentation. Vidare utgör validering och verifiering en skillnad i den nya versionen i jämförelse med den gamla då de definieras och beskrivs mer utförligt än tidigare. Två skillnader som resultatet slutligen visar på gäller områdena IT-säkerhet och MTO. IT-säkerhet är ett av de områden som är helt nytt och som är ett tydligt krav i den nya versionen. MTO-perspektivet framgår i den nya versionen då flertalet krav har identifierats som kopplas till mänskliga fel, användarvänlighet och vikten av att studera systemet under verkliga

förhållanden. Det faktum att IT-säkerhet och MTO introduceras allt mer i standarden följer den historiska utveckling kring säkerhet som Hale och Hovden (1998) beskriver i den teori som har presenterats. I och med att järnvägens signalsystem blir mer komplext och framförallt digitaliserat blir dessa aspekter allt mer relevanta, vilket även visar sig i den nya versionen.

De nämnda skillnaderna i denna del som utgår från resultatet är de delar som har valts ut för denna studie. Påverkan på ERTMS-programmet och vilka åtgärder som bör vidtas kommer vidare att diskuteras.

6.2 Påverkan på ERTMS-programmet

Hur påverkar dessa skillnader ERTMS-programmet?

De identifierade skillnaderna är väsentliga för ERTMS-programmet att vara medvetna om då den nya versionen ska följas senast år 2021. Trots att respondenterna uttryckt en viss okunskap om den nya versionen visar resultatet på att det redan finns en medvetenhet på ERTMS-programmet om en betydande andel av de nya kraven. I en övervägande del av fallen tycks det dessutom som att de nya kraven redan uppfylls. Detta kan tänkas bero på att den nya versionen till stor del bygger på innehållet från den gamla versionen, vilket är en standard som har följts på ERTMS-programmet under många år. Dessutom har den nya versionen skapats med hänsyn till den nya versionen av EN 50126, vilket ERTMS-programmet i dagsläget håller på att övergå till. Därmed finns det en indirekt medvetenhet om skillnaderna i EN 50129 vilket i sin tur influerar hur mycket ERTMS-programmet påverkas av uppdateringen till den nya versionen.

Trots att SIL-klassning bevisligen kan ha stor påverkan på säkerhetsstyrningen blir uppdateringen och införandet av BI i den nya versionen mer av informativ karaktär för ERTMS-programmet. På sikt har dock förändringen påverkan då man måste gå över till BI när även EN 50128 byter ut SIL 0. Något den nya versionen kan bidra med är att underlätta övergången från SIL 0 till BI. Framförallt i förhållande till leverantörerna då det verkar finnas en viss okunskap och otydlighet kring definitionsbytet. I den aspekten kan applicering av den nya versionen förtydliga oklarheter och etablera BI både hos ERTMS-programmet och dess leverantörer. Nya krav på hur organisationen ska struktureras och oberoende av roller blir också informativt vid uppdatering till den nya versionen då kunskapen redan finns i och med de senaste versionerna av EN 50126 och EN 50128. Det är dessutom något som redan följs och uppfylls på ERTMS-programmet. Vidare påverkar den nya delen angående granskning och ISA i sig inte ERTMS-programmet då man redan följer de anvisningarna som finns i den nya versionen. Däremot skapar de nya förtydligande kraven följdeffekter i samband med att andra standarder, som också ställer krav på granskning, appliceras. ISA eller AsBo är en sådan diskussion som påverkar programmet och där ett ställningstagande på sikt bör tas kring hur detta ska fungera i praktiken.

Det nya kravet på att kvalitetsstyrningen ska följa ISO 9001 får dock tydliga effekter på ERTMS-programmets arbete med kvalitet. Till följd av kravets införande ska nu ISO 9001 implementeras vilket inte uppfylls i dagsläget. Även kravet på att rollbeskrivning ska finnas är något som ska implementeras. Ytterligare en skillnad mellan de två versionerna av standarden som kommer få påverkan på ERTMS-programmet gäller rollfördelning inom SQT. I och med att roller har bytts ut i den nya versionen inom SQT behöver inte längre ERTMS-programmet rapportera utförande av SQT till Transportstyrelsen. Detta beskrivs som en positiv förändring och något som kommer att påverka ERTMS-programmet i den aspekten att det blir enklare då Transportstyrelsen inte behöver involveras. Utöver detta ska även SQT beskrivas i säkerhetsrapporten vilket inte genomförs utförligt i dagsläget vilket bör förändras.

Vidare utgör införandet av krav gällande IT-säkerhet en betydande förändring som ERTMS-programmet påverkas av. IT-säkerhet är ett område som måste tas hänsyn till och involveras i säkerhetsarbetet och säkerhetsrapporten då det idag hanteras som ett separat område. Slutligen påverkas ERTMS-programmet av det faktum att det finns ett ökat MTO-perspektiv i den nya versionen. De krav som explicit står i den nya versionen gällande användarvänlighet och mänskliga faktorer tas hänsyn till på ERTMS-programmet. Däremot visar de utökade MTO-aspekterna i den nya versionen på vikten av att dessa faktorer hanteras på ett etablerat sätt vilket inte genomförs på ERTMS-programmet idag. Den nya versionen påverkar således ERTMS-programmet i den aspekten att ett ökat fokus på MTO bör etableras.

Med undantag för de redan diskuterade tillagda kraven påverkas ERTMS-programmet inte i någon större grad av de identifierade skillnaderna. Däremot visar resultatet på ett flertal områden där standarden kan underlätta det framtida säkerhetsarbetet. Områden som i dagsläget innefattar brister och som kan hjälpas av det som kravställs i den nya versionen. Dokumentation är ett sådant område där respondenterna explicit har uttryckt att den nya kravtexten är hjälpande, framförallt i relationen till leverantörerna. Kravtexten om SRAC-hantering är ytterligare ett exempel på detta samt det utökade MTO-perspektivet. Med detta i åtanke är följande frågeställning något som bör utvärderas vidare inom programmet; Hur kan standarden utnyttjas på ett fördelaktigt sätt på ERTMS-programmet?

En viktig aspekt i frågan hur ERTMS-programmet påverkas av den nya versionen är de tolkningsmöjligheter som standarden innehåller. Det finns en hel del vaga begrepp och oklarheter i standarden vilket kan ses som positivt då innehållet går att applicera på många områden och det finns ett visst anpassningsutrymme. Däremot kan detta även upplevas negativt då det blir otydligt vad som bör göras som exempelvis inom SQT. Där uttrycker respondenterna att standarden upplevs oanvändbar på grund av begreppets otydliga beskrivning. I och med detta går det också i vissa fall att argumentera för vad som uppfylls och inte. Det finns därmed inte alltid en tydlig gränsdragning kring vilka krav som uppfylls och vilka krav som inte uppfylls. Hur standarden tolkas bidrar således till hur ERTMS-programmet påverkas av krav i standarden. Ytterligare ett relevant perspektiv

kopplat till denna analys som kommit upp under studiens gång är att standarder, även EN 50129, är skrivna utifrån förmågan att kunna appliceras av olika aktörer och inom olika projektområden. Detta ger följdeffekten att även om det är kravställt att EN 50129 ska följas bör inte allting tillämpas till punkt och pricka, vilket även Respondent H belyser:

> *”Man ska ju inte hänga upp sig allt för mycket på vad som står heller faktiskt, till synes är det ändå sunt förnuft som måste gälla liksom. Det är ju ändå säkerheten det handlar om inte hur man tolkar standarderna, dom ska ju vara en hjälp”*

Trots att kraven i EN 50129 ska följas bör standarden kontrolleras och därefter bör det konstateras vad som ska tillämpas och inte utifrån vad som är relevant för just ERTMS-programmet.

6.3 Åtgärder

Vilka åtgärder krävs för att övergå till den nya versionen av standarden?

Säkerheten i ett system påverkas av en mängd olika delsystem och komponenter, vilka alla bör beaktas (Lucic, 2015). EN 50129 är en relativt övergripande standard och i den nya versionen är det många delar som involveras, så som kvalitet, verifiering och validering, MTO, IT-säkerhet och olika aspekter inom säkerhetsstyrning. Uppdateringen av standarden påverkar således ERTMS-programmet på flera områden vilket är en viktig aspekt att ta hänsyn till då standarden uppdateras. Ett första steg kan vara att ta till sig det som faktiskt berör ERTMS-programmet och tydliggöra det. Som nämnt innan är standarden tolkningsbar på många punkter och behöver appliceras på just ERTMS-programmet för att kunna användas på ett lämpligt sätt. Vid övergång från den gamla till den nya versionen krävs det också att tillräcklig kunskap finns om den nya versionen. Detta kan delvis denna studie bidra med då den belyser förändringen och dess påverkan. Eftersom kunskapen om den nya versionen varierar inom programmet kan det vara fördelaktigt att ytterligare vidga kännedomen genom att ha utbildningar och information om standarden, dess uppdatering och påverkan i praktiken.

Resultatet visar på en del krav i den nya versionen som inte uppfylls av ERTMS-programmet och som bör åtgärdas. Dessa är både av konkret och mer generell karaktär som berör förändring på ett mer övergripande plan. Följande konkreta krav, som är direkt kopplande till de nya kraven, bör åtgärdas vid övergång till den nya versionen:

- Följa ISO 9001 i kvalitetsledningssystemet
- Dokumentera vem i programmet som utför vad samt rollbeskrivningar
- Involvera IT-säkerhet i säkerhetsrapporten
- Inte rapportera till Transportstyrelsen gällande SQT
- Dokumentera SQT i säkerhetsrapporten

IT-säkerhet är en tydlig punkt som bör åtgärdas enligt den nya versionen. Hur detta ska gå till är däremot inget som beskrivs konkret i standarden vilket bidrar till en viss otydlighet kring vilka åtgärder som behöver genomföras. Detta gör att det krävs en egen tolkning och definition på ERTMS-programmet om vad standarden avser med IT-säkerhet och till vilken grad detta ska involveras i säkerhetsarbetet och dokumenteras i säkerhetsrapporten. Gällande den sistnämnda punkten visar resultatet på att hela begreppet SQT i standarden anses otydligt samtidigt som respondenterna menar på att det redan genomförs aktiviteter som täcker behovet av SQT. Ett förtydligande av hur begreppet SQT tolkas på ERTMS-programmet och en överenskommelse angående detta med leverantörerna bör således etableras. Dessutom är dokumentering av SQT i säkerhetsrapporten en del som bör åtgärdas.

Eftersom fler av de övrigt identifierade skillnaderna anses vara positiva och hjälpande för ERTMS-programmet bör dessa framhävas inom programmet trots att de inte har någon direkt påverkan vid uppdateringen. Exempel på dessa är kraven angående dokumentation, SRAC-hantering samt verifiering och validering. Även här kan ökad information om standarden vara fördelaktig då det finns bristande kunskap om delar i den nya versionen som kan underlätta arbetet på så sätt att det kan bli mer konkret, definierat och samordnat. En åtgärd som kan utvecklas gällande detta område är att vidare arbeta med hur standarden appliceras i arbetet på ERTMS-programmet.

Som tidigare beskrivet har MTO-relaterade aspekter fått mer utrymme i den nya versionen och det finns ett tydligare fokus på detta perspektiv. Trots att en hel del arbete tycks göras med MTO-relaterade delar har det genom studien framgått att det är ett område som varken är etablerat eller samordnat på ERTMS-programmet. I och med övergången till den nya versionen är det viktigt att MTO får en tydligare roll även på ERTMS-programmet. Som nämns i teorin av bland annat Wallström och Rollenhagen (2014) bör MTO-aspekter tas hänsyn till i säkerhetsarbete. I och med digitaliseringen av järnvägen, dess komplexitet och i det förändringsarbete som utförs med utvecklingen av ERTMS blir MTO-perspektivet allt mer relevant. Som Hollnagel (2014) beskriver kan ett säkert system med få olyckor bidra till en minskad aktivitet i säkerhetsarbetet. Detta är framför allt ett synsätt som innehas i Safety-I begreppet. I en av intervjuerna beskrivs de faktum att det förmodligen är på grund av att järnvägen är ett så pass etablerat och säkert system i Sverige som MTO-perspektivet inom branschen inte har kommit lika långt som i vissa andra branscher. Järnvägen har samtidigt utvecklas till ett mer komplext socioteknisk system vilket ökar relevansen för att det dagliga arbetet och hur olika system integrerar bör studeras. Ett mer Safety-II perspektiv på säkerheten, då säkerhetstyrningen fokuserar på att saker går rätt till och en förståelse för systemet som helhet, skulle därför vara fördelaktigt i detta sammanhang. Genom att öka kunskapen om MTO-perspektivets relevans inom samtliga områden på ERTMS-programmet och samtidigt peka på standardens utveckling kan MTO möjligen bli mer etablerat.

En viktig aspekt angående åtgärder som kan kopplas till Hollnagel Safety-II begrepp är att arbeta proaktivt inför övergången till den nya versionen. En viss oklarhet kring vad

som gäller vid övergång finns och hur övergången ska gå till i praktiken är något som bör ses över i god tid innan. Enligt Hollnagel (2014) kan säkerheten öka genom noggrann planering, detaljerade instruktioner och utbildning av personal. Detta kan även tänkas gälla vid övergång till den nya versionen. För att bibehålla säkerheten borde därför övergången till den nya versionen planeras. Instruktioner och information kring hur de nya kraven ska hanteras bör även genomföras. För att fånga upp dessa aspekter skulle respektive område som berörs av EN 50129 kunna ställa sig frågorna; Vilket arbete utförs på dessa områden idag? Hur definieras, tolkas och appliceras kraven? Hur påverkar förändringen arbetet i praktiken? Denna studie och den genomförda gap-analysen kan ligga som grund för att utvärdera dessa frågor ytterligare.

7. Diskussion

I följande avsnitt diskuteras resultatet och analysen. Detta görs dels utifrån de reflektioner som uppkommit under studiens gång, dels i förhållande till den teori som har presenterats. Mer konkret reflekterar avsnittet först generellt angående uppdateringen till den nya versionen på ERTMS-programmet för att sedan belysa hur säkerhetsstyrningen på ERTMS-programmet stämmer överens med Safety-II begreppet. Avslutningsvis lyfts reflektioner angående studiens teoretiska urval samt metodologiska angreppsätt.

Under studiens gång har en viss brist i användningen av standarden på ERTMS-programmet identifierats. Dels i form av den okunskap som finns angående standarden och dess innehåll, dels med avseende på standardens otydlighet. Detta har lett till frågan; Hur kan användningen och implementeringen av standarden förbättras? Ökad kunskap genom utbildningstillfällen är en del som skulle kunna förbättras. Vidare skulle även odefinierade och otydliga beskrivningar i standarden behöva översättas till tydliga instruktioner som är relevanta för ERTMS-programmet. Detta är något som finns i viss utsträckning men som skulle kunna utökas. Eftersom resultatet visat på att flera krav i den nya versionen kan vara hjälpande i säkerhetsarbetet är det fördelaktigt för ERTMS-programmet att tillgodose dessa delar. Något som troligen även skulle spara både tid och resurser på lång sikt.

I teorin lyfts att säkerhet inte ska hanteras på komponentnivå utan på systemnivå (Leveson, 2011). Detta bör även appliceras vid uppdatering av standarden. Hur ERTMS-programmet påverkas av de identifierade skillnaderna och vilka åtgärder som bör vidtas för att övergå till den nya versionen bör således även studeras utifrån ett helhetsperspektiv för att se hur det påverkar ERTMS-programmet på en mer övergripande nivå. En generell åtgärd som framkommit under studien är att varje område som standarden belyser bör kopplas samman till övriga områden. Det finns en önskan om att ha ett tydligare samband mellan bland annat det arbete som utförs inom säkerhet och inom kvalitet. IT-säkerhet och säkerhet är ännu ett exempel, likväl som att resultatet lyfter att MTO bör vävas in i fler områden. Vilka kopplingar finns det mellan områdena idag? Hur och på vilka punkter kan dessa kopplas samman? I och med en ökad involvering av olika områden skulle säkerheten i helhet kunna vidgas och ett mer överskådligt perspektiv på säkerheten skulle kunna skapas. Hur detta skulle kunna utföras i praktiken är dock en svår uppgift som inte besvaras i denna studie men som lyfts som en aspekt som bör arbetas vidare med på ERTMS-programmet.

Användningen av standarden i relation till övriga standarder och förordningar är också en generell åtgärd som bör ses över. Hur samspelar egentligen olika standarder och förordningar? Resultatet visar att de i vissa aspekter krockar vilket kan leda till att resurser möjligen inte utnyttjas på det mest effektiva sättet. Ett exempel på detta är granskning av ISA och AsBo. Därför bör man på ERTMS-programmet även konstatera hur standarder och förordningar samspelar och vad det får för konsekvenser i praktiken.

För att hantera uppdateringen av standarden, och säkerhetsarbetet generellt, på ett så bra sätt som möjligt är det fördelaktigt om säkerhetsstyrningen på ERTMS-programmet har ett perspektiv på säkerhet som är i linje med Hollnagels Safety-II begrepp. Inom Safety-II ligger fokus på att beskriva det arbete som utförs. Det finns också en förståelse för att det existerar en variabilitet från det som har blivit specificerat och beskrivet (Hollnagel, 2019). Vidare är säkerhetsarbetet något som sker kontinuerligt i Safety-II och inte endast när något gått fel, som i Safety-I. Säkerhetsstyrningen på ERTMS-programmet beskrivs i intervjuer som ett kontinuerligt arbete där man hela tiden försöker se förbättringspotential vilket är något som pekar på ett Safety-II tänk. Säkerheten ses även som något mer komplext än att enbart utgå ifrån att inga oacceptabla risker ska ske vilket är ett perspektiv som Hollnagel (2019) belyser. I teorin beskrivs att Safety-II innebär en förståelse för hur system vanligtvis fungerar för att förklara varför fel inträffar. En förståelse för system som helhet är anledningen till att systemet fungerar som det ska. Inom ERTMS-programmet belyses det faktum att det är viktigt att förstå sig på vilken risknivå som finns och kunna bekräfta att den är acceptabel. Dessutom beskrivs säkerheten som en kombination av hur allt samverkar vilket kan anses vara i linje med ett Safety-II perspektiv.

Konflikten mellan säkerhet och produktivitet som lyfts i teorin beskrivs även på ERTMS-programmet. Driftmål sätts alltid i relation till säkerheten. Dock beskrivs i resultatet att systemets säkerhet aldrig får överskattas men att ju mer den underskattas desto högre kostnad blir det. Inom Safety-II ses en investering i säkerhet som en investering i produktivitet. Med det synsättet på säkerhet blir det enklare att motivera säkerhetsarbetet enligt Hollnagel (2014). Säkerhetsarbetet upplevs och beskrivs dock som en redan utvecklad och given del i ERTMS-programmet. Med andra ord inget som behöver ytterligare motiveras. Däremot skulle det synsättet som Hollnagel lyfter kunna vara en motivering till att väva samman olika delar i säkerhetsarbetet som inte kopplas samman så starkt idag. Möjligen skulle det även kunna motivera ett ökat MTO-perspektiv inom säkerhetsarbetet.

Proaktivt säkerhetsarbete utgör en stor del av Safety-II. Enligt Hollnagel (2014) är ett proaktivt förhållningssätt till säkerheten fördelaktigt då det kan spara både tid och resurser. Då ERTMS-programmet utvecklar signalsystemet i Sverige handlar säkerhetsstyrningen till stora delar om att ta hänsyn till säkerheten i förebyggande syfte och se till att systemet når den säkerhet som har kravställts. Användningen av säkerhetsstandarder på ERTMS-programmet kan också ses som ett proaktivt arbetssätt då det bidrar till att arbetet utförs mer strukturerat än tidigare.

Säkerhetsarbetet på ERTMS-programmet kan anses vara relativt i linje med Hollnagels teorier kring Safety-II. Dock finns det aspekter inom säkerhetsarbete som skulle gynnas av ett tydligare Safety-II perspektiv. Genom att implementera ett starkare Safety-II tänk, i form av proaktivitet och synen på den mänskliga faktorn, så kan även övergången till den nya standarden förenklas och möjligtvis även förbättra nyttjandet av standarden. Detta kan i sin tur på sikt även höja säkerheten för hela ERTMS införande i Sverige.

7.1 Teoretiskt urval

Teoriavsnittet i denna studie består till stor del av Hollnagels teorier om begreppen Safety-I och Safety-II. Således tas inte andra teorier upp i någon större utsträckning. Det finns möjligen även fler perspektiv kring begreppen som Hollnagel beskriver som inte heller har berörts i denna studie. Eftersom ämnet säkerhet innefattar en mängd olika teorier krävdes dock en smal avgränsning som samtidigt ansågs passande. Valet av teori baserar sig på att Hollnagels litteratur och perspektiv på säkerhet ansågs vara mest relevant med avseende på studiens ämne och syfte, vilket var ett beslut som växte fram under litteraturstudiens gång. Det är dessutom ett relativt nytt och framväxande område inom säkerhet vilket gör teorin mer aktuell och förankrad till hur det fungerar i dagens samhälle. I ett ännu mer omfattande och fördjupat arbete hade fler perspektiv varit önskvärt.

7.2 Metodologiskt angreppssätt

Denna studie bygger på kvalitativa metoder i form av litteraturstudie och intervjuer. Kvalitet inom kvalitativ forskning är väl diskuterad och benämns ofta med begreppen validitet och reliabilitet (Eriksson och Widersheim-Paul, 2006). Validitet innebär att studien mäter det som faktiskt avses att mätas medan förmågan att upprepa studien och komma fram till samma resultat beskrivs med termen reliabilitet. Eriksson och Widersheim-Paul (2006) beskriver vidare att hög reliabilitet finns om studien är oberoende av bland annat respondenter, organisationer och undersökare, vilket ofta efterfrågas inom forskning.

Alvehus (2013) anser att begreppen validitet och reliabilitet inte alltid är applicerbart på kvalitativ forskning då det bygger på ett oberoende hos det som mäts och mätningar samt mätinstrument. Exempelvis, eftersom kvalitativ forskning innehåller tolkningsutrymme och forskaren utgör en del i tolkningsarbetet, går det inte att hävda att den kvalitativa forskningen är upprepningsbar i sin helhet. Sannolikt kommer både undersökarens tolkning och respondenternas svar att variera om undersökaren byts ut. Denna studie är därför inte trolig att ge samma resultat för en annan utövare av studien. För att diskutera kvalitet inom kvalitativa metoder finns dock andra relevanta ämnen. Alvehus (2013) belyser bland annat vikten av transparens inom forskning, att alla data och resonemang redovisas i studien samt att studien kan granskas. Gällande en kvalitativ studie kan detta dock vara svårt att uppfylla då studiens resultat ofta består av en liten del av all insamlad data, som exempelvis intervjumaterial, vilket är fallet i denna studie. Det viktiga enligt Alvehus (2013) är att studiens resonemang är transparenta och förståeliga för läsaren.

Ytterligare något som diskuteras och kritiseras inom kvalitativ forskning är giltighet och generaliserbarhet. Exempelvis lyfter Bryman och Bell (2013) att resultat från en kvalitativ studie inte går att generalisera på samma sätt som när studiens metod är kvantitativ. Resultatet i denna studie bygger, som nämnt, på kvalitativa metoder och berör ett specifikt ämne applicerat på ett specifikt fallföretag. Något som bör tas i beaktning är att samtliga respondenter arbetar för TRV. Detta gör att en bredare generalisering utifrån resultatet är

svår att göra. Denna studie kan dock bidra till att utveckla kunskap inom ämnet, visa upp nya aspekter och framhäva den variation och komplexitet en sådan förändring bidrar till, vilket enligt Alvehus (2013) är vad en kvalitativ studie syftar till att göra. Dessutom bygger metoden på intervjuer med personer som har olika befattningar inom TRV vilket bidrar till olika perspektiv och ett utförligare resultat. Lantz (2013) beskriver att resultatens giltighet och generaliserbarhet för en studie baserat på intervjuer inte kan sättas i kontext till hur representativt studien är för populationen. Vidare menar författaren att dessa begrepp istället bör diskuteras ur ett annat perspektiv och att *”Giltigheten kan då förenklat sägas vara i vilken mån data och resultat speglar källan och samtidigt på ett mer allmängiltigt plan ökar förståelse av det som undersökts”*(Lantz, 2013, s.19).

I samband med generaliserbarhet är snöbollsurval kritiserad av en del författare som urvalstrategi då resultatet från en sådan metod kan representera en vinklad och ensidig bild av det studerade ämnet (Alvehus 2013; Bryman och Bell, 2013). Denna studies val av respondenter syftade däremot inte till att få en allmän och bred kunskap om ämnet utan att få insikter och perspektiv från de mest kunniga inom det studerade ämnet. Ett snöbollsurval valdes därmed som en relevant metod. Snöbollsurvalet kombinerades dessutom med ett genomtänkt urval i ett första skede vilket breddade studiens resultat. Antalet intervjuer och intervjupersoner i studien skulle kunna ha utvecklats för att få ytterligare fördjupad förståelse i ämnet. Studien utfördes på TRV kontor i Solna under första halvan av examensarbetet. Detta kan ha bidragit till en ökad öppenhet hos respondenterna och en fördjupad förståelse av verksamheten vilket i sin tur kan ha gynnat studiens resultat.

Under studien gång har det framkommit att den studerade standarden till stor del berör ERTMS-programmets leverantörer. Resultatet visar också på en del områden där samspelet mellan ERTMS-programmet och leverantörerna framhävs. Till följd av detta hade det varit intressant och relevant att även intervjua ERTMS-programmets leverantörer för att få ett vidgat perspektiv på uppdateringen av standarden och dess påverkan. Detta hade dock blivit ett väldigt omfattande arbete, varför studien avgränsades till att studera påverkan för ERTMS-programmet. Ytterligare en förbättring som hade kunnat utföras som komplement till studiens metoder hade varit att studera säkerhetsbevisningen för en specifik produkt som utvecklas utefter EN 50129. Säkerhetsrapporter med mera har studerats under studiens gång men detta har inte skett strukturerat och inte heller framhävts i resultatet vilket hade kunnat utvecklas.

8. Slutsatser

I detta avsnitt avrundas rapporten och studiens frågeställningar besvaras kortfattat utifrån vad som presenterats i resultatet och analysen. Frågeställningarna lyder: Vilka skillnader finns det mellan de två versionerna av standarden EN 50129? Hur påverkar dessa skillnader ERTMS-programmet? Vilka åtgärder krävs för att övergå till den nya versionen av standarden?

De huvudsakliga skillnaderna som identifierats mellan de två versionerna av standarden EN 50129 är bland annat att SIL 0 övergår till BI och att det finns ett nytt krav att kvalitetsstyrningen och kvalitetsledningsrapporten bör följa ISO 9001. Övriga skillnader som har identifierats i resultatet är bland annat nya krav på roller, ansvarsfördelning, organisation och granskning. Resultatet visar även på ett tydligare fokus på säkerhetsstyrningen i form av SRAC och dokumentation. Krav på validering och verifiering utgör en skillnad i den nya versionen i jämförelse med den gamla då de definieras och beskrivs tydligare. Avslutningsvis visar studien även på skillnader gällande områdena IT-säkerhet och MTO.

Dessa identifierade skillnader påverkar ERTMS-programmet i olika grad. Trots att den nya versionen innehåller flera nya krav samtidigt som det uttrycks vara en viss kunskapsbrist av den nya versionen så är en stor del av de nya kraven kända och uppfyllda av ERTMS-programmet sedan tidigare. Detta gäller bland annat bytet från SIL 0 till BI samt kraven på oberoende roller i organisationen och granskning av ISA, vilket har visat sig bero på sambandet mellan de olika CENELEC-standarderna. De nya kraven inom kvalitetsstyrning, roller och dokumentation av SQT, IT-säkerhet samt delvis MTO är områden som påverkar ERTMS-programmet i den meningen att åtgärder bör vidtas. ERTMS-programmet uppfyller således inte alla nya krav som den nya versionen innehåller. Övriga delar i standarden som resultatet visar på väcker i vissa fall en del frågetecken men är inget som inte direkt uppfylls i dagsläget. Vid samtal med experter inom området på ERTMS-programmet framgår att de övriga förändringarna, även om de inte får påtagliga konsekvenser, kan vara hjälpande i arbetet och visa på en tyngd i varför de ska utföras bland annat i relation till ERTMS-programmets leverantörer.

De åtgärder som har identifierats för att ERTMS-programmet ska kunna övergå till den nya versionen kopplas dels till specifika krav i standarden, dels till förändringar på ett mer övergripande plan. Bland annat kan ett mer proaktivt arbete vid uppdatering till den nya versionen vara fördelaktigt, då det finns en viss okunskap angående standarden och övergången. En ökad kunskap inom programmet om den nya versionen, dess innehåll och påverkan anses även vara en viktig åtgärd inför övergången. Ytterligare en väsentlig åtgärd som studien belyser är att de identifierade nya delarna som kan vara hjälpande i säkerhetsarbetet borde framhävas och tas upp av relevanta parter i ERTMS-programmet, för att utnyttja standarden på bästa sätt. Slutligen kan ett utökat systemtänk vara en åtgärd som bör vidtas för att väva samman alla delar som tas upp i standarden i syfte att öka säkerheten.

9. Fortsatta studier

Detta examensarbete har fokuserat på säkerhetsstyrningen på ERTMS-programmet kopplat till uppdateringen av standarden EN 50129. Studien har dock visat att det finns många delar i standarden som berör ERTMS-programmets leverantörer och samspelet dem emellan. Det skulle därmed vara relevant att vidare undersöka uppdateringen av EN 50129 och dess påverkan utifrån leverantörernas perspektiv. Vidare har flera av de identifierade skillnaderna i denna studie nämnts relativt övergripande och har avgränsats till vad den studerade standarden behandlar. Fortsatta studier utifrån detta examensarbete kan därför ytterligare utveckla och analysera de identifierade bristfälliga områdena som bland annat hanteringen av IT-säkerhet och MTO på ERTMS-programmet.

Studiens resultat har visat på att standarder, inkluderat EN 50129, i många fall innehåller vaga krav och definitioner vilket gör de svårapplicerade. En mer generell studie angående användningen av standarder och kravhantering vid utvecklingen av ett infrastruktursystem är ett område värt att utveckla separat. Slutligen vore det intressant att undersöka säkerhetsarbetet för införandet av ERTMS utifrån ett bredare perspektiv och möjligen i relation till andra länders säkerhetsarbete med ERTMS. Detta skulle då kunna kopplas till Hollnagels Safety-I och Safety-II begrepp i syfte att ta lärdom kring säkerhet vid utveckling av sociotekniska system.

Referenser

Tryckta källor

Alvehus, J. (2013), Skriva uppsats med kvalitativ metod: En handbok, Första upplagan, Liber AB: Stockholm.

Bryman, A. och Bell, B. (2013), Företagsekonomiska forskningsmetoder, Andra upplagan, Liber AB: Stockholm.

Ciancabilla, A. (2019), "Guidance on EN 50129:2018", SC9XA/Sec1013A/INF, European Committee for Electrotechnical Standardization: Bryssel.

Eriksson, L.T., och Wiederstam, P. (2006), Att forska, utreda och rapportera, Upplaga 8:1, Liber AB: Malmö.

Fejes, A. och Thornberg, R. (2015), Handbok i kvalitativ analys, Andra upplagan, Liber AB: Stockholm.

Hale, A.R. och Hovden, J. (1998),"Management and culture: The third age of safety – A review of approaches to organisational aspects of safety, health and environment": i Feyer, A.M. och Williamson (Red.), Occupational Injury: Risk prevention and Intervention, Taylor & Francis: London.

Hollnagel, E. (2014), Safety-I and Safety-II – the Past and Future of Safety Management, CRC Press LLC.

Hollnagel, E. (2018), Safety-II in practice – Developing the resilience potentials, Routledge: New York.

Hollnagel, E., Wears, R.L. och Braithwaite, J. (2015) From Safety-I to Safety-II: A White Paper, The Resilient Health Care Net: Publicerad samtidigt av University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia.

Kvale, S. och Brinkmann, S. (2014), Den kvalitativa forskningsintervjun, Översatt av Sven-Erik Torhell, Upplaga 3:2, Studentlitteratur AB: Lund.

Lantz, A. (2013), Intervjumetodik, Upplaga 3:2, Studentlitteratur AB: Lund.

Leveson, G.N. (2011), Engineering a Safer World – System Thinking Applied to Safety, The MIT Press: London

Lucic, I. (2015), Risk and Safety in Engineering Process, Cambridge Scholars Publishing: Cambridge.

Palmer, C. (2019),The Boeing 737 Max Saga: Automating Failure, Engineering, Vol.6, nr.1, ss.2-3.

Smith, P., Majumdar, A. och Y. Ochieng, W. (2012), "An overview of lessons learnt from ERTMS implementation in European railways", Journal of Rail Transport Planning & Management, Vol.2, nr.4, ss.79-87.

Stålhane, T. och Myklebust, T. (2016), The Agile Safety Case, Elsevier: Trondheim.

Trafikverket (2015), Införandeplan för ERTMS 2015-2025, TRV 2015/63202, Trafikverket: Solna.

Wahlström, B. och Rollenhagen, C. (2014), Safety management – A multi-level control problem, Safety Science, Vol.69, ss.3-17.

Åkeson, A. (2017), Projekt ERTMS årsrapport 2016, TRV 2017/40851, Trafikverket: Solna.

Intern dokumentation

Klawitter, M. (2019), Övergripande beskrivning av framtidens signalsystem och dess möjligheter, Utbildningsmaterial, TRV 2019/108223, Trafikverket: Borlänge.

Trafikverksskolan (2017), Allmän järnvägsteknik för ingenjörer, Internt utbildningsmaterial, v.1.4, Trafikverket: Ängelholm

Trafikverket (2020), Required Standards and Norms ERTMS Level 2, ERTMS18-058, v.2.

Standarder

CENELEC (2018), Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, EN 50129:2018, European Committee for Electrotechnical Standardization: Bryssel.

CENELEC (2003), Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, EN 50129:2003, European Committee for Electrotechnical Standardization: Bryssel.

CENELEC (2017a), Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, EN 50126-1:2017, European Committee for Electrotechnical Standardization: Bryssel.

CENELEC (2017b), Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety, EN 50126-2:2017, European Committee for Electrotechnical Standardization: Bryssel.

CENELEC (2011), Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, EN 50128, European Committee for Electrotechnical Standardization: Bryssel

SIS (2015), Ledningssystem för kvalitet – Krav, ISO 9001:2015, utgåva 4, Svenska Institutet för Standarder: Stockholm.

Källor online

Analysgruppen (2006), Forsmarksincidenten den 25 juli 2006 – Bakgrund. Tillgänglig online: https://analys.se/wp-content/uploads/2015/05/forsmarksincidenten-bakgrund2006-5.pdf (2020-05-07).

Boverket (2018), Vägledning om standarder. Tillgänglig online: https://www.boverket.se/sv/byggande/vagledning-om-standarder/ (2020-03-03).

ERA (2016), Set of specifications 3 (ETCS B3 R2 GSM-R B1) Subset-026. Tillgänglig online: https://www.era.europa.eu/content/set-specifications-3-etcs-b3-r2-gsm-r-b1_en (2020-03-18).

European Commission (2020), Transport Modes – Rail. Tillgänglig online: https://ec.europa.eu/transport/modes/rail (2020-03-03).

Regeringskansliet (2016), Nystart för Nollvisionen – Ett intensifierat arbete för trafiksäkerheten i Sverige. Tillgänglig online: https://www.regeringen.se/4a509c/contentassets/00c9b57223d74e1fa0fe4da50e1e4e83/trafiksakerhet_160905_webb.pdf (2020-05-15)

SEK (2019), Kalender 2019. SEK Svensk Elstandard: Kista. Tillgänglig online: https://elstandard.se/wp-content/uploads/SEK_Kalender_2019.pdf (2020-02-28).

SVT (2016), Dom väntas kring tågolycka i Kimstad. Tillgänglig online: https://www.svt.se/nyheter/lokalt/ost/dom-vantas-kring-tagolyckan-i-kimstad (2020-05-24)

Trafikverket (2019a), ERTMS- nytt signalsystem. Tillgänglig online: https://www.trafikverket.se/for-dig-i-branschen/teknik/ertms--nytt-signalsystem/ (2020-03-10).

Trafikverket (2019b), Om oss. Tillgänglig online: https://www.trafikverket.se/om-oss/var-verksamhet/ (2020-02-25).

Trafikverket (2019c), Tåg i tid. Tillgänglig online: https://www.trafikverket.se/om-oss/vi-gor-sverige-narmare/Tag-i-tid/ (2020-05-14)

Vinnova (2013), Strategisk F&I-agenda Signalsystem för Spårtrafik. Tillgänglig online: https://www.vinnova.se/contentassets/f99e5fcca12d494ca3a475e3eb7dc5e8/signalsystem-for-spartrafik.pdf (2020-05-14).

Appendix A

Intervjuguide för semistrukturerade intervjuer

Allmänt (frågor som förekommit under de flesta intervjuer)

- Vad har du för roll och vad arbetar du med?
- Vad innebär X (MTO, Kvalitet, Säkerhet, IT-säkerhet med mera) inom TRV och ERTMS-programmet?
- Anser du att X är etablerat inom ERTMS-programmet?

Standarder

- Har du bra koll på standarderna, tex. EN 50126, EN 50128, EN 50129?
- Är arbetet upplagt efter dessa?
- Finns det någon problematik gällande standarderna?

EN 50129

- Kommer du i kontakt med EN 50129 i ditt arbete?
- Hur insatta är ni i EN 50129 och uppdateringen?
- Har du koll på den nya versionen EN 50129:2018?
- Vet du något som ändrats som påverkar ditt arbete?
- Har du ändrat/lagt till/utvecklat något utifrån uppdateringen av EN50129?
- Någon del av standarden som ni vill diskutera/som påverkar ert arbete?

Genomgång av utvalda delar från gap-analysen beroende på befattning

- Hur appliceras den här delen på er verksamhet?
- Vad har de här nya delarna för påverkan?
- Följs det som står i standarden?
- Är det några delar som inte följs alls?
- Vad skulle behöva förbättras?

Frågor ställda till Respondent J

Historiskt perspektiv

- När införde man CENELEC-standarderna EN 50126, EN 50128 och EN 50129?
- Vad var syftet med införandet av standarderna?

Standardiseringsarbetet

- Hur skrivs standarderna?
- Hur ska standarderna efterlevas/appliceras?
- Hur fungerar uppdateringarna?
- Pågår det något förändringsarbete idag?
- Fördelar och nackdelar med standarder?

EN 50129

- EN50129, vad innebär den?
- Hur jobbade ni med uppdateringen av EN 50129?
- Vilka är de största förändringarna i den nya versionen?
- Varför gjordes dessa förändringar?
- Hur påverkar förändringarna arbetet?

Frågor ställda till Respondent C, E, F

Allmänt om Säkerhet

- Vad innebär säkerhet för dig i ditt arbete?
- Var ligger fokus på vid säkerhetsarbete?
- Hur jobbar man för att veta att systemet är säkert?
- Anser du att det finns några brister i säkerhetsarbetet på TRV?

Standarder

- Hur arbetar man för att veta att man följer standarderna, framförallt EN 50129?
- Hur kan man säkerställa att allt följs?
- Finns det brister i säkerhetsarbetet kopplade till hur man applicerar standarder?
- Vid versionsuppdatering/förändring, hur följer man bäst ett nytt krav?