

IVA | Svenska framtider

Säkerhetskritisk mjukvara

En teknikrapport inom Svenska framtider om mjukvara för kritiska fysiska system

Innehåll

Förord 4

Sammanfattning 6

English Summary 8

Utgångspunkter i arbetet med mjukvara för kritiska fysiska system 10

- Definition och avgränsningar 11
- Motivering till att IVA prioriterat en teknikrapport inom mjukvara för kritiska fysiska system 13

Nulägesbeskrivning av mjukvara för kritiska fysiska system 14

- Mjukvara som styr den fysiska världen 15
- Mjukvara för kritiska fysiska system styrs av flera regelverk 18
- Internationell utblick 20

Utveckling inom mjukvara för kritiska fysiska system 24

Nyckelfrågor för mjukvara för kritiska fysiska system 27

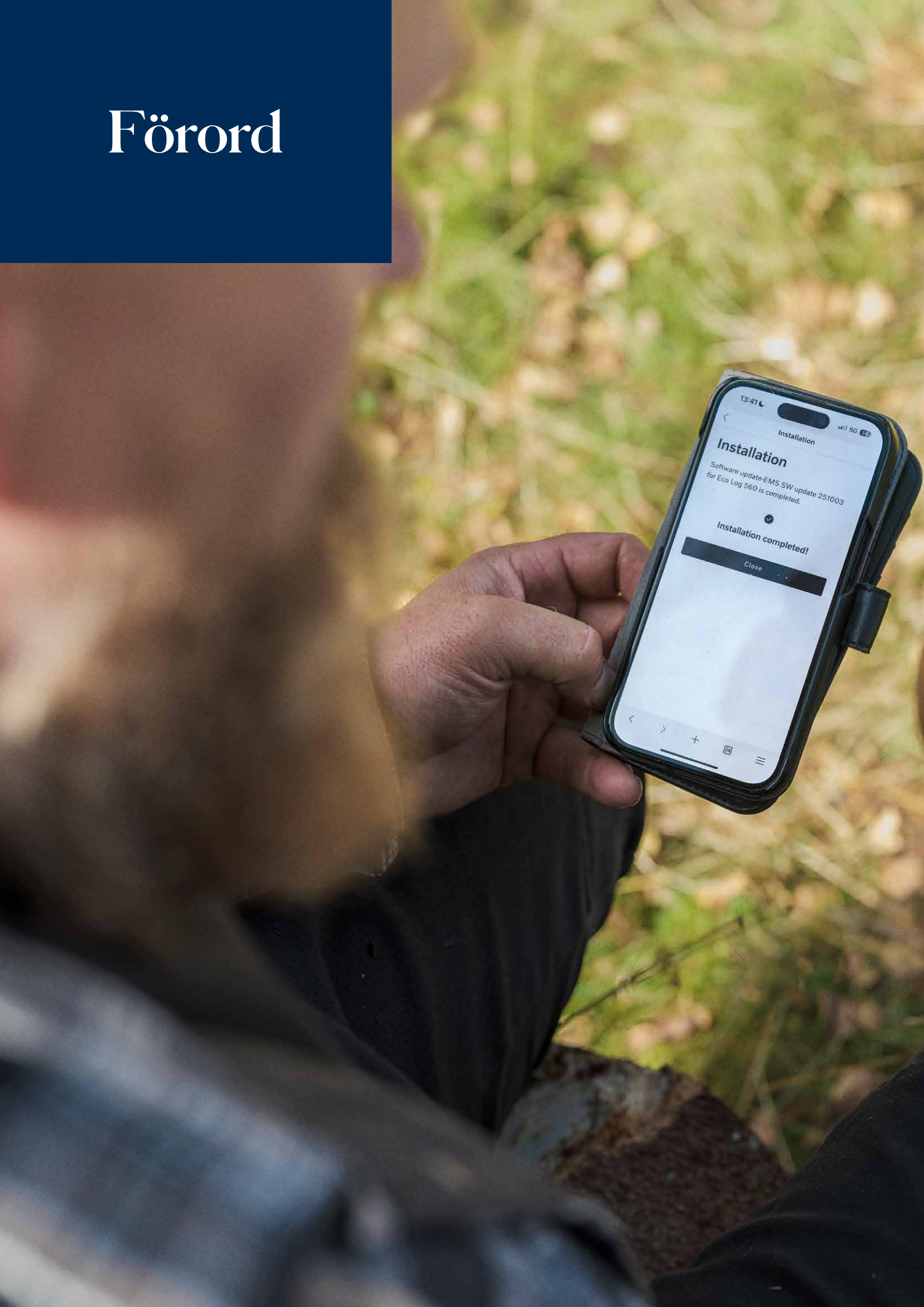
Önskad framtida riktning 33

- Målbild 34
- Fem förslag för utveckling av mjukvara för kritiska fysiska system i Sverige 36
- Rekommendationer 51

Appendix 52

- Referenser 53
- Ordlista 56

Förord


13:41
5G
Installation
Installation
Software update-EMS SW update 251003 for Eco Log 560 is completed.
Installation completed!
Close

IVA driver projektet *Svenska framtider* med syftet att formulera en vision för Sverige som ledande inom teknik och innovation år 2035. *Svenska framtider* samlar aktörer från akademi, näringsliv och offentlig sektor för att identifiera möjligheter, utmaningar och strategiska riktningar för framtida konkurrenskraft och hållbar utveckling. Arbetet startades hösten 2025.

Projektet omfattar bland annat arbetsgrupper som snabbt och målinriktat analyserar utmaningar och möjligheter inom olika teknikområden. Grupperna tar fram teknikrapporter med tydligt fokus på respektive område. Rapporterna ger en överblick över nuläge och framtidsutsikter inom området och innehåller konkreta förslag till åtgärder. De fungerar också som viktiga underlag för att forma en övergripande vision för Sverige år 2035.

Denna arbetsgrupp har fokuserat på mjukvara för kritiska fysiska system. Gruppens analys visar att det finns problem men också möjligheter där Sverige kan stärka konkurrenskraften genom att omsätta industriell styrka och teknisk spets i säkra och skalbara lösningar för en växande marknad.

Som i alla IVA-projekt har deltagarna medverkat i sin personliga kapacitet och inte som företrädare för de organisationer där de är verksamma. Rapportens analyser och förslag bygger i stor utsträckning på diskussioner inom arbetsgruppen samt på erfarenheter och den kunskap som dess medlemmar bidragit med. Arbetsgruppen står bakom rapporten i sin helhet, men det innebär inte att samtliga medlemmar nödvändigtvis står bakom varje enskild formulering.

Arbetsgruppen inom mjukvara för kritiska fysiska system har arbetat under april till oktober 2026.

Arbetsgrupp

Ödgärd Andersson (ordförande), Zenseact
David Broman, Kungliga Tekniska högskolan
Said Chahin, Volvo Cars
Ivan Cronie, Volvo Group
Björn Ekelund, Ericsson
Daniel Fäldt, Saab AB
Fredrik Hedenfalk, ABB Robotics
Karl Henrik Johansson, Kungliga Tekniska högskolan
Mathias Larsson Carlander, Traton Group
Anders Mattsson, Husqvarna Group
Olof Sundin, Saab AB
Taraneh Vosough Westerberg, Zenseact

Stöd till arbetsgruppen

Lisa Thelin, projektledare
Charlotte Hall, skribent

Sammanfattning



Mjukvara får en allt större betydelse i produkter som fordon, robotar och industrimaskiner. När mjukvaran styr funktioner som påverkar den fysiska omgivningen kan fel få allvarliga konsekvenser för människor, miljö eller samhällsviktiga funktioner. Det ställer höga krav på säkerhet, tillförlitlighet och möjligheten att testa och kontrollera produkterna under hela deras livslängd. AI förändrar också hur mjukvara och produkter utvecklas. AI kan både användas för att utveckla mjukvara och bli en del av själva produkten. Det kan öka utvecklingstakten, men ställer också nya krav på kompetens, arbetssätt och kontroll. Givet den snabba utvecklingen behöver kompetensen utvecklas i takt med tekniken. När AI tar över delar av det traditionella programmeringsarbetet blir förståelsen för produkter, system och arkitektur allt viktigare.

Förutsättningarna förändras också när handel, teknik och leverantörskedjor blir mer regionala och i högre grad påverkas av säkerhetspolitiska och geopolitiska hänsyn. Tillgången till exempelvis komponenter, data, beräkningskraft och digital infrastruktur kan påverkas av var teknik utvecklas och används. Svenska företag behöver därför kunna hantera olika marknader och regelverk och minska sårbarheten i strategiskt viktiga beroenden. Förändringen innebär också möjligheter att stärka Sveriges och Europas förmåga inom områden där säkerhet och tillförlitlighet blir viktigare.

När produkter går från att främst vara hårdvarudefinierade till att i allt högre grad styras och utvecklas genom mjukvara förändras också företagens arbetssätt. Utvecklingen behöver ske i kortare cykler, med möjlighet att prova nya lösningar och få återkoppling tidigt. Svenska företag behöver kunna fatta beslut och utveckla nya lösningar snabbare, även när all information inte finns på plats och viss risk måste accepteras. För etablerade industriföretag innebär det en särskild utmaning, eftersom nya arbetssätt och kompetenser behöver utvecklas parallellt med den befintliga verksamheten.

Sverige har goda förutsättningar genom en stark industriell bas, teknisk kompetens och erfarenhet av komplex produktutveckling. Utmaningen är att använda dessa styrkor för att utveckla och skala säkra och tillförlitliga produkter där mjukvara och AI får en allt större betydelse.

Arbetsgruppen har tre sammanfattande rekommendationer om vad Sverige bör satsa på för att skapa svensk konkurrensförmåga, uppnå hållbarhet samt bidra till svensk och global säkerhet. Dessa baseras på en nulägesanalys av Sveriges position inom mjukvara för kritiska fysiska system, internationella utvecklingstrender samt en genomgång av nyckelfrågor som identifierar hinder och möjligheter för Sveriges fortsatta utveckling. De sammanfattar ett antal förslag och handlingspunkter som redovisas mer utförligt i rapporten.

- **Öka företagens omställningstakt** från traditionella produkter till lärande AI-system genom nya affärsmodeller, organisationsformer och utökat samarbete mellan olika aktörer. Dessutom behöver styrelse- och ledningskompetensen stärkas.

- **Bygg kompetens och erfarenhet för säkra kritiska fysiska system.** Anpassa utbildning och kompetensutveckling snabbare till industrins behov av säker och tillförlitlig mjukvara.

- **Korta vägen från utveckling till marknad.** Skapa arenor för att utveckla, testa och validera mjukvara i realistiska miljöer i samverkan mellan företag, akademi och offentlig sektor.

English Summary



Software is playing an increasingly important role in products such as vehicles, robots and industrial machinery. When software controls functions that affect the physical world, failures can have serious consequences for people, the environment and critical societal functions. This places high demands on safety and reliability, as well as on the ability to test and verify products throughout their life cycle.

AI is also changing how software and products are developed. It can be used to develop software and incorporated into the products themselves. This can speed up development, but also brings new demands in terms of skills, working methods and oversight. As technology advances rapidly, skills need to keep pace. As AI takes over some of the tasks traditionally performed by programmers, a sound understanding of products, systems and architecture becomes increasingly important.

The landscape is also changing as trade, technology and supply chains become more regional, with security and geopolitical considerations playing an increasingly important role. Access to components, data, computing power and digital infrastructure can be affected by where technologies are developed and used. Swedish companies therefore need to navigate different markets and regulatory frameworks while reducing their exposure to strategically important dependencies. These shifts also create opportunities for Sweden and Europe to strengthen their capabilities in areas where safety and reliability are becoming increasingly important.

As products become less dependent on hardware design alone and increasingly rely on software for their functions and ongoing development, companies need to adapt the way they work. Development cycles need to be shorter, allowing new solutions to be tested and feedback gathered early on. Swedish companies need to make decisions and develop new solutions more quickly, even when information is incomplete and some risks must be accepted. This is a particular challenge for established industrial companies, which must develop new skills and ways of working while maintaining their existing operations.

Sweden has a strong industrial base, considerable technical expertise and extensive experience in complex product development. The challenge is to build on these strengths to develop and scale up safe, reliable products in which software and AI play an increasingly important role.

The working group presents three overarching recommendations on where Sweden should focus its efforts to strengthen Swedish competitiveness, achieve sustainability, and contribute to security in Sweden and globally. These recommendations are based on an analysis of Sweden's current position in software for critical physical systems, international development trends, and a review of key issues identifying barriers and opportunities for further development. They bring together a number of proposals and actions, which are set out in greater detail in the report.

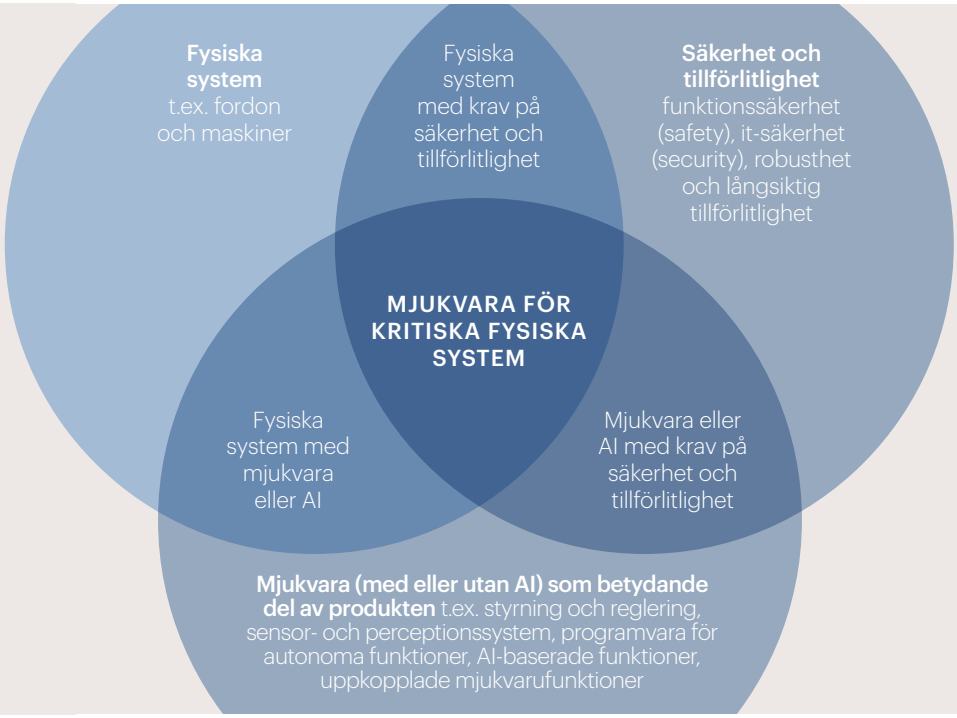
- **Accelerate business transformation** from traditional products to AI-driven, learning systems by developing new business models, organisational structures and stronger collaboration between stakeholders. Board members and senior management also need to strengthen their expertise in this area.

- **Build expertise and experience in safety-critical physical systems.** Adapt education and professional training more quickly to industry's needs for safe and reliable software.

- **Bridge the gap between development and market.** Create environments where businesses, academia and the public sector can work together to develop, test and validate software under realistic conditions.

Utgångspunkter i arbetet med mjukvara för kritiska fysiska system





FIGUR 1: Beskrivning av mjukvara för kritiska fysiska system.

Definition och avgränsningar

I denna rapport används begreppet *mjukvara för kritiska fysiska system*. Med mjukvara (eng. software) menas program och andra instruktioner som kan köras på en dator, såsom operativsystem, applikationer, skript och drivrutiner.[1] Enligt Datatermgruppen kan ordet också förklaras som data i form av instruktioner som en dator kan tolka och utföra (exekvera).

I kritiska fysiska system är säkerhet och tillförlitlighet avgörande. Exempel på sådana system är flygplan, robotar, lastbilar, bilar, drönare, båtar och anläggningsmaskiner.

I denna rapport har vi begränsat oss till fysiska system där inbäddad mjukvara och/eller AI utgör en betydande del av själva produkten. Rapporten omfattar både funktionssäkerhet (eng. safety) och it-säkerhet (eng. security). Tillämpningar inom medicinsk teknik ingår dock inte.

Begreppet *mjukvara för kritiska fysiska system* omfattar inte bara färdiga system, utan också den mjukvara och de verktyg som används för att utveckla dem. När AI och annan avancerad mjukvara får en allt större roll i utveckling, programmering och testning av dessa system behöver krav på säkerhet och tillförlitlighet beaktas genom hela processen, från utveckling och testning till drift och uppdatering. Den ökande användningen av AI i mjukvaruutvecklingen förändrar utvecklingsprocessen. Delar av programmeringsarbetet kan automatiseras, exempelvis genom AI-genererad kod, vilket kan göra arbetet betydligt snabbare. Tidigare

1 Computer Sweden. IT-ord.

TABELL 1: IVAs val att genomföra en teknikrapport utgår från åtta kriterier.

KRITERIUM	MJUKVARA FÖR KRITISKA FYSISKA SYSTEM I SVERIGE
Globalt ledarskap	Sverige kan bli världsledande inom ett antal områden där inbäddad mjukvara eller AI utgör en betydande del av fysiska produkter och där höga krav ställs på säkerhet och tillförlitlighet.
Turn around (möjlighet att vända rådande utveckling)	Sverige har möjlighet att gå från en stark men utspridd kompetens till en mer samlad förmåga att utveckla, testa och använda mjukvara för kritiska fysiska system.
Positionsförflyttning	När en allt större del av exempelvis ett fordon, en maskin eller ett försvarssystem består av mjukvara förändras också var produktens funktion och värde skapas.
Möjliggörande teknologi	Inbäddad mjukvara och AI utvecklas mot att bli centrala för hur fysiska produkter fungerar, styrs och övervakas. När systemen är kritiska måste mjukvaran samtidigt vara säker, tillförlitlig och möjlig att uppdatera över lång tid.
Internationellt	Sveriges starka exportindustri inom bland annat fordon, flyg, försvar och rymd ger en god grund för att utveckla och sälja produkter där mjukvara för kritiska fysiska system är en betydande del av själva produkten.
Megatrender	Automatisering, elektrifiering och ökad autonomi gör att allt fler fysiska produkter blir beroende av avancerad mjukvara för centrala funktioner.
Geopolitik	Växande beroenden av utländsk teknik gör förmågan att utveckla, kontrollera och säkra mjukvara för kritiska fysiska system viktig för Sveriges säkerhet och tekniska handlingsfrihet.
Hett område	Mjukvara blir allt viktigare för industrins konkurrenskraft när fysiska produkter blir mer mjukvarustyrda och autonoma.

har programmering och förändringar i mjukvaran i hög grad varit en uppgift för specialiserade programmerare och systemutvecklare. AI-baserade verktyg gör det möjligt för exempelvis ingenjörer och andra som arbetar med de produkter och system som mjukvaran ingår i att i större utsträckning själva skriva och ändra kod. För mjukvara som styr fysiska system innebär det att förändringar i säkerhetskritisk mjukvara kan genomföras snabbare och av personer med olika yrkesroller. Det ställer nya krav på hur säkerheten hanteras, kontrolleras och verifieras genom hela utvecklingsprocessen. Begreppet inbäddad (eng. embedded) används traditionellt för mjukvara som är integrerad direkt i en fysisk produkt, exempelvis i ett fordon eller ett industrisystem. För den avgränsning som görs här är det dock inte avgörande var mjukvaran finns, utan vilken roll den har i det fysiska systemet. Dagens fysiska produkter är ofta uppkopplade och beroende av mjukvara och tjänster utanför själva produkten, exempelvis i molninfrastruktur. Funktionaliteten kan därför vara fördelad mellan den fysiska produkten, mjukvaran i produkten och externa digitala tjänster.

Motivering till att IVA prioriterat en teknikrapport inom mjukvara för kritiska fysiska system

IVA har gjort en datadriven analys av patent, vetenskapliga publikationer och startup-investeringar för att kartlägga Sveriges globala position inom 48 strategiskt viktiga teknikområden som har stor betydelse för landets framtida välstånd, ekonomiska motståndskraft och nationella säkerhet.[2]

Analysen gav bland annat insikten att Sverige behöver ta ett mer strategiskt angreppssätt för att säkra sin internationella position. Mot denna bakgrund har IVA valt att göra en fördjupad analys av mjukvara för kritiska fysiska system och ta fram förslag för den önskade framtida riktningen inom detta område. Valet utgår från åtta kriterier, se tabell 1.

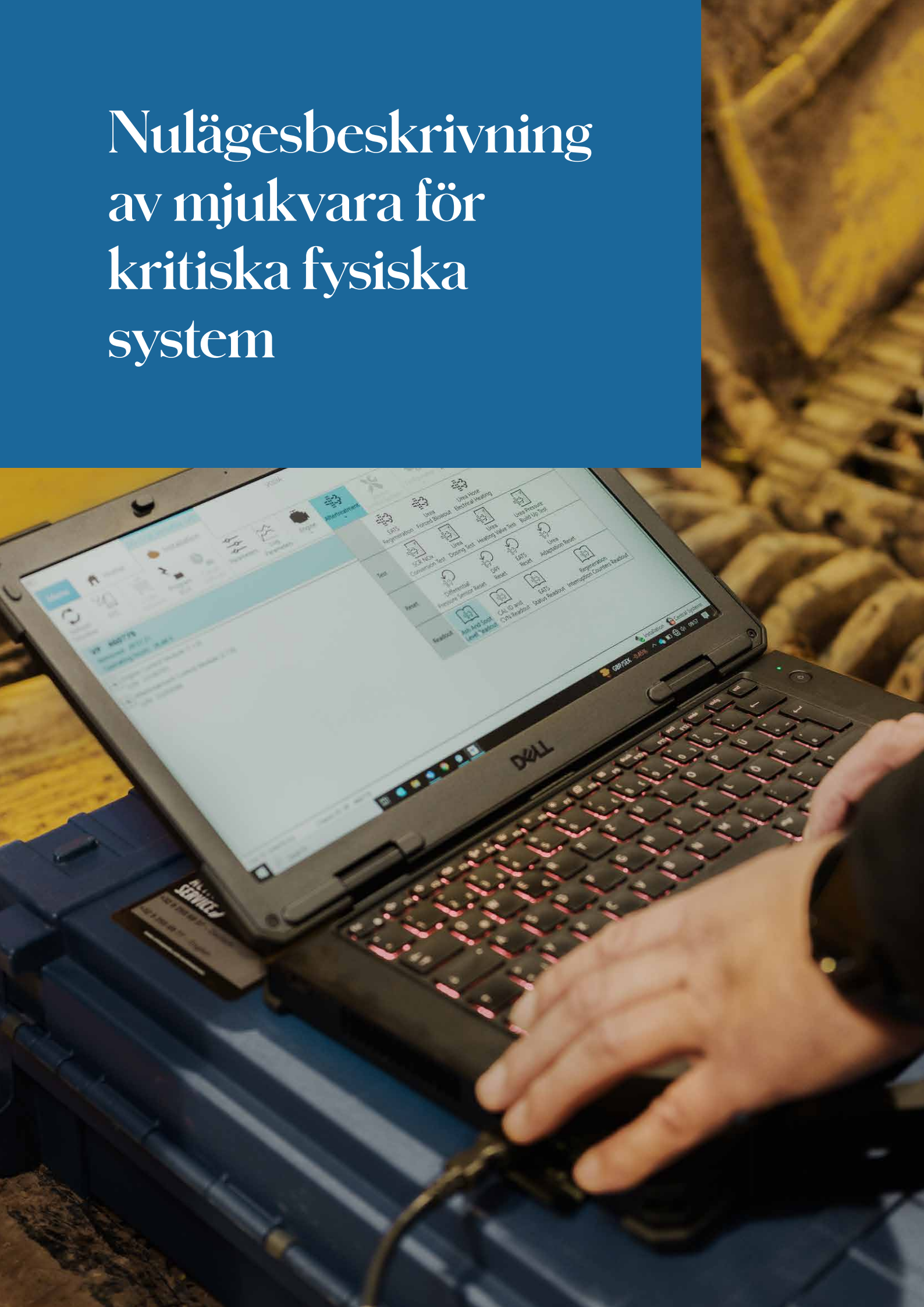
Svensk industriexport är stark inom områden som fordon, maskiner, flyg, försvarssystem och rymdprodukter. Nu genomgår dessa sektorer en snabb förändring där mjukvara i allt högre grad avgör hur systemen fungerar, hur säkra de är och vilket värde de skapar. Det innebär att mjukvara tar över funktioner som tidigare utfördes av mekanik och elektronik.

Det här ställer helt andra krav på mjukvara för kritiska system än på mjukvara för vanliga konsumenttjänster. Den måste tåla fel, störningar och angrepp. Den får inte medföra risk för fysisk skada på utrustning eller människor och måste fungera stabilt över mycket lång tid med löpande uppdateringar utan att säkerheten försämras.

Nya arbetssätt, som fragmenterade utvecklingskedjor, uppdelad leverans av mjukvara och mer AI-genererad kod, gör det svårare att ha full kontroll och spårbarhet i utvecklingen. Sverige har stark kompetens inom både industri och teknik, men saknar en samlad ansats för hur man utvecklar säker och tillförlitlig mjukvara för den här typen av kritiska system. En viktig del i en sådan ansats är att skapa strategisk handlingsfrihet för att Sverige ska kunna ha kontroll över kritiska områden där säkerhet, data eller kritiska beroenden måste beaktas. Inom andra områden kan det vara möjligt att använda europeiska och kommersiella lösningar för att dra nytta av större skala och snabbare utveckling.

2 IVA (2025). *Sveriges position inom strategiskt viktiga tekniker. Investeringsprioriteringar, styrkor och utmaningar*.

Nulägesbeskrivning av mjukvara för kritiska fysiska system



Mjukvara som styr den fysiska världen

Mjukvara för kritiska fysiska system styr, övervakar eller påverkar tekniska system där mjukvarans funktion får direkta konsekvenser i den fysiska världen. I traditionella informationssystem kan ett fel leda till att information förloras eller att funktionaliteten begränsas. Men ett fel i ett kritiskt fysiskt system kan i stället orsaka fysisk skada, påverka människors säkerhet eller störa samhällsviktiga funktioner. Exempel på sådana system finns inom transportsektorn, där mjukvara i dag är en självklar del av flygplan, personbilar, lastbilar, tåg och autonoma transportsystem. Andra exempel finns inom energiområdet och inom industriella tillämpningar. Begreppet cyberfysiska system används för tekniska system där mjukvara, datorer och fysisk utrustning samverkar för att övervaka, analysera och styra olika processer i den verkliga fysiska världen.[3] Systemen använder sensorer för att samla in information från omgivningen, bearbeta informationen med hjälp av mjukvara och därefter påverka den fysiska världen genom olika styrfunktioner. Mjukvaran utgör den logiska kärnan i dessa system genom att samla in information från omgivningen, analysera systemets tillstånd och generera styrsignaler som påverkar den fysiska processen. I ett modernt fordon kan sensorer exempelvis mäta hastighet, position, omgivande trafik och fordonets tekniska status. Mjukvaran bearbetar denna information för att kunna styra funktioner som bromssystem, drivsystem, batterihantering eller automatiserade körfunktioner. På motsvarande sätt styr mjukvara centrala funktioner i flygplan, järnvägssystem och industriella processer.[4] Med hjälp av AI kan moderna system förstå sin omgivning, förutse vad som kan hända och agera utifrån det. En självkörande bil kan till exempel upptäcka andra trafikanter, bedöma hur de kan röra sig och anpassa sin körning.

Mjukvara består av instruktioner, logik och modeller som anger hur ett datorsystem ska behandla information och utföra olika uppgifter. I traditionella IT-system används mjukvara främst för att hantera information, kommunikation och administrativa funktioner. I kritiska fysiska system har mjukvaran däremot en direkt påverkan på den fysiska världen genom att styra och övervaka tekniska processer. Det innebär att mjukvaran inte bara måste ge rätt resultat, utan också göra det vid rätt tidpunkt och under förhållanden där ett fel kan få allvarliga konsekvenser. Därför ställs särskilt höga krav på hur sådan mjukvara utvecklas, testas och verifieras för att säkerställa att systemen fungerar tillförlitligt under hela sin livslängd.[5]

Fel i ett kritiskt system ger allvarliga konsekvenser

Att ett system är kritiskt innebär att ett fel i systemet kan få allvarliga konsekvenser för människor, miljö, ekonomi eller samhällsviktiga funktioner. Därför ställs särskilda krav på hur systemet utvecklas, testas, övervakas och underhålls under hela livscykeln. Kritiska system måste vara säkra, tillförlitliga och tillgängliga. De måste också kunna hantera störningar och fel på ett kontrollerat sätt. Inom säkerhetskritiska tillämpningar är det särskilt viktigt att systemet kan förebygga farliga situationer eller begränsa konsekvenserna när en komponent eller mjukvarufunktion inte fungerar som avsett. Tillförlitlighet handlar därför inte enbart om att systemet fungerar under normala förhållanden, utan

3 Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). *Cyber-physical systems: The next computing revolution.* Proceedings of the IEEE, 98(8), 1305–1320.

4 Lee, E. A. (2008). *Cyber physical systems: Design challenges* (Technical Report No. UCB/EECS-2008-8). University of California, Berkeley.

5 Kopetz, H. (2011). *Real-time systems: Design principles for distributed embedded applications* (2nd ed.). Springer.

AI FÖRÄNDRAR FÖRUTSÄTTNINGARNA FÖR HELA MJUKVARUUTVECKLINGEN

AI används redan i utvecklingen av mjukvara för kritiska fysiska system. Den kan till exempel hjälpa till att skriva och granska kod, hitta fel, skapa tester och dokumentera arbetet. Utvecklingen har gått snabbt på kort tid och AI har på några år blivit ett etablerat verktyg inom mjukvaruutveckling.

AI blir också en allt viktigare del av själva produkterna. I fordon, robotar och andra fysiska system kan AI till exempel användas för att tolka information från omgivningen, fatta beslut och styra systemets funktioner. Det kan beskrivas som AI i fysiska system, där det engelska begreppet *physical AI* oftast används. Det innebär att mjukvarans förmåga att uppfatta och agera i den fysiska världen blir en allt viktigare del av produktutvecklingen.

AI förändrar inte bara enskilda arbetsuppgifter utan också hur utvecklingsarbetet bedrivs. Delar av arbetet kan utföras snabbare och mer automatiserat, vilket ger utvecklare mer tid för problemlösning, arkitektur och andra uppgifter som kräver erfarenhet och bedömning. Det blir också lättare att pröva olika lösningar och att snabbt gå från idé till test och vidare utveckling.

För företagen innebär utvecklingen möjligheter att öka utvecklingstakten och använda kompetens och resurser på ett annat sätt. Men utvecklingen ställer också krav på nya arbetssätt och kompetenser. Företagen behöver förstå hur AI kan användas och hur resultat från utvecklingsarbetet ska granskas, testas och följas upp.

För kritiska fysiska system är detta särskilt viktigt. AI kan göra fel, vilket innebär att kod eller andra lösningar som tas fram med hjälp av AI måste kontrolleras och testas noggrant innan de används.

även om dess förmåga att upptäcka fel, anpassa sig till störningar och återgå till ett säkert läge.[6]

För säkerhetskritiska system räcker det inte att visa att mjukvaran fungerar i ett antal testfall. Utvecklarna måste också kunna argumentera för att systemet uppfyller definierade säkerhetskrav under hela sin livscykel. Detta kräver systematiska metoder för kravhantering, riskanalys, verifiering och validering. Inom exempelvis fordonsindustrin används standarder för att strukturera arbetet med funktionell säkerhet i elektriska och elektroniska system.[7] Liknande principer används inom andra områden där mjukvarufel kan påverka människors säkerhet.

Beslut måste både vara korrekta och fattas vid rätt tidpunkt

En viktig skillnad mellan kritiska fysiska system och många andra tekniska system är att de måste kunna reagera snabbt och på ett förutsägbart sätt. I dessa system är det inte bara viktigt att ett beslut är korrekt, utan även att det fattas vid rätt tidpunkt. Ett bromssystem i ett fordon, ett styrsystem i ett flygplan eller ett industriellt kontrollsystem måste exempelvis kunna reagera inom definierade tidsgränser för att säkerheten ska kunna upprätthållas. Ett beslut som i sig är korrekt kan ändå leda till allvarliga konsekvenser om det fattas för sent.

6 Avizienis, A. et al. (2004). *Basic concepts and taxonomy of dependable and secure computing*. IEEE Transactions on Dependable and Secure Computing, 1(1), 11–33.

7 ISO. (2018). *ISO 26262: Road vehicles – Functional safety*. International Organization for Standardization.

Därför ställs särskilda krav på den mjukvara som används i dessa system. Den måste säkerställa att rätt funktion utförs, att resultatet blir korrekt och att funktionen genomförs inom den tid som krävs för att systemet ska fungera säkert.[8]

Mjukvara för kritiska fysiska system skiljer sig därmed på flera avgörande sätt från annan mjukvara. För det första finns en direkt koppling mellan mjukvarans beteende och fysisk säkerhet. För det andra krävs en hög grad av förutsägbarhet eftersom systemets beteende måste kunna analyseras, verifieras och ofta garanteras. För det tredje måste utvecklingen ske med metoder som kan hantera mycket komplexa system med lång ekonomisk livslängd och många beroenden mellan olika komponenter.[9]

Mjukvara styr många system i dagens fordon

Utvecklingen är särskilt tydlig inom fordonsindustrin, där moderna personbilar och lastbilar har blivit avancerade tekniska system som i stor utsträckning styrs av mjukvara. Mjukvaran hanterar i dag allt från drivsystem och energianvändning till säkerhetsfunktioner, förarstöd och uppkopplade tjänster. Fordonet har därmed utvecklats från att huvudsakligen vara en mekanisk konstruktion till att bli ett komplext system där mjukvara spelar en central roll för funktion, prestanda och säkerhet. Den ökande mängden och komplexiteten hos mjukvara medför nya utmaningar när det gäller utveckling, testning, verifiering och långsiktigt underhåll.[10] För autonoma fordon blir utmaningarna ännu större eftersom mjukvaran måste kunna tolka en komplex omgivning, fatta beslut och agera säkert i situationer som inte alltid kan förutses i förväg.[11]

Autonoma transportsystem illustrerar tydligt skillnaden mellan ”vanlig” mjukvara och mjukvara för kritiska fysiska system. Ett traditionellt program kan ofta korrigeras efter att ett fel upptäckts, medan ett autonomt fordon måste kunna fatta säkra beslut i realtid utan mänsklig inblandning. Detta kräver nya metoder för verifiering och validering där simulering, modellbaserad utveckling och formella analysmetoder kombineras med omfattande tester i verkliga miljöer. Transportstyrelsen har pekat på att automatiserade fordon innebär nya krav på säkerhet, juridisk ansvarsfördelning och teknisk utveckling inom transportsystemet.[12, 13]

Både teknik och organisation har betydelse

Utöver kraven på funktionell säkerhet blir cybersäkerhet allt viktigare i takt med att kritiska fysiska system blir mer uppkopplade och beroende av digital kommunikation. Moderna fordon och transportsystem utbyter information med externa tjänster, andra fordon och digital infrastruktur, vilket skapar nya möjligheter till effektivare och mer automatiserade funktioner men också nya sårbarheter. Ett angrepp mot ett uppkopplat fysiskt system kan få konsekvenser som sträcker

8 Kopetz, H. (2011). *Real-time systems: Design principles for distributed embedded applications* (2nd ed.). Springer.

9 Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.

10 Rumez, M., et al (2020), *An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures*, IEEE Access, vol. 8, pp. 221852-221870.

11 Koopman, P., & Wagner, M. (2017). *Autonomous vehicle safety: An interdisciplinary challenge*. IEEE Intelligent Transportation Systems Magazine, 9(1), 90–96.

12 Transportstyrelsen. (2014). *Autonom körning – Förstudie* (Dnr: TSG 2014–1316).

13 Transportstyrelsen. (2025). *Förslag till en nationell trafikregleringsmodell – säker användning av automatiserade fordon* (Dnr: TSV 2025–12812).



sig bortom den digitala miljön och påverka den fysiska världen. Därför måste säkerheten i mjukvaran hanteras ur ett helhetsperspektiv där både tekniska lösningar och organisatoriska faktorer beaktas. Utvecklingsprocesser, kompetens och en stark säkerhetskultur är avgörande för att kunna utveckla och underhålla mjukvara som är robust och motståndskraftig mot fel och angrepp.[14]

Mjukvara för kritiska fysiska system styrs av flera regelverk

Regelverken syftar till att minska säkerhetsrisker

Mjukvara för kritiska fysiska system omfattas av flera olika regelverk beroende på vilket område systemet används inom. Det handlar om en kombination av europeiska regler, svenska lagar, myndighetsföreskrifter och internationella standarder. Gemensamt för dessa är att de ska bidra till att systemen utvecklas, testas och förvaltas på ett sätt som minimerar risken för fel som kan påverka människors säkerhet, samhällsviktiga funktioner eller fysisk infrastruktur.

En viktig princip är att säkerheten måste hanteras under hela systemets livscykel, från de första kraven och den tekniska utformningen till testning, drift och underhåll. Inom olika branscher används därför standarder som stöd för säker utveckling, exempelvis ISO 26262 inom fordonsområdet och motsvarande standarder inom flyg och järnväg.

Kraven på cybersäkerhet ökar

I takt med att kritiska fysiska system blir allt mer uppkopplade och beroende av digital kommunikation ökar kraven på cybersäkerhet.

14 Karlzén, H., et al. (2024). *Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder* (FOI-R--5691--SE).

På europeisk nivå finns krav på att verksamheter inom samhällsviktiga områden ska arbeta systematiskt med cybersäkerhet, riskhantering och incidentrapportering.[15] I Sverige implementeras dessa krav genom cybersäkerhetslagen (2025:1506). För verksamheter som är viktiga för Sveriges säkerhet gäller även säkerhetsskyddslagen (2018:585), som ställer krav på att skydda känslig information, tekniska system och viktiga funktioner.

Utvecklingen av uppkopplade produkter påverkas även av nya EU-regler, exempelvis cyberresiliensförordningen.[16] Förordningen innebär att tillverkare får ett större ansvar för att utveckla säkra produkter, hantera sårbarheter och säkerställa att säkerhetsuppdateringar kan genomföras under produktens livslängd.

Krav inom transport, industri och försvar

Transportsektorn är ett område där kraven på säker mjukvara är särskilt höga eftersom fel kan få direkta konsekvenser för människors säkerhet. För vägfordon regleras säkerhetskrav genom EU:s typgodkännanderegler.[17] För moderna uppkopplade fordon kompletteras dessa krav med internationella regler, till exempel om cybersäkerhet[18] och om hantering av mjukvaruuppdateringar.[19]

Även inom flyg, järnväg och industri ställs höga krav på att säkerhetskritiska system utvecklas och kontrolleras på ett strukturerat sätt. I Sverige ansvarar Transportstyrelsen för tillsyn och regler inom flera transportområden. Försvarsområdet ställer liknande höga krav på robusthet och tillförlitlighet, eftersom systemen måste kunna fungera även vid störningar, angrepp och svåra förhållanden. Säkerhetsskyddslagen reglerar verksamheter där skyddet av känsliga system och information är viktigt och kompletteras av försvarsspecifika krav inom exempelvis systemsäkerhet och informationssäkerhet.

Skydd av människor och säker användning

Utöver krav på teknisk funktion och cybersäkerhet finns regelverk som fokuserar på att skydda människor som använder eller påverkas av tekniska system. Arbetsmiljölagen (1977:1160) ställer krav på att arbetsgivare ska förebygga risker och säkerställa att tekniska system och arbetsutrustning används på ett säkert sätt. För maskiner och industriella system kompletteras detta av Arbetsmiljöverkets föreskrifter och EU:s maskinförordning (EU) 2023/1230, som ställer krav på att maskiner och deras styrsystem ska vara säkra och tillförlitliga.

Gemensamt för regelverken är att säkerhet inte kan läggas till i efterhand, utan måste byggas in redan från början i utvecklingen av systemet. När mjukvara får en allt större roll i att styra fysiska processer blir samspelet mellan funktionell säkerhet, cybersäkerhet, arbetsmiljö och produktkrav avgörande. Detta är särskilt viktigt för framtidens autonoma och uppkopplade transportsystem, där mjukvarans beslut direkt kan påverka människor och den fysiska omgivningen.

15 NIS 2-direktivet (EU) 2022/2555.

16 Cyberresiliensförordningen (EU) 2024/2847.

17 Bland annat förordning (EU) 2018/858.

18 UN Regulation No. 155 – Cyber security and cyber security management system.

19 UN Regulation No. 156 – Software update and software update management system.

Internationell utblick

Utvecklingen av säkerhetskritisk mjukvara är koncentrerad till länder där avancerade tekniska system kombinerar fysisk funktion med komplex mjukvara. Internationella standarder har tagits fram i nära anslutning till starka industriella miljöer i USA, Europa och Japan.

USA kopplar samman försvar, samhälle och säkerhet

USA har en stark position inom säkerhetskritisk mjukvara genom sin koppling mellan försvar, flygindustri, rymdteknik och cybersäkerhet. Inom flygområdet har USA haft en central roll i utvecklingen av processer för säker mjukvaruutveckling och certifiering. Standarden för utveckling av mjukvara i luftburna system används internationellt och representerar en etablerad modell för kravhantering, verifiering och dokumentation av säkerhetskritisk mjukvara.[20] USA:s styrka ligger inte enbart i utveckling av avancerade tekniska lösningar utan även i etablerade metoder för att visa att komplex mjukvara uppfyller säkerhetskrav genom systematisk verifiering och validering. USA är även starkt inom cybersäkerhet för kritisk infrastruktur genom utvecklingen av ramverk för riskhantering och skydd av samhällsviktiga digitala system. Till exempel har ett amerikanskt institut för standarder, NIST, tagit fram ett ramverk för cybersäkerhet. Detta används internationellt som en modell för att identifiera, hantera och reducera cyberrisker i kritiska system.[21]

USA har sedan 1960-talet bedrivit forskning om datorer och mjukvara för försvarsändamål genom en myndighet för försvarsforskning, DARPA. Myndigheten har senare utvecklat detta arbete till bland annat autonoma system och metoder för att göra mjukvara säkrare och mer tillförlitlig.[22]

Erfarenheter från den amerikanska flygindustrin visar att brister i hur mjukvarustyrda funktioner utformas, testas och godkänns kan få mycket allvarliga konsekvenser. I ett uppmärksammat fall bidrog problem i ett automatiserat flygkontrollsystem till två flygolyckor, där systemet kunde aktiveras utifrån felaktiga sensoruppgifter.[23] Inom försvarsindustrin har omfattande mjukvaruproblem försenat uppgraderingar av avancerade flygsystem, bland annat genom stabilitetsproblem, brister som upptäckts under tester och behov av flera nya mjukvaruversioner.[24]

Storbritannien satsar på flexibla system

Storbritannien har en stark industri inom försvar, flyg, rymd och avancerad tillverkning. Inom försvaret satsar landet på att utveckla system där mjukvaran lättare kan uppdateras och anpassas när nya behov uppstår. Ett exempel är arbete med flygsystem där olika delar ska kunna bytas ut och uppgraderas utan att hela systemet behöver göras om.[25]

20 Radio Technical Commission for Aeronautics. *Software Considerations in Airborne Systems and Equipment Certification*. RTCA DO-178C.

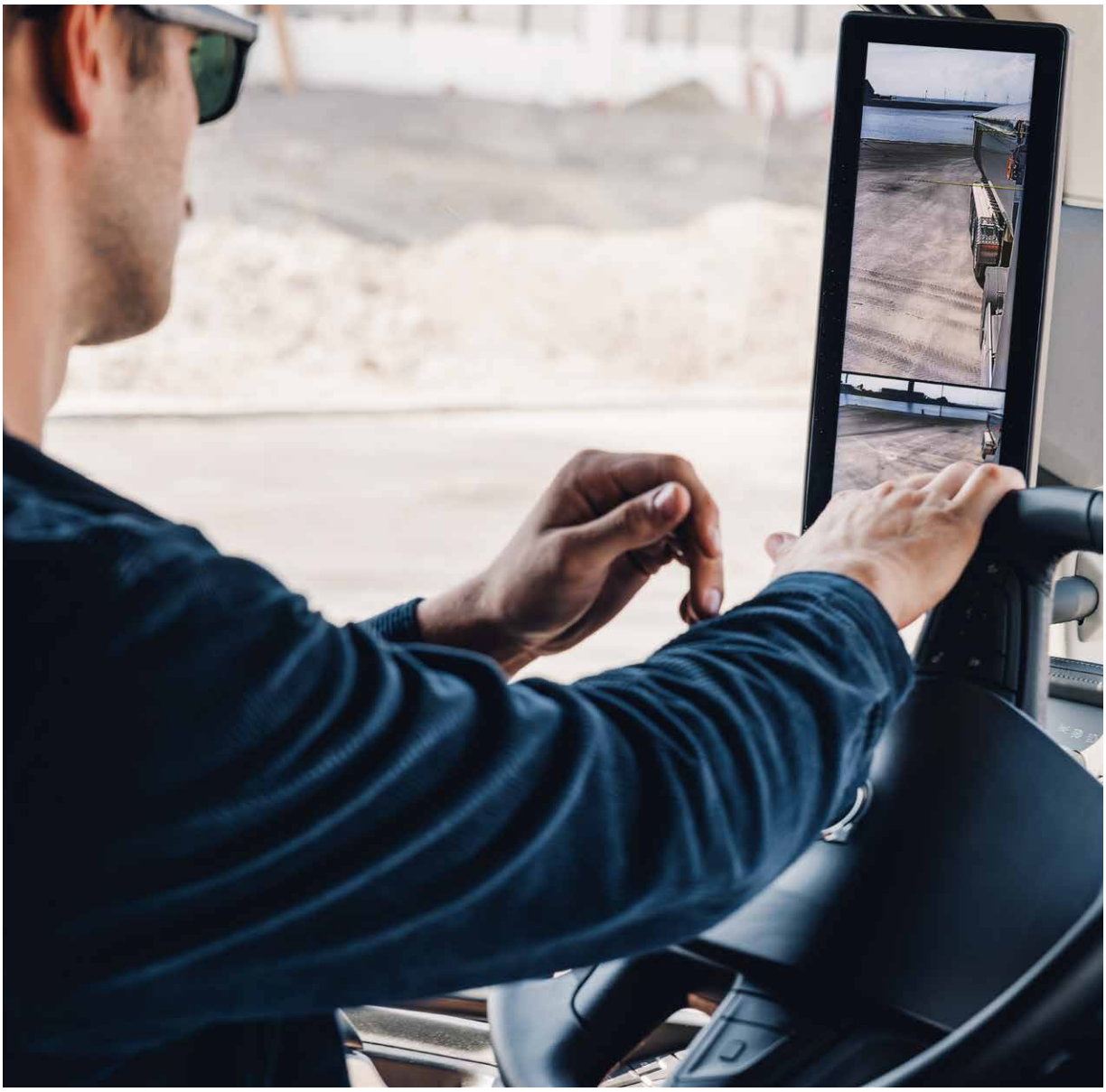
21 National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1.

22 Cybersecurity and Infrastructure Security Agency, Defense Advanced Research Projects Agency, Office of the Under Secretary of Defense for Research and Engineering, & National Security Agency. (2025). *Closing the software understanding gap*. U.S. Department of Homeland Security.

23 Sgobba, T. (2019). *B-737 MAX and the crash of the regulatory system*. Journal of Space Safety Engineering, 6(4), 299–303.

24 Military Watch Magazine. (2025). *US failed upgrades: F-35 software and modernization problems*.

25 Ministry of Defence. *PYRAMID: Rapid adaptability for avionics systems*. GOV.UK. Webbsida: www.gov.uk/guidance/pyramid-rapid-adaptability-for-avionics-systems. Information hämtad den 7 oktober, 2026.



Storbritannien satsar också på AI, data och autonoma system inom försvaret och betonar behovet av att snabbare få ny teknik från forskning och företag till praktisk användning. Samtidigt finns det en brist på digital kompetens och behov av bättre gemensamma lösningar för hur olika system ska kunna fungera tillsammans.[26] Storbritannien visar därmed både på möjligheterna och svårigheterna med att ställa om avancerade system när mjukvaran får en allt större betydelse.

26 Ministry of Defence. (2025). *The Strategic Defence Review 2025: Making Britain safer, secure at home, strong abroad*. Policy paper. GOV.UK.

Tysklands position bygger på industriell tradition

Tyskland har en stark industri inom fordonsområdet, tillverkning och automation. Den stora satsning på industrins digitalisering som inleddes under 2010-talet byggde vidare på landets starka tillverkningsindustri och kompetens inom automation, inbyggda system och informationsteknik.[27] Sedan dess har digital teknik fått en allt större roll i både produktion och produkter, bland annat genom att fysiska system kopplas samman med digital teknik.[28]

För den tyska fordonsindustrin har utvecklingen mot mjukvarudefinierade fordon blivit en stor utmaning. Företagen har länge haft stark kompetens inom exempelvis mekanik, drivlinor, säkerhet och industriell produktion, men behöver nu bygga upp mer kompetens inom mjukvara och digital teknik. Det har krävt både intern kompetensuppbyggnad och samarbete med externa aktörer, vilket har skapat utmaningar när det gäller organisation, beroenden och den tid som krävs för att bygga upp ny kompetens.[29] Utvecklingen har också lett till omorganisationer och neddragningar inom mjukvaruverksamheten, samtidigt som samarbetet med externa aktörer har ökat.[30] OECD har dessutom pekat på att tyska företag har släpat efter i digitaliseringen och att detta hämmar produktivitetsutvecklingen.[31] Tyskland har därmed en stark industriell bas, men omställningen till produkter där mjukvara spelar en allt större roll är en tydlig utmaning.

Sydkorea kombinerar industri och AI

Sydkorea har en stark industri inom bland annat fordon, elektronik, halvledare och tillverkning. Landet inledde redan 2014 en omfattande satsning på att digitalisera fabriker och har sedan dess stöttat tiotusentals projekt i företag över hela landet.[32]

Satsningen har gjort det lättare för företag att använda digital teknik i produktionen. Sydkorea arbetar nu också med att använda AI mer brett i industrin. OECD pekar på att landet behöver stärka företagens förmåga att utveckla och använda ny teknik för att behålla sin konkurrenskraft.[33] Sydkorea kan ses som ett exempel på hur en stark tillverkningsindustri kan kombineras med en snabb digital omställning.

Israel kopplar samman försvar och cybersäkerhet

Israel skiljer sig från de övriga länderna genom sin särskilda styrka inom cybersäkerhet. OECD beskriver Israel som ett land med hög innovationsförmåga och stark utveckling inom digital säkerhetsteknik.[34] Inom säkerhetskritiska system

27 Kagermann, H., et al. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry*. Forschungsunion & acatech.

28 Xu, L. et al. (2018). *Industry 4.0: State of the art and future trends*. International Journal of Production Research. 56(8). 2941–2962.

29 Burr, W. (2026). *Competence building in software technologies: The case of the German automotive industry*. Technology Analysis & Strategic Management, 38(1), 96–108.

30 Deutsche Presse-Agentur. (2026, 1 oktober). *Kreise: VW-Softwaretochter steht vor weiterem Stellenabbau*. WELT.

31 OECD. (2025). *OECD Economic Surveys: Germany 2025*. OECD Publishing.

32 OECD (2026), *Korea's Smart Manufacturing Innovation Initiative*. OECD Publishing.

33 OECD (2023), *OECD Reviews of Innovation Policy: Korea 2023*, OECD Publishing.

34 OECD. (2024). *OECD Digital Economy Outlook 2024*. OECD Publishing.



är denna kompetens särskilt relevant eftersom cyberangrepp kan påverka både digitala funktioner och fysisk säkerhet.[35]

OECD framhåller Israels starka högteknologiska sektor och nära koppling mellan försvar, forskning och näringsliv som viktiga för landets innovationsförmåga. När det gäller mjukvara för kritiska fysiska system är särskilt kombinationen av försvarsrelaterad kompetens, AI och avancerad teknik relevant, eftersom den ger företag möjlighet att utveckla och använda teknik i säkerhetskritiska tillämpningar.[36]

Kina har nationella strategier för storskalig och snabb implementering

Kina har byggt upp en snabbt växande kapacitet inom industriell digitalisering och avancerade produktionssystem. Landets nationella strategier har fokuserat på att utveckla digital industri, artificiell intelligens och smart tillverkning.[37] Kinas främsta styrka ligger i möjligheten att snabbt implementera avancerade tekniska system i stor skala, medan de västerländska industriländerna traditionellt har haft längre erfarenhet av utveckling av reglerade säkerhetskritiska system.

Kinas styrka ligger inte bara i att utveckla ny teknik, utan också i förmågan att snabbt omsätta den i produkter och skala upp produktionen genom täta leverantörsnätverk och nära kopplingar mellan företag och tillverkning. För mjukvara för kritiska fysiska system visar detta betydelsen av att kunna förena teknisk kompetens med industriell kapacitet, leverantörskedjor och förmåga att snabbt gå från utveckling till produktion.[38]

Europa och Kina har olika sätt att organisera produktion och innovation. Kina har till exempel en långsiktig industripolitik med statliga satsningar på strategiska områden.[39]

35 Humayed, A. et al. (2017). *Cyber-Physical Systems Security—A Survey*. IEEE Internet of Things Journal, 4(6), 1802–1831.

36 OECD. (2025). *OECD economic surveys: Israel 2025*. OECD Publishing.

37 Xu, L. et al (2018). *Industry 4.0: State of the art and future trends*. International Journal of Production Research. 56 (8). 2941–2962.

38 Wang, D. (2023). *China's hidden tech revolution: How Beijing threatens U.S. dominance*. Foreign Affairs, 102(2), 66–75.

39 IVA (2026). *Avancerad produktion – En teknikrapport inom Svenska framtider om komplex diskret produktion*. Se särskilt avsnittet "Europa och Kina har olika förhållningssätt", där det finns flera referenser.

Utveckling inom mjukvara för kritiska fysiska system



Flera aktuella svenska initiativ har betydelse för utvecklingen av mjukvara för kritiska fysiska system. Initiativen stärker flera av de förutsättningar som behövs för att utveckla, testa och använda ny teknik. Det handlar bland annat om beräkningskapacitet, forskning och utveckling, kompetens, finansiering och säkerhet.

Tillgången till avancerad beräkningskraft är ett exempel. I juli 2026 fick Skatteverket i uppdrag att ingå ett gemensamt avtal inom EU:s program för superdatorer. Det ska bland annat ge svensk offentlig sektor tillgång till beräkningskraft från en AI-anläggning i Finland, vilket regeringen bedömer vara viktigt för forskning, innovation och användning av AI.[40]

Även forskning och utveckling av ny digital teknik får stöd. Regeringen har gett Vinnova i uppdrag att under 2026 använda minst 570 miljoner kronor inom programmet Avancerad digitalisering.[41] Programmet ska bland annat stödja utveckling av ny teknik och AI som kan användas i industrin. Regeringen har också satsat på forskning inom AI och andra strategiskt viktiga teknikområden av betydelse för mjukvara för kritiska fysiska system.[42]

Kompetensförsörjningen är ett annat viktigt område. I juli 2026 tillsatte regeringen en utredning om hur universitetens utbildningar bättre kan anpassas till arbetsmarknadens och samhällets framtida behov.[43] För utvecklingen av mjukvara som ska fungera säkert tillsammans med fysiska produkter behövs både god kunskap om mjukvara och förståelse för de produkter och system där den ska användas.

Även möjligheterna att finansiera nya teknikföretag uppmärksammas. I juni 2026 fick Tillväxtverket och Vinnova i uppdrag att utreda hur finansieringsgap för nya teknikföretag kan hanteras bättre.[44] Uppdraget omfattar både tillgången till privat kapital och hur offentliga och europeiska pengar kan användas mer effektivt. Detta är värdefullt för företag som utvecklar avancerad mjukvara, eftersom det ofta krävs stora investeringar för att utveckla och prova en produkt innan den kan börja säljas.

Försvarsområdet har samtidigt fått en tydligare roll i utvecklingen och användningen av ny teknik. I juni 2026 beslutade regeringen om en satsning på fem miljarder kronor på bland annat digitala ledningssystem, AI, molnlösningar och nya kommunikationsnät i Försvarsmakten.[45] Syftet är bland annat att förbättra möjligheterna att snabbt dela information, upptäcka hot och fatta beslut. I juli 2026 fick Försvarsmakten dessutom i uppdrag att tillsammans med Försvarets materielverk (FMV), Totalförsvarets forskningsinstitut (FOI) och Vinnova inrätta en samlad funktion för försvarsinnovation.[46] Syftet är att göra det möjligt för försvaret att snabbare anpassa sig till nya hot och att bättre ta till vara ny teknik. Detta är särskilt relevant för mjukvara som ska fungera tillsammans med avancerad militär utrustning och andra fysiska system.

Säkerheten i digitala system har också fått större betydelse. Den nya cybersäkerhetslagen (2025:1506) började gälla i januari 2026 och den innebär högre krav på verksamheter inom flera samhällsviktiga områden. Kraven omfattar bland

40 Regeringen (2026). *Sverige och EU tar första steg mot AI-gigafabriker*. Pressmeddelande publicerat 30 juli 2026.

41 Regeringen (2025) *Regleringsbrev för budgetåret 2026 avseende Verket för innovationssystem*. (KN2025/02359, delvis, KN2025/02393).

42 Regeringen (2024). *Forskning och innovation för framtid, nyfikenhet och nytta* (prop. 2024/25:60).

43 Regeringen (2026). *Ett utbildningsutbud av hög kvalitet som är relevant för arbetsmarknadens och samhällets behov. Kommittédirektiv* (dir. 2026:82).

44 Regeringen (2026). *Uppdrag till Tillväxtverket och Verket för innovationssystem att utreda kapitalförsörjning av kunskapsintensiva företag* (KN2026/01433). Publicerat 29 juni 2026.

45 Regeringen (2026). *Stor satsning moderniserar Försvarsmaktens krigföring*. Pressmeddelande publicerat 18 juni 2026.

46 Regeringen (2026). *Uppdrag om stärkt försvarsinnovation och snabb anpassning* (Fö2025/01745). Publicerat 20 juli 2026.



annat åtgärder för att skydda digitala system och rapportering av allvarliga incidenter. För företag som utvecklar mjukvara för samhällsviktiga system innebär detta både högre krav och en ökad efterfrågan på säkra lösningar.

Det pågår ett bredare arbete med att förenkla regler och myndighetskontakter för företag. Regeringens digitaliseringsstrategi pekar bland annat ut enklare regler och snabbare tillståndsprocesser som viktiga förutsättningar för företagens utveckling.[47] För företag som utvecklar och testar ny teknik kan enklare och mer förutsägbara regler göra det lättare att gå från utveckling till testning och vidare till användning.

För närvarande finns alltså flera pågående initiativ som stärker viktiga delar av området. Beräkningskapacitet, forskning och utveckling, kompetens, finansiering, försvarsinnovation och säkerhet omfattas redan av olika satsningar. Samtidigt är initiativen bredare än mjukvara för kritiska fysiska system och tar inte fullt ut hänsyn till de särskilda krav som uppstår när mjukvara och AI blir en del av produkter där säkerhet och tillförlitlighet är avgörande.

AI-kommissionen pekade på att Sverige behöver agera snabbt för att stärka sin förmåga inom AI.[48] Sedan dess har regeringen tagit fram en nationell AI-strategi och en handlingsplan som tar upp flera av kommissionens förslag.[49] Utvecklingen inom AI och cybersäkerhet går snabbt, vilket gör att arbetet behöver fortsätta i högt tempo.[50]

47 Regeringskansliet (2025). *Sveriges digitaliseringsstrategi 2025–2030*.

48 AI-kommissionen. (2025). *AI-kommissionens Färdplan för Sverige* (SOU 2025:12).

49 Regeringskansliet. (2026). *Handlingsplan för Sveriges AI-strategi*.

50 Kungl. Ingenjörsvetenskapsakademien. (2026). *AI-drivna cyberhot: De kommande tolv månaderna*.

Nyckelfrågor för mjukvara för kritiska fysiska system



Arbetsgruppen har identifierat tre nyckelfrågor för svensk konkurrenskraft inom mjukvara för kritiska fysiska system.

Det handlar om **kompetens**, **regionalisering** och **transformationstakt**.

Nyckelfråga 1: Kompetens för att möta framtidens behov

Sveriges kompetensförsörjning räcker i dag inte till för att möta den snabba utvecklingen inom mjukvara för kritiska fysiska system. Bristen gäller både spetskompetens inom AI för fysiska system (eng. *physical AI*) och den bredare mjukvarukompetens som behöver finnas i fler utbildningar och yrkesroller.

Frågan handlar om hela kompetenskedjan från att utbilda tillräckligt många med rätt kunskaper, att attrahera internationell talang och att skapa förutsättningar för att kompetensen stannar och utvecklas i Sverige. Den handlar också om hur kompetensbehoven förändras. När AI tar över delar av det traditionella programmeringsarbetet blir förmågan att förstå produkter, system och arkitektur allt viktigare. Det ställer nya krav både på utbildningarna och på hur industrin tar emot och utvecklar unga ingenjörer.

Dessutom behöver industrin satsa brett på livslångt lärande. Det behövs både för att hjälpa medarbetare med annan bakgrund att lära sig mjukvaruutveckling och för att låta dem som redan är verksamma inom området fördjupa och uppdatera sina kunskaper i takt med teknikutvecklingen.

Problem

Det finns ett växande gap mellan utbildningarnas innehåll och industrins behov. Ämnen som är relevanta för att kunna arbeta med mjukvara för kritiska fysiska system behöver få större plats i fler ingenjörsutbildningar, samtidigt som kompetensen inom exempelvis inbyggda och säkerhetskritiska system behöver stärkas. Utbildningarna förändras långsamt och industrin erbjuder inte tillräckligt många praktikplatser, projekt och andra vägar in i arbetslivet.

Utvecklingen inom området förändrar dessutom vägen från junior arbetstagare till senior medarbetare. När programmeringen automatiseras blir det svårare att få den erfarenhet som tidigare byggdes upp genom instegsjobb. Utvecklingen drivs i hög grad av den snabba utvecklingen inom AI. I dag hanterar AI inte längre bara enkel programmering, utan löser även komplexa problem som tidigare krävde traditionell regelbaserad programmering. Den höga utvecklingstakten hos mjukvarusystem och AI ställer därmed allt större krav på dagens ingenjörer.

Kompetensfrågan handlar inte bara om hur många som utbildas, utan om hur snabbt människor kan bygga den kompetens som industrin behöver och hur väl Sverige lyckas behålla den.

Möjligheter

Sverige har goda förutsättningar att både bredda ingenjörsutbildningarna och att bygga spets

inom strategiskt viktiga områden. Det handlar inte om samma åtgärder för alla lärosäten. Vissa behöver stärka sin forskning och excellens, medan regionala högskolor framför allt kan behöva fokusera på att attrahera fler studenter till tekniska utbildningar och möta näringslivets kompetensbehov.

I denna allt snabbare förändringstakt kan civilingenjörsutbildningen vinna på att tidiga delar av utbildningen blir bredare med fokus på baskunskap som är relativt stabil över tid, medan snabb förändring kan mötas i mer projektorienterade utbildningsblock som är lättare att ändra utan att hela kursplaner måste göras om.

Ingenjörsutbildningen behöver ge större utrymme åt systemförståelse, organisation och ledarskap. Det är viktigt för att förbereda studenterna på att verka i komplexa organisationer och kunna driva hållbar förändring. När AI och stora språkmodeller blir en del av ingenjörens vardag blir en bred förståelse ännu viktigare. AI kan förstärka både kunskap och intentioner, vilket ställer högre krav på att förstå sammanhang, bedöma konsekvenser och göra etiska avvägningar.

En närmare koppling mellan utbildning och arbetsliv kan ge studenter tidigare erfarenhet av verklig produktutveckling och göra det lättare att bygga kompetens över tid.

Det finns också möjlighet att använda den internationella kompetens som redan söker sig till svenska lärosäten bättre, till exempel genom att se till att personer får möjlighet att stanna kvar och arbeta i Sverige när de är klara med sin utbildning. Tillsammans med tidiga insatser i skolan och bättre vägar från utbildning till arbetsliv kan det skapa en bredare och mer uthållig kompetensbas.

Arbetsgruppen ser positivt på de satsningar som gjorts för att stärka utbildning och intresse inom teknikområdet. Sådana insatser är viktiga eftersom dagens kompetensförsörjning inte är tillräcklig för att möta den snabba utvecklingen inom mjukvara för kritiska fysiska system. Arbetsgruppen understryker dock att det brådskar.

Nyckelfråga 2: Regionalisering och nya globala spelregler

Sveriges konkurrenskraft har länge byggt på globala värdekedjor och marknader. Nu blir handel, teknik och leverantörskedjor mer regionala och i högre grad styrda av säkerhetspolitiska och geopolitiska hänsyn. För ett litet land som är beroende av att kunna exportera har detta stor påverkan på förutsättningarna för hur produkter kan utvecklas, tillverkas och säljas.

Inom mjukvara för kritiska fysiska system blir utvecklingen särskilt tydlig. Tillgång till beräkningskraft, data, molntjänster och avancerade komponenter påverkas allt mer av var systemen utvecklas och används. Produkter som tidigare kunde utvecklas för en global marknad kan behöva anpassas till mer lokala tekniska, regulatoriska och säkerhetspolitiska förutsättningar.

Problem

Sverige är beroende av externa leverantörer inom flera strategiskt viktiga områden, bland annat komponenter från Kina och digital infrastruktur och tjänster från USA. Den hårdvara som krävs för mjukvaruutveckling är dessutom ett geopolitiskt känsligt område, där exportkontroll, regulatoriska krav och begränsningar av vilka aktörer som får använda viss teknik får allt större betydelse.

Det innebär att svenska företag inte längre kan utgå från att samma produkt kan säljas på samma sätt överallt. Samtidigt är tillgången till kapital och avancerad infrastruktur begränsad i Sverige och Europa, vilket kan göra det mer attraktivt för företag och kompetens att söka sig till större ekosystem. Men det handlar inte bara om begränsningar av hårdvara. Även data, mjukvara och uppkopplade system omfattas av nya regler, vilket kan begränsa svenska företags möjligheter att sälja och använda sina produkter på vissa marknader.

Möjligheter

Regionaliseringen behöver inte bara ses som en begränsning. När säkerhet, tillförlitlighet och kontroll över data och infrastruktur blir allt viktigare kan efterfrågan öka på teknik som utvecklas och produceras inom Europa.

Detta gäller inte bara exportföretagen. Sverige har en stark industriell bas med både stora företag och ett stort nätverk av specialiserade teknikföretag och underleverantörer. Det ger goda förutsättningar att bidra till europeiska värdekedjor och utveckla kapacitet inom områden där Europa behöver minska sina strategiska beroenden. Här kan Sverige spela en särskild roll eftersom vi har en hög digital mognad och starka industriella miljöer. En möjlighet är att se Sverige som test- och hemmamarknad för lösningar som senare kan skalas i Europa.

Det finns en potential i att svenska företag blir ännu bättre på att anpassa produkter och lösningar till olika marknader och regelverk. Konkurrenskraft handlar inte längre bara om att kunna sälja globalt, utan också om att bygga starka värdekedjor och etablera sig i flera regionala ekosystem. Det ger Sverige möjlighet att stärka både den egna kapaciteten och Europas förmåga inom mjukvara för kritiska fysiska system.

Nyckelfråga 3: Industrins förmåga att ställa om i tid

Den kanske mest grundläggande utmaningen är hur snabbt svensk industri kan ställa om från hårdvarudefinierade till mjukvarudefinierade produkter. När mjukvara och AI får större betydelse förändras inte bara tekniken utan också hur produkter utvecklas, hur företag organiseras och hur beslut fattas. Sverige är särskilt beroende av de stora företagens förmåga att ställa om i takt med den tekniska utvecklingen. Eftersom dessa företag utgör Sveriges industriella bas blir deras omställningstakt



också avgörande för Sveriges förmåga att hävda sig internationellt. Om svenska företag ställer om långsammare än konkurrenterna i andra länder riskerar Sverige att tappa investeringar och tekniskt försprång inom mjukvara för kritiska fysiska system. Detta är en växande utmaning som hela Europa kämpar med.

Skiftet går från system där hårdvaran i stor utsträckning bestämmer produktens funktion till system där mjukvara kan förändra och förbättra produkten under hela dess livslängd. Det kräver andra kompetenser, kortare utvecklingscykler och i många fall nya affärsmodeller. När mjukvaran utvecklas kontinuerligt kan också produktens värde för kunden öka över tid. Det kräver affärsmodeller som tar hänsyn till att produktens värde förändras under dess livslängd. Det är svårt att sätta ett pris från början på en produkt som ska användas och fortsätta att utvecklas under många år framöver. För etablerade industriföretag är omställningen särskilt krävande eftersom befintliga produkter, organisationer och arbetssätt behöver förändras samtidigt som den nuvarande verksamheten ska fungera.

Det är viktigt att uppmärksamma att den snabba teknikutvecklingen kräver förändringar i hela samhället, inte bara i företagens ledningar och styrelser. Företagen behöver snabbare utveckla nya produkter, kompetenser och arbetssätt samtidigt som utbildningssystemet och andra delar av offentlig sektor behöver anpassa utbildningar, regler och verksamheter till nya tekniska förutsättningar.

Problem

Teknikutvecklingen går snabbare än många företags förmåga att förändra organisationer och arbetssätt. Företagsledningar och styrelser saknar ibland tillräcklig förståelse för mjukvara för kritiska fysiska system för att kunna driva omställningen strategiskt. Samtidigt kräver mjukvaru- och AI-utveckling andra sätt att prioritera och hantera risk än traditionell industriell utveckling.

En viktig skillnad är att utvecklingen inte längre kan planeras på samma sätt från början till slut. Mjukvarubaserade lösningar kräver mer experimenterande och tätare återkoppling. Långa beslutsvägar, krav på att minimera risk och processer som är utformade för mer förutsägbara tekniker kan därför bromsa utvecklingen. Utmaningen är inte bara att få fram ny teknik, utan att få hela organisationen att arbeta på ett annat sätt.

Möjligheter

Svensk industri har erfarenhet av komplex produktutveckling och starka miljöer inom både teknik och systemintegration. Det ger en bra grund för omställningen. Nästa steg är att utveckla ledarskap, arbetssätt och beslutsmodeller som passar säkerhetskritiska produkter där mjukvara spelar en allt större roll.

Det finns också stora möjligheter att lära mellan företag och branscher. Många av problemen är branschoberoende och gemensamma för företag som utvecklar flygplan, fordon, försvarssystem, drönare och andra säkerhetskritiska produkter.

Genom att dela erfarenheter och pröva nya arbetssätt kan omställningen gå snabbare. Förmågan att omsätta ny teknik i befintliga företag och produkter blir därmed minst lika viktig som förmågan att utveckla tekniken i sig.

Sverige har en särskild möjlighet i den starka teknik- och startupmiljö som har vuxit fram under lång tid. I Stockholm finns en stark koncentration av digitala företag och kunskapsintensiva verksamheter, och regionen har en särskilt stor andel av landets högteknologiska och kunskapsintensiva sysselsättning.[51] Många nya företag är digitala från början och har AI och mjukvara som en självklar del av verksamheten. Här finns mycket för svensk industri att lära, inte minst om hur ny teknik kan utvecklas, användas och skalas snabbt.

Traditionell svensk industri har en djup kunskap om teknik, produktion och globala värdekedjor. Den erfarenheten är värdefull för unga teknikföretag som vill växa och nå internationella marknader. Ett tätare utbyte mellan miljöerna skulle därför kunna stärka båda sidor. När entreprenörskap och digital kompetens möter industrins produktionskunnande skapas nya möjligheter att utveckla produkter, företag och lösningar.[52] På så sätt kan Sverige bättre ta vara på två starka miljöer som kompletterar varandra.

51 André, C. and M. Pak (2021), *Regional differences in productivity in Sweden: Insights from OECD regions*, OECD Economics Department Working Papers, No. 1688, OECD Publishing, Paris.

52 OECD (2026), *Incubation in Entrepreneurial Ecosystems: Hatching Growth, OECD Studies on SMEs and Entrepreneurship*, OECD Publishing, Paris.

Önskad framtida riktning



Målbild

År 2035 är Sverige världsledande inom ett antal områden där inbäddad mjukvara eller AI utgör en betydande del av fysiska produkter och där höga krav ställs på säkerhet och tillförlitlighet. Dessutom har Sverige ett starkt ekosystem inom mjukvara för kritiska fysiska system. Det handlar särskilt om produkter där säkerhet och tillförlitlighet är avgörande, såsom flygplan, robotar, lastbilar, bilar, drönare, båtar och anläggningsmaskiner. Om tio år är Sverige världsledande och har en stark industriell förmåga och teknisk spetskompetens när det gäller att omsätta avancerad teknik i komplexa produkter och system.

Sverige har en stark global position inom mjukvara för kritiska fysiska system. Vi har spetskompetens inom teknik som är säker, tillförlitlig och möjlig att testa, verifiera och certifiera. Sverige har ett gott internationellt anseende inom området. Andra länder ser Sverige som ett föregångsland och svenska företag är eftertraktade samarbetspartners. Utgångspunkten är vår etablerade styrka inom inbyggda säkerhetskritiska system. Ambitionen är inte att konkurrera med USA och Kina om stora AI-modeller, utan att bygga en stark position där svensk industri och forskning redan har hög kompetens, lång erfarenhet och goda förutsättningar. År 2035 har Sverige ytterligare stärkt sin position inom säkerhetskritiska tillämpningar där mjukvara kombineras med fysisk teknik, avancerad industriell kompetens och krav på hög säkerhet och tillförlitlighet.

Detta förutsätter att det finns relevant kompetens genom hela utbildningskedjan. Teknikintresset väcks tidigt genom engagerade lärare och praktiska förebilder. Civilingenjörsutbildningarna ger en bred grund och möjlighet till spets inom mjukvaruområdet. Fler industridoktorander, adjungerade professurer och praktikplatser har stärkt kontakterna mellan akademi och industri. Sverige har också blivit bättre på att attrahera och behålla internationella studenter och forskare inom områden som är relevanta för mjukvara för kritiska fysiska system. Kompetensförsörjningen är nära kopplad till industrins utveckling och utbildningarna uppdateras löpande i takt med att tekniken och förutsättningarna ändras. Dessutom är livslångt lärande, omställning och vidareutbildning ett självklart och brett implementerat arbetssätt inom industrin.

En annan förutsättning är tillgången till digital infrastruktur. Beräkningskapacitet, energi, data, molntjänster och strategiska komponenter finns tillgängliga under förutsägbara villkor. Sverige har säkrat att både stora och små aktörer har tillgång till en gemensam nationell infrastruktur för utveckling, test och validering som minskar behovet av att varje företag bygger upp egen kapacitet. Men att enbart ha ett nationellt perspektiv kan vara för snävt när det gäller digital infrastruktur inom mjukvara för kritiska fysiska system. Vissa delar kommer sannolikt att utvecklas på europeisk nivå, exempelvis europeiska molntjänster som kan komplettera eller på sikt ersätta de amerikanska tjänster som vi i dag är beroende av. Sverige behöver vara djupt integrerat i europeisk kapacitet och bygga nationellt endast där säkerhet, tillgänglighet eller kontroll faktiskt kräver det.

Utveckling och träning av säkerhetskritiska system där mjukvara integreras med fysiska produkter kan också kräva gemensam infrastruktur som flera aktörer kan använda. Samtidigt är det troligt att Europa bygger upp egen kapacitet för den avancerade datorkraft som krävs för att utveckla sådana system. Denna kapacitet kan göras tillgänglig via molntjänster, så att företag och andra aktörer kan använda den utan att själva behöva äga och driva den tekniska utrustningen. Fysiska testarenor, som liknar de verksamheter som i dag till exempel finns i form av WARA-PS, testverksamheten i Vidsel Test Range och AstaZero, ger industri och akademi möjlighet att pröva teknik i realistiska miljöer. Utbyggd svensk lagrings- och beräkningskapacitet minskar samtidigt beroendet av utländska leverantörer. År 2035 är Sverige en del av europeiska

EXEMPEL PÅ FYSISKA ARENOR FÖR TEST OCH UTVECKLING

WARA-PS (WASP Research Arena for Public Safety) är en forskningsarena inom det svenska forskningsprogrammet WASP (Wallenberg AI, Autonomous Systems and Software Program). Syftet är att snabba upp forskning och utveckling kring autonoma system, AI och mjukvara för samhällssäkerhet och räddningstjänst. Arenan fokuserar på hur människor och autonoma maskiner kan samverka i komplexa situationer. Ett område i närheten av Västervik har sedan 2018 använts som en permanent testbädd.

Vidsel Test Range i Lappland, i närheten av Älvsbyn, är en militär provplats som drivs av Försvarets materielverk. Syftet är att testa, utvärdera och öva med militära vapen- och flygsystem i en säker och kontrollerad miljö.

AstaZero AB är ett aktiebolag som ägs av forskningsinstitutet RISE. AstaZero driver bland annat testbanor för fordonssäkerhet och ett uppkopplat transportsystem.

infrastrukturer och använder europeisk kapacitet där det är mer effektivt än att bygga nationella lösningar.

Även regelverk och certifiering har utvecklats. Företag kan tidigt förstå vilka krav som gäller, vilken myndighet som ansvarar för olika delar av processen och hur lång tid ett godkännande kan ta. Regelverken fokuserar i högre grad på säkerhet och resultat än på detaljerade tekniska lösningar. Regulatoriska sandlådor används för att pröva nya lösningar och regelverk i mindre skala innan de införs bredare. Sverige har dessutom blivit bättre på att omsätta europeiska regler och standarder i praktiskt användbara processer. Företag kan gå från utveckling och test till bedömning av överensstämmelse och godkännande med större förutsägbarhet.

Sverige ses som ett attraktivt land för kompetens, kapital och företag inom mjukvara för kritiska fysiska system. Företag kan utvecklas och växa i Sverige, samtidigt som internationell kompetens och investeringar söker sig hit. Sverige fungerar också som en attraktiv test- och referensmarknad för nya lösningar. Stora industriföretag och offentliga aktörer bidrar genom att vara tidiga användare av ny teknik, vilket gör det lättare för svenska företag att utveckla, skala och exportera sina lösningar.

En viktig del är samarbetet mellan industri, akademi och offentlig sektor. Gemensamma test- och demonstrationsmiljöer, kunskapsutbyte och strategiska samarbeten gör det lättare att gå från forskning till utveckling och produktion. Företag har också utvecklat sin förmåga att samarbeta. Även företag som är konkurrenter kan samarbeta kring gemensamma tekniska lösningar och infrastruktur som behövs för mjukvara för kritiska fysiska system. Samverkan har blivit mer långsiktig, med fokus på att möta gemensamma utvecklingsbehov snarare än att genomföra enskilda projekt. Företagen har redan i dag många av de arenor och den kompetens som behövs för att utveckla och testa mjukvara för kritiska fysiska system. Utmaningen är att samverka på ett sätt som säkerställer att vi tar tillvara sådant som redan finns, i stället för att företagen arbetar var och en för sig. År 2035 har vi hittat former för att bättre koppla samman befintliga resurser som kan stärka det svenska ekosystemet för utveckling, testning och införande av ny teknik. Om tio år har Sverige utvecklat sitt sätt att arbeta hela vägen från kompetens och forskning till testning, godkännande,

användning och internationell expansion. Kompetens, infrastruktur, regelverk, samverkan och efterfrågan har stärkt Sveriges förmåga att utveckla och skala säkra fysiska system. Det har gett svenska företag bättre förutsättningar att konkurrera internationellt inom mjukvara för kritiska fysiska system, ett område som blir allt viktigare för både industrin och för Sveriges säkerhet.

Fem förslag för utveckling av mjukvara för kritiska fysiska system i Sverige

Detta avsnitt presenterar fem övergripande förslag för att stärka Sveriges konkurrenskraft inom mjukvara för kritiska fysiska system. Förslagen bör genomföras som delar av samma utvecklingskedja snarare än som separata satsningar.

Vi föreslår följande:

- öka takten i företagens omställning,
- gör samverkan mellan industri, akademi och offentlig sektor mer långsiktig,
- bygg en sammanhållen kompetenskedja,
- skapa en sammanhållen struktur för utveckling och test,
- gör regelverk och certifiering mer förutsägbara

För vart och ett av våra förslag presenteras ett antal konkreta handlingspunkter som beskriver vilka åtgärder som behövs och vilka aktörer som bör ha ansvar för att genomföra dem. Dessutom tar vi upp olika alternativ för hur förslagen skulle kunna genomföras över en tioårsperiod. Det finns ingen inbördes prioritering mellan förslagen. Alla behöver genomföras och arbetet bör starta omedelbart.

Förslag: Öka takten i företagens omställning

Svenska företag behöver ställa om från produkter där hårdvaran i hög grad bestämmer funktionerna till produkter där mjukvara får en allt större betydelse. Det förändrar hur produkter utvecklas, produceras och säljs och ställer nya krav på hur företag organiserar arbetet, prioriterar investeringar och fattar beslut. Företagen behöver också utveckla arbetssätt där mjukvara kan uppdateras och produkterna förbättras löpande även efter lansering. För etablerade industriföretag är omställningen särskilt krävande eftersom nya arbetssätt och affärsmodeller behöver utvecklas samtidigt som den befintliga verksamheten ska fungera. Det kan också kräva större förändringar av verksamheten, nya sätt att finansiera utveckling samt styrelser och företagsledningar med tillräcklig kunskap för att fatta beslut om den tekniska och strategiska utvecklingen. Den snabba teknikutvecklingen innebär också att företag behöver kunna fatta beslut innan all information finns på plats och vara beredda att ta en viss risk för att kunna pröva nya lösningar. Det kräver en annan syn på risk och beslutsfattande, men innebär inte att kraven på säkerhet kan sänkas.

Svensk industri har starka förutsättningar genom lång erfarenhet av avancerad produktutveckling, produktion och systemintegration. Den tekniska utvecklingen går snabbt och företag i andra länder utvecklar nya produkter och arbetssätt. För att kunna växa behöver svenska företag också få tillgång till tidiga kunder och marknader där nya produkter

kan prövas och utvecklas. De behöver kunna hantera beroenden till andra länder och anpassa sina produkter och affärsmodeller till olika marknader. Det krävs också kapital för att gå från utveckling till industriell produktion och för att kunna växa internationellt. Om svenska företag inte hinner ställa om i samma takt finns en risk att investeringar och tekniskt försprång flyttar till andra länder.

Konkreta handlingspunkter för att öka takten i företagens omställning:

- **Säkerställ att företagens ledningsgrupper har aktuell och relevant kompetens inom mjukvara för kritiska fysiska system.** Företagen har ett tydligt ansvar för att de produkter och system de utvecklar är säkra under hela sin livscykel. När mjukvaran får en allt större roll i produkternas funktion och säkerhet behöver ledningen också ha tillräcklig förståelse för exempelvis systemarkitektur, cybersäkerhet, testning och uppdateringar. Genom att stärka ledningens kompetens kan företagen ta ett större och mer välgrundat ansvar för säkerheten redan vid produktutveckling och investeringsbeslut.

- **Använd IVAs CTO-nätverk för att dela erfarenheter om mjukvara för kritiska fysiska system.** Skapa en återkommande mötesplats där teknikchefer från olika branscher kan utbyta erfarenheter av utveckling, testning, verifiering och uppdatering av mjukvara i produkter där säkerhet och tillförlitlighet är avgörande. Nätverket kan också identifiera gemensamma hinder och behov inom exempelvis kompetens, testmiljöer, cybersäkerhet, AI, certifiering och regelverk samt sprida fungerande arbetssätt mellan branscher. IVA har ett nätverk för teknikchefer, främst CTO:er, i ledande svenska industriföretag. Nätverket är en del av IVAs Näringslivsråd och fokuserar på kunskapsutbyte kring gemensamma utmaningar, nya teknologier och teknikskiften.

- **Stärk utbytet mellan etablerad industri och nya mjukvaru- och AI-företag.** Skapa strukturer för att etablerade industriföretag och yngre teknikföretag ska kunna dela erfarenheter och utveckla lösningar tillsammans. Etablerade företag kan bidra med kunskap om produkter, produktion och globala värdekedjor, medan nya teknikföretag kan bidra med erfarenheter av mjukvaruutveckling, AI, snabbare utvecklingscykler och nya arbetssätt. Ett tätare utbyte kan göra det lättare att pröva och införa ny teknik i befintliga produkter och verksamheter och därmed påskynda företagens omställning.

- **Inrätta ett programkontor som är inriktat på mjukvara för kritiska fysiska system** inom forsknings- och innovationsprogrammet Avancerad digitalisering. Programkontoret bör få i uppdrag att samla och samordna insatser inom området och stärka samverkan mellan företag, akademi och offentliga aktörer.

- **Följ upp företagens omställning till mjukvarubaserade produkter och arbetssätt.** Uppföljningen bör omfatta exempelvis investeringar, utvecklingstakt, användning av AI och andra nya tekniker samt hinder för omställningen. Resultaten bör användas för att identifiera var utvecklingen går för långsamt och vilka insatser som behövs för att stärka företagens omställningsförmåga och Sveriges konkurrenskraft.

Förslag: Gör samverkan mellan industri, akademi och offentlig sektor mer långsiktig

Sverige har redan många etablerade former för samverkan mellan industri, akademi och offentlig sektor. Till exempel har RISE flera test- och demonstrationsmiljöer där företag, akademi och offentlig sektor kan utveckla och prova nya lösningar tillsammans. Även de strategiska innovationsprogrammen har byggt långsiktiga strukturer för samverkan. Ytterligare ett exempel är forsknings- och innovationsprogrammet *Avancerad digitalisering* som finansieras gemensamt av aktörer inom offentlig sektor och industrin. Programmet kan ge en viktig grund för långsiktig samverkan inom mjukvara för kritiska fysiska system genom att samla företag, akademi och andra aktörer kring forskning, innovation, testmiljöer och kompetensutveckling. Därtill bidrar WASP med forskning och kompetens inom AI, autonoma system och mjukvara. Dessa befintliga program och miljöer bör i högre grad kopplas samman och användas för långsiktigt samarbete inom områden där flera aktörer har gemensamma behov. Utmaningen är alltså inte i första hand brist på nätverk eller mötesplatser. Problemet är i stället att samverkan ofta är projektbaserad och att erfarenheter, kompetens och relationer riskerar att försvinna när ett projekt tar slut. Det finns också en risk att flera aktörer utvecklar liknande lösningar parallellt. För etablerade företag kan det dessutom vara svårt att hitta former för att samarbeta kring teknik som ligger nära den egna kärnverksamheten.

För att stärka Sveriges förmåga att utveckla och införa ny teknik behövs därför mer långsiktiga former för samverkan. Fokus bör ligga på områden där flera aktörer har gemensamma behov men där ingen enskild aktör har tillräckliga incitament eller resurser att driva utvecklingen själv. Det kan exempelvis gälla gemensamma standarder, testmetoder, säkerhetslösningar, data, kompetens och tekniska plattformar.

Förslaget är därför inte att skapa ytterligare ett generellt nätverk. I stället bör befintliga plattformar användas för att identifiera ett begränsat antal strategiska utvecklingsområden där företag, akademi och offentlig sektor kan arbeta tillsammans över längre tid. Samverkan bör kopplas till konkreta problem, gemensamma investeringar och mätbara resultat.

Konkreta handlingspunkter för att göra samverkan mellan industri, akademi och offentlig sektor mer långsiktig:

- **Styr samverkan mellan företag och akademi mot tydliga leveranser och fortsatt användning** genom att utveckla en gemensam arbetsgång för hur samverkansprojekt initieras, följs upp och förs vidare efter projektets slut. Varje projekt bör ha tydliga mål, konkreta leveranser och en plan för hur resultaten ska tas vidare i forskning, utveckling eller industriell tillämpning. Teknikföretagen bör tillsammans med sina medlemsföretag och berörda lärosäten utveckla en sådan modell och ta till vara befintliga erfarenheter från företag som utvecklar mjukvara för kritiska fysiska system. Genomförandeansvaret bör ligga hos de deltagande företagen och lärosätena, medan programansvariga aktörer bör skapa förutsättningar för att framgångsrika samarbeten och resultat kan leva vidare efter projektets slut.

- **Gå från kortsiktiga projekt till fleråriga utvecklingsprogram.** När ett område har identifierats som strategiskt bör samverkan kunna organiseras i tre- till femåriga program med gemensamma mål, finansiering och

ansvar. Här kan arbetssättet inom WASP ses som ett gott exempel. Programmen bör samla företag, akademi och offentlig sektor kring gemensamma problem och långsiktiga mål. De bör ha en tydlig problemägare, definierade resultat och en plan för hur kunskap, metoder och lösningar ska tas vidare efter programmets slut. Det ska vara möjligt att avsluta ett program när målet är uppnått och att flytta resurser till nya områden. Vinnova bör vara ansvarig för samordning i samverkan med RISE, lärosäten, företag och berörda myndigheter. Vinnova bör kunna ta till vara sina erfarenheter från de strategiska innovationsprogrammen och arbetet med *Impact Innovation*. Dessa långsiktiga program har byggt både kapacitet och samverkansstrukturer mellan företag, offentlig sektor och akademi.[53]

- **Koppla samverkansprogrammen till test- och demonstrationsmiljöer.** Varje större samverkansprogram bör redan från början ha en plan för hur resultaten ska testas och valideras. Befintliga testbäddar hos RISE och andra aktörer bör användas som gemensam infrastruktur för företag, forskare och offentlig sektor. Detta bör samordnas av RISE, som har över 130 test- och demonstrationsmiljöer öppna för företag, akademi och offentlig sektor. Exempel på aktörer som kan medverka i genomförandet är Vinnova, lärosäten, företag och berörda myndigheter.

- **Skapa former för samarbete mellan företag inom sektorn** genom att identifiera teknikområden där flera svenska företag har liknande behov, men där det saknas incitament att utveckla gemensamma lösningar. Det kan exempelvis gälla cybersäkerhet, standarder, testmetoder, interoperabilitet, gemensamma dataformat och vissa delar av den tekniska infrastrukturen. Samarbetet bör organiseras så att företagen kan dela erfarenheter utan att behöva dela kommersiellt känslig information eller ge upp kontrollen över sina kärnteknologier. Denna handlingspunkt syftar inte till att få konkurrenter att samarbeta generellt, utan att identifiera icke-konkurrensutsatta delar av värdekedjan där samarbete faktiskt skapar större nytta än parallell utveckling. Forsknings- och innovationsprogrammet *Avancerad digitalisering* skulle kunna samordna detta. Dessutom behöver flera aktörer medverka, såsom berörda företag, branschorganisationer, akademi och relevanta myndigheter.

- **Utveckla standardiserade samarbetsavtal** för gemensam utveckling genom att ta fram avtalsmallar för återkommande situationer där företag, lärosäten och offentliga aktörer samarbetar kring forskning, data, testning och teknikutveckling. Mallarna bör bland annat behandla immaterialrätt, dataåtkomst, sekretess, publicering, ansvar och rättigheter till resultat. Syftet är inte att skapa ett enda avtal för alla samarbeten utan att minska den juridiska startsträckan och skapa en gemensam utgångspunkt för förhandlingar. Teknikföretagen bör samordna arbetet och påskynda det arbete som redan pågår i samverkan med Vinnova, lärosäten, företag, branschorganisationer och juridisk expertis.

53 Vinnova (2026). *Strategiska innovationsprogram. En metastudie av 17 nioårsutvärderingar*. VR:2026:13. Författare: Mona Hallström Hjort et al, Sweco.

På kort sikt bör befintliga nätverk, program och samverkansinitiativ kartläggas med fokus på vilka som redan har en tillräcklig skala och vilka som kan byggas ut. Kartläggningen bör särskilt identifiera områden där flera aktörer utvecklar liknande lösningar eller där det saknas en långsiktig samverkansform. Vinnova bör välja ut två till tre områden för pilotprogram med flerårig finansiering och tydliga mål. Piloterna bör från början kopplas till befintliga test- och demonstrationsmiljöer hos exempelvis RISE.

Inom två till tre år bör Sverige ha etablerat ett begränsat antal fleråriga utvecklingsprogram där företag, akademi och offentlig sektor arbetar mot gemensamma tekniska mål. Det bör också finnas standardiserade avtalsmodeller och en nationell överblick över relevanta projekt, testmiljöer och kompetenser.

Fram till 2035 bör långsiktiga samverkansformer vara en etablerad del av Sveriges innovationssystem. Fokus bör då ligga mindre på att skapa nya nätverk och mer på att snabbt kunna mobilisera befintlig kompetens, infrastruktur och kapital kring nya strategiska teknikområden.

Målet bör vara att Sverige får större utväxling på den samverkanskultur som redan finns genom färre parallella initiativ, längre tidshorisont för gemensam utveckling och bättre samordning av kompetens, infrastruktur och investeringar inom mjukvara för kritiska fysiska system.

Förslag: Bygg en sammanhållen kompetenskedja

Sveriges kompetensförsörjning behöver utvecklas snabbare för att möta den ökade efterfrågan på kompetens inom mjukvara och artificiell intelligens. Utmaningen gäller både bredd och spets. Vi behöver fler möjligheter att utveckla avancerad specialistkompetens i nära kontakt med industrin, fler ingenjörer med aktuell kompetens inom mjukvara för kritiska fysiska system och fler elever och studenter som väljer utbildningar inom STEM.

Sverige bör samla sina befintliga insatser kring en tydlig kompetenskedja, med särskild inriktning på mjukvara för kritiska fysiska system. Målet bör vara att utbildningssystemet snabbare kan svara mot förändrade kompetensbehov, samtidigt som Sverige bygger långsiktig spetskompetens inom strategiskt viktiga teknikområden.

En sådan utveckling pågår redan internationellt. EU har en plan för fler utbildningsplatser på kandidat-, master- och forskarnivå samt pilotprojekt för AI-lärlingsutbildningar.[54, 55] Storbritannien lyfter fram behovet av fler utbildningsvägar in i AI, såsom lärlingsutbildningar och starkare kopplingar mellan högre utbildning och arbetsliv.[56] OECD pekar på att AI-kompetensen behöver byggas både genom

54 EU (2024). *The AI Act*. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.

55 EU. *Shaping and strengthening European AI talent. Webbsida: digital-strategy.ec.europa.eu/en/library/shaping-and-strengthening-european-ai-talent.* Information hämtad den 25 augusti 2026.

56 Secretary of State for Science, Innovation and Technology (2025). *AI Opportunities Action Plan*.

utbildning av specialister och genom kontinuerlig kompetensutveckling i hela arbetslivet.[57]

För industrin är det särskilt viktigt att studenter får erfarenhet av verkliga utvecklingsmiljöer och att utbildningarna har nära kontakt med de kompetensbehov som finns i arbetslivet. Detta är viktigt inte minst för att främja livslångt lärande och vidareutbildning inom industrin. Högre utbildning behöver kombinera en stabil teknisk grund med kunskaper som utvecklas i takt med teknikutvecklingen.

Frågan är inte ny. Regeringen har uppmärksammat kompetensbehovet genom en STEM-strategi[58] och en STEM-delegation[59] samt slagit fast att Sverige ska stärka kompetensbasen inom AI bland annat genom att integrera AI tydligare i utbildningarna.[60] Under 2026 har regeringen dessutom beslutat om ytterligare satsningar på civilingenjörsutbildningarna och ökad genomströmning.[61] Ytterligare ett exempel är IVAs projekt *Framtidens kunskapssamhälle*. Nästa steg bör vara att skapa tätare kopplingar mellan utbildning, forskning och arbetsliv samt att öka kvaliteten och relevansen i högre utbildning.

Konkreta handlingspunkter för att bygga en sammanhållen kompetenskedja inom mjukvara för kritiska fysiska system:

- **Skapa förutsättningar för kontinuerlig kompetensutveckling av ingenjörer i industrin.** Ingenjörer som arbetar med mjukvara för kritiska fysiska system behöver löpande kunna uppdatera sin kunskap när teknik och arbetssätt förändras. Det kan handla om exempelvis nya metoder för att utveckla och testa mjukvara i produkter där säkerhet och tillförlitlighet är avgörande. Lärosäten, företag och branschorganisationer bör därför utveckla kortare och flexibla utbildningar som kan kombineras med arbete och snabbt anpassas när nya tekniker utvecklas. Företagen bör ha ansvar för att identifiera framtida kompetensbehov och ge anställda möjlighet att vidareutbilda sig, medan lärosäten och andra utbildningsaktörer bör erbjuda utbildningar som svarar mot dessa behov. Inspiration till arbetet bör hämtas från det så kallade *Expert Learning Lab*. Detta är ett industrinära initiativ där ledande företag och universitet utvecklar en nationell plattform för kontinuerlig kompetensutveckling av tekniska experter inom området avancerad digitalisering. En ytterligare inspirationskälla är de schweiziska vidareutbildningarna *Nachdiplomstudien*, som ger yrkesverksamma ingenjörer möjlighet att bygga vidare på sin tidigare utbildning och ta en examen på avancerad nivå.[62] Dessa utbildningar ger möjlighet till specialisering och fördjupning inom ett område och kan användas för att bygga aktuell kompetens inom exempelvis säker mjukvaruutveckling för kritiska fysiska system.
- **Skala upp samverkan mellan akademi och industri kring spetskompetens** inom mjukvara för kritiska fysiska system. Detta bör ske genom att öka användningen av

57 OECD (2025), *Trends Shaping Education 2025*, OECD Publishing, Paris.

58 Regeringskansliet (2025). *En STEM-strategi för Sverige*. Utbildningsdepartementet. Publicerad 24 februari 2025.

59 Regeringskansliet (2025). *STEM-delegationen*. Dir. 2025:11.

60 Regeringskansliet (2026). *Sveriges AI-strategi*. Finansdepartementet. Publicerad 20 februari 2026.

61 Regeringskansliet (2026). *Fler civilingenjörer ska ta examen – nya uppdrag till lärosäten*. Pressmeddelande från Utbildningsdepartementet. Publicerad 15 juni 2026.

62 Staatssekretariat für Bildung, Forschung und Innovation. *Höhere Fachschulen*. Länk: www.sbfi.admin.ch/de/hoehere-fachschulen Information hämtad den 5 oktober, 2026.

industridoktorander, adjungerade professorer, gästprofessorer och gemensamma forsknings- och utvecklingsprojekt inom strategiskt viktiga områden som mjukvara för kritiska fysiska system och andra säkerhetskritiska områden. Ett begränsat antal lärosäten bör kunna bygga särskilt starka miljöer där forskning, utbildning och industriell tillämpning möts. Fokus bör ligga på att bygga internationellt konkurrenskraftiga miljöer där Sverige redan har starka förutsättningar, snarare än att sprida dem jämnt över landet. Vetenskapsrådet bör ha ansvar för samordningen i samverkan med lärosäten, berörda branschorganisationer och företag. Även Stiftelsen för strategisk forskning skulle kunna bidra till detta arbete. WASP, *Wallenberg AI, Autonomous Systems and Software Program*, och WISE, *Wallenberg Initiative Materials Science for Sustainability*, är viktiga förebilder. Dessa är långsiktiga forskningsprogram som knyter samman akademi och industri inom strategiska teknikområden. Programmen kombinerar forskning och utbildning med nära samarbete med företag och bidrar på så sätt till att bygga och sprida spetskompetens till näringslivet.

- **Ge ingenjörsutbildningarna en stabil teknisk kärna och snabbare vägar att uppdatera innehållet**. Säkerställ att civilingenjörs- och andra relevanta ingenjörsutbildningar ger en robust grund inom matematik, programmering, datavetenskap, systemutveckling och ingenjörsmetodik. Komplettera med flexibla kurser och moduler inom exempelvis AI, maskininlärning, cybersäkerhet och nya utvecklingsverktyg som kan uppdateras betydligt snabbare än hela utbildningsprogram. Arbetsgruppens erfarenhet är att det i dag saknas utbildningselement med tillräckligt starkt fokus på mjukvara för säkerhetskritiska fysiska system, exempelvis inom feltoleranta system samt programmering av inbyggda system och realtidssystem. Gruppen menar därför att befintliga ingenjörsutbildningar bör kompletteras med relevanta moment och projekt där studenter arbetar med verkliga problem och utvecklingsbehov från industrin. Utbildningarna behöver även kompletteras med kursmoment inom organisation, entreprenörskap, innovation och ekonomi.

  Regeringen bör ansvara för de övergripande förutsättningarna, medan lärosäten och företag bör ha en central roll i att utveckla och genomföra förändringarna. Ett sätt att åstadkomma detta är att inrätta ett permanent forum för samverkan mellan akademi och industri om ingenjörsutbildningarnas innehåll. Forumet skulle ge universitet och företag en strukturerad arena för att diskutera hur utbildningarnas mål, genomförande och kursportföljer svarar mot teknik- och kompetensutvecklingen. Det bör särskilt omfatta civilingenjörsutbildningarna och samla representanter från större industriföretag och universitet till återkommande möten, där lärosätena presenterar utbildningarnas innehåll och utvecklingsplaner och företagen beskriver framtida kompetensbehov. En oberoende organisation med förtroende hos både akademi och industri bör organisera och hålla samman arbetet. Företag och lärosäten bör gemensamt ansvara för att omsätta dialogen i konkreta förändringar av utbildningarna. Modellen bör bygga på initiativ och ansvar hos de aktörer som utvecklar och använder kompetensen, snarare än på central styrning från en myndighet.

- **Förbättra villkoren för internationella studenter och doktorander att stanna i Sverige.** Detta bör göras genom att underlätta övergången från studier till arbete genom tydligare information, snabbare processer och bättre samordning mellan lärosäten, arbetsgivare och myndigheter. Universitet och högskolor bör aktivt erbjuda internationella



studenter kontakt med arbetsgivare, praktik och karriärvägar redan under utbildningen. Genomförandeansvaret bör ligga hos Migrationsverket och lärosätena. Potentiella arbetsgivare bör också involveras. Dessutom har UHR en relevant roll genom sitt arbete med erkännande av utländska utbildningar.

- **Stärk lärarnas STEM-kompetens tidigt i utbildningskedjan** genom att utveckla och skala upp fortbildning för lärare i grundskolan, särskilt inom matematik, naturvetenskap och teknik. Insatserna bör kombineras med bra undervisningsmaterial, lärarhandledning och möjlighet att få fortbildning från lärosäten och andra STEM-aktörer. Skolverket bör vara ansvarig för samordning, inom ramen för regeringens STEM-strategi och i samverkan med STEM-delegationen. Lärosäten med lärarutbildning, kommuner, Science Centers och relevanta branschorganisationer bör medverka.
- **Följ upp kompetenskedjan mot tydliga mål till 2035.** Sätt upp ett begränsat antal mätbara mål för exempelvis tillgången på specialistkompetens inom mjukvara för kritiska fysiska system, genomströmning i ingenjörsutbildningarna, antal industri-doktorander, studentprojekt i företag och andelen internationella studenter som stannar efter examen. Uppföljningen bör framför allt vara inriktad på kvalitet och spets, inte enbart på volym. Teknikföretagen bör vara ansvarig för samordning fram till dess att delegationens uppdrag avslutas. SCB, UKÄ, UHR, Arbetsförmedlingen och berörda branschorganisationer bör medverka.

Arbetet bör börja med att samla och förstärka de initiativ som redan finns. Första steget bör vara en nationell kartläggning av kompetensgapet inom mjukvara för kritiska fysiska system, samtidigt som lärarfortbildning och studenternas kontakt med

arbetslivet byggs ut. Detta bör ske inom ramen för den befintliga STEM-strategin och AI-strategin, snarare än genom att skapa ytterligare en parallell struktur. Arbetet med att stärka förutsättningar för kontinuerlig kompetensutveckling av ingenjörer i industrin bör också börja direkt.

Inom två till tre år bör Sverige ha en etablerad modell för återkommande kompetensanalyser, fler industridoktorander och företagsförlagda projekt samt utbyggda talangprogram. Lärosätena bör också ha fått bättre förutsättningar att uppdatera utbildningarnas innehåll i takt med den tekniska utvecklingen.

Till 2035 bör målet vara en sammanhållen kompetenskedja där fler barn och unga väljer STEM, fler studenter fullföljer tekniska utbildningar, fler får arbetslivserfarenhet under studietiden och Sverige har ett antal internationellt konkurrenskraftiga miljöer för avancerad mjukvarukompetens. För säkerhetskritiska system bör kopplingen till industri och samhällskritiska verksamheter vara särskilt stark.

Förslag: Skapa en sammanhållen struktur för utveckling och test

Tillgången till beräkningskraft, data och testmiljöer blir allt viktigare för Sveriges förmåga att utveckla och använda mjukvara för kritiska fysiska system. För företag och forskare räcker det inte med tillgång till algoritmer och kompetens. Det behövs också kapacitet för att träna och köra modeller, lagra och hantera stora datamängder samt testa lösningar i miljöer som efterliknar verklig användning.

Sverige har redan flera viktiga delar av denna infrastruktur. Ett exempel är *Mimer AI Factory* vid Linköpings universitet som kombinerar AI-optimerad beräkningskapacitet med lagring, AI-kompetens, test och utvärdering och riktar sig till bland annat företag, forskare och offentlig sektor. Det nya systemet installeras vid NAISS under 2026 och omfattar bland annat 400 GPU:er och storskalig lagring för känsliga data.[63] Regeringen har samtidigt stärkt Sveriges deltagande i EuroHPC och beslutat om medfinansiering av en AI-gigafabrik i Finland, vilket ger svenska aktörer tillgång till ytterligare europeisk beräkningskapacitet.[64] Till detta kommer dessutom privata initiativ som exempelvis Sferical AI.

Utmaningen är därför inte främst att skapa beräkningskapacitet från grunden. Den handlar om att skapa en sammanhängande infrastruktur där beräkningskraft, lagring, mjukvarustack, data,

63 The European High Performance Computing Joint Undertaking (2025). *EuroHPC JU Signs Contract to Deploy a New AI-Optimised Supercomputer in Sweden*. Pressmeddelande publicerat 21 april 2026.

64 Regeringskansliet (2026). *Sverige och EU tar första steg mot AI-gigafabriker*. Pressmeddelande från Finansdepartementet. Publicerad 30 juli 2026.

kompetens och testmiljöer kan användas tillsammans. Även mindre företag och forskningsmiljöer bör få tillgång till infrastrukturen utan att själva behöva bygga motsvarande kapacitet.

Det finns också ett behov av fysiska testmiljöer. Mjukvarubaserade autonoma system och andra mjukvarustyrda system måste kunna utvecklas, testas och valideras under realistiska förhållanden innan de kan användas i exempelvis försvar, transport, energi, industri och annan samhällskritisk verksamhet. Sverige har redan ett stort antal testbäddar och Vinnova har en nationell samordnande funktion för test- och demonstrationsmiljöer i verkliga miljöer. Dessutom driver RISE flera testplatser, till exempel för aktörer som är verksamma inom automation. Behovet handlar dock inte bara om enskilda testmoment, utan om att kunna pröva hela system i relevanta och realistiska situationer. Det är särskilt viktigt för autonoma och mjukvarustyrda system, där samspelet mellan mjukvara, fysisk utrustning och omgivning behöver kunna prövas under verkliga förhållanden.

Konkreta handlingspunkter för att skapa en sammanhållen infrastruktur för utveckling och test av mjukvara för kritiska fysiska system:

- **Skapa en mötesarena för experter inom mjukvara för kritiska fysiska system.** Företagen bör skapa en återkommande arena där ingenjörer, utvecklare, systemarkitekter och andra yrkesverksamma kan mötas över företags- och branschgränser för att diskutera gemensamma tekniska utmaningar och dela erfarenheter. Utgångspunkten ska vara industrins konkreta behov, exempelvis hur mjukvara kan utvecklas snabbare samtidigt som kraven på säkerhet och tillförlitlighet uppfylls. Arenan ska inte vara en test- eller utvecklingsmiljö, utan en plats för erfarenhetsutbyte, problemlösning och nya samarbeten. Företagen bör tillsammans ta ansvar för att etablera och driva verksamheten.

- **Knyt samman svensk beräkningskapacitet och gör den enklare att använda** genom att utveckla en gemensam ingång till svensk och europeisk beräkningskapacitet som är relevant för utveckling av mjukvara för kritiska fysiska system. Där ska företag, forskare och offentlig sektor kunna hitta och söka tillgång till relevanta resurser. Den gemensamma infrastrukturen bör omfatta beräkningskraft, lagring, datahantering, säkerhetslösningar och relevanta mjukvarulager. Målet bör vara att användaren i så liten utsträckning som möjligt behöver förstå den underliggande infrastrukturen för att kunna utveckla och testa sin mjukvarubaserade lösning. Detta handlar inte bara om att få tillgång till beräkningskapacitet. Det krävs också säkra sätt att utveckla, testa och uppdatera mjukvaran samt att dokumentera arbetet. Detta är en förutsättning för att kunna använda AI och mjukvara i produkter där fel kan få allvarliga konsekvenser. En tänkbar möjlighet är att använda Mimer som central nod i Sverige, samtidigt som svenska aktörer ska kunna använda kapacitet inom det europeiska EuroHPC-systemet. Om man bygger vidare på Mimer bör Vetenskapsrådet vara ansvarig för samordning genom NAISS och Mimer AI Factory (Mimer och NAISS har redan uppdrag och teknisk kompetens för beräkningsinfrastrukturen). RISE, Vinnova, Digg och relevanta lärosäten bör medverka. Till exempel bör Vinnova bidra till innovations- och företagsdimensionen.

- **Använd EU:s konkurrenskraftskompass som hävstång för utveckling och uppskalning.** EU:s konkurrenskraftskompass (eng. a competitiveness compass for the EU) syftar till att stärka Europas innovationsförmåga,

minska strategiska beroenden och bygga starkare europeiska värdekedjor.[65] Inom mjukvara för kritiska fysiska system skapar detta nya möjligheter för svenska företag att få finansiering för utveckling, testning, demonstration och uppskalning av teknik som bland annat kan vara inriktade på AI och robotik. Företag som utvecklar mjukvara för kritiska fysiska system bör aktivt söka de finansieringsmöjligheter som följer av EU satsningar och bygga europeiska samarbeten för att kunna delta i dem. Teknikföretagen bör stödja företagen i att identifiera relevanta satsningar och hitta europeiska partners, medan företagen själva bör ta ansvar för att utveckla och driva projekten.

- **Utveckla gemensamma tekniska lösningar inom mjukvara för kritiska fysiska system** som gör det enklare att utveckla, träna, testa och använda mjukvara i olika verksamheter. Det kan till exempel handla om verktyg för att samla in, hantera och kvalitetssäkra data, träna AI-system och kontrollera att de fungerar säkert och tillförlitligt. Industrin bör samtidigt samverka mer kring verktyg och metoder som kan användas i flera branscher. Det kan exempelvis handla om att samla in och kvalitetssäkra data, skapa nya data genom datorsimuleringar och träna system som bygger på mjukvara för kritiska fysiska produkter. För fordon, robotar och industrimaskiner behövs stora mängder data för att kunna testa hur produkterna fungerar i olika situationer, även sådana som är ovanliga eller säkerhetskritiska. Företagen bör därför kunna dela på vissa verktyg, metoder och delar av utvecklingsarbetet, medan själva produktutvecklingen även fortsättningsvis sker inom företagen. Satsningen bör inte handla om att bygga en svensk motsvarighet till de stora globala molntjänsterna. Målet bör i stället vara att skapa öppna och säkra lösningar som kan användas tillsammans med olika tekniska plattformar och datorinfrastruktur, både i Sverige och internationellt.

- **Bygg ett nationellt nätverk av test- och demonstrationsmiljöer med fokus på mjukvara för kritiska fysiska system.** Kartlägg befintliga testmiljöer och identifiera vilka kompletteringar som behövs för att kunna testa autonoma och säkerhetskritiska system under realistiska och kontrollerade förhållanden. Det kan exempelvis gälla autonoma fordon, drönare, robotik och andra system där mjukvara samverkar med fysisk utrustning. Vidsel Test Range, Västervik Drone Science Park, WARA-PS och AstaZero är exempel på miljöer som kan ingå, tillsammans med nya civila miljöer inom exempelvis luftfart och industri. Sverige bör inte bygga en enda stor nationell testmiljö eftersom olika system kräver olika testförhållanden. I stället bör befintliga och nya miljöer kopplas samman genom gemensamma standarder, säkerhetskrav och metoder för test och validering. Nätverket bör också ge utrymme för gemensamma utvecklingsprojekt där företag, forskning och offentlig sektor utvecklar och prövar lösningar tillsammans. Nätverket bör vara öppet även för startupföretag och ge tillgång till relevanta öppna dataset. Den tekniska testningen bör kopplas samman med regulatorisk testning genom gemensamma arbetssätt för tekniska testmiljöer och regulatoriska sandlådor. Företag ska kunna pröva både den tekniska funktionen och hur lösningen kan uppfylla gällande regelverk. Detta är särskilt viktigt

65 European commission (2025). *A Competitiveness Compass for the EU*. Brussels, 29.1.2025.

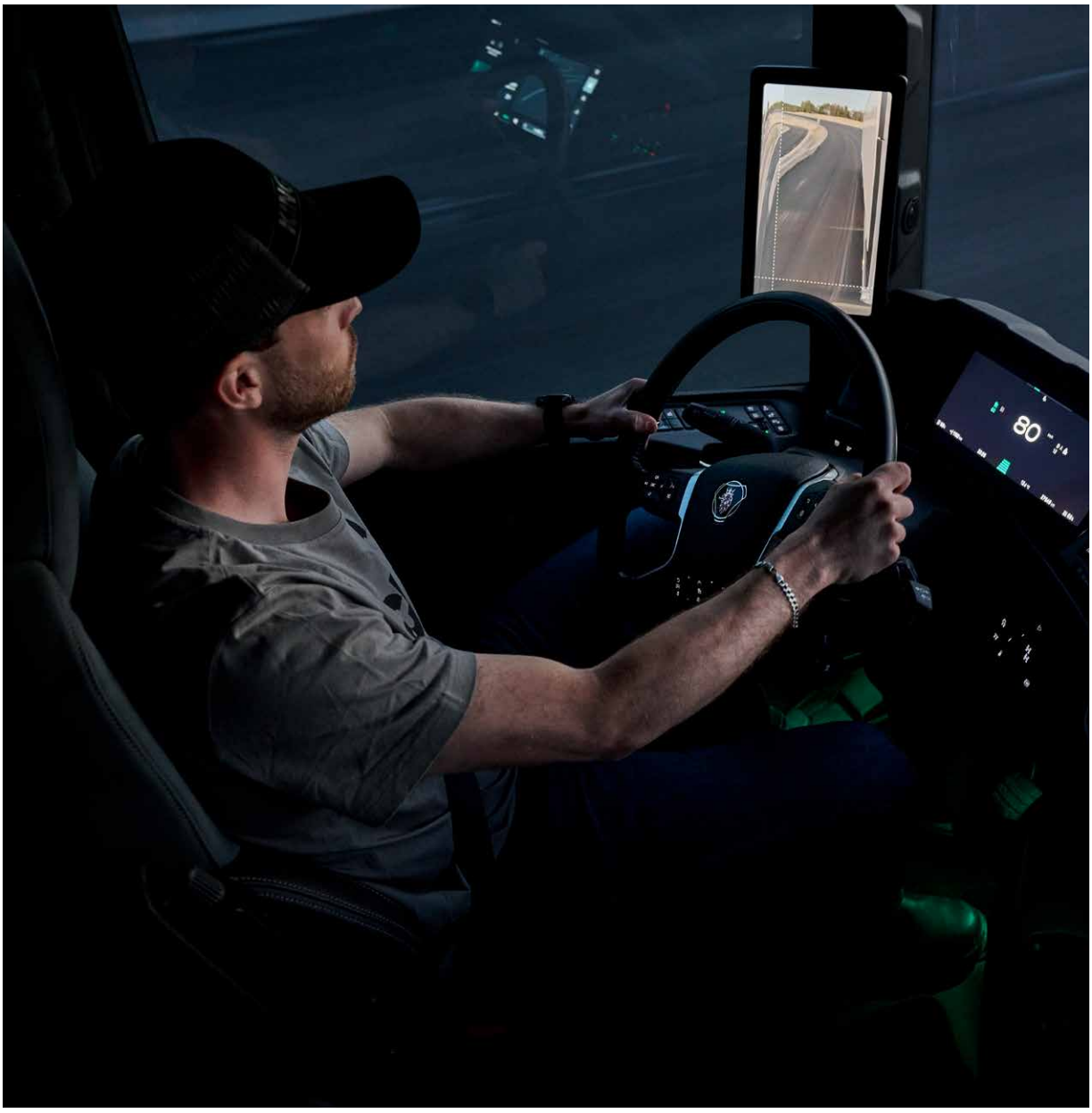
för autonoma system inom transport och annan reglerad verksamhet. Vinnova bör samordna arbetet genom *Testbädd Sverige* i nära samarbete med RISE. Försvarsmakten bör vara en viktig partner, tillsammans med Försvarets materielverk, Trafikverket, Transportstyrelsen, Energimyndigheten, lärosäten och näringslivet. Teknisk och regulatorisk testning bör ses som delar av samma innovationsprocess. Se även handlingspunkten om regulatoriska sandlådor nedan. EU-kommissionen beskriver uttryckligen *AI Factories* och *Testing and Experimentation Facilities* som kompletterande delar av det europeiska AI-ekosystemet.[66]

- **Säkerställ tillgång till svensk och europeisk lagrings- och beräkningskapacitet för känsliga data** genom att bygga ut kapaciteten för säker lagring och behandling av känsliga forsknings- och industridata och skapa tydliga vägar för hur denna kapacitet kan användas tillsammans med beräkningsresurser för mjukvara för kritiska fysiska system. Sverige bör samtidigt använda europeisk kapacitet där det är mer kostnadseffektivt eller strategiskt lämpligt. Målet är inte att Sverige ska vara självförsörjande på all beräkningskraft (det är varken realistiskt eller nödvändigt). Målet bör i stället vara strategisk handlingsfrihet. Sverige behöver ha egen kapacitet för känsliga och strategiskt viktiga användningsområden, samtidigt som vi drar nytta av den infrastruktur som redan finns i Europa. Vi kommer också under överskådlig tid att vara beroende av amerikanska digitala tjänster och bör kunna använda dem där det är ändamålsenligt. Parallellt behöver Sverige och Europa bygga upp egna alternativ, så att vi inte är helt beroende av en enskild leverantör eller region. Det skapar större motståndskraft och handlingsfrihet om förutsättningarna skulle förändras. Vetenskapsrådet/NAISS bör ha ansvar för samordning i samverkan med Sunet, RISE, Digg och relevanta myndigheter. Handlingspunkten ligger i linje med den utveckling som redan sker inom EuroHPC. Sverige har både Mimer och tillgång till europeiska system, medan den nya Mimer-infrastrukturen uttryckligen inkluderar storskalig lagring för känsliga data.[67] Till detta kommer dessutom privata initiativ som exempelvis Sferical AI.

På kort sikt bör Sverige kartlägga hur befintliga testbäddar tillsammans kan täcka hela kedjan från data och beräkning till utveckling, test och validering. Kartläggningen bör identifiera konkreta luckor snarare än utgå från att nya infrastrukturer behöver byggas. Dessutom bör en gemensam ingång till svensk infrastruktur för mjukvara för kritiska fysiska system utvecklas och en nationell plan tas fram för hur befintliga test- och demonstrationsmiljöer kan kopplas samman. Vinnova bör ansvara för kartläggningen av testbäddarna, medan Vetenskapsrådet/NAISS bör ansvara för den digitala infrastrukturen. Arbetet med att skapa en mötesarena för experter inom mjukvara för kritiska fysiska system samt med att använda EU:s konkurrenskraftskompass för att finansiera utveckling och uppskalning bör påbörjas genast.

66 EU. *AI talent, skills and literacy. Shaping Europe's digital future*. Webbsida: digital-strategy.ec.europa.eu/en/policies/ai-talent-skills-and-literacy? Information hämtad den 25 augusti 2026.

67 The European High Performance Computing Joint Undertaking (2025). *EuroHPC JU Signs Contract to Deploy a New AI-Optimised Supercomputer in Sweden*. Press release. 21 April 2026.



Inom två till tre år bör Sverige ha en sammanhängande modell där företag och forskare kan gå från tillgång till data och beräkningskraft till utveckling, testning och validering utan att behöva navigera mellan ett stort antal separata infrastrukturer. Ett nätverk av prioriterade testarenor bör vara etablerat, med särskild kapacitet för autonoma och säkerhetskritiska system.

Fram till 2035 bör kapaciteten skalas i takt med efterfrågan och utvecklingen inom mjukvara för kritiska fysiska system. Sverige bör samtidigt vara fullt integrerat i den europeiska infrastrukturen för AI-beräkning och använda både nationella resurser och EuroHPC:s *AI Factories* och *AI Gigafactories*.

Förslag: Gör regelverk och certifiering mer förutsägbara

Dagens regelverk och processer för provning, bedömning och certifiering är inte fullt anpassade till AI- och mjukvarubaserade system eller till en teknikutveckling som sker snabbare än regelverken hinner utvecklas. Ett problem är också att systemen utvecklas kontinuerligt under sin livstid. För företag kan det vara svårt att tidigt avgöra vilka krav som gäller, vilken myndighet som ansvarar och vilka tester och underlag som kommer att krävas. Problemet blir särskilt tydligt när mjukvara kombineras med fysisk utrustning och används i säkerhetskritiska miljöer, där flera regelverk och myndigheter kan vara relevanta samtidigt.

EU:s AI-förordning har nu börjat tillämpas, samtidigt som kraven för högrisk-AI införs stegvis. AI-förordningen ställer bland annat krav på riskhantering, datakvalitet, dokumentation, spårbarhet, mänsklig kontroll, robusthet och cybersäkerhet.[68]

Det europeiska regelverket är fortfarande under utveckling. Ett nytt regelverk trädde i kraft i juli 2026. Syftet är bland annat att minska den administrativa bördan för företag, ge mer tid för anpassning till vissa högriskkrav och öka möjligheterna till testning och experiment.[69] Det finns också ett europeiskt standardiseringsarbete där harmoniserade standarder ska översätta AI-förordningens övergripande krav till tekniska arbetssätt och därmed skapa större rättslig förutsägbarhet för företagen.[70]

Vi menar att Sverige inte bör försöka skapa ett eget certifieringssystem inom mjukvara för kritiska fysiska system. Däremot anser vi att den europeiska regleringen behöver bli enklare att förstå, tillämpa och testa i Sverige. Det behövs också bättre samordning mellan de myndigheter och standardiseringsorgan som företag möter.

Vårt förslag är därför att bygga en mer sammanhållen väg från utveckling och test till bedömning av överensstämmelse och marknad. Kraven bör så långt som möjligt vara risk- och funktionsbaserade och ge utrymme för teknisk utveckling, samtidigt som säkerhet och grundläggande rättigheter upprätthålls. Företag bör tidigt kunna få vägledning om vilka regelverk som är relevanta, vilka krav som gäller och hur de kan visa hur deras lösningar uppfyller kraven.

Konkreta handlingspunkter för att göra regelverk och certifiering mer förutsägbara för utveckling av mjukvara för kritiska fysiska system:

- **Skapa en gemensam ingång för företag som behöver regulatorisk vägledning** genom att utveckla en nationell funktion där företag tidigt kan få hjälp att identifiera vilka regelverk, myndigheter, standarder och bedömningsförfaranden som är relevanta för en produkt inom mjukvara för kritiska fysiska system. Funktionen bör särskilt rikta sig till mindre företag som saknar egen regulatorisk kompetens. Den bör också erbjuda praktisk vägledning om hur olika regelverk och standarder hänger ihop,

68 EU (2024). *The AI Act*. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.

69 EU (2026). *AI Omnibus enters into force*. Webbsida: digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force? Information hämtad den 25 augusti 2026.

70 EU (2026). *Standardisation of the AI Act*. Webbsida: digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation? Information hämtad den 25 augusti 2026.

vilka krav som gäller för olika typer av system, vilka dokument som behöver tas fram och hur företagen kan visa att kraven är uppfyllda. Det bör vara möjligt att få en första vägledning om exempelvis AI-förordningen, cybersäkerhetskrav, produktsäkerhet och sektorsspecifika regelverk innan företaget investerar i fullskalig utveckling och certifiering. Vägledningen bör särskilt fokusera på områden där flera regelverk överlappar, exempelvis autonoma fordon, robotik, industriella styrsystem och försvarsmateriel. Post- och telestyrelsen (PTS) bör vara ansvarig för samordning eftersom PTS enligt förslaget i den svenska AI-utredningen ska vara huvudansvarig för AI-förordningens marknadskontroll.[71] Berörda sektorsmyndigheter, Vinnova, RISE, Integritetsskyddsmyndigheten, Svenska institutet för standarder, ackrediterade organ och relevanta branschorganisationer bör medverka. Till exempel bör Transportstyrelsen ha en tydlig roll när systemen rör transportsektorns regelverk.

- **Etablera en nationell sandlåda inom mjukvara för kritiska fysiska system med sektorsspecifika spår.** Vi föreslår en regulatorisk sandlåda där företag kan utveckla och testa mjukvarulösningar för kritiska fysiska system under vägledning av berörda myndigheter. Sandlådan bör kunna fungera på en övergripande och generell nivå, men samtidigt ha särskilda spår för exempelvis transport och försvar. Syftet är att ge företag möjlighet att tidigt förstå hur reglerna ska tillämpas, identifiera hinder och samla erfarenheter som kan användas för framtida vägledning och regelutveckling. En viktig aspekt av denna handlingspunkt är att EU:s AI-förordning kräver att medlemsstaterna har minst en AI-regulatorisk sandlåda. Vi föreslår att PTS blir ansvarig för samordningen, i linje med den svenska AI-utredningens förslag. Flera aktörer behöver samverka kring detta, såsom RISE, Vinnova, sektorsmyndigheter och lärosäten.

- **Stärk Sveriges deltagande i utvecklingen av standarder som är relevanta för mjukvara för kritiska fysiska system** genom att öka svenska företags och myndigheters deltagande i det europeiska och internationella standardiseringsarbetet. Sverige bör särskilt prioritera standarder för riskhantering och för AI-systemens kvalitet och robusthet. EU-kommissionen framhåller att harmoniserade standarder är centrala för att skapa rättslig säkerhet och minska kostnaderna för efterlevnad. Standarderna är frivilliga, men kan ge företag viktig information när de har publicerats och hänvisats till i EU:s officiella tidning.[72] För Sverige är detta dessutom ett sätt att påverka regelverkets praktiska utformning snarare än att enbart anpassa sig till färdiga regler. Svenska institutet för standarder (SIS) bör samordna detta arbete i samverkan med PTS, RISE, Vinnova, berörda myndigheter, universitet och företag.

På kort sikt bör Sverige kartlägga var företag i dag möter de största regulatoriska flaskhalsarna och identifiera de vanligaste situationerna där flera regelverk eller myndigheter överlappar. Kartläggningen bör särskilt omfatta mjukvarubaserade produkter och system som används i säkerhetskritiska fysiska miljöer.

Inom två till tre år bör Sverige ha en fungerande modell där företag tidigt kan få besked om vilka regelverk som gäller. För mindre företag bör det finnas gemensamma verktyg, mallar och testmiljöer som minskar kostnaderna för att uppfylla kraven.

71 Statens offentliga utredningar (2025). *Anpassningar till AI-förordningen. Säker användning, effektiv kontroll och stöd för innovation* (SOU 2025:101).

72 EU. *Standardisation of the AI Act*. Webbsida: digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation? Information hämtad den 25 augusti 2026.



Fram till 2035 bör regelverket och standardiseringsarbetet utvecklas kontinuerligt i takt med tekniken. Aktörer i Sverige bör använda sina erfarenheter för att påverka EU:s vägledningar, standarder och framtida regelutveckling.

Vi vill understryka att förslaget inte syftar till att minska säkerhetskraven. I stället vill vi uppnå samma eller högre säkerhet med kortare, tydligare och mer förutsägbara vägar från utveckling till godkänd produkt.

Rekommendationer

Arbetsgruppen har tre sammanfattande rekommendationer om vad Sverige bör satsa på för att skapa svensk konkurrensförmåga, uppnå hållbarhet samt bidra till svensk och global säkerhet. Dessa baseras på en nulägesanalys av Sveriges position inom mjukvara för kritiska fysiska system, internationella utvecklingstrender samt en genomgång av nyckelfrågor som identifierar hinder och möjligheter för Sveriges fortsatta utveckling. De sammanfattar ett antal förslag och handlingspunkter som redovisas mer utförligt i rapporten.

- **Öka företagens omställningstakt** från traditionella produkter till lärande AI-system genom nya affärsmodeller, organisationsformer och utökat samarbete mellan olika aktörer. Dessutom behöver styrelse- och ledningskompetensen stärkas.

- **Bygg kompetens och erfarenhet för säkra kritiska fysiska system.** Anpassa utbildning och kompetensutveckling snabbare till industrins behov av säker och tillförlitlig mjukvara.

- **Korta vägen från utveckling till marknad.** Skapa arenor för att utveckla, testa och validera mjukvara i realistiska miljöer i samverkan mellan företag, akademi och offentlig sektor.

Appendix



Referenser

AI-kommissionen. (2025). *AI-kommissionens Färdplan för Sverige* (SOU 2025:12).

André, C. and M. Pak (2021), *Regional differences in productivity in Sweden: Insights from OECD regions*, OECD Economics Department Working Papers, No. 1688, OECD Publishing, Paris.

Avizienis, A. et al. (2004). *Basic concepts and taxonomy of dependable and secure computing*. IEEE Transactions on Dependable and Secure Computing, 1(1), 11–33.

Burr, W. (2026). *Competence building in software technologies: The case of the German automotive industry*. Technology Analysis & Strategic Management, 38(1), 96–108.

Cybersecurity and Infrastructure Security Agency, Defense Advanced Research Projects Agency, Office of the Under Secretary of Defense for Research and Engineering, & National Security Agency. (2025). *Closing the software understanding gap*. U.S. Department of Homeland Security.

Deutsche Presse-Agentur. (2026, 1 oktober). *Kreise: VW-Softwaretochter steht vor weiterem Stellenabbau*. WELT.

EU (2024). *The AI Act*. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.

EU. *Shaping and strengthening European AI talent*. Webbsida: digital-strategy.ec.europa.eu/en/library/shaping-and-strengthening-european-ai-talent. Information hämtad den 25 augusti 2026.

EU (2026). *AI Omnibus enters into force*. Webbsida: digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force? Information hämtad den 25 augusti 2026.

EU (2026). *Standardisation of the AI Act*. Webbsida: digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation? Information hämtad den 25 augusti 2026.

European Commission (2025). *A Competitiveness Compass for the EU*. Brussels, 29.1.2025.

Humayed, A. et al. (2017). *Cyber-Physical Systems Security—A Survey*. IEEE Internet of Things Journal, 4(6), 1802–1831.

ISO. (2018). *ISO 26262: Road vehicles – Functional safety*. International Organization for Standardization.

IVA (2025). Sveriges position inom strategiskt viktiga tekniker. Investeringsprioriteringar, styrkor och utmaningar.

IVA (2026). *Avancerad produktion – En teknikrapport inom Svenska framtider om komplex diskret produktion*.

IVA. (2026). *AI-drivna cyberhot: De kommande tolv månaderna*.

Kagermann, H., et al. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry*. Forschungsunion & acatech.

Karlzén, H., et al. (2024). *Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder* (FOI-R--5691--SE).

Koopman, P., & Wagner, M. (2017). *Autonomous vehicle safety: An interdisciplinary challenge*. IEEE Intelligent Transportation Systems Magazine, 9(1), 90–96.

Kopetz, H. (2011). *Real-time systems: Design principles for distributed embedded applications* (2nd ed.). Springer.

Lee, E. A. (2008). *Cyber physical systems: Design challenges* (Technical Report No. UCB/EECS-2008-8). University of California, Berkeley.

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.

Military Watch Magazine. (2025). *US failed upgrades: F-35 software and modernization problems*.

Ministry of Defence. *PYRAMID: Rapid adaptability for avionics systems*. GOV.UK. Webbsida: www.gov.uk/guidance/pyramid-rapid-adaptability-for-avionics-systems. Information hämtad den 7 oktober, 2026.

Ministry of Defence. (2025). *The Strategic Defence Review 2025: Making Britain safer, secure at home, strong abroad*. Policy paper. GOV.UK.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1.

OECD (2023), *OECD Reviews of Innovation Policy: Korea 2023*, OECD Publishing.

OECD. (2024). *OECD Digital Economy Outlook 2024*. OECD Publishing.

OECD (2025), *Trends Shaping Education 2025*, OECD Publishing.

OECD. (2025). *OECD Economic Surveys: Germany 2025*. OECD Publishing.

OECD. (2025). *OECD economic surveys: Israel 2025*. OECD Publishing.

OECD (2026), *Korea's Smart Manufacturing Innovation Initiative*. OECD Publishing.

OECD (2026), *Incubation in Entrepreneurial Ecosystems: Hatching Growth, OECD Studies on SMEs and Entrepreneurship*, OECD Publishing.

Radio Technical Commission for Aeronautics. *Software Considerations in Airborne Systems and Equipment Certification*. RTCA DO-178C.

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). *Cyber-physical systems: The next computing revolution*. Proceedings of the IEEE, 98(8), 1305–1320.

Regeringen (2024). *Forskning och innovation för framtid, nyfikenhet och nytta* (prop. 2024/25:60).

Regeringen (2025) *Regleringsbrev för budgetåret 2026 avseende Verket för innovationssystem*. (KN2025/02359, delvis, KN2025/02393).

Regeringen (2026). *Ett utbildningsutbud av hög kvalitet som är relevant för arbetsmarknadens och samhällets behov. Kommittédirektiv* (dir. 2026:82).

Regeringen (2026). *Stor satsning moderniserar Försvarsmaktens krigföring*. Pressmeddelande publicerat 18 juni 2026.

Regeringen (2026). *Sverige och EU tar första steg mot AI-gigafabriker*. Pressmeddelande publicerat 30 juli 2026.

Regeringen (2026). *Uppdrag om stärkt försvarsinnovation och snabb anpassning* (Fö2025/01745). Publicerat 20 juli 2026.

Regeringen (2026). *Uppdrag till Tillväxtverket och Verket för innovationssystem att utreda kapitalförsörjning av kunskapsintensiva företag* (KN2026/01433). Publicerat 29 juni 2026.

Regeringskansliet (2025). *En STEM-strategi för Sverige*. Utbildningsdepartementet. Publicerad 24 februari 2025.

Regeringskansliet (2025). *STEM-delegationen*. Dir. 2025:11.

Regeringskansliet (2025). *Sveriges digitaliseringsstrategi 2025–2030*.

Regeringskansliet. (2026). *Handlingsplan för Sveriges AI-strategi*.

Regeringskansliet (2026). *Sveriges AI-strategi*. Finansdepartementet. Publicerad 20 februari 2026.

Regeringskansliet (2026). *Fler civilingenjörer ska ta examen – nya uppdrag till lärosäten*. Pressmeddelande från Utbildningsdepartementet. Publicerad 15 juni 2026.

Rumez, M., et al (2020), *An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures*, IEEE Access, vol. 8, pp. 221852-221870.

Secretary of State for Science, Innovation and Technology (2025). *AI Opportunities Action Plan*.

Sgobba, T. (2019). *B-737 MAX and the crash of the regulatory system*. Journal of Space Safety Engineering, 6(4), 299–303.

Staatssekretariat für Bildung, Forschung und Innovation. *Höhere Fachschulen*. Länk: www.sbfi.admin.ch/de/hoehere-fachschulen Information hämtad den 5 oktober, 2026.

Statens offentliga utredningar (2025). *Anpassningar till AI-förordningen. Säker användning, effektiv kontroll och stöd för innovation* (SOU 2025:101).

The European High Performance Computing Joint Undertaking (2025). *EuroHPC JU Signs Contract to Deploy a New AI-Optimised Supercomputer in Sweden*. Pressmeddelande publicerat 21 april 2026.

Transportstyrelsen. (2014). *Autonom körning – Förstudie* (Dnr: TSG 2014–1316).

Transportstyrelsen. (2025). *Förslag till en nationell trafikregleringsmodell – säker användning av automatiserade fordon* (Dnr: TSV 2025–12812).

UN Regulation No. 155 – Cyber security and cyber security management system.

UN Regulation No. 156 – Software update and software update management system.

Vinnova (2026). *Strategiska innovationsprogram. En metastudie av 17 nioårsutvärderingar*. VR:2026:13. Författare: Mona Hallström Hjort et al, Sweco.

Wang, D. (2023). *China's hidden tech revolution: How Beijing threatens U.S. dominance*. Foreign Affairs, 102(2), 66–75.

Xu, L. et al. (2018). *Industry 4.0: State of the art and future trends*. International Journal of Production Research. 56(8). 2941–2962.

Ordlista

Autonoma transportsystem

Lösningar där fordon (till exempel bilar, bussar eller drönare) kan navigera och fatta beslut utan att en förare behöver kontrollera varje moment.

Cybersäkerhet

Arbete med att skydda datorer, program, nätverk och information mot digitala angrepp, obehörig åtkomst och andra hot.

DARPA

Förkortning för *Defense Advanced Research Projects Agency*. DARPA är en amerikansk myndighet som finansierar forskning och utveckling av ny teknik för försvarsändamål. DARPA arbetar med tidsbegränsade forskningsprogram där forskare, företag och andra aktörer samlas kring konkreta tekniska problem och projekt med hög teknisk risk.

GPU

Förkortning för *Graphics Processing Unit*. GPU är en processor som är särskilt bra på att utföra många beräkningar parallellt och därför används bland annat för att utveckla och köra AI.

Inbäddad (eng. embedded)

Begreppet används traditionellt för mjukvara som är integrerad direkt i en fysisk produkt, exempelvis i ett fordon eller ett industrisystem.

Interoperabilitet

Förmågan hos olika system och program att utbyta information och fungera tillsammans.

Kod

Instruktioner skrivna i ett programmeringsspråk som talar om för en dator vad den ska göra och hur ett program eller system ska fungera. Kod är en del av mjukvaran.

Mjukvara (eng. software)

Program och system som består av kod och som kan köras på en dator eller annan digital enhet. Mjukvara omfattar exempelvis operativsystem, applikationer, skript och drivrutiner och kan även innehålla data och inställningar.

NAISS

Förkortning för Nationell akademisk infrastruktur för superdatorer i Sverige. NAISS är en nationell akademisk infrastruktur för superdatorer som tillhandahåller storskaliga beräkningsresurser, lagring samt datatjänster för akademiska användare.

NIST

Förkortning för det amerikanska institutet *The National Institute of Standards and Technology*.



Sferical AI

Sferical AI har grundats av AstraZeneca, Ericsson, Saab, SEB och Wallenberg Investments. Företaget bygger upp en svensk plattform för AI-beräkningar som ska ge företag säker tillgång till kraftfull datorkapacitet för att utveckla och använda AI.

STEM

Förkortning för *science, technology, engineering, mathematics*. På svenska motsvarar det ungefär vetenskap, teknik, problemlösning och matematik.

WASP

Förkortning för *Wallenberg AI, Autonomous Systems and Software Program*. WASP är ett svenskt forskningsprogram som utvecklar forskning och kompetens inom AI, autonoma system och mjukvara.

Kungl. Ingenjörsvetenskapsakademien är en fristående akademi med uppgift att främja tekniska och ekonomiska vetenskaper samt näringslivets utveckling. I samarbete med näringsliv och högskola initierar och föreslår IVA åtgärder som stärker Sveriges konkurrenskraft.

Utgivare: Kungl. Ingenjörsvetenskapsakademien (IVA), 2026
Box 5073, SE-102 42 Stockholm
Telefon: 08-791 29 00

IVA-R 546
ISSN: 1100-5645
ISBN: 978-91-89181-93-9

Författare: Arbetsgruppen i samverkan med Charlotte Hall
Redaktör: Charlotte Hall
Projektledning: Lisa Thelin, IVA
Fotografier: Unsplash (s. 1), Volvo Group (s. 4, 6, 14, 18, 21), Gustav Lindh, Scania CV AB (s. 8), Volvo Cars (s. 10, 23, 24, 31, 51, 57), Dan Boman, Scania CV AB (s. 26, 48), Saab AB (s. 27, 33, 43, 52)
Grafisk form: Pelle Isaksson, IVA

Denna rapport finns att ladda ned på www.iva.se.

IVAs visionsprojekt **Svenska framtider** ska resultera i en väl förankrad och tydlig vision för Sverige som ledande teknik- och innovationsland år 2035 – med fokus på konkurrenskraft, hållbarhet och säkerhet.

Kungl. IngenjörsVetenskaps Akademien