Press release

Whitepaper

Software as the Key to the Continuous Evolution of Modern Defence Systems

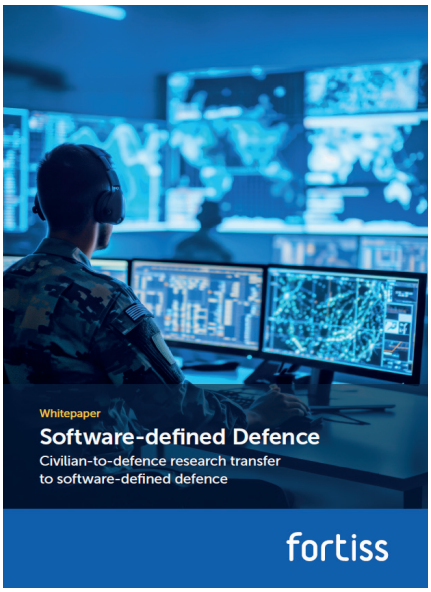
Munich, October 2026 – Modern defence capabilities are increasingly defined by software. While military platforms often remain in service for decades, software and artificial intelligence must be continuously developed, adapted, and secured. In its latest white paper, „Software-defined Defence: Civilian-to-defence research transfer to software-defined defence", fortiss describes this tension as the central "lifecycle paradox" of modern defence systems.

The white paper analyzes the technological and organizational challenges associated with the transformation toward software-defined defence systems. It focuses on three closely interconnected domains: software and systems engineering, AI engineering, and resilient communication and infrastructure solutions. Only by addressing these dimensions together can high-performance, trustworthy, and adaptable defence capabilities be developed.

From Civilian Innovation to Software-Defined Defence Capabilities

The authors demonstrate how existing technologies, methods, and tools from civilian sectors such as automotive, industry, energy, and aerospace can be leveraged for defence-related applications. Rather than starting from scratch, the white paper advocates the targeted transfer of proven approaches into the defence domain, followed by their gradual validation under realistic, adversarial operating conditions.

As a technological solution, fortiss recommends a continuous, DevOps-oriented development lifecycle. Model-based systems engineering, simulation-based testing, edge AI, resilient connectivity, and continuous cybersecurity, compliance, and assurance processes should accompany the entire lifecycle of software-defined systems and enable their rapid evolution.



fortiss-Roadmap for Software-defined Defence

Download Whitepaper >

The white paper also provides concrete recommendations for research organizations, industry, policymakers, and defence authorities.

In the short term, it recommends establishing adversarial test environments, evaluating robust communication solutions, and systematically analyzing regulatory requirements. In the medium term, the focus should shift to incremental certification approaches, open robustness benchmarks, and tactical end-to-end orchestration. In the long term, the goal is the comprehensive validation of software-defined defence systems under realistic operational conditions, including human-machine teaming.

With this white paper, fortiss positions itself as a research partner across the entire software-defined defence value chain. The institute contributes its expertise in software engineering, artificial intelligence, autonomous systems, cybersecurity, and digital infrastructures, supporting the development of resilient, sovereign, and future-ready defence capabilities in Germany and Europe.

fortiss GmbH
Guerickestraße 25, 80805 Munich
www.fortiss.org
Contact: presse@fortiss.org

fortiss

About fortiss

fortiss is the Research Institute of the Free State of Bavaria for software-intensive systems and is among Germany's leading independent research institutions in digitalization, artificial intelligence, and software engineering.

Together with partners from academia, industry, and the public sector, fortiss develops application-oriented technologies and methods, accelerating the transfer of research results into practice.

Its core areas of expertise include trustworthy AI systems, modern software and systems engineering methods, resilient digital infrastructures, autonomous and connected systems, cybersecurity, and digital sovereignty. By combining scientific excellence with practical implementation, fortiss supports companies, public authorities, and policymakers in bringing digital innovations into use in a secure, reliable, and sustainable manner.

Press Contact

Silvia Hervé
Senior Online Marketing & Communication Manager
herve@fortiss.org
Phone: +49 (89) 3603522 145

Research Contacts

Prof. Dr. Rute C. Sofia
sofia@fortiss.org

Dr. Axel von Arnim
vonarnim@fortiss.org