Säkerhetsevidens för IT-system

En inledande studie om bevisföring för systematisk säkerhet

Daniel Eidenskog, Christian Vestlund

FOI-R--5686--SE

December 2024

FOI

Daniel Eidenskog, Christian Vestlund

Säkerhetsevidens för IT-system

En inledande studie om bevisföring för systematisk säkerhet

Titel	Säkerhetsevidens för IT-system – En inledande studie om bevisföring för systematisk säkerhet
Title	Security evidence for IT systems – An initial study on evidential argumentation for systematic security
Rapportnr/Report no	FOI-R--5686--SE
Månad/Month	December
Utgivningsår/Year	2024
Antal sidor/Pages	40
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E38529
Godkänd av/Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: Daniel Eidenskog

Sammanfattning

Säkerhetsevidens utgörs av olika typer av artefakter som påvisar säkerhets-egenskaper hos IT-system, ofta på ganska specifik detaljnivå. Evidens värderas och aggregeras till bevisföring som i sin tur påvisar att IT-systemen uppfyller de säkerhetsbehov som finns på verksamhetsnivå.

Denna studie undersöker hur olika metoder och säkerhetsstandarder inom cybersäkerhet och funktionell säkerhet använder evidens för att påvisa att IT-systemen når tillräcklig säkerhetsnivå. Evidensen utgör en viktig bas för att uppnå assurans, där tillräckligt hög tilltro till såväl IT-systemen i sig som till utvecklare och leverantörer har uppnåtts för att kunna använda systemen i säkerhetskritiska tillämpningar.

Evidens utgörs av konkreta och spårbara underlag som kan ha producerats genom ett brett spektrum av olika metoder, såsom designgenomgångar, kodgranskning, praktiska tester och formella metoder. De processer och standarder som undersökts i studien rekommenderar olika evidensmetoder men inkluderar endast generella beskrivningar av vad metoderna innebär, varför tolkningsutrymmet är stort avseende vad som faktiskt ska utföras. Värdering och aggregering beskrivs endast på övergripande plan vilket ytterligare ökar oklarheterna kring vad som efterfrågas.

Det finns ett stort forskningsbehov inom evidensområdet ända från säkerhetsmål till enskilda evidensmetoder. Området värdering och aggregering tycks vara särskilt outforskat, samtidigt som det finns ett stort behov av att förbättra och utveckla olika evidensmetoder.

Nyckelord: IT-säkerhet, cybersäkerhet, ackreditering, evidens, testning

Summary

Assurance evidence consists of various artefacts that reflect security properties of an IT system, often at a fairly detailed level. Evidence is valued and aggregated into an argumentation that demonstrate that the IT system fulfills the security requirements imposed.

This study investigates how different methods and standards in cyber security and functional safety use evidence to demonstrate how security or safety requirements are met. Evidence is an important basis for assurance, where enough trust in the IT system, developers, and suppliers has been attained to enable usage in security critical applications.

Evidence consists of tangible and traceable artefacts that are produced through a wide spectrum of methods, such as design walkthroughs, code reviews, tests, and formal methods. The processes and standards that are examined in this study recommend various evidence methods but provide only superficial descriptions of them, which leaves ample room for interpretation. Valuation and aggregation are only described in a general manner, which further adds to the vagueness.

There is a considerable research gap within security evidence, encompassing all areas from security goals to detailed evidence methods. While valuation and aggregation seem to be especially unexplored, there is need for additional research to develop and improve evidence methods.

Keywords: IT security, cybersecurity, accreditation, evidence, testing

Innehållsförteckning

1 Inledning

IT-system[1] som hanterar verksamhetskritisk information eller styr verksamhetskritiska funktioner behöver hålla en hög säkerhetsnivå över hela systemets livstid. Det är skyddsbehovet för informationen och funktionen som styr vilken kravnivå som IT-systemet – sett som sociotekniskt system – ska uppnå. Ett högt skyddsbehov innebär att systemen omfattas av höga krav på informations- och IT-säkerhet under systemets hela livscykel. Kraven berör dessutom många olika aspekter, såsom användbarhet, design, implementation, förutsättningar för kontinuerligt säkerhetsarbete och förutsättningar för incidentrespons. Säkerhetskraven blir extra höga när informationen eller funktionen i systemet omfattas av säkerhetsskyddslagstiftningen.

Verksamheten ges möjlighet att upprätthålla skyddsnivån i IT-systemen över tid genom kontinuerligt förebyggande säkerhetsarbete som kompletteras med verksamhetens förmåga till reaktiva säkerhetsåtgärder och att återställa systemets funktion efter en incident. I det förebyggande arbetet ingår bland annat att tillse att systemet är sunt utformat med tillräckligt bra säkerhetsdesign och tillräcklig säkerhetsmässig kvalitet. Det är viktigt att kunna analysera och bedöma systemens säkerhetsegenskaper för att säkerställa att säkerhetskraven möts och att säkerhetsbehoven därmed tillfredsställs. Att kunna analysera och bedöma säkerhetsegenskaperna är dessutom en förutsättning för att kontinuerligt kunna upprätthålla systemens skyddsnivå genom systematiskt säkerhetsarbete över hela livscykeln, inklusive när förändringar sker i systemen, i deras användning eller i deras miljö.

Ett ord som ofta används i sammanhanget är *assurans* – en relativt vag term som ungefär går att tolka som tilltro till systemet och dess leverantörer. Standarden ISO 15026-1 definierar den engelska termen assurance som ”ett välgrundat förtroende för att en utfästelse är eller kommer att bli sann”.[2] Problemet med att förlita sig på den generella definitionen av assurans vid utveckling och godkännande av säkerhetskritiska system är den vaghet som begreppet bär med sig. Vilka utfästelser handlar det om för att uppnå ett säkert system? Hur välgrundat måste förtroendet vara? Vilka metoder kan användas för att uppnå förtroendet? Assuranskonceptet är en bra utgångspunkt men kräver förtydliganden i form av exempelvis processer, metoder och bedömningsgrunder.

Denna rapport undersöker *säkerhetsevidens* som en viktig byggsten för att uppnå assurans genom analys och bedömning av systemens egenskaper.

[1] I denna rapport används termerna ”system” och ”IT-system” utbytbart och avser alla typer av system som innehåller IT-komponenter. De inkluderar således inte bara vanliga kontorsdatorer och servrar utan även andra typer av produkter och system, såsom mobiltelefoner och utrustning med inbäddade datorer.

[2] ISO/IEC/IEEE, 2019, avsnitt 3.1.1 (författarnas översättning).

Säkerhetsevidens utgör konkreta och spårbara underlag som påvisar någon form av specifik säkerhetsegenskap hos systemet och som kan användas för bevisföring kring säkerhetsegenskaper hos systemet som helhet. Säkerhetsevidensen är viktig vid granskning och godkännande av alla typer av verksamhetskritiska IT-system men blir extra relevant i produkter och system med höga säkerhetskrav, såsom signalskyddssystem, datadioder och dataslussar. Förutom att evidensen bidrar till att få en känd säkerhetsnivå för systemen så ligger värdet även i att evidensen kan bidra till att ackrediterings- och certifieringsprocesser blir mer förutsägbara, exempelvis genom väldokumenterade konkreta och underbyggda resonemang och motiveringar.

1.1 Syfte och mål

Syftet med studien är att undersöka vad säkerhetsevidens är och hur den kan användas för att påvisa säkerhetsegenskaper hos IT-system. Målet med studien är att presentera en grund för fortsatt forskning inom framtagning, hantering och värdering av IT-säkerhetsevidens. Studien fokuserar på IT-system med omfattande skyddsbehov, däribland IT-system som omfattas av säkerhetsskyddslagen (2018:585) eller där oönskade händelser kan ge allvarliga konsekvenser.

För att nå fram till målet har följande forskningsfrågor satts upp med avsikten att de ska besvaras på en övergripande nivå:

- Vilka komponenter behövs för att säkerhetsevidens ska kunna användas i bevisföringen för att påvisa att IT-system är säkra?
- Vilka evidensmetoder förespråkas i befintliga standarder, processer och metoder inom IT-säkerhet och funktionell säkerhet i IT-system?

Studien har utförts inom ramen för Försvarsmaktens samlingsbeställning inom forskning och teknikutveckling (FoT). Studien har genomförts i projektet *Analys av koncept och teknik för cyberförsvar och informationssäkerhet* som ingår i FoT-området *Operationer i cyberdomänen*. Rapportens ämne, säkerhetsevidens, utgör bryggan mellan tekniknära aktiviteter (såsom tester och granskningar) som ämnar visa systemens säkerhetsnivå och de två högnivåperspektiven assurans och ackreditering.

1.2 Metod och avgränsningar

Studien är huvudsakligen en litteraturgenomgång av forskningsresultat och standarder inom IT-säkerhet och funktionell säkerhet. Studien utgår från såväl akademisk som icke-akademisk litteratur samt befintliga processer och standarder för säkerhetsarbete inom dessa områden. Litteraturen har samlats in genom explorativa sökningar efter forskningsresultat inom evidensområdet samt standarder för funktionell säkerhet och IT-säkerhet i hårdvara och mjukvara. De

explorativa sökningarna har inkluderat evidens och evidensmetoder för såväl IT-säkerhet som funktionell säkerhet.

Studiens fokus är att undersöka begreppet evidens och dess användande kopplat till välkända standarder och metoder inom säkerhet. Med säkerhet åsyftas i detta sammanhang såväl systemens informationssäkerhetsegenskaper som förmågan att upprätthålla en funktionellt säker funktion.

Studien är inte avsedd att vara en heltäckande, strukturerad litteraturstudie. Studien ämnar inte heller till att utvärdera specifika metoder för att producera evidens.

2 Bakgrund

Elektronik och mjukvara ingår numera i väldigt många olika typer av produkter och system. Under de senaste decennierna har komplexiteten i såväl elektronik som mjukvara ökat enormt samtidigt som cyberhoten har ökat i såväl komplexitet som förmåga. Tillsammans leder detta till en mycket utmanande situation när det gäller att skydda IT-systemen och innebär mycket höga krav på IT-säkerheten, speciellt när systemen används i verksamhetskritiska eller säkerhetskritiska tillämpningar.

IT-säkerhet är ett mångfacetterat och svårt problem, där angriparna har en fördel genom att de endast behöver hitta ett hål i säkerheten för att kunna påverka systemet. Försvararna behöver i stället täppa igen alla hål för att systemet ska vara fullständigt säkert. En sådan absolut säkerhet är dock inte uppnåelig i praktiskt användbara system på grund av systemens komplexitet; det skulle krävas synnerligen enkla system för att möjliggöra absoluta garantier på säkerhet. Därför måste målsättningen i stället vara att försöka nå *tillräckligt hög säkerhet* så att den kvarstående risknivån är acceptabelt låg i relation till respektive systems användning och förutsättningar. För system med höga säkerhetskrav tenderar detta att bli ett mycket omfattande arbete.

Utöver svårigheterna att designa och implementera ett system för att möta höga säkerhetskrav är det dessutom en svår uppgift att avgöra när systemet uppnått tillräckligt hög säkerhet för sin användning. I praktiken kommer avgörandet alltid att utgå från inkompletta underlag då komplexiteten hos systemen blir för hög för att det ska vara möjligt att genomföra en heltäckande genomlysning av systemets alla delar.

2.1 Olika typer av säkerhet

Betydelserna hos det svenska begreppet *säkerhet* inkluderar bland annat att något är skyddat mot fara och att det inte utgör en fara för någon annan. De sammanhang som är av relevans i denna rapport är skydd mot skador i IT-miljön och skydd mot fysiska skador såsom personskador och materiella skador. I denna rapport används termen *IT-säkerhet* för skydd mot skador i IT-miljön medan skyddet mot fysiska skador benämns som *funktionell säkerhet*. I båda sammanhangen kan de bakomliggande orsakerna till potentiella skador vara såväl antagonistiska handlingar som olyckor, även om fokus för skyddet mot fysiska skador traditionellt sett har handlat om skydd mot olyckor medan IT-säkerhet i betydligt större utsträckning har inkluderat antagonistiska handlingar. I rapporten förekommer säkerhet i båda betydelserna och där det är relevant kommer det specificeras vilken typ av säkerhet som åsyftas.

Ibland görs det skillnad på IT-säkerhet och cybersäkerhet, där en tolkning är att IT-säkerhet avser skydd mot alla former av avsiktliga och oavsiktliga risker för

IT-systemen medan cybersäkerhet endast avser antagonistiska hot. För att undvika missförstånd kommer begreppen att användas på detta sätt i rapporten.

2.2 Vad är säkerhetsevidens?

Säkerhetsevidens utgör information om hur ett säkerhetsbehov uppfylls, vanligtvis på en relativt detaljerad nivå. Säkerhetsevidensen kan bestå av många olika typer av informationsartefakter, inkluderande både evidens på konkret implementationsnära nivå och metaevidens som sammanväger annan evidens. Den implementationsnära nivån omfattar exempelvis testspecifikationer med tillhörande testresultat, utlåtanden från kodgranskning och felträdsanalyser. Metaevidensen utgörs till exempel av spårning från säkerhetsbehov till konkreta säkerhetsfunktioner, aggregering av evidens till högre nivå och assuransfall.

Mer formellt går det att uttrycka att respektive evidensartefakt stödjer (eller förkastar) en eller flera hypoteser om att ett eller flera specifika, detaljerade säkerhetsbehov är korrekt hanterade.[3]

Vissa typer av säkerhetsevidens ger absoluta resultat inom sina avgränsningar, till exempel om systemet helt saknar USB-anslutningar och USB-relaterad mjukvara finns inte heller några säkerhetsrisker relaterade till USB. Många typer av säkerhetsevidens ger dock inte ett absolut resultat, utan måste värderas utifrån sina avgränsningar och sin styrka som evidens för den specifika säkerhets-egenskap som analyseras. Exempel på detta är kodgranskning, där bland annat granskarnas erfarenhet, granskningens målsättning och den granskade kodens komplexitet spelar in i evidensvärdet.

Som nämnts tidigare förekommer säkerhetsevidens på många olika nivåer, från evidens för lågnivåegenskaper på källkods- och elektroniknivå till evidens som visar att säkerhetsbehoven som helhet möts på systemnivå. Evidens handlar dock inte enbart om *vad* som producerats, såsom källkod, dokument och elektronik. Evidens kan även handla om *hur* en artefakt producerats. Exempel på detta är mjukvaruutvecklingsprocesser och kodningsstandarder som styr hur mjukvara produceras samt granskningsprocesser som styr hur systemet granskas.

Det går att dra tydliga paralleller mellan säkerhetsevidens och bevisning inom juridiken. De juridiska bevisen utgör en samlad informationsmängd som vägs samman för att komma till en slutsats – att styrka eller vederlägga ett påstående, exempelvis om en individs skuld i ett brottmål. Olika bevis har olika värde som vägs samman genom juridiska bedömningar till en slutsats kring individens skuld. Vissa bevis utgörs av faktum, det vill säga verkliga händelser eller sakförhållanden som direkt knyter till verkliga händelser, medan andra bevis

[3] Se exempelvis ACWG, 2021, kapitel ”Glossary”.

utgörs av indicier som indirekt tyder på att något är sant.[4] Juridiska bevis är sällan heltäckande utan lämnar informationsluckor som måste hanteras när slutsatsen ska dras om huruvida bevisningen uppnår ”utom rimligt tvivel”.[5]

Samma grundläggande förhållanden gäller inom säkerhetsevidensen. Viss evidens utgör faktum inom sina avgränsningar, såsom positiva testresultat som påvisar att testerna faktiskt har genomförts med godkända resultat. Denna typ av evidens visar på ett faktum inom evidensens ramar – i detta fall att systemet uppfyller det som täcks av de genomförda testerna. Annan evidens utgör indicier som tyder på att något sannolikt är på ett visst sätt. Detta kan exempelvis vara process- och metodbeskrivningar som pekar på att arbetet har utförts enligt god sed. Denna senare typ av evidens kan värderas upp eller ner genom olika former av kompletterande undersökningar, såsom revisioner där faktiskt arbetssätt jämförs med dokumenterade processer. Säkerhetsevidensen kommer inte att vara heltäckande, då systemens komplexitet i praktiken alltid är för stor, varför slutsatsen ur ett säkerhetsgranskningsarbete i praktiken alltid blir en bedömning av systemets säkerhetsnivå.

En skillnad mellan juridik och IT-säkerhet är hur brist på bevis rimligtvis bör hanteras. Medan juridiken går mot att fria den misstänkte så bör beslutet inom IT-säkerhet kanske snarare vara att fälla – i alla fall för säkerhetskritiska system. I dessa fall bör systemen rimligen inte anses som tillräckligt säkra om viktiga underlag saknas vid bedömningen.

[4] Se exempelvis *Allt om juridiks* ordlista, https://www.alltomjuridik.se/ordlista/

[5] Se exempelvis *Två avgöranden om bevisvärdering i brottmål*, Högsta Domstolen, https://www.domstol.se/nyheter/2023/02/tva-avgoranden-om-bevisvardering-i-brottmal/

3 Bevisföring

Det är en utmanande uppgift att påvisa om IT-system är att betrakta som säkra. För att uppnå tillförlitliga säkerhetsbedömningar som även är användbara som grund för ett långsiktigt säkerhetsarbete krävs en stabil utgångspunkt som inkluderar verksamhetens behov av säkerhet. Med säkerhetsbehoven som avstamp för en genomarbetad kravbild och tillhörande evidens underlättas bedömningsarbetet vid granskning och ackreditering av systemen.

Detta kapitel beskriver några aspekter av kravställning och bevisföring som påverkar behoven av evidens.

3.1 Utgå från säkerhetsbehoven

Då alla system har olika förutsättningar behöver säkerhetsarbetet utgå från säkerhetsbehoven för respektive system i sin kontext. Säkerhetsbehoven behöver därmed analyseras och sammanställas specifikt för respektive system. Först därefter kan de förädlas och förfinas till en uppsättning säkerhetsmål och säkerhetskrav som sedan omhändertas i de olika faserna av systemets livscykel. Evidens för hur säkerhetskraven omhändertas blir därefter viktiga underlag till analysen av den faktiska säkerhetsnivån för systemet som helhet och hur systemet möter säkerhetsbehoven.

Att analysera säkerhetsbehoven och planera de konkreta åtgärder som ska vidtas är centrala punkter i ett strukturerat säkerhetsarbete. Behovet av analyser tas därför upp redan i 2 kap. 1 § säkerhetsskyddslagen (2018:585):

> *Den som till någon del bedriver säkerhetskänslig verksamhet (verksamhetsutövare) ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras.*
>
> *Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.*

Behovet förtydligas även genom 3 kap. 1 § säkerhetsskyddsförordningen (2021:955):

> *Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift ska verksamhetsutövaren genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Säkerhetsskyddsbedömningen ska dokumenteras.*

Inom Försvarsmakten dokumenteras analysen i en säkerhetsmålsättning, vars roll i IT-säkerhetsarbetet beskrivs i Försvarsmaktens *Handbok Säkerhetstjänst Informationssäkerhet*, kap 14:

> *I en säkerhetsmålsättning för ett IT-system dokumenteras analyser över vilket skydd IT-systemet kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. […]*
>
> *En säkerhetsmålsättning används under ett IT-systems livscykel som ett samlat kravdokument för IT-säkerhet. Fokus i en säkerhetsmålsättning ligger på vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. En säkerhetsmålsättning används bl.a. i ackrediteringsarbetet […] genom att granskningen utgår från målsättningen för att kunna bedöma om de framtagna skyddsåtgärderna tillgodoser de uppställda förväntningarna.*[6]

Att fånga upp och dokumentera säkerhetsbehoven bidrar till en samsyn på systemens övergripande förutsättningar. Säkerhetsbehoven utgör de övergripande och designoberoende förutsättningar som måste uppfyllas för att systemet ska kunna upprätthålla skyddet av verksamheten och informationen. Säkerhetsbehoven omfattar bland annat vilken sekretess, riktighet och tillgänglighet som gäller för den information som systemet hanterar och skyddsvärdet hos de funktioner som systemet bidrar med i verksamheten.

Även om det ovanstående resonemanget utgår från reglerna för hantering av säkerhetsskyddsklassificerad information inom Försvarsmakten, så är de grundläggande principerna för utveckling och förvaltning av säkra system liknande oavsett kontext. För att ett system ska kunna hålla en hög och känd säkerhetsnivå krävs kontinuerligt, strukturerat säkerhetsarbete även i andra sammanhang.[7]

3.2 Relevanta och tydliga krav

För att säkerhetsbehoven ska bli praktiskt användbara under utveckling och vidmakthållande av IT-systemen behöver de förfinas till mer formaliserade, mätbara och konkreta säkerhetskrav.[8] Steget från säkerhetsbehov till säkerhetskrav är kritiskt i ett systems utveckling då kravens utformning till stor del styr urval och utformning av skyddsmekanismer i systemet. Dessutom styr kraven till

[6] Försvarsmakten, 2017.

[7] Se exempelvis problembeskrivningen kring cybersäkerhetsarbete i fordons- och medicinteknikindustrin i Mohamad m.fl., 2024, avsnitt 1.

[8] Bildsten m.fl., 2018.

viss del hur granskning kan genomföras, bland annat genom att påverka vilken evidens som tas fram. Samtidigt kan kravarbetet inte utföras utan en solid grund av identifierade säkerhetsbehov då kravarbetet annars tenderar att sakna verksamhetsförankring.

Vid upphandlingar inkluderar kravställningen avseende IT-säkerhet sällan konkreta och mätbara sätt att påvisa att säkerhetskraven är uppfyllda.[9] Detta gäller oavsett om de upphandlade systemen är säkerhetskritiska eller inte. Detta leder till problem eftersom olika parter – helt naturligt – tolkar kraven och förväntningarna på olika sätt. Problem som kan uppstå inkluderar bland annat att säkerhetskrav helt missas, att leverantörerna underskattar arbetsinsatsen som krävs och att inköpande organisation godkänner leveranser trots att de inte uppfyller relevanta säkerhetskrav.

Kravställning vid upphandling eller inköp av IT-system är svårt och blir snabbt ett komplext problem ju större systemen är. Det har skrivits mycket om detta, bland annat med fokus på säkerhetsaspekter, såsom FOI-rapporten *RASK – Ramverk för IT-säkerhetskravställning,*[10] och med fokus på anskaffning, såsom FOI-rapporten *Effektivare anskaffning och integration av ledningsstödsystem.*[11] En viktig aspekt är säkerhetskravens mätbarhet – det vill säga hur parterna ska kunna veta och vara överens om vad ett säkerhetskrav betyder och hur kravets uppfyllnad ska bedömas. Detta är en av de aspekter som belyses i RASK-rapporten.[12]

Hur krav tas fram är inte fokus för den här studien. Det viktiga att belysa i kopplingen mellan krav och evidens är att kraven, explicit eller implicit, styr vilken evidens som bör tas fram. Krav formulerade på sätt som till exempel ”ska vara säkert”, ”ska kunna godkännas” eller ”ska kunna ackrediteras” är direkt olämpliga om det inte finns tydliga underlag som definierar vad som anses säkert eller vad som krävs för att systemet ska kunna godkännas eller ackrediteras.

Det finns IT-säkerhetsstandarder (exempelvis Common criteria[13]) som styr hur säkerhetskrav kan formuleras och brytas ner, men att följa en sådan standard är ingen garanti för en heltäckande kravställning. Risken finns att systemet utvecklas för att uppfylla de ställda kraven snarare än för att möta säkerhets-behoven, vilket kan leda till säkerhetsbrister om kraven inte är heltäckande.[14] Det är således av stor vikt att kraven tas fram på ett adekvat sätt för att faktiskt täcka

[9] Vestlund m.fl., 2024, s. 61.

[10] Bildsten m.fl., 2018.

[11] Nordström m.fl., 2020.

[12] Bildsten m.fl., 2018.

[13] Common Criteria, 2022a.

[14] Karlzén m.fl., 2017, s. 23 och 30.

säkerhetsbehoven snarare än för att uppfylla en specifik standard eller möta en generell kravbild.

3.3 Spårbarhet

En viktig aspekt i att påvisa hur mål och krav på systemnivå uppfylls är spårbarhet i form av strukturerad och dokumenterad nedbrytning av mål och krav ända ner till implementationen. Spårningen bygger typiskt på två distinkta komponenter: dels nedbrytningen från respektive abstraktionsnivå till en eller flera delar på mer detaljerad nivå, dels underlag som påvisar att nedbrytningen uppfyller kraven på den högre nivån. Att spårning av krav ner till implementation har effekt på kvaliteten hos mjukvara har påvisats av bland annat Rempel och Mäder som undersökte spårningens korrelation mot antalet defekter i mjukvaran.[15] I studien konstaterade de att det finns en statistiskt signifikant koppling mellan spårning och minskat antal defekter. Även om undersökningen inte särskilde olika typer av krav så går det att förmoda att resultaten även är giltiga för underkategorin säkerhetskrav.

Spårbarhet från säkerhetsmål till evidens har en central roll i flera standarder för att utveckla säkra IT-system, exempelvis i de högre nivåerna i Common criteria.[16] Genom spårningen förenklas arbetet med att bedöma systemens säkerhet vid exempelvis ackrediteringsbeslut, då det finns en tydligare koppling mellan säkerhetskraven och hur de implementeras – oavsett om implementationen innebär krav på miljön, användarinstruktioner, systemarkitektur eller säkerhetsfunktioner i hårdvara och mjukvara.

Spårning ger även möjlighet att bedöma hur förändringar i systemen och i systemens omgivning påverkar säkerheten. Förändringar kan exempelvis vara att systemet ska användas i andra sammanhang, att sårbarheter upptäcks, att hotbilden ändras eller att nya funktioner läggs till i systemet. Genom spårningen går det lättare att hitta de säkerhetsaspekter i systemet som påverkas av förändringen, så att en bedömning kan göras av vilka eventuella åtgärder som krävs för att upprätthålla säkerhetsnivån. Om det inte redan tidigare gjorts ett systematiskt säkerhetsarbete försvåras arbetet med att bedöma förändringarnas påverkan då det saknas en stabil utgångspunkt för bedömningen.

Spårningen kan också tydliggöra vilken evidens som saknas för att kunna bedöma säkerhetsegenskaperna. Det är dock viktigt att behoven av säkerhetsevidens är klargjord i förväg så att alla parter är medvetna om vad som förväntas.

[15] Rempel & Mäder (2017).

[16] Se exempelvis kravkomponent ADV_FSP.1.4c (Common Criteria, 2022b, s. 75) som ingår på nivå EAL 1 (Common Criteria, 2022c, s. 15).

Det är i regel bättre att producera relevant säkerhetsevidens i samband med utvecklingen då det kan vara kostnadsdrivande att göra det i efterhand.[17]

3.4 Argumentation och värdering

Den strukturerade, spårbara och dokumenterade argumentationen som beskrivs i föregående avsnitt är en viktig komponent för att möjliggöra väl underbyggda och repeterbara bedömningar av hur väl säkerhetsmålen uppfylls. Det finns dock stor frihet i hur argumentationen ska göras och det går att anta att olika ansatser kan ge varierande effektivitet. Hawkins m.fl. noterar att den strukturerade argumentationen i till exempel goal structuring notation (GSN)[18] bör separeras i två delar: (1) ett säkerhetsfall som tar upp konkret evidens och konkreta resonemang kring säkerhetsnivå och riskreducerande åtgärder samt (2) ett konfidensfall som behandlar tilltron till argumentationen i säkerhetsfallet.[19] Motiveringen till uppdelningen är att göra tilltron mer explicit för att granskaren lättare ska kunna se vilka delar som omfattas av svagare argumentation.[20]

Li m.fl. förslår en modell för källor till tilltro (eng. trust) till systemet och dess säkerhetspåståenden.[21] I modellen ingår tre huvudsakliga källor till tilltro: direkt evidens, indirekt evidens och leverantörernas trovärdighet. Direkt evidens visar på ett konkret sätt att säkerhetspåståenden är uppfyllda och möjliga att förstå, samtidigt som evidensen visar att leverantörerna gjort det som utlovats. Indirekt evidens utgörs av information från tredje parter, såsom granskare eller externa certifieringsorgan. Leverantörernas trovärdighet baseras på vad Li m.fl. kallar för prestation, förmåga, moral och social position.[22] Dessa fyra komponenter i leverantörernas trovärdighet antas indikera förutsägbarheten i hur respektive leverantör kan förväntas uppfylla de uppsatta säkerhetskraven och ger därmed en indikation på leverantörens trovärdighet.

Duan m.fl. lyfter osäkerhet som en viktig aspekt i värdering av evidens, vilket också innebär att det är relevant hur osäkerhet hanteras i samband med evidensvärdering.[23] De delar upp osäkerheter i två olika typer, benämnda aleatorisk osäkerhet och epistemisk osäkerhet. Aleatorisk osäkerhet, även kallad statistisk osäkerhet, behandlar okända aspekter av känd art som vanligen kan värderas

[17] Nair m.fl, 2014, s. 690.

[18] Hawkins m.fl., 2011.

[19] Hawkins m.fl., 2011.

[20] Hawkins m.fl., 2011.

[21] Li m.fl., 2021.

[22] Li m.fl., 2021.

[23] Duan m.fl., 2017.

genom sannolikheter eller sannolikhetsfördelningar. Epistemisk osäkerhet, även kallad systematisk osäkerhet, inkluderar snarare de okända aspekter som är av okänd art och som i regel är svåra att åsätta sannolikheter.[24]

Uppdelningen i aleatoriska respektive epistemiska osäkerheter leder naturligt till användning av olika metoder för att resonera kring och hantera osäkerheterna. Kvantitativa metoder i form av statistik och sannolikhetsberäkningar lämpar sig för aleatoriska osäkerheter medan epistemiska osäkerheter lättare hanteras med kvalitativa metoder.[25] I de kvantitativa metoderna accepteras osäkerheter som en realitet som måste bedömas och hanteras, exempelvis genom olika mått på konfidens. De kvalitativa metoderna inkluderar i stället olika sätt att eliminera eller minimera osäkerheterna, exempelvis genom logiska resonemang eller genom att identifiera och eliminera orsaker till osäkerhet.[26]

Osäkerhet och tilltro (konfidens) behöver inte vara direkt relaterade till varandra; de kan även anses vara mått på olika typer av egenskaper.[27] Exempelvis bygger metoden som Ayoub m.fl. presenterar på att konfidensbedömningar ska genomföras för att värdera såväl om evidensen påvisar att säkerhetsegenskapen är uppfylld som om evidensen påvisar motsatsen.[28] Genom dubbelriktad bedömning ska risken för bekräftelsebias (eng. confirmation bias) minimeras.[29]

I denna studie har flera artiklar identifierats som diskuterar olika former av kvalitativa och kvantitativa metoder för att resonera kring konfidens och osäkerhet.[30] Själva evidensvärderingen tycks däremot oftast göras genom mänskliga bedömningar.[31]

Tilltro till evidensen och evidensens tyngd är olika saker; de pekar på hur trovärdigt det är att evidensen visar verkliga förhållanden respektive hur övertygande evidensen är om att säkerhetsegenskapen uppfylls.[32] Evidensens tyngd består av flera olika komponenter, såsom hur mycket evidens som finns, hur stor del av säkerhetsegenskapen som täcks och vilken styrka evidensens olika delar uppnår. Som en del i resonemanget om tyngd poängterar Grigorova och

[24] Duan m.fl. (2017) beskriver aleatoriska och epistemiska osäkerheter som ”kända okända” respektive ”okända okända”.

[25] Duan m.fl., 2017.

[26] Duan m.fl., 2017.

[27] Duan m.fl., 2017.

[28] Ayoub m.fl., 2013.

[29] Ayoub m.fl., 2013.

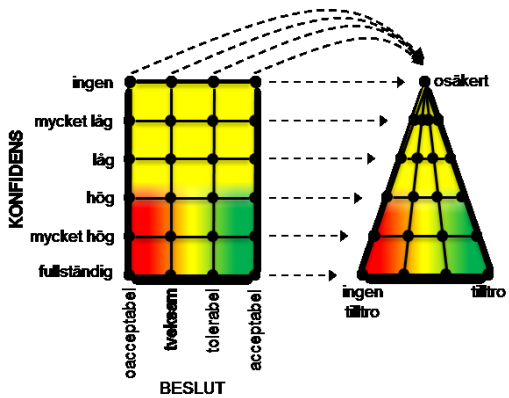
[30] Exempelvis Duan m.fl., 2017; Grigorova & Maibaum, 2013; Idmessaoud m.fl., 2022; Nair m.fl., 2014.

[31] Se Li m.fl., 2021.

[32] Grigorova & Maibaum, 2013.

Maibaum att frågan om en tillräcklig mängd evidens uppnåtts behöver behandlas separat i bevisföringen.[33] Även om evidensen är av god kvalitet med hög tilltro och stor tyngd kanske den ändå inte är tillräckligt omfattande för att täcka in säkerhetsegenskapen.

Cyra och Górski kombinerar två aspekter – beslut och konfidens – i en matris som de sedan mappar till en triangel, vilket i praktiken ger tre möjliga utfall angående tilltro: att tilltron finns, att tilltron saknas eller att tilltron inte kan fastställas.[34] Figur 1 visar principen för deras sammanvägning och hur brist på konfidens avspeglas i en osäkerhet om systemets säkerhetsnivå – att säkerhets-frågan är obesvarad – snarare än att det med visshet saknas tilltro till systemet.



Figur 1. Kombination av beslut och konfidens (Cyra & Górski, 2011).

[33] Grigorova & Maibaum, 2013.

[34] Cyra och Górski, 2011.

4 Evidens i befintliga standarder, processer och metoder

Evidens kan produceras på många olika sätt som kan skilja sig åt signifikant då evidens kan påvisa allt från detaljegenskaper hos ett tekniskt system till en organisations sätt att ta beslut. Exempelvis kan direkt evidens för ett systems beteende tas fram genom att genomföra specifika tester medan indirekt evidens kan tas fram genom att intervjua utvecklare på ett företag om hur de använder en specifik mjukvaruutvecklingsprocess.

Flera standarder ger exempel på metoder som kan användas i olika faser i utvecklingen av ett tekniskt system. Det kan däremot skilja en hel del i standardernas beskrivningar av metoderna och deras beskrivningar för hur resultaten ska utvärderas.

Detta kapitel ger exempel på metoder som olika standarder rekommenderar för att producera evidens. Utöver de standarder, processer och metoder som behandlas här finns det flera andra som berör evidens för cybersäkerhet, såsom NIST SP 800-160[35], NIST:s Cyber security framework[36] och UK NCSC:s Cyber Assessment Framework[37]. Gemensamt för dessa är dock att de inte går in i detalj på vilken evidens som förväntas i olika sammanhang.

4.1 Assuransfall (ISO/IEC/IEEE 15026)

Ett assuransfall utgår från ett påstående om ett systems egenskaper följt av en strukturerad argumentation och tillhörande evidens för varför påståendet är sant. Ett av syftena med assuransfall är att tydliggöra resonemanget kring systemets säkerhet. Assuransfall kan göras olika detaljerade beroende på hur mycket konfidens som ska uppnås för ett påstående om systemets egenskaper.

I assuransfall utgör evidens definierade entiteter i ett större argument. Metoden ger möjlighet till att aggregera olika evidens genom den argumentation som ska tas fram för att motivera att assuransfallet har uppfyllts. Standarden innehåller ett avsnitt med resonemang kring osäkerhet och konfidens i assuransfallen:

> *Graden av konfidens som kan tas fram eller är försvarbart framtagen baserat på ett specifikt assuransfall kan variera beroende på individ, organisation och situation. Ju mindre osäkerhet i ett assuransfalls*

[35] Ross m.fl., 2022.

[36] NIST, 2024.

[37] NCSC, 2024.

> *påståenden desto högre grad av försvarbar konfidens. Dock är omvandlingen från en mängd osäkerhet till en grad av försvarbar konfidens för specifika tillämpningar varken rättfram eller välförstådd.*[38]

I branscher där fokus ligger på funktionell säkerhet kallas motsvarigheten till assuransfall vanligtvis för *safety case*, en term som tycks sakna vedertagen svensk översättning men som närmast kan kallas för säkerhetsfall. Assuransfall och dess motsvarigheter förekommer i flera olika branscher utöver IT-säkerhetsområdet, till exempel fordon[39], kärnkraft[40] och medicinska IT-system[41].

4.2 Säkerhetsrelaterade system (IEC 61508)

IEC 61508 är en generell standard för funktionell säkerhet inriktad på elektriska, elektroniska och programmerbara system.[42] Standarden definierar fyra så kallade SIL-nivåer (eng. safety integrity level) som används för att bedöma risk för skador och därmed krav på säkerhet.

Standarden ställer inga krav på att ta fram något som motsvarar assuransfall men innehåller många krav om vilken evidens som ska produceras för att påvisa ett systems säkerhetsegenskaper.

Standarden specificerar rekommendationer på olika metoder som kan användas vid hantering av krav eller verifiering av mjukvaruimplementationer. Olika SIL-nivåer har olika rekommendationer för vilka metoder som är lämpliga att använda.

4.2.1 Verifiering av mjukvara i IEC 61508

IEC 61508 innehåller rekommendationer för metoder för verifiering av mjukvara. Standarden ger även en viss vägledning i val av metoder och hur de ska genomföras:

> *Att testa att mjukvarumodulen korrekt uppfyller sin testspecifikation är en verifieringsaktivitet […]. Det är kombinationen av kodgranskning och*

[38] ISO/IEC/IEEE, 2019, s. 11, förf. övers.

[39] ISO/SAE, 2021 och SIS, 2018a.

[40] Office for Nuclear Regulation, 2020.

[41] IEC, 2017.

[42] IEC, 2010a.

modultestning som ger assurans för att mjukvarumodulen uppfyller sin tillhörande specifikation, dvs. att den är verifierad.[43]

Tabell 1 listar föreslagna metoder för mjukvaruverifiering på modul- och integrationsnivå i IEC 61508-3 samt för vilken SIL-nivå som metoderna rekommenderas.[44] Utöver tabellen som återges nedan finns rekommendationer för flera andra verifieringsområden, såsom för programmerbar elektronik och i samband med modifieringar.[45]

Tabell 1. Metoder för verifiering av mjukvara i IEC 61508.

Metod	**SIL-nivå**			
	1	2	3	4
Probabilistisk testning	---	R	R	R
Dynamisk analys och testning	R	HR	HR	HR
Datainspelning och analys	HR	HR	HR	HR
Funktionell testning och svartlådetestning[46]	HR	HR	HR	HR
Prestandatestning	R	R	HR	HR
Modellbaserad testning	R	R	HR	HR
Gränssnittstestning	R	R	HR	HR
Testhantering och verktyg för automatisering	R	HR	HR	HR
Spårbarhet från mjukvaru-designspecifikation till modultest- och integrations-testspecifikationer	R	R	HR	HR
Formell verifiering	---	---	R	R

HR = Starkt rekommenderad, R = Rekommenderad, --- = Ingen rekommendation för eller mot, NR = Ej rekommenderad

[43] IEC, 2010b, s. 35, förf. övers.

[44] IEC, 2010b, tabell A.5.

[45] IEC, 2010b, se exempelvis tabeller A.6 och A.8.

[46] Eng. black box testing

4.3 Fordonssäkerhet (ISO/IEC 26262)

Standarden ISO/IEC 26262 bygger på IEC 61508 och är en väletablerad standard för säkerhet i vägfordon. Standarden uttrycker tydligt att det finns behov av att ta fram olika typer av evidens för att stödja argumentationen för olika säkerhetsmål.[47] Bland annat kräver standarden att ett säkerhetsfall (eng. safety case) tas fram för att systematiskt argumentera för att ett säkert system har uppnåtts. [48] Säkerhetsmålen utgör högnivåkrav på säkerhet som i sin tur leder till funktionella säkerhetskrav som ska motverka oacceptabla risker. Metoden ger möjlighet till att aggregera olika evidens genom den argumentation som ska tas fram för att motivera att säkerhetsfallet har uppfyllts.

I standarden används begreppet ASIL (eng. automotive safety integrity level) för att bedöma risk för skador och därmed krav på säkerhet.[49] Begreppet är en specialisering av SIL (som definieras i IEC 61508). Standarden definierar fyra nivåer av ASIL, där A utgör den lägsta nivån av säkerhetskrav och D utgör den högsta nivån. Utifrån de olika ASIL-nivåerna rekommenderar standarden olika metoder som kan användas vid verifiering av exempelvis mjukvaruimplementation. Olika ASIL-nivåer har olika rekommendationer för vilka metoder som är lämpliga att använda.

4.3.1 Verifiering av mjukvarudesign i ISO/IEC 26262

ASIL-nivåerna i ISO/IEC 26262 ger implicit vilken nivå av assurans systemets olika säkerhetsåtgärder behöver uppvisa.

Vad evidensen ska påvisa i verifieringen av mjukvarudesignen är beskrivet på en hög nivå i standarden. Ett exempel på en aspekt som ska påvisas är att riktlinjer för mjukvarudesign har följts. Tabell 2 listar de metoder för verifiering av mjukvarudesign som tas upp i ISO/IEC 26262 samt för vilka ASIL-nivåer de rekommenderas.

[47] SIS, 2018a.

[48] SIS. 2018b. avsnitt 6.4.8.

[49] SIS, 2018a, avsnitt 3.6.

Tabell 2. Verifieringsmetoder för att verifiera mjukvarudesign i ISO/IEC 26262.

Metod	**ASIL-nivå**			
	A	B	C	D
Genomgång av design	++	+	o	o
Inspektion av design	+	++	++	++
Simulering av dynamiska beteenden i designen	+	+	+	++
Prototypgenerering	o	o	+	++
Formell verifiering	o	o	+	+
Kontrollflödesanalys	+	+	++	++
Dataflödesanalys	+	+	++	++
Schemaläggningsanalys	+	+	++	++

++ = Starkt rekommenderad, + = Rekommenderad, o = Ingen rekommendation för eller mot

4.3.2 Verifiering av mjukvara i ISO/IEC 26262

Likt den närbesläktade standarden ISO/IEC 61508 innehåller ISO/IEC 26262 rekommendationer för metoder för mjukvaruverifiering. ISO/IEC 26262 ger också vägledning i val av metoder och genomförandet av dem:

> *Design och implementation av mjukvarumodulerna verifieras genom att använda en lämplig kombination av verifieringsaktiviteter, t.ex. granskningar, analyser och testning.*[50]

Även om båda standarderna ger viss vägledning så går ISO/IEC 26262 längre samt är mer konkret i fråga om rekommendationer av metoder och vad den framtagna evidensen ska påvisa. Tabell 3 listar föreslagna metoder för mjukvaruverifiering i ISO/IEC 26262 samt för vilken ASIL-nivå som metoderna rekommenderas.[51]

[50] SIS, 2018b, s. 20, förf. övers.

[51] SIS, 2018c, tabell 7.

Tabell 3. Metoder för verifiering av mjukvara i ISO/IEC 26262.

Metod	ASIL-nivå			
	A	B	C	D
Genomgång	++	+	o	o
Parprogrammering	+	+	+	+
Inspektion	+	++	++	++
Semiformell verifiering	+	+	++	++
Formell verifiering	o	o	+	+
Kontrollflödesanalys	+	+	++	++
Dataflödesanalys	+	+	++	++
Statisk kodanalys	++	++	++	++
Statisk kodanalys baserad på abstrakt tolkning	+	+	+	+
Kravbaserad testning	++	++	++	++
Gränssnittstestning	++	++	++	++
Felinjiceringstestning	+	+	+	++
Utvärdering av resursanvändning	+	+	+	++
Jämförande tester mellan modell och kod (om applicerbart)	+	+	++	++

++ = Starkt rekommenderad, + = Rekommenderad, o = Ingen rekommendation för eller mot

4.4 Cybersäkerhet i vägfordon (ISO/SAE 21434)

ISO/SAE 21434 är en relativt ny standard som behandlar cybersäkerhet för vägfordon.[52] Analogt med ISO/IEC 26262 ställer ISO/SAE 21434 krav på att ett cybersäkerhetsfall (eng. cybersecurity case) ska tas fram för att systematiskt argumentera för säkerheten i systemet. Metoden ger möjlighet till att aggregera olika evidens genom den argumentation som ska tas fram för att motivera att cybersäkerhetsfallet har uppfyllts.

Standarden använder inte begreppet ASIL som i ISO/IEC 26262. I stället definierar standarden begreppet CAL (eng. cybersecurity assurance level) som används för att bedöma hur mycket konfidens som krävs för en komponent i systemet. Det finns fyra CAL-nivåer, CAL1 till CAL4, som bestäms utifrån hur

[52] ISO/SAE, 2021.

stor effekt en attack mot systemet kan få samt vilken attackvektor som attacken använder. Standarden listar också exempel på metoder för att verifiering av säkerhetsegenskaper men innehåller också en skalning för testmetoderna beroende på CAL.

4.4.1 Säkerhetstestning i ISO/SAE 21434

ISO/SAE 21434 innehåller exempel på metoder för säkerhetstestning. Standarden rekommenderar lämpliga metoder beroende på vilken nivå av säkerhet som krävs. Metoderna som tas upp i tabell 4 är relativt generella men ska genomföras med olika grad av noggrannhet beroende på önskad säkerhetsnivå.[53] Tabellen pekar på två så kallade testparameteruppsättningar som definierar hur omfattande testning som ska ske för respektive metod. Testparameteruppsättning 1 (T1) omfattar följande:

- Funktionell testning baserad på krav.
- Sårbarhetsscanning efter kända sårbarheter.
- Fuzztestning med slumpmässigt val av indata.
- Penetrationstestning baserat på att en attackerare har medelhög (eng. moderate) expertis, kännedom om komponent och/eller resurser.

Testparameteruppsättning 2 inkluderar följande:

- Funktionell testning baserad på krav och interaktioner mellan komponenter.
- Sårbarhetsscanning efter kända sårbarheter.
- Fuzztestning med ett ökat antal testfallsiterationer och/eller adaptivt val av indata.
- Penetrationstestning baserat på att en attackerare har hög expertis, kännedom om komponenten och/eller resurser.

Tabell 4. Metoder för säkerhetstestning i ISO/SAE 21434.

Aktivitet	**CAL-nivå**			
	CAL1	CAL2	CAL3	CAL4
Funktionell testning	T1	T1	T2	T2
Sårbarhetsscanning	T1	T1	T1	T1
Fuzztestning	-	T1	T2	T2
Penetrationstestning	-	-	T1	T2

[53] ISO/SAE, 2021, tabell E.4.

Andra testmetoder omnämns också i standarden men saknar resonemang baserat på CAL-nivå. Dessa metoder är:

- kravbaserad testning
- gränssnittstestning
- utvärdering av resursanvändning
- verifiering av kontrollflöden och dataflöden
- dynamisk analys
- statisk analys.

4.5 Testkrav på kryptomoduler (ISO/IEC 24759)

Standarden ISO/IEC 24759[54] ställer upp ett antal testkrav för kryptomoduler som utvecklats enligt kraven i standarden ISO/IEC 19790[55]. Standarden riktar sig i första hand till de testlaboratorier som anlitas för att verifiera att en framtagen produkt möter kraven. ISO/IEC 19790 och ISO/EIC 24759 utgör tillsammans grunden för den amerikanska standarden FIPS 140-3.[56]

ISO/IEC 24759 ställer många krav på vad leverantören ska beskriva och tillhandahålla samt vad den oberoende testaren ska genomföra för uppgifter. Några av de områden som ska täckas in är specifikationer, gränssnitt, roller, autentisering, mjukvarusäkerhet, operativ miljö, fysisk säkerhet, självtester samt skydd av kryptografiska parametrar.[57]

Kraven som ställs på tillverkaren innebär i många fall att någon form av evidens ska produceras för att testarna ska ha relevanta underlag att utgå ifrån. Evidens som omnämns inkluderar huvudsakligen olika former av dokumentation, såsom systemdokumentation; listor över säkerhetsrelevanta algoritmer och funktioner; resonemang över varför icke-säkerhetsfunktioner inte kan påverka säkerhets-relevanta delar; hårdvaruspecifikationer och hårdvarubeskrivningar; samt listor över vilka mjukvaror som ingår. Utöver granskning av tillverkarens evidens ska testaren även genomföra inspektioner och praktiska tester av det faktiska systemet vid verifieringen.

Standardens beskrivningar av testarens aktiviteter ligger generellt sett på en relativt hög nivå såsom exemplifieras i de två följande citaten.

[54] ISO/IEC, 2017.

[55] SIS, 2020a.

[56] NIST, 2019.

[57] ISO/IEC, 2017, avsnitt 6.

> *TE02.13.03: Testaren ska manipulera (t.ex. orsaka att komponenten inte fungerar som designat) de exkluderade komponenterna på ett sådant sätt att det orsakar felaktig funktion hos den exkluderade komponenten. Testaren ska verifiera att den felaktiga funktionen hos den exkluderade komponenten inte interfererar med modulens säkerhetsgodkända funktion.*[58]

> *TE03.09.02: Om gränssnittet för styrutgångar är specificerat [i leverantörens dokumentation. övers. anm.], ska testaren verifiera, genom inspektion, att gränssnittet för styrutgångar fungerar som specificerats.*[59]

Generellt sett så föreskriver inte standarden hur testaren verifierar de olika egenskaperna, utan bara att de ska verifieras. Därtill föreskrivs inte till vilken visshetsgrad som verifieringen ska säkerställa att kraven uppfyllts.

4.6 Common criteria (ISO/IEC 15408)

ISO/IEC 15408, mest känd som Common criteria är en standard framtagen för att kunna ge internationellt erkända certifikat för en produkts säkerhetsegenskaper.[60] Common criteria bygger på en uppsättning säkerhetskrav som ställs genom dokumenten *protection profile* och *security target*. Protection profile kan tas fram för en enskild produkt, men det finns även generella protection profiles för vissa produktkategorier. Security target är alltid produktspecifik. Kravnivån bestäms delvis genom vilken av sju definierade *evaluation assurance levels* (EAL) som produkten ska möta enligt dessa dokument. Standardens definitioner av EAL ger en basnivå som kan utökas med tilläggskrav i protection profile och security target för att hantera det specifika systemets förutsättningar.[61]

Common criteria bygger på en kombination av dokumentation, tester och oberoende granskningar som evidens för uppfyllnad av säkerhetskraven. Standarden pekar egentligen inte ut några obligatoriska evidensartefakter men tar ändå upp ett antal olika aktiviteter som bidrar till assuransen, såsom process-granskningar, överensstämmelse mellan dokumentation och implementation, verifiering av tester, penetrationstester, oberoende funktionella tester och sårbarhetsanalyser.[62]

---

[58] ISO/IEC, 2017, s. 7, författarnas översättning.

[59] ISO/IEC, 2017, s. 25, författarnas översättning.

[60] Common Criteria, 2022a, och ISO/IEC, 2022.

[61] Common Criteria, 2022c, avsnitt 4.

[62] Common Criteria, 2022b, part 3, s. 22.

4.7 Krav på IT-säkerhetsförmågor

Krav på IT-säkerhetsförmågor hos IT-system (KSF) är en samling krav som tagits fram av Försvarsmakten.[63] Kraven består av både funktionella krav samt assuranskrav. KSF ställer inga krav på hur evidensen för ett systems säkerhets-egenskaper ska vara strukturerad men beskriver att syftet med assuranskraven är att få förtroende för systemets säkerhetsegenskaper genom att försäkra sig om:

- *förtroende för systemutvecklaren och dennes utvecklingsprocesser,*
- *förtroende för arkitekturen, designen och implementation av säkerhetsfunktionerna,*
- *förtroende för att drift- och förvaltningsdokumentation är korrekt och fullständig,*
- *genom sårbarhetsanalys och riskanalys påvisa att systemet, för den tänkta användningen, har tillräckliga IT-säkerhetsförmågor.*[64]

KSF är tydlig med att de beskrivna kraven inte ska tolkas som en fullständig kravbild för ett systems säkerhet utan andra krav kan tillkomma, till exempel från verksamhetsanalyser.

Eftersom det tillkommer assuranskrav på högre säkerhetsnivåer går det att dra slutsatsen att evidens kopplat till de kraven bidrar till ett högre värde av assurans. KSF innehåller dock ingen explicit vägledning om hur evidens kan aggregeras eller värderas.

4.8 ISD-processen

Informationssäkerhetsdeklaration (ISD) är en stödprocess som används av FMV när IT-system tas fram eller vidmakthålls.[65] Ett av syftena med processen är att, ur flera olika perspektiv, kontinuerligt bedöma realiserbarheten för ett system. Ett av perspektiven som bedöms är ackrediterbarhet, vilket syftar till att säkerställa att systemet uppfyller kraven från KSF.

Ett antal artefakter produceras under ISD-processens olika faser, varav många innehåller analyser och bedömningar av olika underlag. ISD-processen gör det tydligt att dokumentationen ska påvisa hur säkerhetsmålen uppnås samt att det ska genomföras granskning och tester för att bekräfta detta, men ger endast begränsad vägledning om hur dessa aktiviteter kan genomföras.[66]

---

[63] Försvarsmakten, 2014.

[64] Försvarsmakten, 2014, underbilaga 1:4, s. 3.

[65] FMV, 2021a.

[66] FMV, 2021a, avsnitt 5.3 och 5.4 samt FMV, 2021b, avsnitt 3.

5 Diskussion

Otydligheterna och spretigheten i hur tilltro mäts (eller inte mäts) vid utvärdering av IT-systemens säkerhetsegenskaper visar tydligt att assurans är ett svår-definierat koncept. Krav och förväntningar i standarder och metoder är ofta vaga och lämnar stor tolkningsmån avseende vad systemen ska uppfylla och hur detta ska påvisas. Gemensamt för de exempel på standarder och metoder som tas upp i kapitel 4 är att de rekommenderar framtagning av ökande mängder evidens när högre nivåer av assurans eller riskreduktion eftersträvas. Däremot beskriver inte standarderna och metoderna hur evidensen ska tas fram, värderas eller aggregeras för att bli rättvisande, utan detta lämnas i stora delar till utvecklare och utvärderare att bestämma och bedöma.

Trots tolkningsmån och otydligheter är evidens för säkerhetsegenskaper en viktig pusselbit i bevisföringen för att påvisa att systemets säkerhetsmål är uppfyllda. Samtidigt är den tekniska komplexiteten i IT-systemen så pass hög i alla praktiskt tänkbara system att en absolut bevisföring inte är möjlig. Detta innebär att bevisföringen i praktiken blir baserad till stor del på indicium som stödjs av fragmentariska faktum med omfattande evidensmässiga hål mellan dem. Evidens och bevisföring kring uppfyllnad av säkerhetsmålen blir därmed till stor del en fråga om att prioritera vilka evidensartefakter som bör tas fram i det specifika fallet för att kunna bedöma säkerhetsegenskaperna för helheten – inklusive egenskaperna hos delar där evidens saknas. Syftet med evidensen bör därmed vara att ge en så pass bra bild av systemets säkerhet att helheten kan bedömas utifrån målet att sammantaget lämna tillräckligt låg kvarstående risk.

5.1 Assurans är komplext

Utveckling av IT-system är i många fall en utmanande verksamhet, med lång utvecklingstid, kravändringar, ändringar i omvärlden, oförutsedd komplexitet och integrationssvårigheter. Med Snowden och Boones terminologi kan det uttryckas som att utvecklingen är ett *komplext* problem.[67] Ett komplext problem kännetecknas av att det förvisso finns en lösning men att den inte kan fastslås i förväg då alltför många parametrar är okända eller kan ändras under tidens gång.

I många fall blir även assuransen ett komplext problem. Dels för att utvecklingen i sig är komplex och att slutprodukten i princip är ett rörligt mål, dels för att assurans bland annat bygger på ett stort antal svårförutsedda, svårkontrollerade och externa faktorer.[68]

[67] Snowden & Boone, 2007.

[68] Se även resonemanget i Mohamad m.fl., 2024, avsnitt 5.4.

Vissa delar av det som i slutändan bidrar till assurans går inte att mäta på ett konkret och strukturerat sätt, såsom förtroendet för en leverantör eller hur väl en process understödjer säkerhetsarbetet. Evidensen utgör i många avseenden ett mer konkret underlag för assurans, även när den gäller abstrakta företeelser såsom processer, vilket innebär att evidensen i högre grad bör gå att hantera med konkreta och strukturerade metoder. Rätt hanterad bör evidens därför kunna förenkla det komplexa problemet med assurans.

5.2 Evidens är komplicerat

Användning av evidens har stöd i flera befintliga standarder och processer, framför allt inom området funktionell säkerhet. Även om evidens omnämns relativt frekvent i dessa standarder och processer (om än ibland med andra termer) så är detaljerna oklara kring vad evidens är och hur den ska hanteras i säkerhetsarbetet. Beskrivningarna i kapitel 4 visar att det redan efterfrågas evidens i de standarder och processer som appliceras i utvecklingen av säkerhetskritiska system. Standarderna tar även till viss del upp vilken typ av evidens som är lämpligast i olika situationer. Dock är den efterfrågade evidensen ofta vagt definierad och endast knapphändigt beskriven om hur den ska tas fram och värderas.

Begreppet evidens omfattar många olika aspekter, bland annat enskilda evidens-artefakter (i form av exempelvis kodanalyser, testrapporter och process-beskrivningar) samt de metoder som används för att ta fram, värdera och aggregera evidens. I många fall går det även att ta fram olika evidens för samma aspekt, till exempel kan både testfall och kodgranskning användas som evidens för kodens korrekthet.

För att bestämma vilka evidensartefakter som är lämpliga att producera bör hänsyn inte bara tas till vilka artefakter som går att ta fram utan även till hur de ska användas i bevisföringen. Faktorer i användningen är exempelvis vilket evidensvärde som respektive artefakt tillför till helheten, hur artefakterna går att använda vid aggregeringen och hur artefakterna relaterar till varandra. Om evidensartefakterna endast betraktas enskilt finns risken att tid och energi läggs på att ta fram flera artefakter som vardera har högt enskilt evidensvärde men som endast tillför marginellt bidrag till helheten. Det kan exempelvis vara så att evidensen rör samma delegenskap eller har stort överlapp i vad som mäts. Överlapp av denna typ ger förvisso större tilltro till den enskilda delegenskapen men ger endast begränsat bidrag till tilltron för säkerheten som helhet.

Följande underavsnitt diskuterar olika perspektiv på evidens och användningen av evidens i bevisföringen.

5.2.1 (O)definierad evidens

Standarderna och metoderna beskriver generellt sett de olika evidensmetoderna på mycket översiktlig nivå. Som exempel på detta tar ISO 26262 upp statisk kodanalys som en lämplig teknik för mjukvaruverifiering, dock endast med en kortfattad och generell beskrivning av vad statisk kodanalys innebär:

> *Statiska analyser är en samlingsterm som inkluderar analyser såsom sökningar i källkoden eller modellen efter mönster som matchar kända fel eller överensstämmelse med modellerings- eller kodningsguider.*[69]

Avsaknaden av förtydliganden betyder att det finns stort tolkningsutrymme – statisk kodanalys kan i princip vara allt från enklare textsökningar till avancerade formella metoder.

5.2.2 Explicit evidens och implicit tilltro

Många evidensmetoder undersöker en relativt liten del av systemet åt gången och producerar därmed relativt smal täckning i varje artefakt. Exempelvis påvisar ett testfall i princip bara egenskaperna hos just det som testas, en kodgranskning bara de egenskaper som undersöks i den kod som faktiskt granskas och en processgranskning bara att just den granskade processen är sund. Testfallet ger egentligen inga fakta om egenskaper som inte testas, kodgranskningen visar inget om den kod som inte granskats och processgranskningen visar inget om andra processer eller ens om processen faktiskt används. Den explicita evidens som dessa metoder ger per undersökt egenskap blir därmed ganska smal även i de fall där det finns omfattande evidens.

Effekten av att evidensartefakterna tenderar att vara smala i sitt täckningsområde är att många egenskaper och detaljer i systemet sannolikt inte täcks in av evidensen. Bedömningen av säkerhetsnivån hos de egenskaper i systemet som saknar säkerhetsevidens kommer därmed att bygga på en implicit tilltro; i princip en känsla av systemets kvalitet och leverantörens eller utvecklarnas tillförlitlighet. Den explicita evidensen ger en fingervisning om den övergripande kvaliteten i systemet och i hur systemet utvecklats. I fall där utvecklingen sköts bra och där säkerhetsegenskaperna hanteras väl skapar explicit evidens även tilltro.

5.2.3 Positiv och negativ evidens

Avsikten med huvuddelen av den evidens som tas fram i ett projekt är rimligen att påvisa att ett säkerhetspåstående är uppfyllt. Viss evidens kan dock motsäga ett eller flera säkerhetspåståenden för systemet. Sådan negativ evidens

[69] SIS 2018c, tabell 7, not d.

(motevidens) kan exempelvis bestå av upptäckta sårbarheter eller indikationer på att arbetsmetoder och processer inte är lämpliga för utveckling av säkra system.

Styrkan hos motevidens kan variera stort, från svaga indikationer på att systemet kan ha brister till flagranta övertramp i säkerhetsarbetet. Ett exempel på det senare kan vara konkreta och tydliga bevis på en bakdörr i ett signalskydds-system vilket rimligtvis innebär att säkerheten är att betrakta som mycket låg. Upptäckt av negativ evidens för ett driftsatt system kan innebära väldigt olika konsekvenser som potentiellt blir mycket påfrestande att hantera.

Samtidigt utgör negativ evidens bara en del i bedömningen av ett säkerhets-påstående. Förekomst av svag evidens för att ett system är osäkert kan mycket väl accepteras i den sammantagna bedömningen om den positiva evidensen överväger.

5.2.4 Evidens kräver struktur

Enskilda evidensartefakter, såsom ett testresultat eller en processgranskning, blir svåra att använda på systemnivå om det saknas en struktur att placera in evidensen i. Några av de perspektiv som spelar in är vilka säkerhetsegenskaper evidensen relaterar till, vilka delar av systemet eller arbetet som evidensen täcker samt hur evidensen relaterar till annan evidens för samma säkerhetsegenskaper. En ytterligare aspekt är att många säkerhetsrelaterade artefakter som redan tas fram kan vara användbara som evidens, men används inte på det sättet idag och hanteras därmed inte som evidens.[70] Exempel på sådana artefakter kan vara motiveringar för designbeslut samt dokumentation av utbildningsinsatser för utvecklarna.

Det behövs även ett strukturerat arbete för att ta fram lämplig evidens. Genom att identifiera och ta fram relevanta säkerhetsegenskaper på ett strukturerat sätt, inklusive nedbrytning till allt mer avgränsade delegenskaper, går det att hitta en struktur som evidensen kan placeras in i. Strukturerat arbete är en av grunderna i flera av standarderna, såsom i ISO 27000[71], ISO 26262[72] och Common criteria[73]. Det strukturerade arbetet behöver också upprätthållas genom systemets hela livscykel för att kopplingen mellan system, evidens och tilltro inte ska förloras på vägen. Definierade processer och metoder underlättar arbetet med att ta fram evidensartefakter och att aggregera dem. Väldefinierade arbetssätt innebär att artefakterna produceras på ett konsekvent sätt och att tilltron till artefakternas värde kan förankras genom etablerade metoder.

[70] Se även Mohamad m.fl., 2024, s. 11.

[71] SIS, 2020b.

[72] SIS, 2018a.

[73] Common Criteria, 2022a.

5.2.5 Evidens kräver organisation

Produktion, hantering, aggregering och värdering av evidens är några av de aktiviteter som krävs för att nå en sammanhängande bevisföring för systemens säkerhetsnivå. Sammantaget kan detta bli ett mycket omfattande och komplext arbete vilket kräver både organisation och processer som är anpassade för ändamålet. Rutinerna kring evidens och bevisföring bör rimligen utformas för att passa förutsättningarna, såsom systemens komplexitet, organisationens storlek och nivån på säkerhetsbehoven.

I en undersökning konstaterade Mohamad m.fl. att många roller kan bli involverade under evidensarbetets gång, inkluderande utvecklare, produktägare, riskägare, säkerhetsexperter, granskare och chefer, vilket även ställer krav på organisationens utformning.[74]

5.3 Aggregering och tillräcklighet

Som framgår i denna rapport är evidens ett komplicerat område där det finns många oklarheter kring såväl framtagning som värdering och aggregering. I det generella fallet kommer evidens knappast att gå att värdera och väga samman på absoluta skalor som objektivt mäter hur väl ett säkerhetsbehov är uppfyllt. Trots detta kommer rimligt värderingsbar evidens i många fall behöva tas fram med så konkreta evidensmetoder som möjligt, där metoderna inkluderar definierade mål, avgränsningar och kriterier.

Bevisföringen för säkerhetsegenskaperna kommer att behöva ta hänsyn till många olika faktorer, såsom säkerhetsbehovens betydelser, evidensens aggregerade värde, evidensens täckningsgrad och vilken evidens som saknas. Evidensens tillräcklighet i bevisföringen blir därmed en bedömningsfråga där någon i slutändan måste ta ett informerat beslut om systemet kan anses tillräckligt bra för att användas. På grund av frågeställningens komplexitet och den mångfald av evidens som kommer användas i de flesta fall blir beslutsfattarens kompetens, kunskap och erfarenhet viktiga förutsättningar.

Värt att notera är att uppfylla standarderna inte utgör någon garanti för att mjukvaran är fri från sårbarheter. Exempelvis tar Halder m fl. upp flera tillfällen då biltillverkare återkallat fordon på grund av allvarliga brister i mjukvaran trots att fordonen utvecklats enligt gällande standarder.[75] Dessa brister kunde exempelvis orsaka att airbags inte löste ut eller att en hackare kunde ta över delar av fordonens datorsystem. Det är viktigt att ha med sig att systemens komplexitet i realiteten gör absolut säkerhet ouppnåelig varför säkerhetsarbetet måste vara en kontinuerlig process. Väl genomförd bevisföring har möjlighet att inte bara göra

[74] Mohmad m.fl., 2024, avsnitt 4.3 och 5.2.

[75] Halder m.fl., 2020.

ackrediterings- och certifieringsprocesserna mer förutsägbara vid ett första godkännande utan även underlätta det kontinuerliga arbetet och framtida uppdateringar av systemet. Bra bevisföring underlättar även formella godkännanden av ett IT-system, exempelvis enligt bestämmelserna 3 kap, 3 § säkerhetsskyddsförordningen (2021:955), och kan ge större konfidens i beslutsskedet.

5.4 Forskningsbehov

Utifrån den information som sammanställts i föregående kapitel och avsnitt så framträder ett omfattande forskningsbehov relaterat till evidens och utveckling av säkra IT-system. Vissa frågeställningar är mer grundläggande inom området, såsom förståelse för svårigheterna med mjukvaruutveckling, medan andra är mer tekniskt orienterade, såsom specifika evidensmetoder.

Det finns ett tydligt behov av förbättrat metodstöd vid värdering, aggregering och tillräcklighetsbedömningar av evidens. Befintliga processer och standarder ger ett visst stöd men inte tillräckligt i termer av att konkret definiera vad för evidens som krävs och hur man bör resonera kring den. För att gå vidare med de frågorna behövs också mer forskning kring vilka metoder som bidrar med högst evidensvärde. Därtill behövs förbättrade processer som ger stöd i evidensvärdering, aggregering och bedömning av tillräcklighet för att effektivare kunna nyttja evidensmetoderna vid utveckling och underhåll.

Några av de områden som behöver fortsatt forskning är:

- Metoder för att definiera säkerhetsmål och säkerhetsegenskaper
- Metoder för nedbrytning och spårbarhet för säkerhetsegenskaper
- Metoder för att ta fram evidensartefakter
- Metoder för att bedöma tillförlitlighet i leverantörskedjor
- Metoder för värdering och aggregering av evidens
- Metoder för att definiera kriterier för tillräcklighet.

Det är också viktigt att omsätta forskningsresultat om evidens, tillförlitlighet och assurans till en praktisk kontext. Säkerhetskritiska system kommer även fortsättningsvis produceras av organisationer som har begränsad tillgång till personal och resurser samtidigt som de ska möta snäva leveransdatum.

6 Slutsatser

Säkerhetsevidens är ett samlingsnamn för olika typer av artefakter som påvisar en säkerhetsegenskap i systemet. Säkerhetsevidens kan vara av många olika slag, såsom resultat från kodgranskningar, testrapporter, resultat från processgranskningar och revisioner hos leverantörer.

Säkerhetsevidensen bidrar till en förståelse av och tilltro till systemets säkerhetsegenskaper och därmed till hur väl systemet uppfyller sina säkerhetsmål. För att kunna bedöma om säkerhetsmålen är tillräckligt väl hanterade krävs värdering, aggregering och tillräcklighetsbedömning av den säkerhetsevidens som producerats. Kvaliteten hos den sammantagna bedömningen av evidensens tillräcklighet är kritisk för att kunna ta väl avvägda och informerade beslut kring systemets lämplighet för användning.

Befintliga standarder, processer och metoder är generellt sett relativt otydliga kring de metoder som de rekommenderar. De tar upp ett brett spektrum av spårbara evidensmetoder och arbetssätt som ger evidens, såsom design-genomgångar, processgranskningar, flödesanalyser, formella verifieringar, kodgranskningar, statiska kodanalyser, dynamiska kodanalyser samt många olika former av testning. Samtidigt är beskrivningarna knapphändiga vad gäller vad respektive evidensmetod innebär, vilket lämnar stor tolkningsmån till de som implementerar evidensmetoderna.

Denna studie visar på att dagens processer och standarder till stor del saknar resonemang om hur värdering, aggregering och bedömning av tillräcklighet ska gå till. Utan vägledning inom dessa områden blir det svårare att genomföra en objektiv bevisföring och att bedöma om systemets säkerhet är tillräcklig, även om kraven från en specifik standard uppfylls. Evidens som tas fram behöver ha en tydlig koppling till ett systems säkerhetsmål. Kontextlös evidens riskerar annars att bli bortkastat arbete eller en onödig pålaga som i värsta fall kan skapa felaktig konfidens i ett system.

Referenser

ACWG (2021). *Goal Structuring Notation Community Standard Version 3*. SCSC-141C. The Assurance Case Working Group (ACWG). https://scsc.uk/r141C:1?t=1

Ayoub, A., Chang, J., Sokolsky, O. & Lee, I. (2013). Assessing the Overall Sufficiency of Safety Arguments. *Proceedings of the Twenty-first Safety-Critical Systems Symposium (SSS'13)*, 127–144. February 2013.

Bildsten, C., Eidenskog, D., Hermelin, J. & Löfvenberg, J. (2018). *RASK – Ramverk för IT-säkerhetskravställning*. FOI-R--4641--SE. Totalförsvarets forskningsinstitut.

Cyra, L. & Górski, J. (2011). Support for argument structures review and assessment. *Reliability Engineering and System Safety*, 96, s. 26–37. https://doi.org/10.1016/j.ress.2010.06.027

Common Criteria (2022a). *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, November 2022, CC:2022 Revision 1, CCMB-2022-11-001. https://commoncriteriaportal.org/cc/index.cfm

Common Criteria (2022b). *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components*, November 2022, CC:2022 Revision 1, CCMB-2022-11-003. https://commoncriteriaportal.org/cc/index.cfm

Common Criteria (2022c). *Common Criteria for Information Technology Security Evaluation – Part 5: Pre-defined packages of security requirements*, November 2022, CC:2022 Revision 1, CCMB-2022-11-005. https://commoncriteriaportal.org/cc/index.cfm

Duan, L., Rayadurgam, S., Heimdahl, M. P. E., Ayoub, A., Sokolsky, O. & Lee, I. (2017). Reasoning About Confidence and Uncertainty in Assurance Cases: A Survey. I: Huhn, M., Williams, L. (red) Software Engineering in Health Care, *Lecture Notes in Computer Science*, 9062. Springer. https://doi.org/10.1007/978-3-319-63194-3_5

FMV (2021a). *ISD 3.1 Processbeskrivning.* 20FMV5903-1:1, ver. 3.1.0. Försvarets materielverk. https://isd.fmv.se/ISD%2031%20dokument/20FMV5903-1_1_ISD_3.1_Processbeskrivning.pdf

FMV (2021b). *ISE Granskningsinstruktion, ISD 3.1*. Underbilaga 2 till ISD-processen 3.1. 20FMV5903-1:1.2, ver. 3.1.0. Försvarets materielverk. https://isd.fmv.se/ISD%2031%20dokument/20FMV5903-1_1.2%20-%20ISD_3.1_ISE_Granskningsinstruktion_ver_1.1.pdf

Försvarsmakten (2014). *KSF – Krav på IT-säkerhetsförmågor hos IT-system*, v3.1. Försvarsmakten.

Försvarsmakten (2017). *Handbok Säkerhetstjänst Informationssäkerhet (H Säk Infosäk 2013)*, ändring 2. Försvarsmakten.

Grigorova, S. & Maibaum, T. S. E. (2013). Taking a page from the law books: Considering evidence weight in evaluating assurance case confidence, *IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, s. 387–390, https://doi.org/10.1109/ISSREW.2013.6688926

Halder, S., Ghosal, A. & Conti, M. (2020). Secure over-the-air software updates in connected vehicles: A survey. *Computer Networks*, 178, nov 2020. https://doi.org/10.1016/j.comnet.2020.107343

Hawkins, R., Kelly, T., Knight, J. & Graydon, P. (2011). A New Approach to Creating Clear Safety Arguments. I: Dale, C., Anderson, T. (red) *Advances in Systems Safety*. Springer. https://doi.org/10.1007/978-0-85729-133-2_1

Idmessaoud, Y., Dubois, D. & Guiochet, J. (2022). A Qualitative Counterpart of Belief Functions with Application to Uncertainty Propagation in Safety Cases. I: Le Hégarat-Mascle, S., Bloch, I., Aldea, E. (red) Belief Functions: Theory and Applications. BELIEF 2022. *Lecture Notes in Computer Science*, 13506. Springer. https://doi.org/10.1007/978-3-031-17801-6_22

IEC (2010a). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*. IEC Standard 61508-1. International Electrotechnical Commission.

IEC (2010b). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*. IEC Standard 61508-3. International Electrotechnical Commission.

IEC (2017). *Application of risk management for it-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities*. Technical Report. IEC TR 80001-2-9. International Electrotechnical Commission.

ISO/IEC (2017). *Information technology – Security techniques – Test requirements for cryptographic modules*. ISO/IEC Standard 24759, third ed., 2017-03. International Organization for Standardization och International Electrotechnical Commission.

ISO/IEC (2022). *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model.* ISO/IEC Standard 15408-1:2022. International Organization for Standardization och International Electrotechnical Commission.

ISO/IEC/IEEE (2019). *Systems and software engineering – Systems and software assurance, Part 1: Concepts and vocabulary*. ISO/IEC/IEEE Standard 15026-1. International Organization for Standardization, International Electrotechnical Commission och Institute of Electrical and Electronics Engineers.

ISO/SAE (2021). *Road vehicles – Cybersecurity engineering.* ISO/SAE Standard 21434:2021. International Organization for Standardization och SAE International.

Karlzén, H., Eidenskog, D. & Löfvenberg, J. (2017). *Erfarenheter från utveckling och förvaltning av IT-system*. FOI-R--4423--SE. Totalförsvarets forskningsinstitut.

Li, J., Mao, B., Liang, Z., Zhang, Z., Lin, Q. & Yao X. (2021). Trust and Trustworthiness: What They Are and How to Achieve Them, *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 711–717. https://doi.org/10.1109/PerComWorkshops51409.2021.9430929

Mohamad, M., Steghöfer, J-P., Knauss, E. & Scandariato, R. (2024). Managing security evidence in safety-critical organizations. *The Journal of Systems & Software*, 214. https://doi.org/10.1016/j.jss.2024.112082

Nair, S., de la Vara, J. L., Sabetzadeh, M. & Briand, L. (2014). An extended systematic literature review on provision of evidence for safety certification. *Information and Software Technology*, 56(7). https://doi.org/10.1016/j.infsof.2014.03.001

NCSC (2024). *Cyber Assessment Framework V3.2*. The National Cyber Security Centre (NCSC). https://www.ncsc.gov.uk/information/cyber-assessment-framework--caf--changelog

NIST (2019). *Security Requirements for Cryptographic Modules*. FIPS 140-3. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.FIPS.140-3

NIST (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.CSWP.29

Nordström, J., Wikström, M., Nilsson, S., Olsén, M. & Bildsten, C. (2020). *Effektivare anskaffning och integration av ledningsstödsystem – Förhållningssätt för att lösa komplexa problem*. FOI-R--5063--SE. Totalförsvarets forskningsinstitut.

Office for Nuclear Regulation (2020, januari). *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 1. Office for Nuclear Regulation.

Rempel, P. & Mäder, P. (2017). Preventing Defects: The Impact of Requirements Traceability Completeness on Software Quality. *IEEE Transactions on Software Engineering*, 43(8), 777–797. https://doi.org/10.1109/TSE.2016.2622264

Ross, R., Winstead, M. & McEvilley, M. (2022). *Engineering Trustworthy Secure Systems*. NIST Special Publication 800-160, vol. 1, rev. 1. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-160v1r1

Schwierz, A. & Forsberg, H. (2018). Assurance Case to Structure COTS Hardware Component Assurance for Safety-Critical Avionics. *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC).* https://doi.org/10.1109/DASC.2018.8569774

SIS (2018a). *Vägfordon – Funktionssäkerhet i el- och elektroniksystem – Del 1: Terminologi*. SS-ISO 26262-1:2018.

SIS (2018b). *Vägfordon – Funktionssäkerhet i el- och elektroniksystem – Del 2: Ledning och hantering av funktionssäkerhet*. SS-ISO 26262-2:2018

SIS (2018c). *Vägfordon – Funktionssäkerhet i el- och elektroniksystem – Del 6: Produktutveckling på mjukvarunivå*. SS-ISO 26262-6:2018.

SIS (2020a). *Informationsteknik – Säkerhetstekniker – Säkerhetskrav för kryptomoduler*. SS-EN ISO/IEC 19790:2020.

SIS (2020b). *Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi (ISO/IEC 27000:2018)*. SS-EN ISO/IEC 27000:2020.

Snowden, D. J. & Boone, M. E. (2007, nov). A Leader's Framework for Decision Making. *Harvard Business Review*. https://hbr.org/2007/11/a-leaders-framework-for-decision-making

Vestlund, C., Nilsson, S., Karlzén, H. & Eidenskog, D. (2024). *IT-säkerhet fram till frontlinjen – Utvecklingsprocesser för IT-system i Försvarsmakten.* FOI-R--5598--SE. Totalförsvarets forskningsinstitut.

FOI

ISSN 1650-1942

www.foi.se