

IVA | Swedish Futures

Safety-critical software

A technical report about software for critical physical systems as part of the *Swedish Futures* series

Contents

Foreword 4

Summary 6

Starting points for work on software for critical physical systems 8

- Definition and scope 9
- Reasons for prioritising a technology report on software for critical physical systems 11

Software for critical physical systems today 12

- Software that controls the physical world 13
- Regulatory frameworks 16
- International perspective 18

Developments in software for critical physical systems 22

Key issues for software in critical physical systems 25

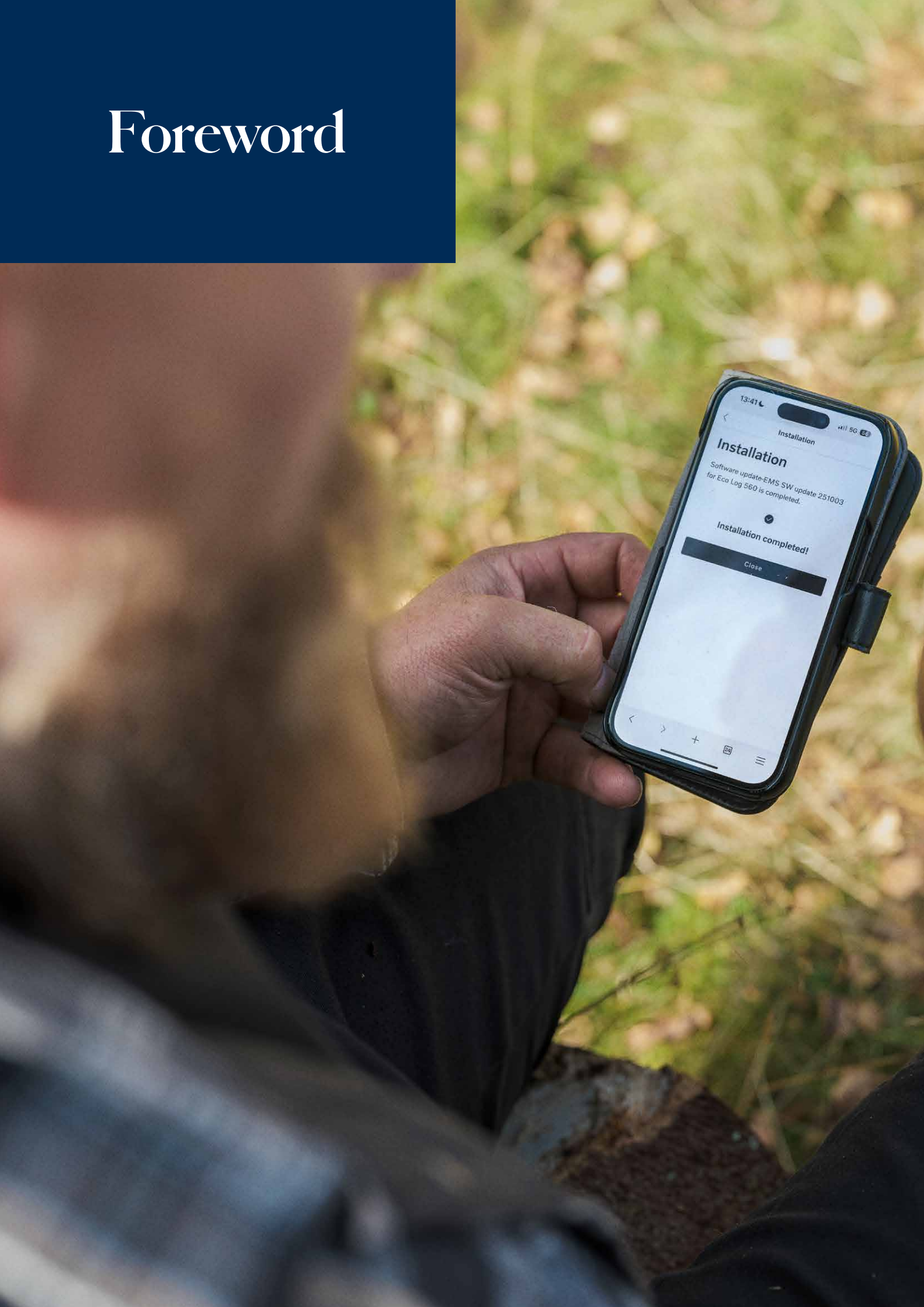
Desired future direction 31

- Vision 32
- Five proposals for the development of software for critical physical systems in Sweden 34
- Recommendations 49

Appendix 50

- References 51
- Glossary 54

Foreword


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

IVA is spearheading the *Swedish Futures* initiative to formulate a vision for Sweden as a leader in technology and innovation by 2035. Since autumn 2025, *Swedish Futures* has brought together stakeholders from academia, industry, and the public sector to identify opportunities, challenges and strategic directions for competitiveness and sustainable development.

Among other things, the initiative convenes working groups that quickly and systematically analyse challenges and opportunities in different technology areas and produce highly focused reports. These reports provide an overview of the status quo and outlook for the field under examination and present concrete proposals for action. They also serve as an important foundation for shaping an overarching vision for Sweden in 2035.

This report was produced by the working group on software for critical physical systems. The group's analysis reveals both issues and opportunities where Sweden can strengthen its competitiveness by translating industrial strength and technological excellence into secure and scalable solutions for a growing market.

As with all IVA projects, the participants have contributed in their personal capacity and not as representatives of the organisations in which they work. The report's analyses and recommendations are largely based on discussions within the working group, as well as on the experience and knowledge contributed by its members. The working group stands behind the report in its entirety, but this does not mean that all members necessarily endorse every formulation.

The working group on software for critical physical systems was active from April through October 2026.

Working group

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

Support for the working group

Lisa Thelin, project manager
Charlotte Hall, writer

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 lifecycle.

AI is also changing how software and products are developed. It can be used to develop software and also 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 reliant on hardware design alone and increasingly depend on software for their functions and ongoing development, companies need to adapt their working methods. Development cycles need to be shorter, allowing new solutions to be tested and feedback gathered at an early stage. 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.

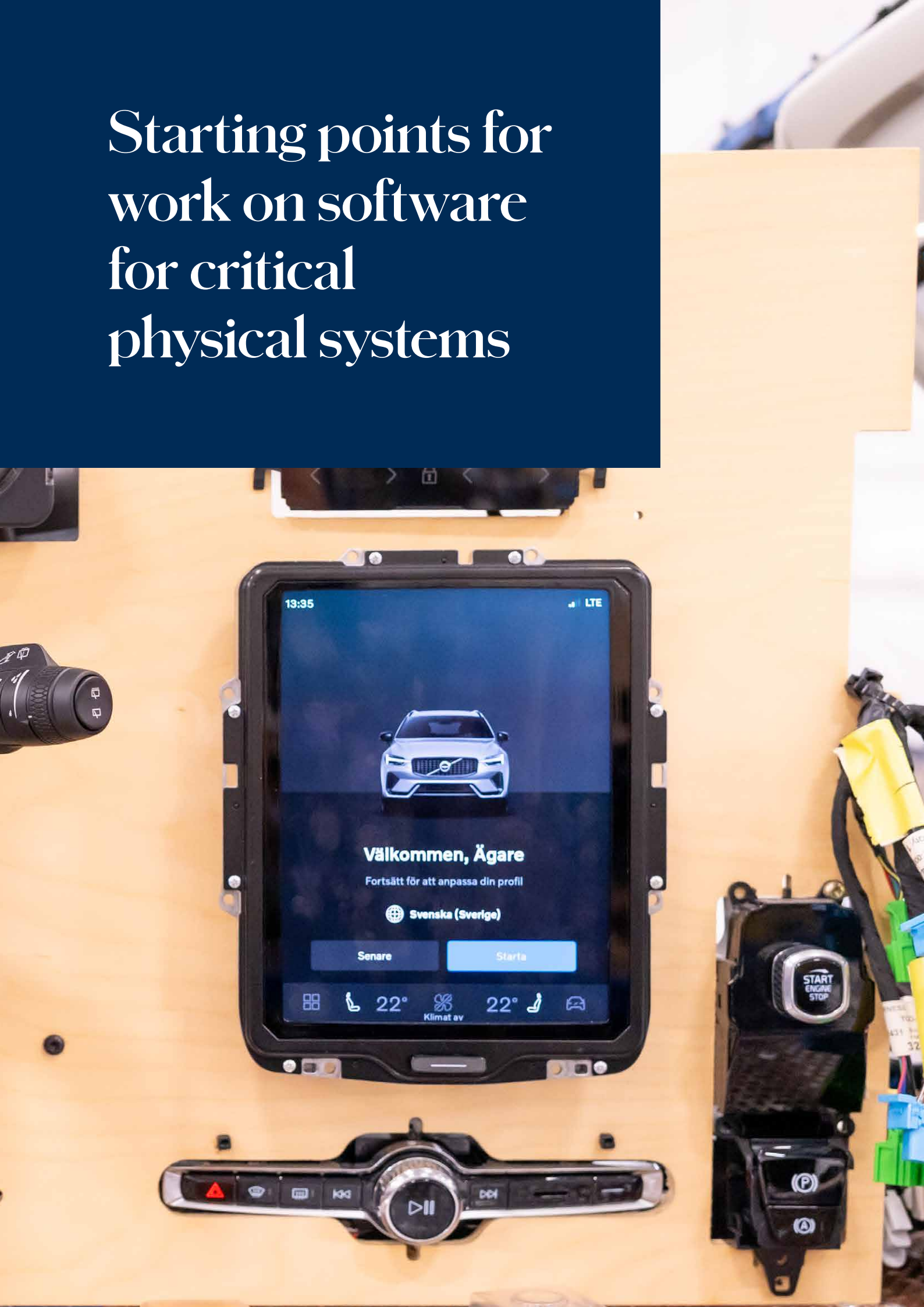
The working group presents three overarching recommendations on where Sweden should focus its efforts to strengthen Swedish competitiveness, achieve sustainability and contribute to security in Sweden and globally. These recommendations are based on an analysis of Sweden's current position in software 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 companies' transition** from traditional products to AI-enabled, learning systems through new business models, organisational structures and stronger collaboration between stakeholders. Strengthen expertise at board and senior management level.

- **Build expertise and experience in securing critical physical systems.** Adapt education and skills development more rapidly to meet industry's need for secure and reliable software.

- **Shorten the path from development to market.** Create platforms for developing, testing and validating software in realistic environments through collaboration between industry, academia and the public sector.

Starting points for work on software for critical physical systems



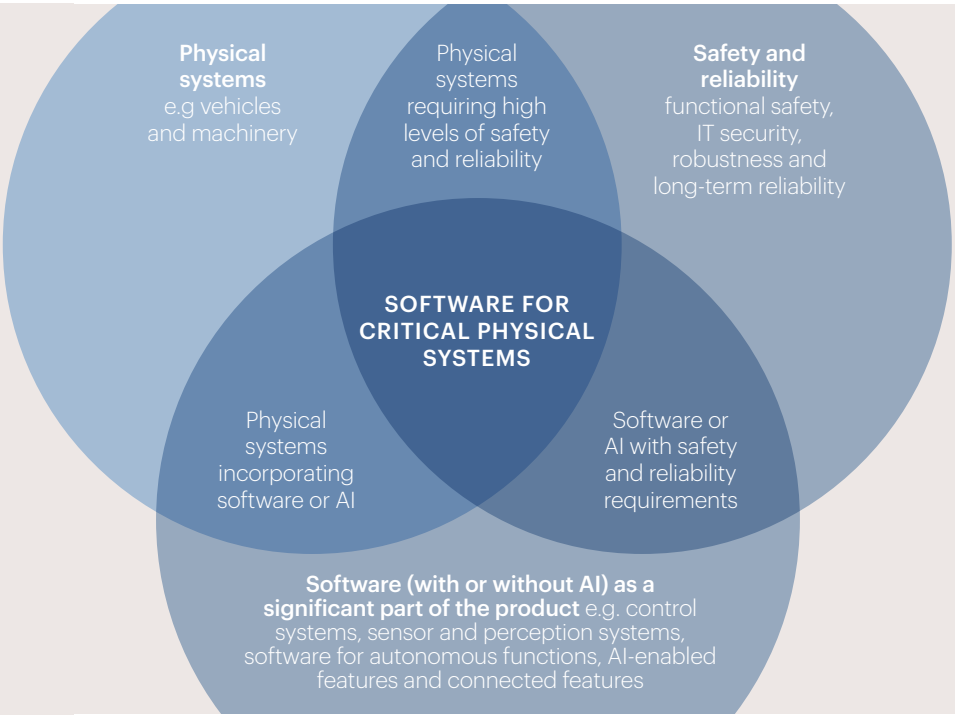


FIGURE 1: Description of software for critical physical systems.

Definition and scope

This report uses the term *"software for critical physical systems"*. Software refers to programmes and other instructions that run on a computer, such as operating systems, applications, scripts and drivers.[1] According to the Dataterm Group, software can also be defined as data in the form of instructions that a computer can interpret and execute.

In critical physical systems, safety and reliability are crucial. Examples of such systems include aeroplanes, robots, lorries, cars, drones, boats and construction machinery.

In this report, we have limited our scope to physical systems where embedded software and/or AI constitute a significant part of the product itself.

The report covers both functional safety and IT security. However, medical technology applications are not included.

Software for critical physical systems encompasses not only finished systems, but also the software and tools used to develop them. As AI and other advanced software play an increasingly significant role in the development, programming and testing of these systems, requirements for safety and reliability must be considered throughout the entire process, from development and testing to operation and updating. The increasing use of AI in software development is transforming the development process. Parts of the programming work can be automated, for example through AI-generated code, which can make the work considerably faster. Previously, programming and changes

1 Computer Sweden. IT terms.

TABLE 1: IVA's selection of topics for technical reports is based on eight criteria.

CRITERION	SOFTWARE FOR CRITICAL PHYSICAL SYSTEMS IN SWEDEN
Global Leadership	Sweden can become a world leader in a number of areas where embedded software or AI constitutes a significant part of physical products and where there is a high demand for security and reliability.
Turnaround (opportunity to reverse current trends)	Sweden has the opportunity to move from strong but scattered expertise to a more consolidated capability in developing, testing and using software for critical physical systems.
Positional shift	As software accounts for an increasing share of a vehicle, machine or defence system, it also changes how the product functions and how value is created.
Enabling technology	Embedded software and AI are becoming central to how physical products function, are controlled and monitored. In critical systems, the software must be secure and reliable while also allowing for updates over the long term.
International dimension	Sweden's strong export industry in sectors such as automotive, aviation, defence and space provides a solid foundation for developing and selling products in which software for critical physical systems makes up a significant part of the product.
Megatrends	Automation, electrification and greater autonomy mean that an increasing number of physical products rely on advanced software in their core functions.
Geopolitics	Growing dependence on foreign technology makes the ability to develop, control and secure software for critical physical systems vital to Sweden's security and technological autonomy.
Hot topic	Software is becoming increasingly important for industrial competitiveness as physical products become more software-controlled and autonomous.

to the software were largely the responsibility of specialist programmers and systems developers. AI-based tools enable, for example, engineers and others working with the products and systems in which the software is embedded to write and modify code themselves to a greater extent. For software that controls physical systems, this means that changes to safety-critical software can be implemented more quickly and by people in different professional roles. This places new demands on how security is managed, controlled and verified throughout the entire development process.

The term "embedded" is traditionally used for software that is integrated directly into a physical product, such as a vehicle or an industrial system. For the purposes of this definition, however, the location of the software is not decisive, but rather the role it plays in the physical system. Today's physical products often rely on software and services beyond the product itself, such as cloud infrastructure. Functionality may therefore be distributed between the physical product, the software within the product and external digital services.

Reasons for prioritising a technology report on software for critical physical systems

IVA has carried out a data-driven analysis of patents, scientific publications, and startup investments to map Sweden's global position within 48 strategically important technology areas that are of great significance to the country's future prosperity, economic resilience and national security.[2]

Among other things, the analysis revealed that Sweden needs to adopt a more strategic approach to secure its position internationally. Against this backdrop, IVA decided to conduct an in-depth analysis of software for critical physical systems and to draw up proposals for the desired future direction in this area. The selection is based on eight criteria; see Table 1.

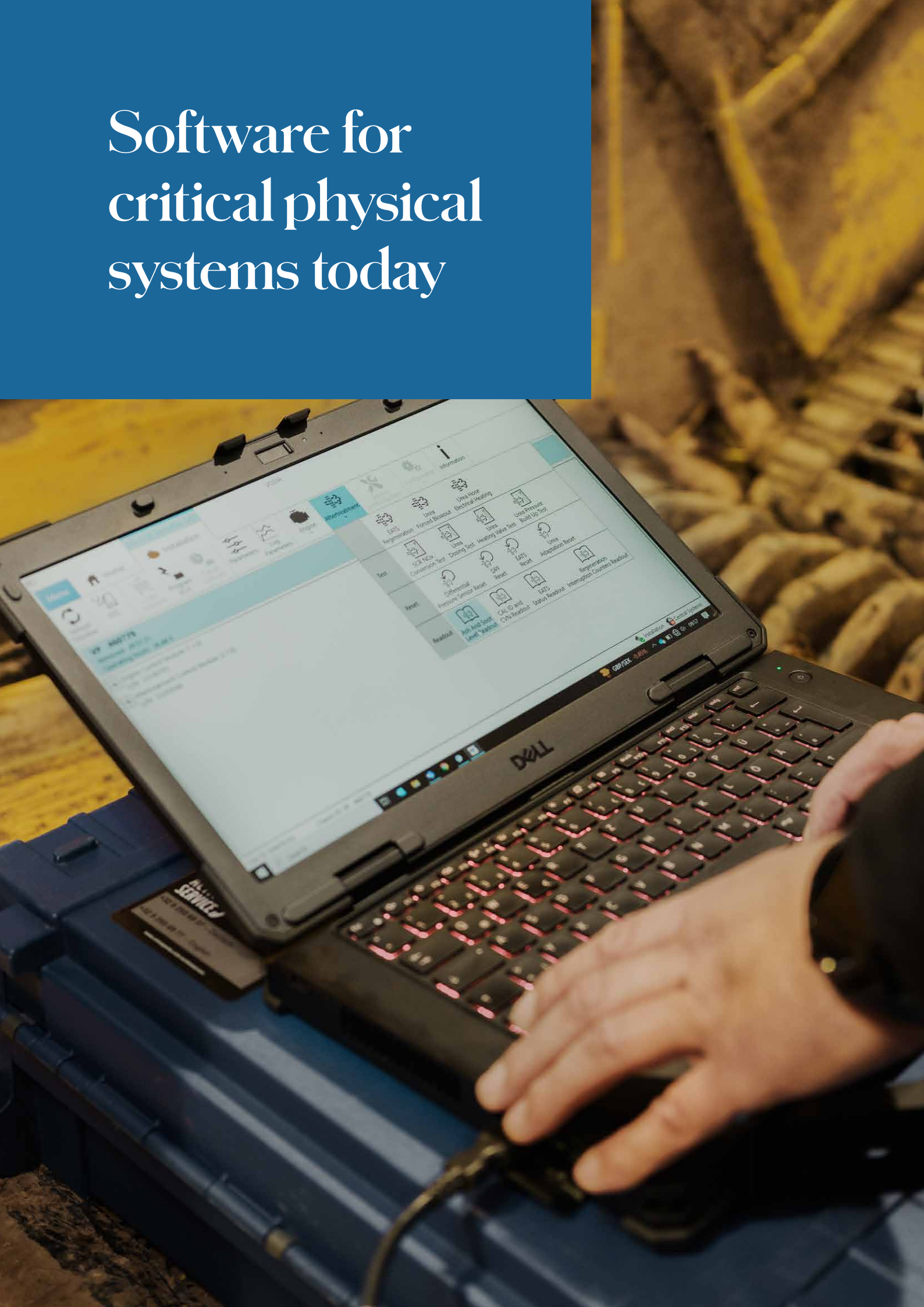
Swedish industrial exports are strong in sectors such as vehicles, machinery, aviation, defence systems and space products. These sectors are now undergoing rapid change, with software increasingly determining how the systems function, how secure they are and what value they create. This means that software is taking over functions previously performed by mechanical and electronic components.

Software for critical systems must meet very different requirements from software used in ordinary consumer services. It must be able to withstand failures, disruptions and attacks. It must not pose a risk of physical harm to equipment or people and must remain reliable over long periods and accommodate ongoing updates without compromising security.

New ways of working – such as fragmented development chains, staged software delivery and more AI-generated code – make it more difficult to maintain full control and traceability throughout the development process. Sweden possesses strong expertise in both industry and technology but lacks a coordinated approach to developing secure and reliable software for this type of critical system. An important part of such an approach is to create strategic freedom of action so that Sweden can maintain control over critical areas where security, data or critical dependencies must be considered. In other areas, it may be possible to use European and commercial solutions to benefit from greater scale and faster development.

2 IVA (2025). *Sweden's position in strategically important technologies. Investment priorities, strengths and challenges.*

Software for critical physical systems today



Software that controls the physical world

Software for critical physical systems controls, monitors or influences technical systems where the software's operation has direct consequences in the physical world. In traditional information systems, a fault may lead to information being lost or functionality being restricted. However, a fault in a critical physical system can cause physical damage, affect people's safety or disrupt functions vital to society. Examples of such systems can be found in the transport sector, where software is now an integral part of aeroplanes, cars, lorries, trains and autonomous transport systems. Other examples can be found in the energy sector and in industrial applications. The term "cyber-physical systems" is used to describe technical systems in which software, computers and physical equipment interact to monitor, analyse and control various processes in the real, physical world.[3] These systems use sensors to collect information from the environment, process this information using software, and then influence the physical world through various control functions. The software forms the logical core of these systems by collecting information from the environment, analysing the system's state and generating control signals that influence the physical process. In a modern vehicle, for example, sensors can measure speed, position, surrounding traffic and the vehicle's technical status. The software processes this information to control functions such as the braking system, the powertrain, battery management or automated driving functions. Similarly, software controls key functions in aeroplanes, railway systems and industrial processes.[4] With the help of AI, modern systems can understand their surroundings, anticipate what might happen and act accordingly. For example, a self-driving car can detect other road users, assess how they might move and adapt its driving.

Software consists of instructions, logic and models that specify how a computer system should process information and perform various tasks. In traditional IT systems, software is primarily used to manage information, communication and administrative functions. In critical physical systems, however, the software has a direct impact on the physical world by controlling and monitoring technical processes. This means that the software must not only produce the correct results but also do so at the right time and under conditions where errors could have serious consequences. Consequently, particularly high standards are set for how such software is developed, tested and verified to ensure that the systems operate reliably throughout their entire lifecycle.[5]

Errors in a critical system have serious consequences

A system is considered critical if a fault could have serious consequences for people, the environment, the economy or functions vital to society. Consequently, specific requirements are imposed on how the system is developed, tested, monitored and maintained throughout its entire lifecycle. Critical systems must be secure, reliable and available. They must also be able to handle disruptions and faults in a controlled manner. In safety-critical applications, it is particularly important that the system can prevent dangerous situations or limit the consequences when a component or software function does not operate as intended.

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 IS TRANSFORMING THE LANDSCAPE OF SOFTWARE DEVELOPMENT

AI is already being used in the development of software for critical physical systems. For example, it can help to write and review code, find errors, create tests and document the work. Development has progressed rapidly in a short space of time, and in just a few years AI has become an established tool in software development.

AI is also becoming an increasingly important part of the products themselves. In vehicles, robots and other physical systems, AI can, for example, be used to interpret information from the environment, make decisions and control the system's functions. This can be described as AI in physical systems, or *"physical AI"*. This means that the software's ability to perceive and act in the physical world is becoming an increasingly important part of product development.

AI is changing not only individual tasks but also development itself. Some of this work can be carried out in a faster and more automated manner, giving developers more time for problem-solving, architecture and other tasks that require experience and judgement. It is also becoming easier to test different solutions and move quickly from idea to testing and further development.

For companies, this presents opportunities to increase the pace of development and utilise skills and resources in a different way. It also requires new ways of working and new skills. Companies need to understand how AI can be used in development and how the results should be reviewed, tested and followed up.

This is particularly important for critical physical systems. AI can make mistakes, which means that code or other solutions developed with the help of AI must be thoroughly checked and tested before being put to use. Clear procedures are also needed to document how the software has been developed and how changes have been made.

AI is therefore changing the conditions for the entire software development process. Developers' work is changing, companies need to adapt their working methods, and the requirements for control, testing and accountability are becoming a key part of the new development process.

Reliability is therefore not merely about the system functioning under normal conditions, but also about its ability to detect faults, adapt to disruptions and return to a safe state.[6]

For safety-critical systems, it is not enough to demonstrate that the software works in a range of test cases. Developers must also be able to demonstrate that the system meets defined safety requirements throughout its entire lifecycle. This requires systematic approaches for requirements management, risk analysis, verification and validation. In the automotive industry, for example, standards are used to structure work on functional safety in electrical and electronic systems.[7] Similar principles are applied in other areas where software faults can affect people's safety.

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.

Decisions must be both correct and timely

An important difference between critical physical systems and many other technical systems is that they must be able to respond quickly and predictably. In these systems, it is not only important that a decision is correct, but also that it is made at the right time. For example, a vehicle's braking system, an aeroplane's flight control system or an industrial control system must be able to react within defined time limits in order to maintain safety. A correct decision can still lead to serious consequences if it is made too late. Consequently, specific requirements are placed on the software used in these systems. It must ensure that the correct function is performed, that the result is accurate, and that the function is executed within the time required for the system to operate safely.[8]

Software for critical physical systems thus differs in several crucial ways from other software. First, there is a direct link between the software's behaviour and physical safety. Second, a high degree of predictability is required, as the system's behaviour must be analysable, verifiable and, in many cases, guaranteed. Third, development must rely on methods capable of handling highly complex systems with a long economic lifespan and numerous interdependencies between different components.[9]

Software controls many systems in today's vehicles

This trend is particularly evident in the automotive industry, where modern cars and lorries have become advanced technical systems that are largely controlled by software. Today, software controls everything from powertrains and energy consumption to safety features, driver assistance and connected services. The vehicle has thus evolved from being primarily a mechanical structure to becoming a complex system in which software plays a central role in its function, performance and safety. The increasing volume and complexity of software present new challenges in terms of development, testing, verification and long-term maintenance.[10] For autonomous vehicles, the challenges are even greater, as the software must be able to interpret a complex environment, make decisions and act safely in situations that cannot always be foreseen in advance.[11]

Autonomous transport systems clearly illustrate the difference between "ordinary" software and software for critical physical systems. A traditional computer programme can often be corrected once a fault has been detected, whereas an autonomous vehicle must be able to make safe decisions in real time without human intervention. This requires new methods of verification and validation, combining simulation, model-based development and formal analysis methods with extensive testing in real-world environments. The Swedish Transport Agency has highlighted that autonomous vehicles entail new requirements for safety,

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.



legal liabilities and technical development within the transport system.[12, 13]

Both technology and organisation are important

In addition to functional safety requirements, cyber security is increasingly important as critical physical systems become more connected and dependent on digital communication. Modern vehicles and transport systems exchange information with external services, other vehicles and digital infrastructure, creating new opportunities for more efficient and automated functions, but also new vulnerabilities. An attack on a connected physical system can have consequences that extend beyond the digital environment and affect the physical world. Therefore, software security must be managed from a holistic perspective that takes into account both technical solutions and organisational factors. Development processes, expertise and a strong security culture are crucial to developing and maintaining software that is robust and resilient to faults and attacks.[14]

Regulatory frameworks

Regulatory frameworks that aim to reduce security risks

The regulatory requirements for software in critical physical systems vary between sectors. This involves a combination of European regulations, Swedish laws, regulatory requirements and international standards. What they all have in common

12 Swedish Transport Agency. (2014). *Autonomous driving – Preliminary study* (Ref. No.: TSG 2014–1316).

13 Swedish Transport Agency. (2025). *Proposal for a national traffic regulation model – safe use of automated vehicles* (Ref. No.: TSV 2025–12812).

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

is that they are intended to ensure that systems are developed, tested and maintained in a way that minimises the risk of faults that could affect people's safety, critical societal functions or physical infrastructure.

A key principle is that security must be managed throughout the system's entire lifecycle, from the initial requirements and technical design through to testing, operation and maintenance. Standards are therefore used across various sectors to support secure development, such as ISO 26262 in the automotive sector and equivalent standards in the aviation and rail sectors.

Cybersecurity requirements are growing

As critical physical systems become increasingly connected and dependent on digital communication, the demands on cyber security are growing.

The EU requires organisations operating in sectors critical to society to work systematically with cyber security, risk management and incident reporting.[15] In Sweden, these requirements are implemented through the Cybersecurity Act (2025:1506). Organisations critical to Sweden's security are also subject to the Security Protection Act (2018:585), which sets out requirements for the protection of sensitive information, technical systems and critical functions.

The development of connected products is also influenced by new EU regulations, such as the Cyber Resilience Regulation.[16] This regulation requires manufacturers to take greater responsibility for developing secure products, managing vulnerabilities and ensuring that security updates can be implemented throughout the product's lifecycle.

Requirements in the transport, industrial and defence sectors

The transport sector is an area where the requirements for secure software are particularly high, as faults can have direct consequences for people's safety. For road vehicles, EU type-approval rules regulate safety requirements.[17] For modern connected vehicles, these requirements are supplemented by international regulations, for example on cyber security[18] and on the management of software updates.[19]

In the aviation, rail and industrial sectors, too, there are high standards requiring that safety-critical systems be developed and monitored in a structured manner. In Sweden, the Swedish Transport Agency is responsible for supervision and regulations across several transport sectors. The defence sector imposes similarly high standards of robustness and reliability, as systems must be able to function even in the event of disruptions, attacks and adverse conditions. The Security Protection Act regulates activities where the protection of sensitive systems and information is crucial and is supplemented by defence-specific requirements in areas such as system security and information security.

15 NIS 2 Directive (EU) 2022/2555.

16 Cyber Resilience Regulation (EU) 2024/2847.

17 Including Regulation (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.

Protection of people and safe use

In addition to requirements concerning technical functionality and cyber security, there are regulatory frameworks that focus on protecting people who use or are affected by technical systems. The Work Environment Act (1977:1160) requires employers to prevent risks and ensure that technical systems and work equipment are used safely. For machinery and industrial systems, this is supplemented by the Swedish Work Environment Authority's regulations and the EU Machinery Regulation (EU) 2023/1230, which require that machinery and its control systems be safe and reliable.

A common feature of these regulatory frameworks is that safety cannot be treated as an afterthought but must be built in from the very start of system development. As software plays an increasingly significant role in controlling physical processes, the interplay between functional safety, cybersecurity, health and safety, and product requirements becomes crucial. This is particularly important for the autonomous and connected transport systems of the future, where software decisions can directly affect people and the physical environment.

International perspective

The development of safety-critical software is concentrated in countries where advanced technical systems combine physical functions with complex software. International standards for the development of safety-critical systems have been developed in close association with strong industrial sectors in the US, Europe and Japan.

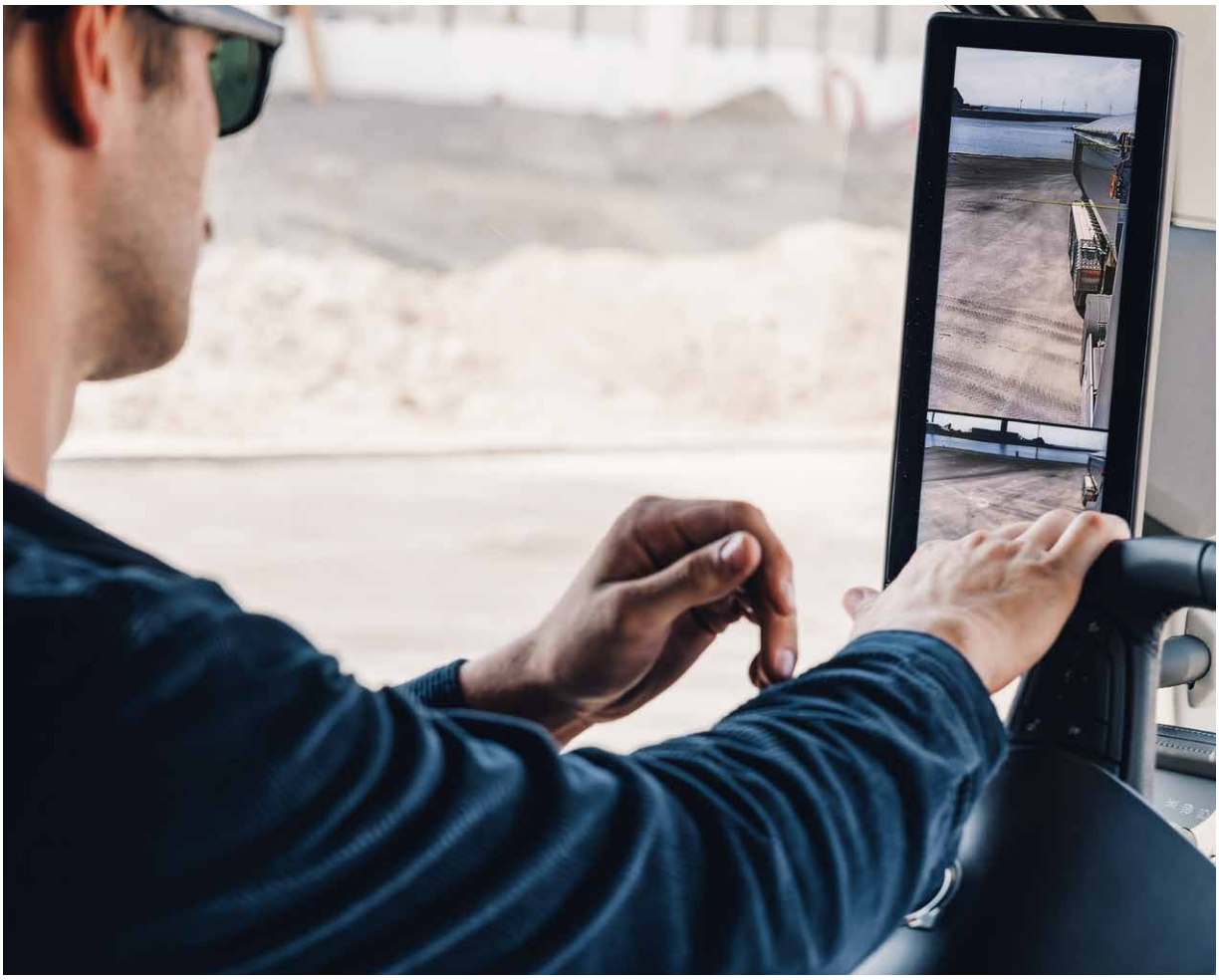
The US links defence, society and security

The US holds a strong position in safety-critical software through its links between defence, the aerospace industry, space technology and cyber security. In the aerospace sector, the US has played a central role in establishing processes for safe software development and certification. The standard for software development in airborne systems is used internationally and is an established model for requirements management, verification and documentation of safety-critical software.[20] The strength of the US lies not only in the development of advanced technical solutions but also in established methods for demonstrating that complex software meets safety requirements through systematic verification and validation. The US is also a leader in cyber security for critical infrastructure through the development of frameworks for risk management and the protection of digitally critical systems. For example, the US National Institute of Standards and Technology (NIST) has developed a cyber security framework. This is used internationally as a model for identifying, managing and mitigating cyber risks in critical systems.[21]

Since the 1960s, the US has conducted research into computers and software for defence purposes through the Defence Advanced Research Projects Agency (DARPA). The agency has subsequently expanded this work to include, among other things,

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.



autonomous systems and methods for making software more secure and reliable.[22]

Experience from the US aviation industry shows that shortcomings in the design, testing and approval of software-controlled functions can have very serious consequences. In a high-profile case, problems in an automated flight control system contributed to two air accidents, where the system could be activated on the basis of incorrect sensor data.[23] Within the defence industry, extensive software problems have delayed upgrades to advanced aviation systems, partly due to stability issues, faults discovered during testing and the need for several new software versions.[24]

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*.

The UK is investing in flexible systems

The UK has strong defence, aerospace and advanced manufacturing sectors. In the defence sector, the country is focusing on developing systems where software can be more easily updated and adapted as new requirements arise. One example is work on aviation systems where different components can be replaced and upgraded without the need to overhaul the entire system.[25]

The UK is also investing in AI, data and autonomous systems within the defence sector and emphasises the need to bring new technology from research and industry into practical use more quickly. At the same time, there is a shortage of digital skills and a need for better common solutions to ensure interoperability between different systems.[26] The UK thus highlights both the opportunities and challenges in adapting advanced systems as software becomes increasingly important.

Germany's position is based on industrial tradition

Germany has strong automotive, manufacturing and automation sectors. The major push towards the digitalisation of industry, which began in the 2010s, built on the country's strong manufacturing sector and expertise in automation, embedded systems and information technology.[27] Since then, digital technology has played an increasingly significant role in both production and products, partly through the integration of physical systems with digital technology.[28]

For the German automotive industry, the shift towards software-defined vehicles has become a major challenge. Companies have long possessed strong expertise in areas such as mechanics, powertrains, safety and industrial production, but now need to build up more expertise in software and digital technology. This has required both internal capacity-building and collaboration with external partners, which has created challenges in terms of organisation, dependencies and the time needed to develop new expertise.[29] This development has also led to reorganisations and cutbacks in the software sector, while collaboration with external partners has grown.[30] The OECD has also highlighted that German companies have lagged behind in digitalisation and that this is hampering productivity growth.[31] While Germany has a strong industrial base, the transition to products in which software plays an increasingly significant role is clearly a challenge.

South Korea combines industry and AI

South Korea has a strong industrial sector in areas such as automotive, electronics, semiconductors and manufacturing. As early as 2014, the country launched a comprehensive initiative to digitise fac-

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.

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

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.

tories and has since supported tens of thousands of projects in companies across the country.[32]

This initiative has made it easier for companies to use digital technology in production. South Korea is also working to expand the use of AI across industry. The OECD points out that the country needs to strengthen companies' ability to develop and use new technology in order to remain competitive.[33] South Korea can be seen as an example of how a strong manufacturing sector can be combined with rapid digital transformation.

Israel links defence and cyber security

Israel stands out from the other countries due to its particular strength in cyber security. The OECD describes Israel as a country with a high capacity for innovation and strong development in digital security technology.[34] Within security-critical systems, this expertise is particularly relevant as cyber attacks can affect both digital functions and physical security.[35]

The OECD highlights Israel's strong high-tech sector and the close links between defence, research and industry as key to the country's innovation capacity. When it comes to software for critical physical systems, the combination of defence-related expertise, AI and advanced technology is particularly relevant, as it enables companies to develop and employ technology in security-critical applications.[36]

China has national strategies for large-scale and rapid implementation

China has built up a rapidly growing capacity in industrial digitalisation and advanced production systems. The country's national strategies have focused on developing digital industry, artificial intelligence and smart manufacturing.[37] China's primary strength lies in its ability to rapidly implement advanced technical systems on a large scale, while Western industrialised nations have traditionally had longer experience in developing regulated safety-critical systems.

China's strength lies not only in developing new technology, but also in its ability to rapidly translate it into products and scale up production through dense supplier networks and close links between companies and manufacturing. For physical systems, this highlights the importance of being able to combine technical expertise with industrial capacity, supply chains and the ability to move rapidly from development to production.[38]

Europe and China have different approaches to organising production and innovation. China, for example, has a long-term industrial policy with state investment in strategic areas.[39]

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.

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

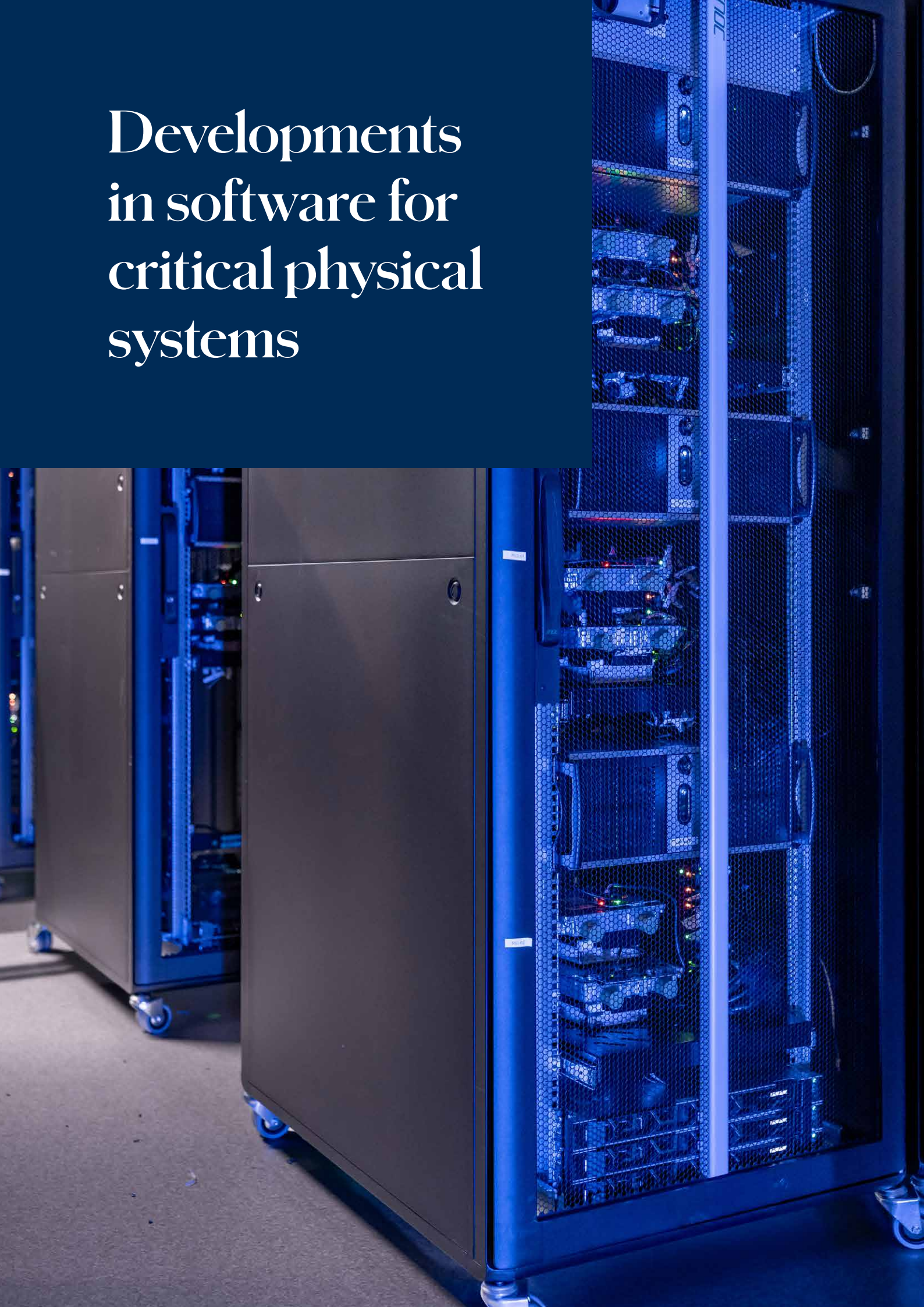
36 OECD. (2025). *OECD economic surveys: Israel 2025*. OECD Publishing.

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). *Advanced Manufacturing: A technical report within the 'Swedish Futures' series on complex discrete manufacturing*. See in particular the section 'Europe and China have different approaches', which contains several references.

Developments in software for critical physical systems



Several current Swedish initiatives are significant for the development of software for critical physical systems. These initiatives strengthen many of the conditions required to develop, test and use new technology. These include computing capacity, research and development, expertise, funding and security.

Access to advanced computing power is one example. In July 2026, the Swedish Tax Agency was tasked with entering into a joint agreement under the EU's supercomputer programme. Among other things, this will give the Swedish public sector access to computing power from an AI facility in Finland, which the Government considers important for research, innovation and the use of AI.[40]

Support is also being provided for research and development in new digital technologies. The Government has tasked Vinnova with allocating at least 570 million kronor in 2026 under the Advanced Digitalisation programme.[41] Among other things, the programme is intended to support the development of new technology and AI that can be used in industry. The Government has also invested in research into AI and other strategically important technological areas relevant to software for critical physical systems.[42]

The supply of skilled labour is another key area. In July 2026, the Government commissioned a review into how university courses can be better adapted to the future needs of the labour market and society.[43] Developing software that can operate safely alongside physical products requires both sound software expertise and an understanding of the products and systems in which it will be used.

Attention is also being paid to the opportunities for financing new technology companies. In June 2026, the Swedish Agency for Economic and Regional Growth and Vinnova were commissioned to investigate how the funding gap for new technology companies can be better addressed.[44] The commission covers both access to private capital and how public and European funds can be used more effectively. This is particularly relevant for companies developing advanced software, as significant investment is often required to develop and test a product before it can be placed on the market.

At the same time, the defence sector has been given a clearer role in the development and use of new technology. In June 2026, the Government approved a five-billion-krona investment in, among other things, digital command and control systems, AI, cloud solutions and new communications networks within the Swedish Armed Forces.[45] One aim is to improve the ability to share information quickly, detect threats and make decisions. In July 2026, the Swedish Armed Forces were also tasked with establishing a unified defence innovation function in collaboration with the Swedish Defence Materiel Administration (FMV), the Swedish Defence Research Agency (FOI) and Vinnova.[46] The aim is to enable the defence sector to adapt more quickly to new threats and to make better use of new technology. This is particularly relevant for

40 The Government (2026). *Sweden and the EU take the first steps towards AI gigafactories*. Press release published on 30 July 2026.

41 The Government (2025) *Regulatory letter for the 2026 financial year concerning the Swedish Agency for Innovation Systems.* (KN2025/02359, in part, KN2025/02393).

42 The Government (2024). *Research and innovation for the future, curiosity and benefit* (Govt Bill 2024/25:60).

43 The Government (2026). *A high-quality range of educational programmes relevant to the needs of the labour market and society. Committee directive* (dir. 2026:82).

44 The Government (2026). *Mandate to the Swedish Agency for Economic and Regional Growth and the Swedish Agency for Innovation Systems to investigate the supply of capital to knowledge-intensive companies* (KN2026/01433). Published 29 June 2026. .

45 The Government (2026). *Major investment to modernise the Swedish Armed Forces' warfare capabilities*. Press release published on 18 June 2026.

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



software designed to operate as part of advanced military equipment and other physical systems.

The security of digital systems has also become more important. The new Cybersecurity Act (2025:1506) came into force in January 2026 and imposes stricter requirements on organisations operating in several areas critical to society. These requirements include, among other things, measures to protect digital systems and the reporting of serious incidents. For companies developing software for systems critical to society, this means both stricter requirements and increased demand for secure solutions.

A broader effort is under way to simplify regulations and dealings with public authorities for businesses. The Government's digitalisation strategy identifies, among other things, simpler regulations and faster licensing processes as key prerequisites for business development.[47] For companies developing and testing new technology, simpler and more predictable regulations can make it easier to move from development to testing and on to deployment.

There are therefore currently several ongoing initiatives that strengthen key aspects of this area. Computing capacity, research and development, skills, funding, defence innovation and security are already covered by various initiatives. At the same time, these initiatives are broader in scope than software for critical physical systems and do not fully take into account the specific requirements that arise when software and AI become part of products where safety and reliability are crucial.

The AI Commission highlighted that Sweden needs to act swiftly to strengthen its capabilities in AI.[48] Since then, the Government has drawn up a national AI strategy and an action plan that address several of the Commission's proposals.[49] Developments in AI and cyber security are progressing rapidly, which means that work needs to continue at a fast pace.[50]

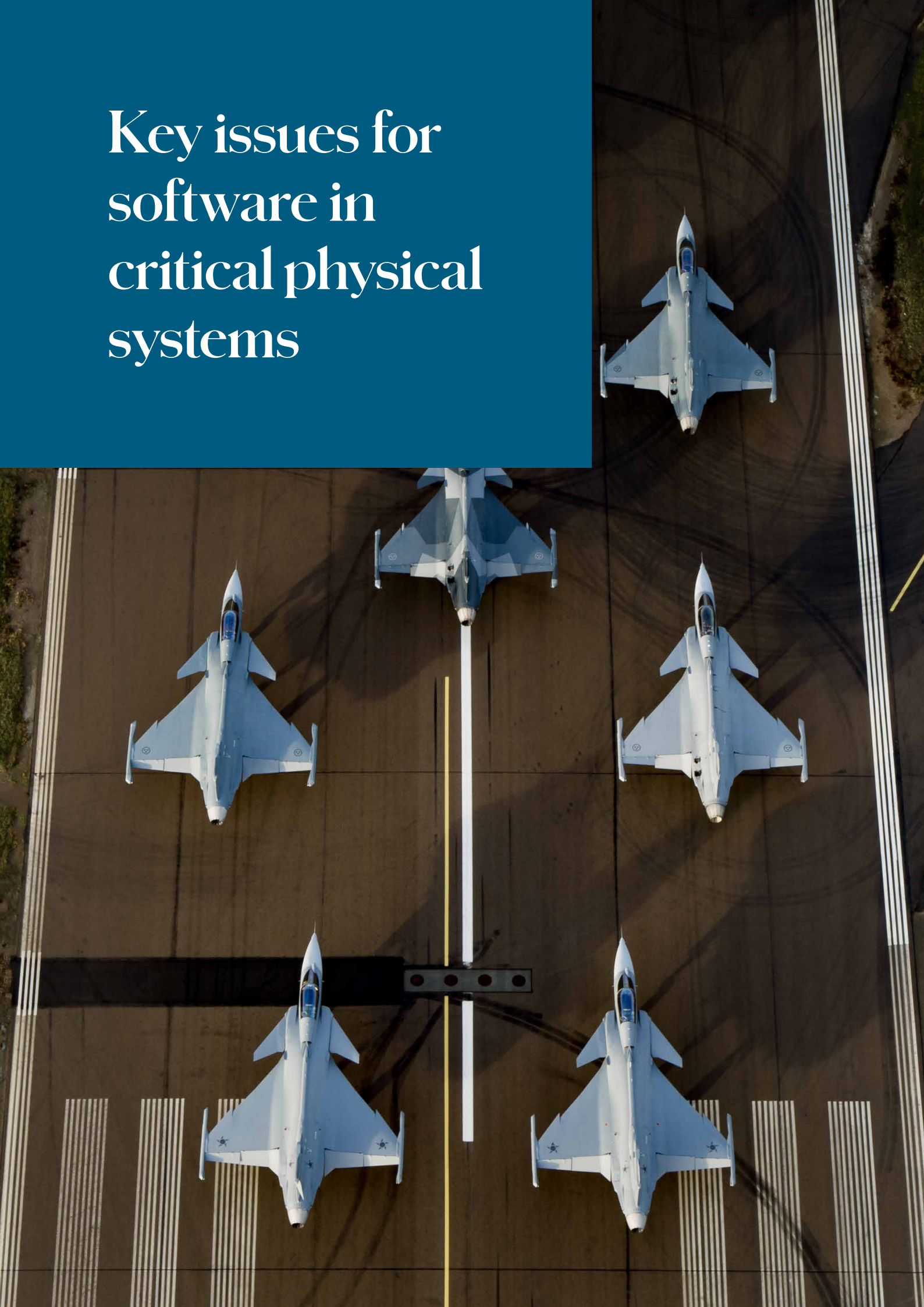
47 The Government (2025). *Sweden's Digitalisation Strategy 2025–2030*.

48 The AI Commission. (2025). *The AI Commission's Roadmap for Sweden* (SOU 2025:12).

49 The Government Offices. (2026). *Action Plan for Sweden's AI Strategy*.

50 The Royal Swedish Academy of Engineering Sciences. (2026). *AI-driven cyber threats: The next twelve months*.

Key issues for software in critical physical systems



The working group has identified three key issues for Swedish competitiveness in software for critical physical systems. These relate to **skills**, **regionalisation** and **the pace of transformation**.

Key issue 1: Skills to meet future needs

The supply of skilled professionals in Sweden is insufficient to keep pace with rapid developments in software for critical physical systems. The shortage applies both to cutting-edge expertise in AI for physical systems *(physical AI)* and the wider range of software skills that need to be developed through educational and incorporated into professional roles.

The issue concerns the entire skills chain, from educating enough people with the right knowledge, attracting international talent, and creating the conditions for them to stay and develop their skills in Sweden. It also concerns how skills requirements are changing. As AI takes over parts of traditional programming work, the ability to understand products, systems and architecture is becoming increasingly important. This places new demands both on educational programmes and on how the industry attracts and develops young engineers.

Furthermore, the industry needs to invest broadly in lifelong learning. This is necessary both to help employees from different backgrounds learn software development and to enable those already working in the field to deepen and update their knowledge in line with technological developments.

Problems

There is a growing gap between the content of educational programmes and the needs of industry. Subjects relevant software for critical physical systems need greater prominence in engineering programmes, while expertise in areas such as embedded and safety-critical systems needs to be strengthened. Educational programmes are slow to change, and the industry offers too few work placements, projects or other opportunities for students to gain practical experience.

Developments in this field are also changing how employees progress from junior to senior roles. As programming becomes increasingly automated, it is becoming harder to gain the experience that was traditionally acquired through entry-level roles. These changes are largely driven by rapid advances in AI. Today, AI is used not only for simple programming tasks but also to solve complex problems that previously required traditional rule-based programming. The rapid development of software systems and AI is therefore placing increasing demands on engineers.

The skills challenge is not just about how many people are trained, but also how quickly they can acquire the skills the industry needs and how effectively Sweden can retain them.

Opportunities

Sweden is well placed both to broaden engineering programmes and to develop cutting-edge expertise in strategically important areas. This does not mean that all higher education insti-

tutions should take the same approach. Some need to strengthen their research and excellence, while regional universities may, above all, need to focus on attracting more students to technical programmes and meeting the skills needs of industry.

In an environment of increasingly rapid change, engineering programmes can benefit from placing greater emphasis on fundamental knowledge in the early stages of education. This knowledge tends to remain relatively stable over time, while more recent developments can be covered through project-based modules that are easier to adapt without having to overhaul entire syllabuses.

Engineering education needs to put greater emphasis on systems thinking, organisation and leadership. This is important for preparing students to work in complex organisations and to drive sustainable change. As AI and large language models become part of engineers' everyday work, a broad knowledge base becomes even more important. AI can amplify both knowledge and intentions, which placing greater demands on the ability to understand context, assess consequences and make ethical judgements.

A closer link between education and working life can give students earlier experience of real-world product development and make it easier to build expertise over time.

There is also scope to make better use of the international talent already seeking to study at Swedish higher education institutions, for example by ensuring that international students have opportunities to stay and work in Sweden after completing their studies. Together with early intervention in schools and stronger links between education and working life, this can help to create a broader and more sustainable skills base.

The working group welcomes the efforts to strengthen education and boost interest in the field of technology.

Key issue 2: Regionalisation and new global rules

Sweden's competitiveness has long been based on global value chains and markets. Trade, technology and supply chains are now becoming more regional and, to a greater extent, governed by security policy and geopolitical considerations. For a small country that relies on exports, this has a major impact on the conditions under which products are developed, manufactured and sold.

This trend is particularly evident in the field of software for critical physical systems. Access to computing power, data, cloud services and advanced components is increasingly influenced by where the systems are developed and used. Products that could previously be developed for a global market may now need to be adapted to more local technical, regulatory and security policy conditions.

Problems

Sweden is dependent on external suppliers in several strategically important areas, including com-

ponents from China and digital infrastructure and services from the US. Furthermore, the hardware required for software development is becoming an increasingly sensitive geopolitical issue. Export controls, regulatory requirements and restrictions on which actors can access certain technologies are becoming increasingly significant.

This means that Swedish companies can no longer assume that the same product can be marketed in the same way everywhere. At the same time, access to capital and advanced infrastructure is limited in Sweden and Europe, which may make it more attractive for companies and talent to seek out larger ecosystems. But it is not just a question of hardware limitations. Data, software and connected systems are also subject to new regulations, which may limit Swedish companies' ability to sell and use their products in certain markets.

Opportunities

Regionalisation need not be viewed solely as a constraint. As security, reliability and control over data and infrastructure become increasingly important, demand may rise for technology developed and produced within Europe.

This applies not only to export-oriented companies. Sweden has a strong industrial base comprising both large companies and an extensive network of specialised technology firms and subcontractors. This provides a solid foundation for contributing to European value chains and developing capacity in areas where Europe needs to reduce its strategic dependencies. Sweden is well placed to play a important role in this area, with its high level of digital maturity and strong industrial base. One opportunity is to view Sweden as a test and home market for solutions that can later be scaled up across Europe.

There is potential for Swedish companies to become even better at adapting products and solutions to different markets and regulatory frameworks. Competitiveness is no longer just about access to global markets. It also depends on building strong value chains and establishing a presence in multiple regional ecosystems. This gives Sweden the opportunity to strengthen both its own capacity and Europe's capabilities in software for critical physical systems.

Key issue 3: The industry's ability to adapt in time

Perhaps the most fundamental challenge is how quickly Swedish industry can transition from hardware-defined to software-defined products. As software and AI become increasingly important, it is not only the technology that changes, but also how products are developed, how companies are organised and how decisions are made. Sweden is particularly dependent on the ability of large companies to adapt in step with technological developments. As these companies form a central part of Sweden's industrial base, the pace of their transition is also crucial to Sweden's ability to compete internationally. If Swedish companies adapt more slowly than



their competitors in other countries, Sweden risks losing investment and its technological lead in software for critical physical systems. This is a growing challenge that the whole of Europe is grappling with.

The shift is away from systems in which hardware largely determines a product's function, towards systems in which software can modify and improve the product throughout its lifecycle. This requires different skills, shorter development cycles and, in many cases, new business models. When software is developed continuously, the product's value to the customer can also increase over time. This calls for business models that take into account that a product's value changes over its lifecycle. It is difficult to set an initial price for a product that is intended to be used and continuously developed over many years to come. For established industrial companies, this transition is particularly challenging, as existing products, organisations and working methods need to be adapted while curent day-to-day operations must continue uninterrupted.

It is important to recognise that rapid technological development requires changes across the whole of society, not just within company management and boards. Companies need to develop new products, skills and working methods more quickly, while the education system and other parts of the public sector need to adapt their courses, regulations and operations to new technological conditions.

Problems

Technological development is outpacing many companies' ability to transform their organisations and working methods. Company management teams and boards sometimes lack sufficient understanding of software for critical physical systems to be able to drive the transition strategically. At the same time, software and AI development require different approaches to prioritising and managing risk than traditional industrial development.

One key difference is that development can no longer be planned in the same way from start to finish. Software-based solutions require more experimentation and more frequent feedback. Lengthy decision-making processes, demands to minimise risk, and processes designed for more predictable technologies can therefore slow down development. The challenge is not just to produce new technology, but to get the whole organisation to work in a different way.

Opportunities

Swedish industry has experience of complex product development and strong capabilities in both technology and systems integration. This provides a solid foundation for the transition. The next step is to develop leadership, working methods and decision-making models suited to safety-critical products where software plays an increasingly significant role.

There are also significant opportunities for learning across companies and sectors. Many of the challenges are sector-agnostic and common to companies developing aircraft, vehicles, defence systems, drones and other safety-critical products. By sharing experiences and trialling new ways of working, the transition can be accelerated. The ability to integrate new technology into existing companies and products thus becomes at least as important as the ability to develop the technology itself.

Sweden has a unique opportunity thanks to the strong technology and start-up ecosystem that has developed over a long period. Stockholm is home to a high concentration of digital companies and knowledge-intensive businesses, and the region accounts for a particularly large share of the country's high-tech and knowledge-intensive employment.[51] Many new companies are digital from the outset and incorporate AI and software as an integral part of their operations. There is much for Swedish industry to learn here, not least about how new technology can be developed, utilised and scaled rapidly.

At the same time, Swedish industry possesses in-depth knowledge of technology, production and global value chains. This experience is valuable for young technology companies seeking to grow and reach international markets. Closer collaboration between these sectors could therefore benefit both sides. When entrepreneurship and digital expertise meet industry's production know-how, new opportunities arise to develop products, businesses and solutions.[52] In this way, Sweden can better capitalise on two strong sectors that complement one another.

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.

Desired future direction



Vision

By 2035, Sweden will be a world leader in a number of areas where embedded software or AI forms a significant part of physical products and where high standards of safety and reliability are required. Furthermore, Sweden will have a strong ecosystem within software for critical physical systems. This applies in particular to products where safety and reliability are crucial, such as aeroplanes, robots, lorries, cars, drones, boats and construction machinery. In ten years' time, Sweden will be a world leader, with strong industrial capacity and cutting-edge technical expertise in translating advanced technology into complex products and systems.

Sweden holds a strong global position in software for critical physical systems. We possess cutting-edge expertise in technology that is secure, reliable and capable of being tested, verified and certified. Sweden enjoys a strong international reputation in this field. Other countries view Sweden as a pioneer, and Swedish companies are sought-after partners. The starting point is our established strength in embedded safety-critical systems. The ambition is not to compete with the US and China over large AI models, but to build a strong position where Swedish industry and research already possess a high level of expertise, extensive experience and favourable conditions. By 2035, Sweden will have further strengthened its position in safety-critical applications where software is combined with physical technology, advanced industrial expertise and requirements for high safety and reliability.

This requires relevant expertise throughout the entire education system. Dedicated teachers and practical role models spark an interest in technology among young people at an early age. Master of Science in Engineering programmes provide a broad foundation and the opportunity to specialise in the field of software. An increase in the number of industry PhD students, adjunct professorships and work placements has strengthened links between academia and industry. Sweden has also become more successful at attracting and retaining international students and researchers in fields relevant to software for critical physical systems. The supply of skilled labour is closely linked to developments in industry, and degree programmes are continuously updated as technology and conditions change. Furthermore, lifelong learning, reskilling and further training are a natural and widely implemented approach within the industry.

Another prerequisite is access to digital infrastructure. Computing capacity, energy, data, cloud services and strategic components are available under predictable conditions. Sweden has ensured that both large and small players have access to a shared national infrastructure for development, testing and validation, which reduces the need for each company to build up its own capacity. However, adopting a purely national perspective may be too narrow when it comes to digital infrastructure within software for critical physical systems. Certain elements are likely to be developed at European level, such as European cloud services that can complement or, in the long term, replace the American services on which we currently depend. Sweden needs to be deeply integrated into European capacity and build national infrastructure only where security, availability or control actually require it.

The development and testing of safety-critical systems in which software is integrated with physical products may also require shared infrastructure that can be used by multiple stakeholders. At the same time, it is likely that Europe will build up its own capacity for the advanced computing power required to develop such systems. This capacity can be made available via cloud services, so that companies and other stakeholders can use it without having to own and operate the technical equipment themselves. Physical test facilities, similar to those currently in operation – such as WARA-PS, the test facilities at the Vidsel Test Range and AstaZero – provide industry and academia with the opportunity to test tech-

EXAMPLES OF PHYSICAL ARENAS FOR TESTING AND DEVELOPMENT

WARA-PS (WASP Research Arena for Public Safety) is a research arena within the Swedish research programme WASP (Wallenberg AI, Autonomous Systems and Software Programme). The aim is to accelerate research and development in autonomous systems, AI and software for public safety and emergency services. The arena focuses on how people and autonomous machines can interact in complex situations. An area near Västervik has been used as a permanent test bed since 2018.

The Vidsel Test Range in Lapland, near Älvsbyn, is a military test site operated by the Swedish Defence Materiel Administration. Its purpose is to test, evaluate and conduct exercises with military weapon and aviation systems in a safe and controlled environment.

AstaZero AB is a Swedish limited company owned by the research institute RISE. Its activities include operating test tracks for vehicle safety and a connected transport system.

nology in realistic environments. At the same time, expanded Swedish storage and computing capacity reduces dependence on foreign suppliers. By 2035, Sweden will be part of European infrastructures and will utilise European capacity where it is more efficient than building national solutions.

Regulatory frameworks and certification processes have also been developed. Companies can gain an early understanding of the applicable requirements, which authority is responsible for different parts of the process, and how long approval may take. The regulatory frameworks focus more on safety and outcomes than on detailed technical solutions. Regulatory sandboxes are used to test new solutions and regulations on a smaller scale before they are introduced more widely. Sweden has also become better at translating European rules and standards into practical processes. Companies can move from development and testing to conformity assessment and approval with greater predictability.

Sweden is seen as an attractive destination for expertise, capital and companies specialising in software for critical physical systems. Companies can develop and grow in Sweden, while international expertise and investment are drawn to the country. Sweden also serves as an attractive test and reference market for new solutions. Major industrial companies and public sector organisations contribute by acting as early adopters of new technology, which makes it easier for Swedish companies to develop, scale up and export their solutions.

A key element is the collaboration between industry, academia and the public sector. Joint testing and demonstration environments, knowledge exchange and strategic partnerships make it easier to move from research to development and production. Companies have also developed their capacity for collaboration. Even competing companies can work together on shared technical solutions and the infrastructure required for software used in critical physical systems. Collaboration has, to a greater extent, taken on a long-term form and focuses on specific shared development needs rather than merely time-limited projects. Companies already possess many of the platforms and the expertise required to develop and test software for critical physical systems. The challenge is to collaborate in a way that ensures we make the most of what already exists, rather than companies working in isolation. By 2035, we will have found ways to better link existing resources that can strengthen the Swedish ecosystem for the development, testing and deployment of new

technology. In ten years' time, Sweden will have developed its approach to working through the entire process, from expertise and research to testing, approval, use and international expansion. Expertise, infrastructure, regulatory frameworks, collaboration and demand have strengthened Sweden's ability to develop and scale secure physical systems. This has given Swedish companies a better foundation for competing internationally in the field of software for critical physical systems, an area that is becoming increasingly important for both industry and Sweden's security.

Five proposals for the development of software for critical physical systems in Sweden

This section presents five overarching proposals to strengthen Sweden's competitiveness in software for critical physical systems. The proposals should be implemented as parts of the same development chain rather than as separate initiatives.

We propose the following:

- accelerate business transformation,
- foster long-term collaboration between industry, academia and the public sector,
- build a cohesive skills chain,
- create a coherent structure for development and testing,
- make regulations frameworks and certification more predictable

For each of our proposals, we present a number of concrete action points describing the measures required and the stakeholders who should be responsible for implementing them. We also outline various options for how the proposals could be implemented over a ten-year period. There is no order of priority among the proposals. All need to be implemented, and work should begin immediately.

Proposal: Accelerate business transformation

Swedish businesses need to transition from products where hardware largely determines functionality to products where software plays an increasingly significant role. This is changing the way products are developed, manufactured and marketed, and is placing new demands on how companies organise their work, prioritise investments and make decisions. Companies also need new ways of working that allow them to update software and continuously improve products after launch. For established industrial companies, this transition is particularly demanding. They must develop new ways of working and new business models while keeping existing operations running. It may also require major changes to operations, new ways of financing development, and boards and senior management with the knowledge needed to make decisions about technical and strategic development. Rapid technological development also means that companies need to be able to make decisions before all the information is available and be prepared to take a certain amount of risk in order to test new solutions. This requires a different approach to risk and decision-making but does not mean that safety standards can be lowered.

Swedish industry is well positioned, thanks to its long experience of advanced product develop-

ment, production and systems integration. Technology is advancing rapidly, and companies in other countries are developing new products and working methods. In order to grow, Swedish companies also need access to early-adopter customers and markets where new products can be tested and developed. They need to be able to manage dependencies on other countries and adapt their products and business models to different markets. Capital is also required to move from development to industrial production and to enable international growth. If Swedish companies are unable to adapt at the same pace, there is a risk that investment and technological leadership will shift to other countries.

Specific action points to accelerate business transformation:

- **Ensure that management teams possess up-to-date and relevant expertise in software for critical physical systems.** Companies are responsible for ensuring that the products and systems they develop remain secure throughout their lifecycle. As software becomes increasingly important to the functionality and security of products, management must have a sound understanding of areas such as system architecture, cyber security, testing and updates. By strengthening management's expertise, companies can take greater and more informed responsibility for safety from the outset rt of product development and investment planning.

- **Use IVA's CTO network to share experiences regarding software for critical physical systems.** Create a regular forum where chief technology officers from different sectors can exchange experiences on the development, testing, verification and updating of software in products where safety and reliability are crucial. The network can also identify common challenges and needs in areas such as skills and expertise, test environments, cyber security, AI, certification and regulations, and disseminate effective working methods across sectors. IVA has a network for technical managers, primarily CTOs, in leading Swedish industrial companies. The network is part of IVA's Business Council and focuses exchanging knowledge about shared challenges, new technologies and technological shifts.

- **Strengthen collaboration between established industrial companies and new software and AI firms.** Create structures to enable established industrial companies and younger technology firms to share experiences and develop solutions together. Established companies can contribute expertise inproducts, production and global value chains, while newer technology firms bring experience in software development, AI, faster development cycles and new ways of working. Closer collaboration can make it easier to test and introduce new technology into existing products and operations, thereby accelerating the transition of companies.

- **Establish a programme office focused on software for critical physical systems** within the *Advanced Digitalisation* research and innovation programme, which is jointly funded by the public sector and industry. The programme office should be tasked with gathering and coordinating initiatives in this area, while strengthening collaboration between businesses, academia and public sector organisations.

- **Monitor companies' transition to software-based products and working methods.** This monitoring should cover, for example, investments, the pace of development, the adoption of AI and other new technologies, as well as barriers to the transition. The results should be used to identify where progress is too slow and what measures are needed to strengthen companies' ability to adapt and Sweden's competitiveness.

Proposal: Foster long-term collaboration between industry, academia and the public sector

Sweden already has many established forms of collaboration between industry, academia and the public sector. For example, the research institute RISE has several test and demonstration environments where businesses, academia and the public sector can develop and trial new solutions together. The strategic innovation programmes have also established long-term structures for collaboration. Another example is the *Advanced Digitalisation* research and innovation programme, which is jointly funded by stakeholders in the public sector and industry. The programme can provide an important foundation for long-term collaboration in the field of software for critical physical systems by bringing together companies, academia and other stakeholders around research, innovation, test environments and skills development. In addition, WASP contributes research and expertise in AI, autonomous systems and software. These existing programmes and environments should be linked more closely and utilised for long-term collaboration in areas where several stakeholders share common needs. The challenge, therefore, is not primarily a lack of networks or meeting places. The problem is rather that collaboration is often project-based and that experience, expertise and relationships risk being lost when a project comes to an end. There is also a risk that several stakeholders will develop similar solutions in parallel. For established companies, it can also be difficult to find ways to collaborate on technology that is closely related to their own core business but where development costs are high and the benefits are greater if several stakeholders share the work.

To strengthen Sweden's capacity to develop and deploy new technologies, more long-term forms of collaboration are needed. The focus should be on areas where several stakeholders share common needs, but no single stakeholder has sufficient incentives or resources to drive development on their own. These areas may include common standards, testing methods, security solutions, data, expertise and technical platforms.

The proposal is therefore not to create yet another general network. Instead, existing platforms should be used to identify a limited number of strategic development areas where businesses, academia and the public sector can work together over the longer term. Collaboration should be linked to specific problems, joint investments and measurable results.

Specific action points to foster long-term collaboration between industry, academia and the public sector:

- **Steer collaboration between businesses and academia towards clear deliverables and continued use.** This could be achieved by establishing a joint process for initiating and monitoring collaborative projects, and and for ensuring that their results are taken forward after the projects have ended. Each project should have clear objectives, concrete deliverables and a plan for taking the results forward into research, development or industrial applications. The Swedish Association of Engineering Industries (Teknikföretagen), together with its member companies and relevant higher education institutions, should develop such a model and draw on existing experience from companies that develop software for critical physical systems. Responsibility for implementation should lie with the participating companies and higher

education institutions, while the programme's governing bodies should create the conditions for successful collaborations and results to continue beyond the end of the project.

- **Move from short-term projects to multi-year development programmes.** Once an area has been identified as strategic, collaboration should be organised into three- to five-year programmes with shared objectives, funding and responsibilities. The approach taken within WASP is a good example. The programmes should bring together companies, academia and the public sector around shared challenges and long-term objectives. They should have a clear problem owner, defined outcomes and a plan for how knowledge, methods and solutions are to be taken forward once the programme has ended. It should be possible to conclude a programme once the objective has been achieved and to redeploy resources to new areas. Vinnova should be responsible for coordination in collaboration with RISE, higher education institutions, businesses and relevant public authorities. Vinnova should be able to draw on strategic innovation programmes and the initiative *Impact Innovation*. These long-term programmes have built both capacity and collaboration structures between businesses, the public sector and academia.[53]

- **Link the collaboration programmes to test and demonstration environments.** Every major collaboration programme should, from the outset, have a plan for how the results should be tested and validated. Existing test beds at RISE and other organisations should be used as shared infrastructure for businesses, researchers and the public sector. This should be coordinated by RISE, which has over 130 test and demonstration environments open to businesses, academia and the public sector. Organisations that could participate in the implementation include Vinnova, universities, businesses and relevant government agencies, among others.

- **Establish frameworks for collaboration between companies in the sector** by identifying areas of technology where several Swedish companies have similar needs, but where there is a lack of incentives to develop joint solutions. This could, for example, relate to cyber security, standards, testing methods, interoperability, common data formats and certain elements of the technical infrastructure. The collaboration should be organised in such a way that companies can share experiences without having to disclose commercially sensitive information or relinquish control over their core technologies. This action point is not intended to encourage competitors to collaborate in general, but rather to identify non-competitive parts of the value chain where collaboration actually yields greater benefits than parallel development. The *Advanced Digitalisation* research and innovation programme could coordinate this. Furthermore, this must involve a range of stakeholders, such as the relevant companies, industry organisations, academia and public authorities.

- **Develop standardised collaboration agreements** for joint development by drawing up contract templates for recurring

53 Vinnova (2026). *Strategic innovation programmes. A meta-study of 17 nine-year evaluations.* VR:2026:13 Authors: Mona Hallström Hjort et al, Sweco.

situations where companies, higher education institutions and public sector bodies collaborate on research, data, testing and technology development. The templates should address, among other things, intellectual property rights, data access, confidentiality, publication, liability and rights to results. The aim is not to create a single agreement for all collaborations, but to reduce the legal hurdles at the outset and establish a common basis for negotiations. The Swedish Association of Technology Industries should coordinate this work and accelerate the efforts already underway in collaboration with Vinnova, higher education institutions, companies, industry organisations and legal experts.

In the short term, existing networks, programmes and collaboration initiatives should be mapped, with a focus on those that already operate at sufficient scale and those with potential for expansion. The mapping exercise should, in particular, identify areas where several actors are developing similar solutions or where a long-term form of collaboration is lacking. Vinnova should select two to three areas for pilot programmes with multi-year funding and clear objectives. From the outset, the pilots should be linked to existing test and demonstration environments at, for example, RISE.

Within two to three years, Sweden should have established a limited number of multi-year development programmes in which businesses, academia and the public sector work towards common technical objectives. There should also be standardised contract models and a national overview of relevant projects, test environments and expertise.

By 2035, long-term forms of collaboration should be an established part of Sweden's innovation system. The focus should then be less on creating new networks and more on being able to rapidly mobilise existing expertise, infrastructure and capital around new strategic technology areas.

The aim should be for Sweden to derive greater benefit from the existing culture of collaboration through fewer parallel initiatives, a longer time horizon for joint development and better coordination of expertise, infrastructure and investment in software for critical physical systems.

Proposal: Build a cohesive skills chain

Sweden's skills supply needs to develop more rapidly to meet the increased demand for expertise in software and artificial intelligence. The challenge concerns both breadth and depth. We need more opportunities to develop advanced specialist expertise in close collaboration with industry, more engineers with up-to-date expertise in software for critical physical systems, and more pupils and students choosing STEM courses.

Sweden should consolidate its existing initiatives around a clear skills pathway, with a particular focus on software for critical physical systems. The aim should be for the education system to respond more swiftly to changing skills needs, while Sweden at the same time builds long-term, cutting-edge expertise in strategically important areas of technology.

Such developments are already underway internationally. The EU has a plan to increase the number of places at bachelor's, master's and doctoral levels, as well as pilot projects for AI apprenticeships.[54, 55] The UK highlights the need for more pathways into AI, such as apprenticeships and stronger links between higher education and the world of work.[56] The OECD points out that AI skills need to be developed both through the training of specialists and through continuous professional development throughout working life.[57]

For industry, it is particularly important that students gain experience of real-world development environments and that degree programmes are closely aligned with the skills requirements of the workplace. This is important not least for promoting lifelong learning and further training within industry. Higher education needs to combine a solid technical foundation with knowledge that evolves in step with technological developments.

This is not a new issue. The government has recognised the need for skills through a STEM strategy[58] and a STEM delegation,[59] and has established that Sweden should strengthen its skills base in AI, among other things by integrating AI more clearly into educational programmes.[60] In 2026, the government also decided on further investments in engineering programmes and increased completion rates.[61] Another example is IVA's project *The Knowledge Society of the Future*. The next step should be to forge closer links between education, research and the world of work, and to improve the quality and relevance of higher education.

Specific action points for building a coherent skills chain within software for critical physical systems:

- **Create the conditions for the continuous professional development of engineers in industry.** Engineers working with software for critical physical systems must be able to continuously update their knowledge as technology and working methods change. This may involve, for example, new methods for developing and testing software in products where safety and reliability are crucial. Higher education institutions, companies and industry organisations should therefore develop shorter and more flexible training programmes that can be combined with work and rapidly adapted as new technologies emerge. Companies should be responsible for identifying future skills needs and providing employees with opportunities for further training, while higher education institutions and other training providers should offer programmes that meet these needs. Inspiration for this work should be drawn from the collaborative Swedish initiative *Expert Learning Lab (ELL)*. This is an industry-led initiative in which leading companies and universities are forming a national platform for the continuous profes-

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*.

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

58 Government Offices of Sweden (2025). *A STEM Strategy for Sweden*. Ministry of Education. Published 24 February 2025.

59 Government Offices of Sweden (2025). *The STEM Delegation*. Dir. 2025:11.

60 Government Offices of Sweden (2026). *Sweden's AI Strategy*. Ministry of Finance. Published 20 February 2026.

61 Government Offices of Sweden (2026). *More engineers to graduate – new mandates for higher education institutions*. Press release from the Ministry of Education. Published 15 June 2026.

sional development of technical experts in the field of advanced digitalisation. A further source of inspiration is the Swiss postgraduate course of studies *Nachdiplomstudium*, which offers practising engineers the opportunity to build on their education and obtain an advanced-level qualification.[62] These programmes provide opportunities for specialisation and in-depth study within a particular field and can be used to gain cutting edge skills in areas such as secure software development for critical physical systems.

- **Expand collaboration between academia and industry to develop cutting-edge expertise** in software for critical physical systems. This should be achieved by increasing the use of industrial PhD students, adjunct professors, visiting professors and joint research and development projects in strategically important areas such as software for critical physical systems and other safety-critical fields. A limited number of higher education institutions should be able to build particularly strong environments where research, education and industrial application converge. The focus should be on developing internationally competitive environments where Sweden has a strong foundation, rather than seeking to establish them across the country. The Swedish Research Council should be responsible for coordination in collaboration with higher education institutions, relevant industry organisations and companies. The Foundation for Strategic Research could also contribute to this work. WASP *(Wallenberg AI, Autonomous Systems and Software Programme)* and WISE *(Wallenberg Initiative Materials Science for Sustainability)* are important models. These are long-term research programmes that bring together academia and industry in strategic technology areas. The programmes combine research and education with close collaboration with companies, thereby helping to build and disseminate cutting-edge expertise to the business sector.

- **Ensure that engineering degree programmes provide a solid technical foundation while allowing their content to be updated more quickly**. Ensure that Master of Science in Engineering and other relevant engineering degree programmes provide a robust foundation in mathematics, programming, computer science, systems development and engineering methodology. Supplement these with flexible courses and modules in areas such as AI, machine learning, cyber security and new development tools, which can be updated considerably more quickly than entire degree programmes. The working group's experience is that there is currently a lack of educational elements with a sufficiently strong focus on software for safety-critical physical systems, for example in fault-tolerant systems and the programming of embedded and real-time systems. The group therefore believes that existing engineering programmes should be supplemented with relevant modules and projects in which students work on real-world problems and development needs from industry. The programmes also need to be supplemented with modules in organisation, entrepreneurship, innovation and economics.

  The government should be responsible for the overarching framework, while higher education institutions and businesses should play a central role in developing and implementing the changes. One way to achieve this is to establish a permanent forum for collaboration between academia and industry on the content of engi-

62 State Secretariat for Education, Research and Innovation. *Higher Technical Colleges*. Link:www.sbfi.admin.ch/de/hoehere-fachschulen Information retrieved on 5 October 2026.



neering programmes. The forum would provide universities and businesses with a structured arena to discuss how the programmes' objectives, delivery and course portfolios respond to developments in technology and skills. It should focus in particular on Master of Science in Engineering programmes and bring together representatives from major industrial companies and universities for regular meetings, at which the universities present the content and development plans of the programmes and the companies outline future skills requirements. An independent organisation trusted by both academia and industry should organise and coordinate this work. Companies and higher education institutions should share responsibility for translating this dialogue into concrete changes to the programmes. The model should be based on the initiative and responsibility of the stakeholders who develop and utilise the skills, rather than on centralised control by a public authority.

- **Improve the conditions for international students and PhD students to stay and work in Sweden.** This should be achieved by making the transition from study to employment easier through clearer information, faster processes and better coordination between higher education institutions, employers and public authorities. Universities and colleges should actively offer international students access to employers, work placements and career pathways while they are still studying. Responsibility for implementation should lie with the Swedish Migration Agency and higher education institutions. Potential employers should also be involved. Furthermore, UHR has a relevant role to play through its work on the recognition of foreign qualifications.

- **Strengthen teachers' STEM skills early on in the education system** by developing and scaling up professional development for primary school teachers, particularly in mathematics, natural sciences and technology. These efforts should be combined with high-quality teaching materials, teacher guidance and opportunities for professional development from higher education institutions and other STEM stakeholders. The Swedish National Agency for Education should be responsible for coordination, in collaboration with the government's STEM Delegation and within the framework of its STEM strategy. Higher education institutions offering teacher training, together with local authorities, Sweden's network of Science Centres and relevant industry organisations should be involved.

- **Monitor progress in skills development against clear targets up to 2035.** Set a limited number of measurable targets covering areas such as the availability of specialist expertise in software for critical physical systems, completion rates in engineering programmes, the number of industrial PhD students, student projects carried out in companies, and the proportion of international students who remain in Sweden after graduation. Monitoring should focus primarily on quality and excellence rather than simply on numbers. Teknikföretagen should be responsible for coordination until the delegation's mandate concludes. Statistics Sweden (SCB), the Swedish Higher Education Authority (UKÄ), the Swedish Council for Higher Education (UHR), the Swedish Public Employment Service and relevant industry organisations should be involved.

The work should begin by bringing together and strengthening existing initiatives. The first step should be a national survey of the skills gap in software for critical physical systems, while at the same time expanding teacher training and students' contact with the world of work. This should take place within the framework of the existing STEM strategy and AI strategy, rather than by creating yet another parallel structure. Work to strengthen the conditions for the continuous professional development of engineers in industry should also begin immediately.

Within two to three years, Sweden should have an established model for regular skills assessments, more industry PhD students and company-based projects, as well as expanded talent programmes. Higher education institutions should also be better equipped to update the content of their programmes in line with technological developments.

By 2035, the aim should be a cohesive skills chain in which more children and young people choose STEM subjects, more students complete technical degree programmes, more gain work experience while studying, and Sweden has a number of internationally competitive environments for advanced software expertise. For safety-critical systems, the link to industry and critical societal functions should be particularly strong.

Proposal: Create a coherent structure for development and testing

Access to computing power, data and test environments is becoming increasingly important for Sweden's ability to develop and use software for critical physical systems. For companies and researchers, access to algorithms and expertise alone is not enough. There is also a need for the capacity to train and run AI models, store and manage large volumes of data, and test solutions in environments that simulate real-world conditions.

Sweden already has several key components of this infrastructure. One example is *the Mimer AI Factory* at Linköping University, which combines AI-optimised computing capacity with storage, AI expertise, testing and evaluation, and is aimed

at businesses, researchers and the public sector, among others. The new system will be installed at Sweden's National Academic Infrastructure for Supercomputers (NAISS) in 2026 and will include, among other things, 400 GPUs and large-scale storage for sensitive data.[63] At the same time, the government has strengthened Sweden's participation in the European High Performance Computing Joint Undertaking (EuroHPC JU) and decided to co-fund an AI gigafactory in Finland, which will give Swedish stakeholders access to additional European computing capacity.[64] In addition to this, there are private initiatives such as Sferical AI.

The challenge is therefore not primarily to create computing capacity from scratch. It is about creating a coherent infrastructure where computing power, storage, software stacks, data, expertise and test environments can be used together. Even smaller companies and research organisations should have access to the infrastructure without having to build equivalent capacity themselves.

There is also a need for physical test environments. Software-based autonomous systems and other software-controlled systems must be developed, tested and validated under realistic conditions before they can be deployed in areas such as defence, transport, energy, industry and other critical societal functions. Sweden already has a large number of test beds, and Vinnova has a national coordinating role for test and demonstration environments in real-world settings. In addition, RISE operates several test sites, for example for organisations active in the field of automation. However, the need is not merely for individual test phases, but for the ability to test entire systems in relevant and realistic situations. This is particularly important for autonomous and software-controlled systems, where the interaction between software, physical equipment and the environment needs to be tested under real-world conditions.

Specific action points for creating a cohesive infrastructure for the development and testing of software for critical physical systems:

- **Establish a forum for experts in software for critical physical systems.** Companies should create a regular forum where engineers, developers, system architects and other professionals can meet across company and sector boundaries to discuss common technical challenges and share experiences. The work should be guided by the industry's specific needs, such as how to accelerate software development while meeting safety and reliability requirements. The forum should not be a testing or development environment, but a place for exchanging experiences, problem-solving and forging new collaborations. Companies should jointly take responsibility for establishing and running the initiative.

- **Consolidate Swedish computing capacity and make it easier to access.** This could be achieved by creating a single access point for Swedish and European computing resources relevant to the development of software for critical physical systems. This should enable companies, researchers and

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

64 The Government Offices (2026). *Sweden and the EU take the first steps towards AI gigafactories*. Press release from the Ministry of Finance. Published 30 July 2026.

the public sector to find and access relevant resources. The shared infrastructure should encompass computing power, storage, data management, security solutions and relevant software layers. The aim should be to minimise the need for users to understand the underlying infrastructure when developing and testing software-based solutions. This is not merely a matter of gaining access to computing capacity. It also requires secure ways of developing, testing and updating the software, as well as documenting the work. This is a prerequisite for using AI and software in products where errors can have serious consequences. One possible option is to use Mimer as a central node in Sweden, while ensuring that Swedish organisations can utilise capacity within the European EuroHPC system. If Mimer is to be further developed, the Swedish Research Council should be responsible for coordination through NAISS and the Mimer AI Factory (Mimer and NAISS already have the remit and technical expertise for the computing infrastructure). RISE, Vinnova, Digg and relevant higher education institutions should be involved. For example, Vinnova should contribute to the innovation and business aspects.

- **Use the EU's Competitiveness Compass as a lever for development and upscaling.** The EU Competitiveness Compass aims to strengthen Europe's capacity for innovation, reduce strategic dependencies and build stronger European value chains.[65] In the field of software for critical physical systems, this creates new opportunities for Swedish companies to secure funding for the development, testing, demonstration and upscaling of technology that may, among other things, focus on AI and robotics. Companies developing software for critical physical systems should actively seek out the funding opportunities arising from EU initiatives and build European partnerships to enable them to participate in these. The Swedish Association of Technology Industries should support companies in identifying relevant initiatives and finding European partners, while the companies themselves should take responsibility for developing and running the projects.

- **Develop common technical solutions within software for critical physical systems** that make it easier to develop, train, test and use software in different applications. These could include tools for collecting, managing and assuring the quality of data, training AI systems, and verifying that they operate safely and reliably. At the same time, industry should collaborate more closely on tools and methods that can be used across multiple sectors. This could, for example, involve collecting and assuring the quality of data, generating new data through computer simulations, and training systems based on software for critical physical products. For vehicles, robots and industrial machinery, large amounts of data are needed to test how the products perform in different situations, including those that are unusual or safety-critical. Companies should therefore be able to share certain tools, methods and aspects of the development work, while the actual product development continues to take place within the companies themselves. The initiative should not be about building a Swedish equivalent of the major global cloud services. The aim should instead be to create open and secure solutions for use with various technical platforms and

65 European Commission (2025). *A Competitiveness Compass for the EU*. Brussels, 29 January 2025.

computing infrastructure, both in Sweden and internationally.

- **Establish a national network of test and demonstration environments focusing on software for critical physical systems.** Map existing test environments and identify what additional resources are needed to test autonomous and safety-critical systems under realistic and controlled conditions. This may, for example, concern autonomous vehicles, drones, robotics and other systems where software interacts with physical equipment. Vidsel Test Range, Västervik Drone Science Park, WARA-PS and AstaZero are examples of environments that could be included, alongside new civilian environments within, for example, aviation and industry. Sweden should not build a single large national test environment, as different systems require different test conditions. Instead, existing and new environments should be linked through common standards, safety requirements and methods for testing and validation. The network should also provide scope for joint development projects in which businesses, research organisations and the public sector develop and test solutions together. The network should also be open to start-ups and provide access to relevant open datasets. Technical testing should be linked to regulatory testing through common working methods for technical test environments and regulatory sandboxes. Companies must be able to test both the technical functionality and how the solution complies with applicable regulations. This is particularly important for autonomous systems in transport and other regulated sectors. Vinnova should coordinate this work through *Testbädd Sverige* in close collaboration with RISE. The Swedish Armed Forces should be a key partner, alongside the Swedish Defence Materiel Administration, the Swedish Transport Administration, the Swedish Transport Agency, the Swedish Energy Agency, higher education institutions and the business sector. Technical and regulatory testing should be viewed as parts of the same innovation process. See also the action point on regulatory sandboxes below. The European Commission explicitly describes *AI Factories* and *Testing and Experimentation Facilities* as complementary parts of the European AI ecosystem.[66]

- **Ensure access to Swedish and European storage and computing capacity for sensitive data** This should be achieved by expanding capacity for the secure storage and processing of sensitive research and industrial data, and by establishing clear procedures for accessing and using this capacity alongside computing resources for software for critical physical systems. Sweden should also make used of European capacity where it is more cost-effective or strategically appropriate. The aim is not for Sweden to be self-sufficient in all computing power (this is neither realistic nor necessary). Instead, the aim should be strategic freedom of action. Sweden needs to have its own capacity for sensitive and strategically important areas of application, while at the same time benefiting from the existing European infrastructure. We will also, for the foreseeable future, be dependent on US digital services and should be able to use them where appropriate. At the same time, Sweden and Europe need to develop their own alternatives, so that we are not entirely dependent on a single supplier

66 EU. *AI talent, skills and literacy. Shaping Europe's digital future*. Website: digital-strategy.ec.europa.eu/en/policies/ai-talent-skills-and-literacy? Information retrieved on 25 August 2026.



or region. This will create greater resilience and freedom of action should circumstances change. The Swedish Research Council/NAISS should be responsible for coordination in collaboration with Sunet, RISE, Digg and relevant authorities. This action point is in line with developments already taking place within EuroHPC. Sweden has both Mimer and access to European systems, while the new Mimer infrastructure explicitly includes large-scale storage for sensitive data.[67] In addition to this, there are private initiatives such as Sferical AI.

In the short term, Sweden should assess how existing testbeds can collectively cover the entire chain from data and computation to development, testing and validation. The assessment should identify specific gaps rather than assume that new infrastructure needs to be built. Furthermore, a single point of access to Swedish infrastructure for software for critical physical systems should be developed, and a national plan drawn up for how existing test and demonstration environments can be linked together. Vinnova should be responsible for mapping the testbeds, while the Swedish Research Council/NAISS should be responsible for the digital infrastructure. Work on creating a forum for experts in software for critical physical systems, and on using the EU's Competitiveness Compass to fund development and upscaling, should begin immediately.

Within two to three years, Sweden should have a coherent model in which companies and researchers can progress from access to data and computing power to development, testing and validation without having to navigate between a large number of separate infrastructures. A network of prioritised test facilities should be established, with specific capacity for autonomous and safety-critical systems.

By 2035, capacity should be scaled in line with demand and developments in software for critical physical systems. At the same time, Sweden should be fully integrated into the European infrastructure for AI computing and utilise both national resources and EuroHPC's *AI Factories* and *AI Gigafactories*.

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.

Proposal: Make regulations and certification more predictable

Current regulations and processes for testing, assessment and certification are not fully adapted to AI- and software-based systems, nor to technological developments that are outpacing the evolution of the regulatory framework. Another problem is that systems undergo continuous development throughout their lifecycle. It can be difficult for companies to determine at an early stage which requirements apply, which authority is responsible, and what tests and supporting documentation will be required. The problem becomes particularly evident when software is combined with physical equipment and used in safety-critical environments, where several regulatory frameworks and authorities may all be relevant.

The EU AI Act has entered into force, while the requirements for high-risk AI are being phased in. The act sets out requirements relating to, among other things, risk management, data quality, documentation, traceability, human oversight, robustness and cybersecurity.[68]

The European regulatory framework is still under development. A new regulatory framework came into force in July 2026. Its aims include reducing the administrative burden on businesses, allowing more time to adapt to certain high-risk requirements, and increasing opportunities for testing and experimentation.[69] There is also a European standardisation initiative in which harmonised standards are intended to translate the AI Act's overarching requirements into technical approaches, thereby creating greater legal predictability for businesses.[70]

We believe that Sweden should not attempt to create its own certification system for software used in critical physical systems. However, we do believe that European regulations need to be made easier to understand, apply and test in Sweden. There is also a need for better coordination between the authorities and standardisation bodies with which companies interact.

Our proposal is therefore to establish a more coherent pathway from development and testing through to conformity assessment and market entry. The requirements should, as far as possible, be risk- and function-based and allow scope for technical development, while maintaining security and fundamental rights. Companies should be able to obtain guidance at an early stage on which regulatory frameworks are relevant, which requirements apply and how they can demonstrate that their solutions meet those requirements.

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*. Website: digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force? Information retrieved on 25 August 2026.

70 EU (2026). *Standardisation of the AI Act*. Website: digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation? Information retrieved on 25 August 2026.

Specific action points to make regulatory frameworks and certification more predictable for the development of software for critical physical systems:

- **Create a single point of contact for companies seeking regulatory guidance.** Develop a national service that provides companies with early guidance on the regulatory frameworks, relevant authorities, standards and assessment procedures that applies to products involving software for critical physical systems. The service should be aimed in particular at smaller companies that lack in-house regulatory expertise. It should also offer practical guidance on how different regulatory frameworks and standards interrelate, the requirements applicable to different types of systems, the documents that need to be produced, and how companies can demonstrate compliance with the requirements. It should be possible to obtain initial guidance on, for example, the AI Act, cybersecurity requirements, product safety and sector-specific regulations before a company invests in full-scale development and certification. The guidance should focus in particular on areas where several regulatory frameworks overlap, such as autonomous vehicles, robotics, industrial control systems and defence equipment. The Swedish Post and Telecom Authority (PTS) should be responsible for coordination, as, according to the proposal in the Swedish AI inquiry, PTS is to have primary responsibility for market surveillance under the AI Act.[71] Relevant sectoral authorities, Vinnova, RISE, the Swedish Data Protection Authority, the Swedish Standards Institute, accredited bodies and relevant industry organisations should be involved. For example, the Swedish Transport Agency should have a clear role where systems relate to the transport sector's regulatory framework.

- **Establish a national regulatory sandbox for software in critical physical systems, with sector-specific tracks.** We propose a regulatory sandbox where companies can develop and test software for critical physical systems under the guidance of the relevant authorities. The sandbox should be able to operate at a comprehensive and general level, while also having specific tracks for transport and defence, for example. The aim is to enable companies to understand at an early stage how the rules are to be applied, to identify obstacles and to gather experience that can be used for future guidance and regulatory development. An important consideration is that the EU AI Act requires each Member State to establish at least one AI regulatory sandbox. We propose that PTS be responsible for coordination, in line with the proposals of the Swedish AI Inquiry. Several stakeholders need to collaborate on this, such as RISE, Vinnova, sectoral authorities and higher education institutions.

- **Strengthen Sweden's involvement in the development of standards relevant to software for critical physical systems** by increasing the participation of Swedish companies and public authorities in European and international standardisation work. Sweden should give particular priority to standards for risk management and for the quality and robustness of AI systems. The European Commission emphasises that harmonised standards are key to creating legal certainty and reducing compliance costs. The standards are voluntary but can provide companies with

71 Government Reports (2025). *Adaptations to the AI Act. Safe use, effective control and support for innovation* (SOU 2025:101).

important information once they have been published and referenced in the Official Journal of the European Union.[72] For Sweden, this is also a way of influencing the practical design of the regulatory framework rather than merely adapting to ready-made rules. The Swedish Standards Institute (SIS) should coordinate this work in collaboration with PTS, RISE, Vinnova, relevant authorities, universities and businesses.

In the short term, Sweden should map out where companies currently face the greatest regulatory bottlenecks and identify the most common situations where multiple regulatory frameworks or authorities overlap. The mapping exercise should specifically cover software-based products and systems used in safety-critical physical environments.

Within two to three years, Sweden should have a functioning model whereby companies can be informed at an early stage about which regulatory frameworks apply. For smaller companies, there should be shared tools, templates and test environments that reduce the costs of compliance.

Up until 2035, the regulatory framework and standardisation work should be developed continuously in step with technological progress. Stakeholders in Sweden should use their experience to influence the EU's guidance, standards and future regulatory developments.

We wish to emphasise that the proposal is not intended to lower safety requirements. Instead, we aim to achieve the same or a higher level of safety through shorter, clearer and more predictable pathways from development to an approved product.

Recommendations

The working group has three summary recommendations on what Sweden should focus on to build Swedish competitiveness, achieve sustainability and contribute to Swedish and global security. These are based on an analysis of the current situation regarding Sweden's position in the field of software for critical physical systems, international development trends and a review of key issues that identify obstacles and opportunities for Sweden's continued development. They summarise a number of proposals and action points which are set out in greater detail in the report.

- **Accelerate companies´ transition** from traditional products to AI-enabled, learning systems through new business models, organisational structures and stronger collaboration between stakeholders. Strengthen expertise at board and senior management level

- **Build expertise and experience in securing critical physical systems.** Adapt education and skills development more rapidly to meet industry's need for secure and reliable software.

- **Shorten the path from development to market.** Create platforms for developing, testing and validating software in realistic environments through collaboration between industry, academia and the public sector.

72 EU. *Standardisation of the AI Act*. Website: digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation? Information retrieved on 25 August 2026.

Appendix



References

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.

Glossary

Autonomous transport systems

Solutions in which vehicles (such as cars, buses or drones) can navigate and make decisions without a driver having to control every step.

Cyber security

Efforts to protect computers, software, networks and information against digital attacks, unauthorised access and other threats.

DARPA

Abbreviation for *the Defence Advanced Research Projects Agency*. DARPA is a US government agency that funds research and development into new technologies for defence purposes. DARPA runs time-limited research programmes in which researchers, companies and other stakeholders collaborate on specific technical problems and projects involving high technical risk.

GPU

Abbreviation for *Graphics Processing Unit*. A GPU is a processor that is particularly well suited to performing many calculations in parallel and is therefore used, among other things, to develop and run AI.

Embedded

The term is traditionally used for software that is integrated directly into a physical product, such as a vehicle or an industrial system.

Interoperability

The ability of different systems and programmes to exchange information and work together.

Code

Instructions written in a programming language that tell a computer what to do and how a programme or system should function. Code is part of the software.

Software

Programmes and systems consisting of code that can be run on a computer or other digital device. Software includes, for example, operating systems, applications, scripts and drivers, and may also contain data and settings.

NAISS

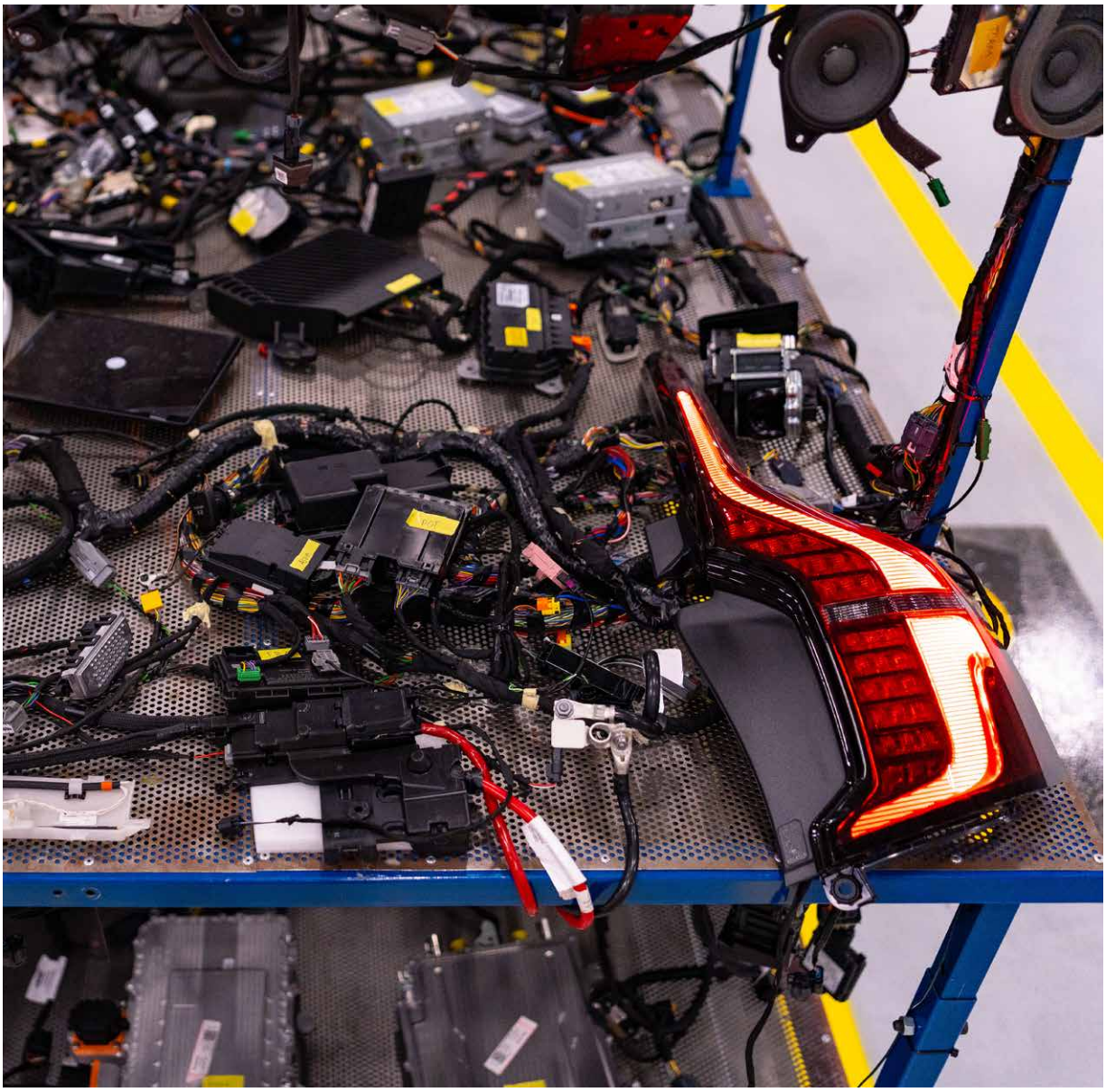
Abbreviation for the National Academic Infrastructure for Supercomputers in Sweden. NAISS is a national academic infrastructure for supercomputers that provides large-scale computing resources, storage and data services for academic users.

NIST

Abbreviation for the *National Institute of Standards and Technology*.

Sferical AI

Sferical AI was founded by AstraZeneca, Ericsson, Saab, SEB and Wallenberg Investments. The company is building a Swedish platform for AI



computing that will provide businesses with secure access to powerful computing capacity to develop and utilise AI.

STEM

Abbreviation for *science*, *technology*, *engineering* and *mathematics*.

WASP

Abbreviation for *Wallenberg AI, Autonomous Systems and Software Programme*. WASP is a Swedish research programme that develops research and expertise in AI, autonomous systems and software.

The Royal Swedish Academy of Engineering Sciences (IVA) is an independent academy whose mission is to promote the engineering and economic sciences and the advancement of business and industry. In cooperation with the business community and academia, IVA initiates and proposes measures to improve Sweden's industrial expertise and competitiveness. For more information about IVA and the Academy's projects, see the website www.iva.se.

Published by: The Royal Swedish Academy of Engineering Sciences (IVA), 2026
Box 5073, SE-102 42 Stockholm, Sweden
Tel: +46 (0)8 791 29 00

IVA-R 548
ISSN: 1100-5645
ISBN: 978-91-89181-95-3

Authors: The working group in cooperation with Charlotte Hall
Editor: Charlotte Hall
Project management: Lisa Thelin, IVA
Photos: Unsplash (s. 1), Volvo Group (s. 4, 6, 12, 16, 19),
Volvo Cars (s. 8, 22, 29, 55), Dan Boman, Scania CV AB (s. 24, 46),
Saab AB (s. 25, 31, 41, 50)
Graphic design: Pelle Isaksson, IVA

This report is available to download as a pdf file at www.iva.se

IVA's project **Swedish Futures** seeks to establish an overarching and coherent vision for Sweden as a leading nation in technology and innovation by the year 2035 – with a focus on competitiveness, sustainability, and security.



Royal Swedish Academy of Engineering Sciences