Schlussbericht

RESISTANT - Resilient Zero-Trust Avionics Platform
supported by Digital Security Twins and Aircraft-SOCs

Teilvorhaben: Handhabung, Verteilung und Synchronisation digitaler Zwillinge für die Überwachung von Security Anforderungen von sich im Flug befindenden Komponenten

Autoren:	Mario Thron, Piyumi Pathirathna
Projektlaufzeit:	01.11.2022 – 28.02.2026
Version:	1.00
Datum:	31.08.2026

ifak

Institut für Automation und Kommunikation e.V.

Werner-Heisenberg-Str. 1
39106 Magdebug

Das diesem Bericht zugrunde liegende Teilvorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie unter dem Förderkennzeichen **20D2116H** gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Inhaltsverzeichnis

1 Aufgabenstellung 3
2 Voraussetzungen für das Vorhaben 3
3 Planung und Ablauf des Vorhabens 5
4 Wissenschaftlich technischer Stand an den angeknüpft wurde 6
5 Zusammenarbeit mit anderen Stellen 8
6 Erzielte Ergebnisse 8
6.1 HAP 0: Projektmanagement 8
6.2 HAP 1: Anforderungen, Anwendungsfälle, Angreifermodell und Architektur 9
6.3 HAP 2: Rekonfigurierbare Zero-Trust-Plattform 10
6.4 HAP 3: Datenerfassung und Digitaler Security-Zwilling 12
6.5 HAP 4: Angriffserkennung, Risikobewertung, Angriffsbehandlung und Aircraft-SOC 15
6.6 HAP 5: Integration und Evaluation 15
7 Wichtigste Positionen des zahlenmäßigen Nachweises 16
8 Notwendigkeit und Angemessenheit der geleisteten Arbeit 16
9 Nutzung und Verwertung der Ergebnisse 17
10 Bekannt gewordener Fortschritt bei anderen Stellen 18
11 Veröffentlichungen, akademische Arbeiten und Wissenstransfer 18
Literaturverzeichnis 19
Abbildungsverzeichnis 21
Abkürzungen 22

1 Aufgabenstellung

Das Vorhaben RESISTANT war in den förderpolitischen und technologischen Rahmen des sechsten zivilen Luftfahrtforschungsprogramms, zweiter Programmaufruf (LuFo VI-2), eingebettet. Auf Programmebene bestand die Aufgabenstellung darin, Beiträge zu einer sicheren und zuverlässigen Digitalisierung der Luftfahrt zu ermöglichen und zugleich die hierfür erforderlichen technologischen Kompetenzen am Luftfahrtstandort Deutschland weiterzuentwickeln. Mit der zunehmenden Vernetzung, dem wachsenden Einsatz softwaregesteuerter Funktionen und der stärkeren funktionalen Integration von Avioniksystemen entstanden neue Anforderungen an die Beherrschung sicherheitskritischer digitaler Systeme. Daraus ergab sich insbesondere die Aufgabe, Cybersecurity nicht ausschließlich auf Ebene einzelner Komponenten zu betrachten, sondern in den Zusammenhang des Gesamtsystems und seines Betriebs einzuordnen.

Für das Verbundprojekt RESISTANT bestand die übergeordnete Aufgabenstellung darin, die Voraussetzungen für eine gegenüber Cyberangriffen widerstandsfähige Avionikarchitektur zu untersuchen. Hierzu waren sicherheitsrelevante Zustände von Komponenten und Teilsystemen zu erfassen und hinsichtlich möglicher Abweichungen vom erwarteten Verhalten zu bewerten. Eine wesentliche Herausforderung lag dabei in der Unterscheidung zwischen regulären Abweichungen, technischen Fehlfunktionen und sicherheitsrelevanten Auffälligkeiten. Darüber hinaus war zu berücksichtigen, dass die hierfür benötigten Informationen aus unterschiedlichen Komponenten und Systembereichen stammen und innerhalb einer vernetzten Avionikumgebung zuverlässig zur Verfügung stehen müssen.

Innerhalb des Verbundprojekts bestand die zentrale Aufgabe des ifak darin, digitale Zwillinge für die Überwachung von Security-Anforderungen einzusetzen. Dazu war zu untersuchen, wie digitale Zwillinge in einer verteilten Systemumgebung betrieben, koordiniert und mit den aktuellen Zustandsdaten realer Flugzeugkomponenten abgeglichen werden können. Ein weiterer Schwerpunkt lag auf den dafür benötigten Monitoringdaten. Es war zu klären, welche Anforderungen an deren Herkunft, Vertrauenswürdigkeit und sichere Übertragung gestellt werden müssen, damit sie eine verlässliche Grundlage für die Bewertung des Systemzustands und die Erkennung sicherheitsrelevanter Abweichungen bilden.

Eine weitere Aufgabenstellung ergab sich aus dem zu erwartenden Rechenaufwand und der verteilten Ausführung der digitalen Zwillinge. Hieraus entstanden Anforderungen an deren Koordination und Synchronisation sowie an die zeitlich und inhaltlich konsistente Bereitstellung der benötigten Daten. Gleichzeitig mussten die Monitoringdaten in einer Form vorliegen, die einen Vergleich mit dem jeweils erwarteten Zustand des digitalen Zwillings ermöglicht. Zu klären war daher, welche Informationen für diesen Vergleich erforderlich sind und wie reale Mess- und Zustandsdaten mit den simulierten Zuständen in Beziehung gesetzt werden können. Besondere Aufmerksamkeit erforderte schließlich die Bewertung der dabei auftretenden Abweichungen. Simuliertes und tatsächlich beobachtetes Verhalten sind in realen technischen Systemen nicht vollständig deckungsgleich, ohne dass daraus unmittelbar auf eine Fehlfunktion oder einen Angriff geschlossen werden kann. Für das ifak bestand deshalb die Aufgabe darin, geeignete Verfahren zur Bewertung solcher Unterschiede zu untersuchen. Dabei war insbesondere zu berücksichtigen, inwieweit daten- beziehungsweise KI-gestützte Methoden eine belastbare Unterscheidung zwischen tolerierbaren Abweichungen und sicherheitsrelevanten Auffälligkeiten unterstützen können. Die konkrete technische Ausgestaltung und Umsetzung dieser Aufgabenstellungen wird in den nachfolgenden Kapiteln dargestellt.

2 Voraussetzungen für das Vorhaben

RESISTANT wurde als Verbundvorhaben durchgeführt, in dem unterschiedliche Kompetenzen aus den Bereichen Avionik, IT-Sicherheit, Kommunikation, Simulation und Systemintegration

zusammengeführt wurden. Die Arbeiten des ifak waren dabei in eine übergreifende System- und Security-Architektur eingebettet und standen in engem Zusammenhang mit den Entwicklungen der weiteren Projektpartner. Für die Bearbeitung des Teilvorhabens war daher nicht nur die fachliche Ausgestaltung der eigenen Arbeiten relevant, sondern auch die Abstimmung von Schnittstellen, Datenformaten und Informationsflüssen innerhalb des Verbundes. Insbesondere die Bereitstellung von Monitoring- und Zustandsdaten sowie deren Einordnung in den Gesamtkontext des Projekts waren von den angrenzenden Teilentwicklungen abhängig.

Für die Durchführung der Arbeiten konnte das ifak auf langjährige Erfahrungen in den Bereichen industrielle Kommunikation, Automatisierung, Datenerfassung und -integration, Simulation sowie Safety und Security zurückgreifen. Diese Kompetenzen waren in zahlreichen vorangegangenen Forschungs- und Entwicklungsprojekten aufgebaut worden. Hinzu kamen Erfahrungen mit verteilten Automatisierungssystemen, serviceorientierten Architekturen, sicheren Kommunikationsstrukturen und der Integration heterogener Datenquellen. Das Institut verfügte damit über die fachlichen und methodischen Voraussetzungen, um Fragestellungen an der Schnittstelle zwischen realen technischen Systemen, deren digitalen Abbildern und der Verarbeitung von Zustands- und Monitoringdaten zu bearbeiten.

Auch auf technischer Ebene bestanden geeignete Ausgangsbedingungen. Vorhandene Softwarekomponenten und Entwicklungswerkzeuge aus früheren Arbeiten konnten als Grundlage für die Projektarbeiten herangezogen werden. Dazu gehörten insbesondere Werkzeuge und Module für die integrierte Automation und Simulation sowie Erfahrungen mit FMI-/FMU-basierten Simulationsmodellen. Diese Vorarbeiten stellten keine fertige Lösung für die im Projekt zu bearbeitenden Fragestellungen dar, reduzierten jedoch den Aufwand für grundlegende Entwicklungs- und Integrationsaufgaben und ermöglichten es, unmittelbar an projektbezogenen Fragestellungen anzusetzen.

Die Arbeiten wurden zudem durch die fachliche Einbindung des ifak in nationale und internationale Normungs- und Fachgremien unterstützt. Mitarbeiter des Instituts wirkten unter anderem in Arbeitskreisen zu Industrie 4.0, industrieller Kommunikation und funktionaler Sicherheit mit. Berührungspunkte zu Standardisierungsaktivitäten ergaben sich im Vorhaben insbesondere durch die Nutzung des Functional Mock-up Interface (FMI) als standardisierte Schnittstelle für die Entwicklung und Kopplung digitaler Zwillinge. Eine unmittelbare Beteiligung des ifak an der FMI-Standardisierung bestand jedoch nicht.

Während der Projektlaufzeit änderten sich einzelne technologische Rahmenbedingungen. Dies betraf insbesondere die Verfügbarkeit leistungsfähiger Large Language Models (LLMs). Zu Projektbeginn standen diese Modelle für die vorgesehene Nutzung noch nicht in einer Form zur Verfügung, die einen praktischen Einsatz für spezialisierte Entwicklungsaufgaben nahelegte. Im weiteren Projektverlauf wurden jedoch zunehmend Modelle verfügbar, die Programmcode erzeugen und auch lokal betrieben werden konnten. Damit veränderten sich die Voraussetzungen für eine teilautomatisierte Erstellung von Simulationsmodellen. Diese Entwicklung wurde im Projekt aufgegriffen und hinsichtlich ihrer Eignung für den betrachteten Anwendungsfall untersucht. Von besonderem Interesse war dabei die Möglichkeit einer lokalen Ausführung der LLMs, da hierdurch Daten und Modelle innerhalb der eigenen Infrastruktur verarbeitet werden können. Die konkrete Nutzung und die daraus gewonnenen Erkenntnisse werden in den späteren Ergebniskapiteln dargestellt.

Der Durchführung des Vorhabens standen nach Kenntnis der Projektpartner keine Patente oder sonstigen Schutzrechte Dritter entgegen. Insgesamt waren damit sowohl die erforderlichen personellen und fachlichen Kompetenzen als auch geeignete technische und organisatorische Voraussetzungen vorhanden, um die vorgesehenen Forschungs- und Entwicklungsarbeiten im Verbund durchzuführen. Gleichzeitig blieb die Bearbeitung durch die für Forschungsprojekte typische Abhängigkeit von technischen Entwicklungen, verfügbaren Daten, Schnittstellen zu Partnerarbeiten und sich während der Laufzeit verändernden technologischen Möglichkeiten geprägt.

3 Planung und Ablauf des Vorhabens

Abbildung 1 zeigt den ursprünglichen Gesamt-Terminplan für das Verbundprojekt RESISTANT, wobei Monat 1 dem November 2022 entspricht.

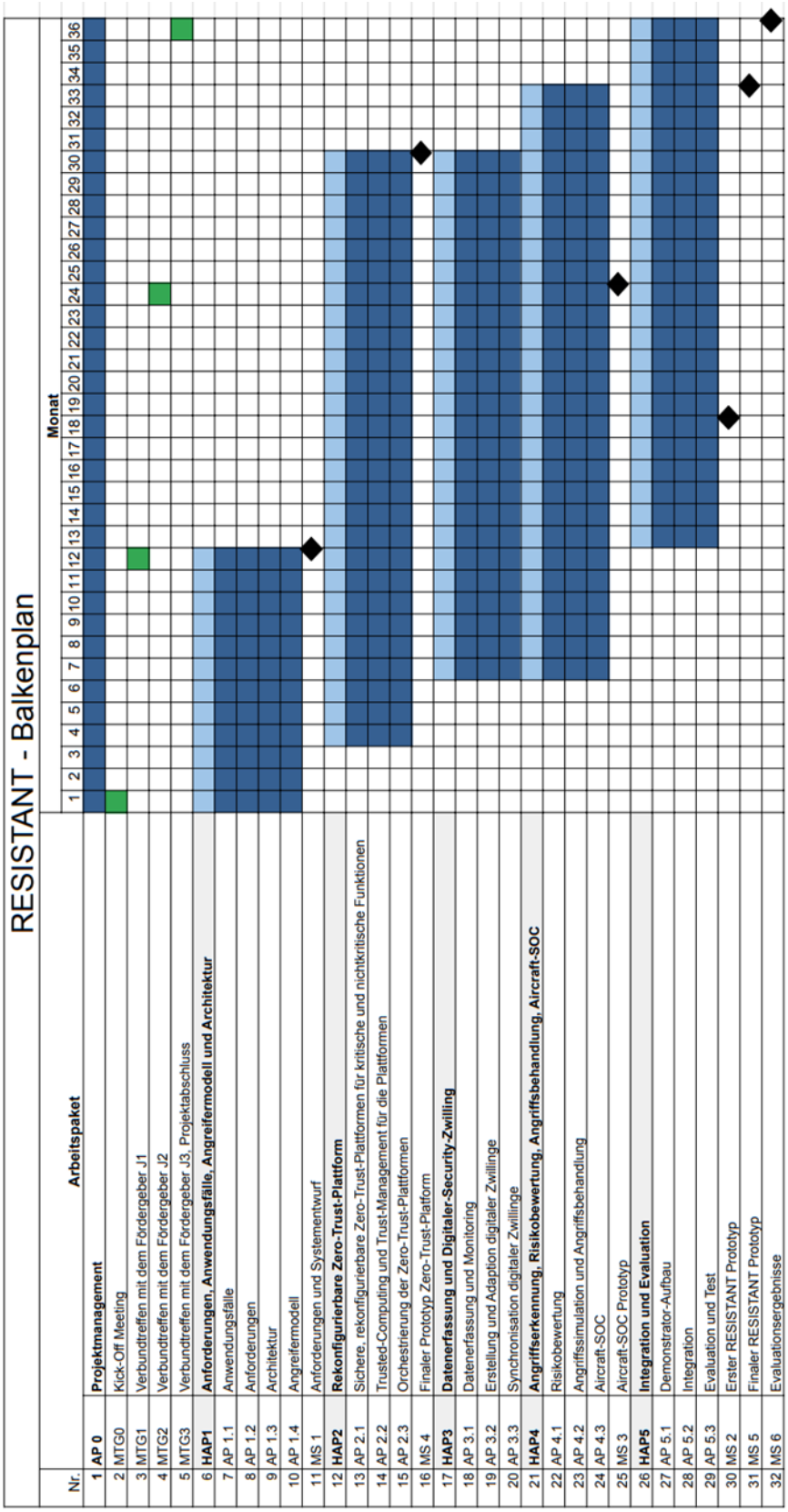

Abbildung 1: Ursprünglicher Gesamt-Terminplan des Verbundprojekts RESISTANT

Das Vorhaben verlief von November 2022 bis Februar 2026 weitgehend planmäßig in vier Phasen. Nach Projektstart, Kick-off und Anforderungsanalyse wurden 2023 die Anwendungsfälle strukturiert, Anforderungen und Architektur entwickelt sowie erste technische Konzepte zur verteilten Co-Simulation, Anomalieerkennung und FMU-Generierung erarbeitet. 2024 lag der Schwerpunkt auf der Implementierung und Erweiterung der Demonstratoren. Im Jahr 2025 wurden die verteilte Co-Simulation, zusätzliche KI-basierte Vorhersageverfahren, die Synchronisation zwischen digitalem Zwilling und physikalischem Prozess sowie der FMU-Generator fertiggestellt und die Integration vorbereitet. Anfang 2026 erfolgte die Übertragung der ifak-Software auf die Airbus-Knoten der TSN-basierten RESISTANT-Infrastruktur und die Inbetriebnahme der durchgängigen Verarbeitungskette von der Datenerfassung über die Simulation bis zur Anomalieerkennung und Alarmierung. Die Projektergebnisse wurden am 26.02.2026 beim Final Review Meeting in Stuttgart vorgestellt.

Für das ifak entsprach der Vorhabensstand in den ersten Berichtszeiträumen der ursprünglichen Arbeits-, Zeit- und Kostenplanung. Im Jahr 2023 wurde etwas weniger am Projekt gearbeitet als geplant, weil neu eingestellte Mitarbeitende ihre Arbeitsleistung erst ab 2024 entfalteten; dieser geringe Verzug wurde im Folgejahr aufgeholt. Im Jahr 2024 ergab sich eine Verzögerung der Integrationsarbeiten mit einer Verschiebung geringer Anteile der Arbeitsaufwände in das Folgejahr. Ursache war, dass einige Projektpartner die notwendigen Personalkapazitäten erst später aufbauen konnten und die Arbeiten des ifak zur Angriffserkennung auf einer von den Partnern entwickelten Infrastruktur aufsetzen. Entsprechend wurden auch etwas weniger Mittel abgerufen als geplant. Da sich die Integration in die gemeinsam abzustimmende RESISTANT-Gesamtarchitektur schwieriger gestaltete als ursprünglich angenommen (der Aufwand lag dabei weniger in der Software selbst als in den gegenseitigen Abstimmungen zu IP-Adressvergabe, Kubernetes- und Tenzir-Konfiguration), beantragten alle Partner eine kostenneutrale Projektverlängerung. Diese wurde bewilligt und verlängerte die Laufzeit bis zum 28.02.2026. Die verbleibenden Integrations- und Evaluierungsschritte konnten dadurch in den Monaten Januar und Februar 2026 abgeschlossen werden. Änderungen der Zielsetzung des Vorhabens waren zu keinem Zeitpunkt erforderlich, und die Aussichten für die Erreichung der Projektziele haben sich über die gesamte Laufzeit gegenüber dem ursprünglichen Antrag nicht verschlechtert.

4 Wissenschaftlich technischer Stand an den angeknüpft wurde

Zu Beginn des Vorhabens lagen bereits umfangreiche Forschungsarbeiten zu digitalen Zwillingen, simulationsgestützter Systembewertung, maschinellem Lernen und der Überwachung technischer Systeme vor. Die einzelnen Technologien waren jedoch unterschiedlich weit entwickelt und insbesondere für ihre gemeinsame Nutzung in einer sicherheitskritischen Avionikumgebung bestanden weiterhin offene Fragestellungen. RESISTANT knüpfte daher nicht an eine einzelne bestehende Technologie an, sondern an mehrere Forschungsrichtungen, die für die Überwachung und Bewertung des Zustands vernetzter Flugzeugkomponenten zusammengeführt werden sollten.

Digitale Zwillinge hatten sich bereits vor Projektbeginn insbesondere im industriellen Engineering, bei der virtuellen Inbetriebnahme und bei der Zustandsbewertung komplexer Anlagen etabliert. In der Forschung bestand allerdings kein einheitliches Verständnis darüber, wie ein digitaler Zwilling aufgebaut sein sollte und welche Modelle, Daten und Schnittstellen hierfür erforderlich sind. Ein wesentlicher Schwerpunkt bestehender Arbeiten lag auf der möglichst realitätsnahen Abbildung des physischen Systems und auf der Nutzung realer Betriebsdaten (eines physischen Demonstrators) zur Aktualisierung und Validierung der Modelle. Für industrielle und luftfahrtbezogene Anwendungen war bereits gezeigt worden, dass digitale Zwillinge zur frühzeitigen Designvalidierung, zur Zustandsüberwachung und zur Unterstützung von Wartungs- und Entscheidungsprozessen eingesetzt werden können. Weniger geklärt war dagegen ihre Nutzung als Bestandteil einer laufenden Security-

Überwachung, insbesondere wenn Modelle und zugehörige Datenverarbeitung verteilt betrieben werden müssen.

Für die technische Umsetzung simulationsbasierter digitaler Zwillinge konnte auf etablierte Ansätze zum Modellaustausch und zur Co-Simulation zurückgegriffen werden. Von besonderer Bedeutung war das Functional Mock-up Interface (FMI), das eine werkzeugunabhängige Bereitstellung und Kopplung von Simulationsmodellen ermöglicht. In Form von Functional Mock-up Units konnten Teilmodelle in gemeinsame Simulationsumgebungen integriert werden. FMI und verwandte Ansätze waren bereits in verschiedenen Forschungs- und Industrieprojekten für die Kopplung heterogener Modelle und die virtuelle Inbetriebnahme eingesetzt worden. Damit bestand ein geeigneter technischer Ausgangspunkt für die Einbindung Physik-basierter Modelle. Offen blieben jedoch Fragestellungen hinsichtlich ihrer Nutzung in einer dynamischen, verteilten Überwachungsarchitektur und der Synchronisation mit kontinuierlich eintreffenden Daten des realen Systems.

An diese Problemstellung knüpfte der Stand des maschinellen Lernens und der Anomalieerkennung an. Zu Projektbeginn standen bereits leistungsfähige Verfahren aus dem Bereich des maschinellen Lernens und des Deep Learning für Klassifikations-, Prognose- und Anomalieerkennungsaufgaben zur Verfügung. In unterschiedlichen Anwendungsfeldern wurden solche Methoden eingesetzt, um komplexe Datenmuster zu erfassen und das Verhalten technischer Prozesse vorherzusagen. Für den Anwendungsfall von RESISTANT waren insbesondere Verfahren von Interesse, die Zusammenhänge zwischen mehreren Prozessgrößen berücksichtigen und daraus Erwartungswerte für das zukünftige Systemverhalten ableiten können. Ein hierfür relevanter Ansatz bestand in der Kombination selbstorganisierender Karten mit Verfahren zur multivariaten Zeitreihenprognose. Dadurch sollten charakteristische Strukturen und Abhängigkeiten in hochdimensionalen Prozessdaten für die Vorhersage des erwarteten Systemverhaltens genutzt werden.

Der Forschungsbedarf bestand insbesondere darin, solche Verfahren für die im Projekt betrachteten heterogenen Monitoringdaten auszugestalten und ihre Eignung für die Erkennung sicherheitsrelevanter Auffälligkeiten zu untersuchen. Die eigentliche Anomalieentscheidung konnte dabei weiterhin auf der Bewertung der Abweichung zwischen vorhergesagtem und beobachtetem Verhalten beruhen, beispielsweise anhand geeigneter Toleranz- oder Triggerschwellen. Entscheidend war daher insbesondere die Qualität des zugrunde liegenden Erwartungsmodells und dessen Fähigkeit, normale Zusammenhänge und zeitliche Verläufe der Prozessgrößen hinreichend genau abzubilden.

Parallel dazu existierten bereits Forschungs- und Entwicklungsarbeiten zu Cybersecurity und Resilienz in vernetzten technischen Systemen. Projekte wie MonIKA [1], INDI oder IMMUNE [2] beschäftigten sich mit Anomalieerkennung, verteilten Sicherheitsfunktionen und der Erkennung von Angriffen in industriellen Netzen. Im Luftfahrtumfeld bestanden Arbeiten zu Zero-Trust-Konzepten, Security Operations Centern und modellbasierter Security-Analyse. Auch Projekte wie TALIA [3] und PAFA-ONE [4] adressierten Aspekte zukünftiger Avionikarchitekturen, ihrer Vernetzung und ihrer Absicherung. Diese Arbeiten zeigten die grundsätzliche Relevanz verteilter Security-Mechanismen und systemweiter Überwachung, stellten jedoch noch keine unmittelbar übertragbare Lösung für die Kombination aus digitalen Zwillingen, verteiltem Monitoring und Security-Bewertung in der von RESISTANT betrachteten Form bereit.

Auf Seiten des ifak bestanden darüber hinaus einschlägige Vorarbeiten aus Forschungsprojekten wie IMC-AESOP, SOCRADES, SIVIKO-SCADA, autoAPSint, ECOSSIAN, AVANTI, ENTOC und IMMUNE. Aus diesen Arbeiten lagen Erfahrungen mit serviceorientierten und verteilten Architekturen, industrieller Kommunikation, Datenerfassung und -modellierung, Simulation sowie der Security-Überwachung technischer Netze vor. Mit bestehenden Arbeiten zu FMI/FMU und dem Framework für integrierte Automation und Simulation konnte zudem an vorhandene methodische und softwaretechnische Grundlagen angeknüpft werden. Der wissenschaftlich-technische Ausgangspunkt des Teilvorhabens lag somit in der Verbindung dieser bislang überwiegend getrennt betrachteten Themenfelder: digitale

Zwillinge und Simulation, kontinuierliche Monitoringdaten, datenbasierte Bewertung sowie Security in verteilten technischen Systemen.

5 Zusammenarbeit mit anderen Stellen

Das Vorhaben RESISTANT wurde im Verbund mit Airbus Defence and Space GmbH, der Fraunhofer-Gesellschaft, der Universität Stuttgart (UST), Siemens AG, der Universität Hamburg (UHH) und der Industrieanlagen-Betriebsgesellschaft mbH (IABG) durchgeführt. Die Koordination erfolgte in HAP0 mit regelmäßigen Online-Meetings sowie mehreren physischen Konsortialtreffen. In HAP1 wurden mit Airbus als industriellem Anwendungspartner Anwendungsfälle strukturiert, Anforderungen an die Flugzeugsteuerungszone (Aircraft Control Domain) abgeleitet und die auf dem DELIA-Projekt [5] aufbauende RESISTANT-Knotenarchitektur entworfen. In AP 2.3 (mit UHH und UST) gestaltete das ifak den Informationsfluss zwischen Simulationseinheiten und die Verteilung digitaler Zwillinge über RESISTANT-Knoten. In HAP3 wurde mit Airbus, UHH, Siemens und IABG zusammengearbeitet, wobei ifak die ML-basierte Anomalieerkennung (BSOM-WMVFTS, später ergänzt durch LSTM), der LLM-gestützte FMU-Generator („FMU Factory“ mit lokalem Modell Codestral der französischen Firma Mistral) und die verteilte Co-Simulationsplattform entwickelte. In HAP5 wurden die ifak-Komponenten auf die Airbus-Knoten übertragen und in den RESISTANT-Demonstrator integriert; die Kopplung über AMQP/MQTT ([6], [7]) und Datendiode erforderte umfangreiche Detailabstimmungen (IP-Adressvergabe, Kubernetes- und Tenzir-Konfiguration) mit den Partnern.

Neben der technischen Zusammenarbeit trug das ifak über die Otto-von-Guericke-Universität Magdeburg durch die Unterstützung einer Master-Arbeit zur Wissensvermittlung bei. Die im Verbund erzielten Ergebnisse wurden in der Abschlussveranstaltung zusammengefasst. Die Kooperationen mit den akademischen und industriellen Partnern sollen nach Projektende fortgeführt und auf angrenzende Branchen (Fertigungs- und Prozessindustrie) ausgeweitet werden.

6 Erzielte Ergebnisse

6.1 HAP 0: Projektmanagement

In HAP 0 waren die für die Koordination des Verbundvorhabens erforderlichen Managementstrukturen und Prozesse zu etablieren. Dazu gehörten die Planung und Durchführung regelmäßiger Treffen des Gesamtverbunds, das Risikomanagement sowie die Verbreitung des Projekthintergrunds und der Arbeitsergebnisse. Als Ergebnisse waren insbesondere eine effiziente Zusammenarbeit, eine Projekt-Homepage und wissenschaftliche Veröffentlichungen vorgesehen.

Das ifak sollte die erforderlichen Aktivitäten des Projektmanagements unterstützen. Dies umfasste insbesondere das Verfassen von Statusberichten sowie die Vorbereitung von Reviews und Konsortialtreffen.

Das ifak beteiligte sich während der gesamten Projektlaufzeit kontinuierlich an der organisatorischen und fachlichen Abstimmung im Konsortium. Bereits 2022 wirkte es am Projektauftakt, an der Festlegung der Zusammenarbeit und an der Erarbeitung des Konsortialvertrags mit. Neben regelmäßigen Online-Besprechungen nahm das ifak an diversen Konsortialtreffen teil.

Die Arbeiten und Ergebnisse wurden in den jährlichen Zwischenberichten dokumentiert und für das Final Review Meeting am 26. Februar 2026 in Stuttgart aufbereitet und präsentiert. Zur wissenschaftlichen Verbreitung trug die Veröffentlichung von Pathirathna, Xin und Thron, „Comparative Analysis of SOM-WMVFTS and BSOM-WMVFTS in High-Dimensional Multivariate Time Series Forecasting“ [9], bei. Der Beitrag wurde auf der 11th IFAC Conference on Manufacturing

Modelling, Management and Control (MIM 2025) vorgestellt. Darüber hinaus wurden eine Masterarbeit betreut und damit Projektergebnisse in die universitäre Ausbildung eingebracht.

Mit der kontinuierlichen Teilnahme an den Projektabstimmungen, der Erstellung der Statusberichte, der Mitwirkung an Konsortial- und Integrationstreffen sowie der Vorbereitung und Durchführung des Abschlussvortrags setzte das ifak seinen vorgesehenen Beitrag zu HAP 0 um. Die wissenschaftliche Veröffentlichung und der Transfer in die Lehre unterstützten zusätzlich die vorgesehene Dissemination.

6.2 HAP 1: Anforderungen, Anwendungsfälle, Angreifermodell und Architektur

HAP 1 hatte die Aufgabe, für moderne, stark vernetzte Flugzeugsysteme geeignete Anwendungsfälle, Anforderungen und Konzepte zur Informationssicherheit zu erarbeiten. Die Anwendungsfälle sollten die Gültigkeit der Anforderungen und Grundannahmen demonstrieren und neben der Informationssicherheit auch Aspekte wie Systemleistung, Betriebssicherheit und Wartung berücksichtigen. Aus ihnen waren relevante Anforderungen aus Betrieb, Entwicklung und Zulassung abzuleiten, zu klassifizieren und zu verallgemeinern. Darauf aufbauend sollte eine beispielhafte Systemarchitektur als Grundlage des Demonstrators entstehen. Ergänzend waren Schutzbedarf, Kritikalität, mögliche Folgen von Fehlfunktionen und Angriffsszenarien zu untersuchen und in einem Angreifermodell zusammenzuführen.

In AP 1.1 sollte das ifak die von den Industriepartnern definierten Anwendungsfälle strukturieren, formalisieren und hinsichtlich ihrer Übertragbarkeit verallgemeinern. In AP 1.2 sollte es die Anforderungen mit den Anwendungsfällen verknüpfen und zu ihrer Klassifikation, Formalisierung und Abstraktion beitragen. Für AP 1.3 war ein Design für die Zusammenarbeit digitaler Zwillinge und für eine dynamische Netzkonfiguration vorgesehen, das eine Zustandsüberwachung mithilfe digitaler Zwillinge und KI-Verfahren ermöglicht. In AP 1.4 sollte das ifak Risiken beim Einsatz digitaler Zwillinge untersuchen und daraus Empfehlungen für deren Implementierung und Nutzung ableiten.

Gemeinsam mit Airbus und den weiteren Projektpartnern strukturierte und bewertete das ifak die aus den industriellen Szenarien abgeleiteten Anwendungsfälle. Dabei wurde auch untersucht, inwieweit sich die Anwendungsfälle auf andere Branchen und technische Kontexte übertragen lassen. Als repräsentatives Beispiel wurde ein Tanksystem ausgewählt, das Komponenten und dynamische Vorgänge eines Flugzeugtanksystems abbildet. Das betrachtete Angriffsszenario kombiniert physischen Zugriff auf das System, eine zeitverzögert ausgelöste Attacke und die Manipulation des Tankfüllstands. Daraus wurde als zentrale Anforderung eine physikbezogene Angriffserkennung durch betriebsparallele Simulation und den Vergleich gemessener mit simulierten Prozesswerten abgeleitet.

Weitere Anforderungen betrafen die Gewinnung von Daten aus der Aircraft Control Domain, den rückwirkungsfreien Informationsübergang über eine Datendiode, die standardisierte und werkzeugunabhängige Modellierung digitaler Zwillinge mithilfe des Functional Mockup Interface (FMI, [8]) sowie deren teilautomatisierte Erstellung. Die Trennung der Informationszonen stellte eine wesentliche Randbedingung für die Architektur und die spätere Integration dar.

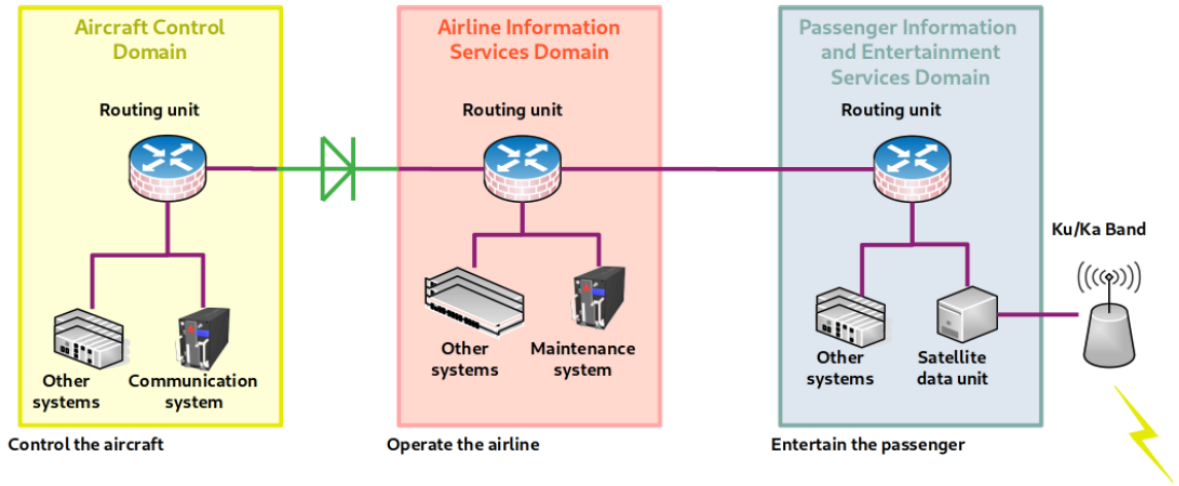

Abbildung 2: Informationszonen in modernen Flugzeugen (Quelle: Airbus)

Für die Netzwerkarchitektur wirkte das ifak an der Weiterentwicklung eines aus dem Forschungsprojekt DELIA stammenden Ansatzes mit. Digitale Zwillinge sollten über mehrere physische und logische RESISTANT-Knoten verteilt, über sichere Verbindungen gekoppelt und für Zustandsüberwachung und Simulation genutzt werden. Als technische Randbedingungen wurden eine möglichst transparente Kommunikation über Knotengrenzen hinweg sowie portable und gekapselte Implementierungen auf Linux-basierten Plattformen festgelegt. Hierfür wurden unter anderem Docker-Container und reproduzierbare Nix-Pakete betrachtet.

Im Angreifermodell untersuchte das ifak insbesondere technische Manipulationen, die sich als Abweichungen zwischen dem Verhalten des realen Systems und dem digitalen Zwilling zeigen und mit simulations- oder ML-basierten Methoden erkannt werden können. Zugleich wurden Risiken des digitalen Zwillings selbst sowie die Notwendigkeit vertrauenswürdiger Daten- und Kommunikationswege berücksichtigt. Das resultierende Domänen- und Architekturmodell mit Aircraft Control Domain, Aircraft Information Domain beziehungsweise Airline Information Services Domain und Passenger Information and Entertainment Services Domain bildete die Grundlage für die nachfolgenden Demonstratorarbeiten.

Die Strukturierung und Verallgemeinerung des Tanksystem-Anwendungsfalls, die Ableitung und Zuordnung der Anforderungen, das Design der verteilten Digital-Twin-Architektur sowie die Untersuchung eines konkreten Manipulationsszenarios setzen die in AP 1.1 bis AP 1.4 vorgesehenen Beiträge des ifak um. Die Ergebnisse wurden in HAP 2, HAP 3 und HAP 5 unmittelbar als fachliche und technische Grundlage weiterverwendet.

6.3 HAP 2: Rekonfigurierbare Zero-Trust-Plattform

In HAP 2 sollte auf Basis der Anforderungen, Anwendungsfälle, Angriffsszenarien und Architektur aus HAP 1 eine cybersichere Rechnerplattform für sicherheitskritische und nicht sicherheitskritische Flugzeugfunktionen sowie für die Boden-IT entstehen. Die einzelnen Plattformen und ihre Verbindung sollten dem Zero-Trust-Prinzip folgen und hierfür unter anderem Virtualisierung, Isolation, Laufzeitorchestrierung, dynamische Rekonfiguration und Trust Management einsetzen. AP 2.3 adressierte eine übergeordnete Orchestrierungsinstanz zur Koordination und Anpassung von Anwendungen mit verteilten Diensterbringern unter Berücksichtigung verfügbarer Ressourcen und Kommunikationsanforderungen.

Das ifak hatte keine Beiträge zu AP 2.1 und AP 2.2. In AP 2.3 sollte es digitale Zwillinge auf mehrere Netzwerkknoten verteilen und die Informationsflüsse zwischen ihnen verknüpfen. Hierzu waren die Netzwerkströme zur Laufzeit zu analysieren, Verfahren zur Rekonfiguration abzuleiten und die

gefundenen Lösungen einschließlich ihrer Leistungsfähigkeit zu evaluieren. Bei einer Verlagerung digitaler Zwillinge auf andere Knoten sollten Netzwerk und Informationsflüsse entsprechend angepasst werden können.

Das ifak entwickelte zunächst das Konzept eines Co-Simulators als Orchestrator verteilter Simulationsmodelle (siehe Abbildung 3). Die digitalen Zwillinge (Simulation 2a und Simulation 2b) werden dabei über verschiedene RESISTANT-Knoten verteilt, um auf mehreren Rechnern verfügbare Rechen- und Speicherressourcen für eine betriebsparallele Simulation nutzen zu können.

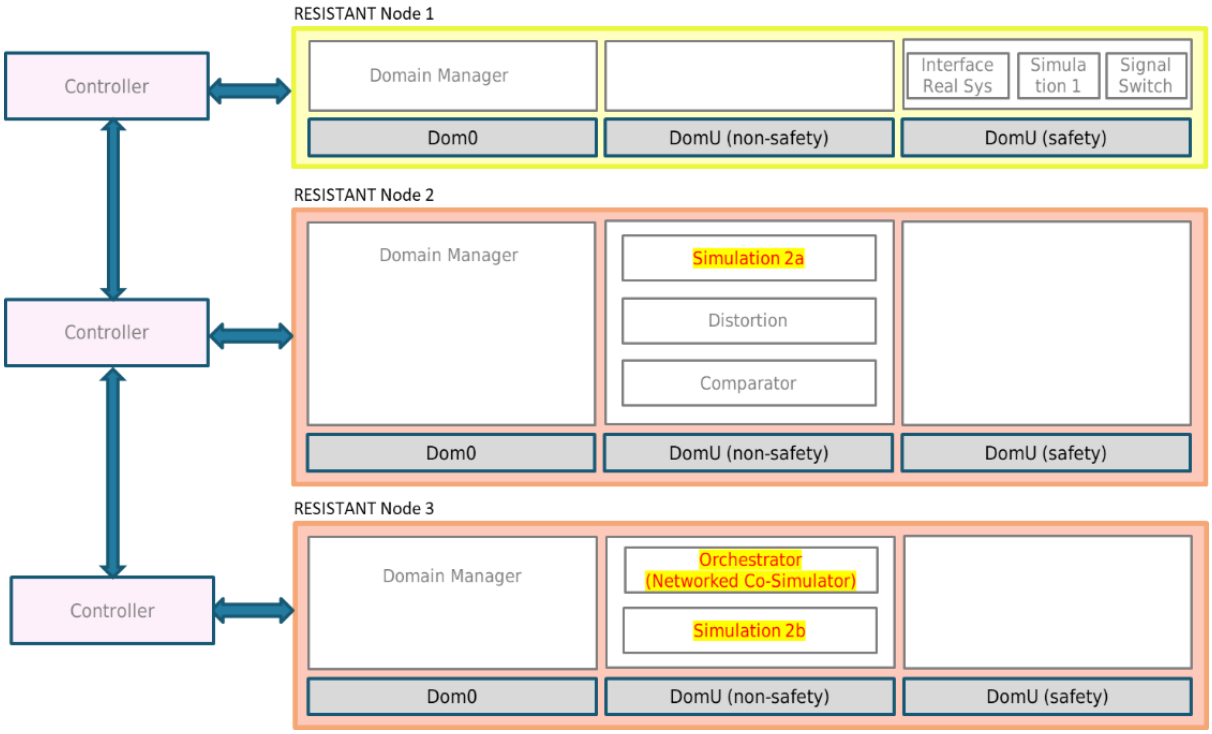

Abbildung 3: Co-Simulator als Orchestrator zur Steuerung verteilter Simulationsmodelle

Da FMI Simulationsmodelle grundsätzlich innerhalb eines Betriebssystemprozesses verwaltet werden, wurde die lokale Ausführung um eine netzwerkfähige Kopplung erweitert. Ein zentraler, auf *libcosim* basierender Co-Simulator steuert die Simulation (siehe Abbildung 4). Für eine entfernte FMU startet er lokal eine Proxy-FMU. Diese kommuniziert über das Netzwerk mit einem FMU-Boot-System, das die eigentliche FMU auf dem entfernten Rechner startet und verwaltet. Damit wurden Start, Stopp und Datenaustausch von Simulationskomponenten über RESISTANT-Knoten hinweg ermöglicht. Die technische Umsetzung nutzte *libcosim*, *proxyfmu* und *pyfmu*. Aufwendige Build-Prozesse und eine unvollständige Dokumentation der Bibliotheken wurden durch gezielte Analyse und Reverse Engineering bewältigt.

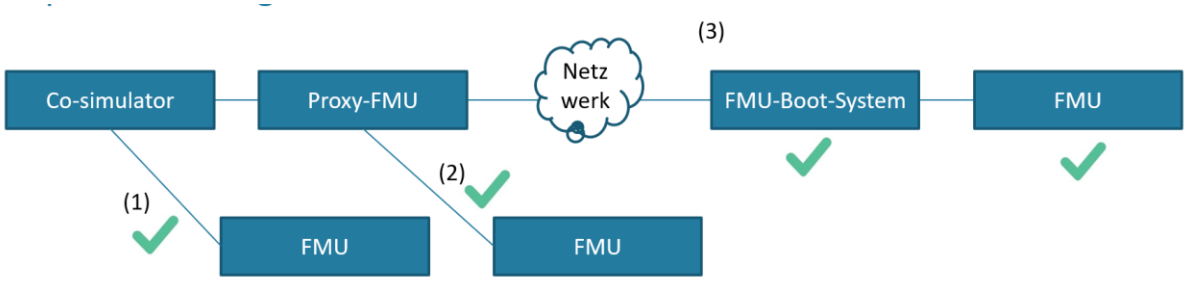

Abbildung 4: Prinzip der verteilten Co-Simulation

Die Lösung wurde schrittweise im ifak-Labor aufgebaut: zunächst mit einer lokalen FMU, danach mit einer Proxy-FMU und schließlich mit der vollständigen Verbindung zwischen Proxy-FMU und

entferntem FMU-Boot-System. Der Laboraufbau verteilte die Funktionen auf drei Linux- beziehungsweise Docker-Hosts und koppelte sie über Ethernet. Er umfasste unter anderem die Schnittstelle zum realen System, Simulationskomponenten, Signalumschaltung, Störungseinprägung, Comparator und Orchestrator. Mit der 2025 fertiggestellten Verbindung war die vollständige Kommunikation prinzipiell möglich und die verteilte FMI-Co-Simulation funktionsfähig. Die Anwendung musste jedoch noch auf die gemeinschaftliche Infrastruktur (TSN, Kubernetes) für den Abschlussdemonstrator migriert werden (siehe HAP 5).

Die realisierte Proxy-FMU-/FMU-Boot-Architektur verteilt digitale Zwillinge auf verschiedene Rechnerknoten, stellt ihre Informationsflüsse her und erlaubt die orchestrierte entfernte Ausführung. Der stufenweise Laborversuch und die anschließende Integration dienten der funktionalen Evaluierung der Lösung. Damit wurden die für AP 2.3 vorgesehenen Beiträge des ifak zur Analyse, Kopplung, Orchestrierung und Rekonfiguration verteilter Simulationskomponenten umgesetzt.

6.4 HAP 3: Datenerfassung und Digitaler Security-Zwilling

HAP 3 befasste sich mit der Erstellung und dem Betrieb digitaler Security-Zwillinge. Dazu sollten reale Zustände erfasst und überwacht, sicherheitsrelevante Abweichungen zwischen Ist- und Sollzuständen erkannt, digitale Abbilder möglichst automatisiert erzeugt und parallel betriebene Zwillinge mit dem physikalischen Prozess synchronisiert werden. Standardisierte Schnittstellen wie FMI sollten die Erstellung und Kopplung der Modelle erleichtern. Da unvermeidbare Modellabweichungen langfristig zu einer Drift zwischen Simulation und Prozess führen, war außerdem eine sichere periodische Synchronisation erforderlich, ohne manipulierte Prozesszustände unkritisch in den Zwilling zu übernehmen.

In AP 3.1 sollte das ifak die Aussagekraft zusammengeführter Ergebnisse vertrauenswürdiger digitaler Zwillinge mit KI-Methoden untersuchen und insbesondere unüberwachte Lernverfahren, beispielsweise selbstorganisierende Karten, prototypisch umsetzen. In AP 3.2 sollte es zur effizienten Erstellung digitaler Zwillinge beitragen, Informationen aus Steuerungskomponenten wiederverwenden und Sensordaten in allgemeiner Form für Simulations- und Auswertungskomponenten verfügbar machen. Im AP 3.3 sollte eine skalierbare Co-Simulationsplattform entstehen, welche digitale Zwillinge mit standardisierten FMU-Schnittstellen auf mehrere Rechnerknoten verteilt, synchronisiert und evaluiert.

Für AP 3.1 entwickelte das ifak eine physik- und datenbezogene Anomalieerkennung an einem prozesstechnischen Tanksystem. Die Anlage stellt binäre, ganzzahlige und kontinuierliche Variablen über OPC bereit und durchläuft wiederholte Befüll- und Entleerungsvorgänge. Prozessdaten konnten aufgezeichnet und wiedergegeben werden; ein Signalgenerator erlaubte die reproduzierbare Einprägung definierter Störungen. Beim simulationsbasierten Verfahren läuft der digitale Zwilling parallel zum realen System. Ein Comparator ermittelt Abweichungen zwischen gemessenen und simulierten Werten, aus denen ein Feedback-Generator Status- oder Alarmsignale ableitet.

Als ML-basiertes Verfahren wurde zunächst ein hybrides Modell aus Bi-level Self-Organizing Maps (BSOM, [10]) und Weighted Multivariate Fuzzy Time Series (WMVFTS) ausgewählt und für Demonstrationszwecke umgesetzt. Dies erweiterte das Konzept von dos Santos et al (2021, [11]), welches auf einfachen selbstorganisierenden Karten [12] basiert. Mehrere selbstorganisierende Karten mit unterschiedlichen Lernparametern bilden dabei die erste Ebene; ihre Gewichtsmatrizen gehen in eine zweite BSOM-Ebene ein. Am Tanksystem konnte gezeigt werden, wie aus der Abweichung zwischen tatsächlichen und vorhergesagten Werteverläufen nach Überschreiten einer zeitabhängigen Triggerschwelle ein Alarm abgeleitet wird (siehe Abbildung 5).

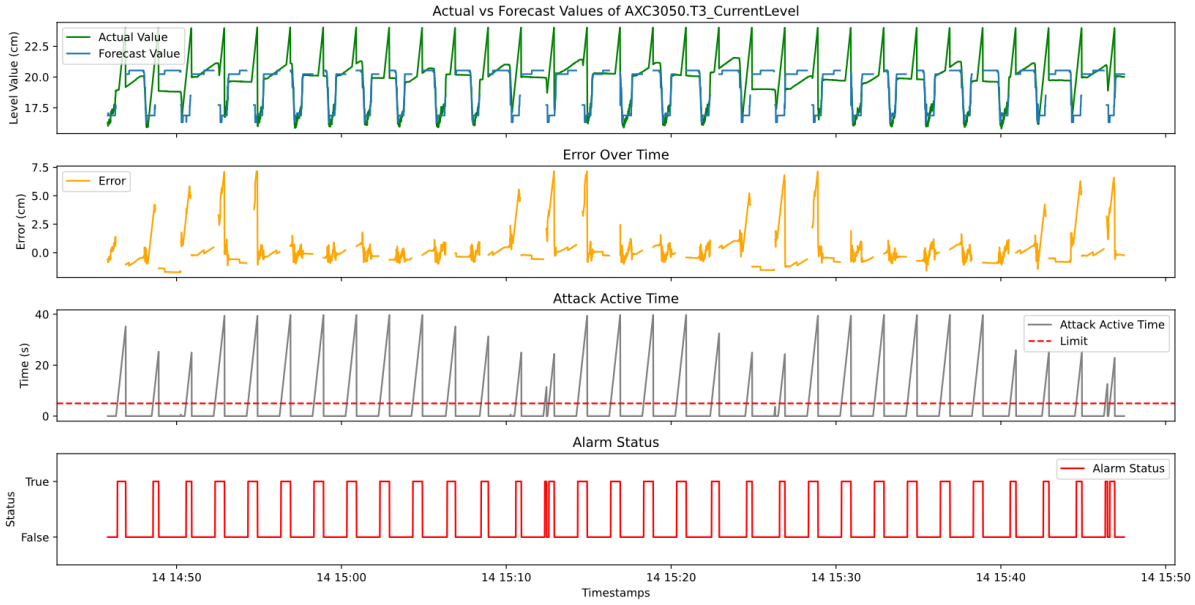

Abbildung 5: Anomalieerkennung (unten, rot) mit einer Kombination aus neuronalen Netzen und Fuzzy-Logik

Eine Webanwendung unterstützt das Einlesen mehrerer Trainingsabläufe, die Auswahl vermuteter abhängiger Variablen, die Einstellung der Lernparameter, das Trainieren und Speichern der Modelle sowie ihre Anwendung auf Echtzeitdaten (Screenshots siehe Abbildung 6 und Abbildung 7).

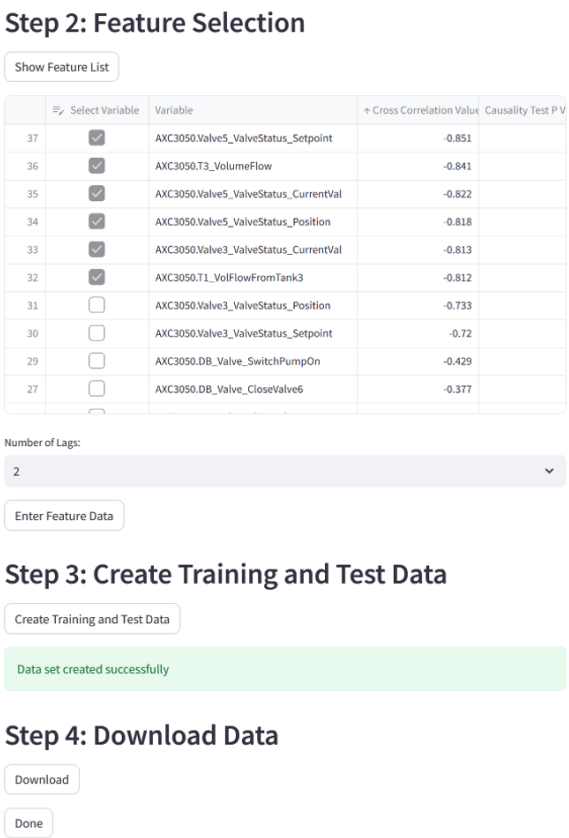

Abbildung 6: Wahl der vermuteten abhängigen Variablen.

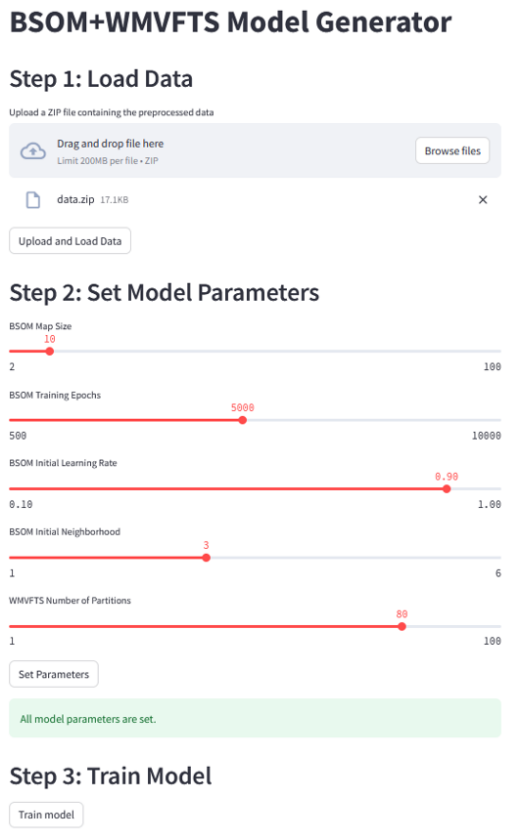

Abbildung 7: Einstellung der Modellparameter.

Ergänzend wurde ein LSTM-basiertes Verfahren eingeführt. Im Demonstrator verringerte es den Vorhersagefehler gegenüber BSOM-WMVFTS auf ungefähr ein Viertel. Da der Foliensatz weder Fehlermaß noch Bezugsdatensatz benennt, ist diese quantitative Aussage als Ergebnis des Demonstrators und nicht als allgemeingültige Leistungsangabe zu verstehen. Beide Verfahren wurden beibehalten: LSTM erzielte die höhere Vorhersagegenauigkeit, während BSOM-WMVFTS bessere Rückschlüsse auf mögliche Ursachen eines Fehlverhaltens erlaubte. Die Resultate zu SOM-WMVFTS und BSOM-WMVFTS wurden 2025 auf der IFAC MIM veröffentlicht und präsentiert.

Für AP 3.2 entstand die Webanwendung „FMU Factory“ zur teilautomatisierten Erstellung von Simulationsmodellen (siehe Abbildung 8 und Abbildung 9). Grundlage ist eine Bibliothek wiederverwendbarer Teilmodelle, beispielsweise für Tanks, Ventile, Pumpen und PID-Regler. Anwenderinnen und Anwender beschreiben das gewünschte System sprachlich; ein lokal betriebenes Sprachmodell wählt passende Bausteine aus und schlägt deren Vernetzung vor. Weil die automatisch erzeugte Topologie nicht in jedem Fall zuverlässig ist, wurde ein grafischer Knoteneditor als Human-in-the-Loop-Korrekturinstanz integriert. Darin lassen sich Parameter und Verbindungen prüfen und anpassen. Nach dieser Korrektur erzeugt ein Codegenerator auf Basis von Python und pythonfmu/Fmi2Slave den FMU-Quellcode und erzeugt die Binärdateien als herunterladbare FMU.

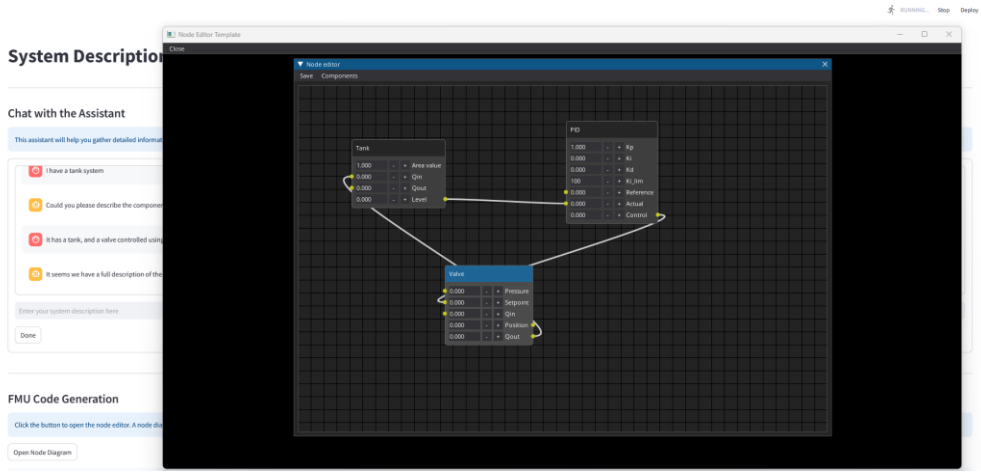

Abbildung 8: Webanwendung zur FMU-Erzeugung mit Netzwerk-Editor

Für die Wahrung möglicher Betriebsgeheimnisse wurde das lokal im Intranet ausführbare Codestral-Modell von Mistral eingesetzt. Dadurch konnten Anlageninformationen lokal verarbeitet und zugleich eine auf moderater Hardware ausreichende Qualität und Geschwindigkeit bei der Code-Generierung erreicht werden. Die zum Projektende stabile Lösung kombiniert damit LLM-gestützte Komponentenauswahl, grafische Korrektur durch Fachanwender und deterministische Codegenerierung.

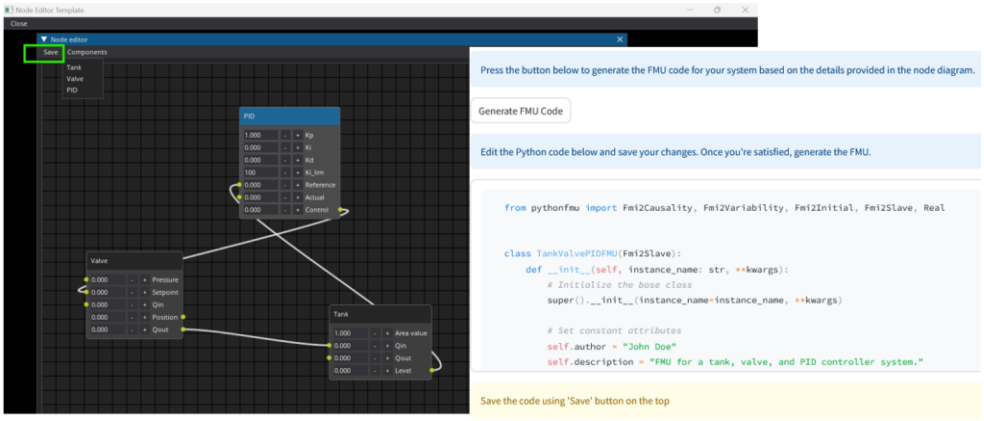

Abbildung 9: FMU-Codegenerierung mit LLM, Knoteneditor und Human-in-the-Loop

In AP 3.3 wurde die verteilte Co-Simulationsplattform aus Co-Simulator, Proxy-FMU, FMU-Boot-System und entfernten Simulationsmodellen fertiggestellt. Zusätzlich wurde der Zustand des auf BSOM-WMVFTS beziehungsweise LSTM basierenden digitalen Zwillings regelmäßig mit physisch gemessenen Werten synchronisiert. Co-Simulator und verteilte Simulation wurden so angepasst, dass eine periodische Zustandskorrektur die Drift zwischen Modell und Prozess begrenzt und der Vergleich von Ist- und Erwartungswerten über standardisierte Komponentenschnittstellen möglich bleibt.

Die prototypische Umsetzung und vergleichende Bewertung von BSOM-WMVFTS und LSTM erfüllt den Beitrag des ifak zu Datenerfassung, Monitoring und KI-gestützter Ergebnisbewertung in AP 3.1. Die FMU Factory mit Komponentenbibliothek, lokalem Sprachmodell, Knoteneditor und Codegenerator realisiert die in AP 3.2 vorgesehene effiziente und teilautomatisierte Erstellung digitaler Zwillinge. Die knotenübergreifende FMI-Co-Simulation und die periodische Zustandskorrektur setzen schließlich die vom ifak verantworteten Aufgaben zur Verteilung, Synchronisation und Evaluierung in AP 3.3 um.

6.5 HAP 4: Angriffserkennung, Risikobewertung, Angriffsbehandlung und Aircraft-SOC

Für das ifak war in HAP 4 kein eigener Arbeitsbeitrag vorgesehen.

6.6 HAP 5: Integration und Evaluation

In HAP 5 sollten die Zero-Trust-Plattformen, digitalen Security-Zwillinge und Verfahren zur Angriffserkennung und -behandlung in einem gemeinsamen Laboraufbau aus Hard- und Software zusammengeführt werden. AP 5.2 hatte die Kopplung der Implementierungen aus HAP 2, HAP 3 und HAP 4 zum finalen RESISTANT-Prototyp zum Gegenstand. In AP 5.3 sollten anschließend die in HAP 1 definierten Anwendungsfälle ausgeführt, die Systemreaktionen beobachtet und die Wirksamkeit der Gesamtarchitektur bewertet werden. Zugleich sollten Probleme, fehlende Eigenschaften und nächste Schritte für eine Industrialisierung herausgearbeitet werden.

In AP 5.2 sollte das ifak auf Basis der Ergebnisse aus HAP 2 und HAP 3 prototypische digitale Zwillinge sowie Komponenten zur Aufnahme realer Prozesswerte und zum Vergleich des Istzustands mit dem Simulationserwartungswert erstellen und in den Laboraufbau integrieren. Für AP 5.3 war vorgesehen, diese Komponenten in der Laborumgebung mit mehreren Instanzen auszuführen und die erzielten Ergebnisse anhand der in HAP 1 erarbeiteten Anforderungen zu evaluieren.

Abbildung 10: Labordemonstrator

Zunächst integrierte das ifak seine Komponenten in einen eigenen Labordemonstrator aus drei über Ethernet verbundenen Rechnern (siehe Abbildung 10). Darin wurden reale beziehungsweise aufgezeichnete Tanksystemdaten, definierte Angriffssignale, mehrere Simulationskomponenten, der verteilte Co-Simulator und die Anomalieerkennung zu einer durchgängigen Verarbeitungskette verbunden. Die Verwendung von Recording und Play-back sowie eines Störungsgenerators ermöglichte reproduzierbare Versuche.

Für die Integration in die gemeinsame TSN-basierte RESISTANT-Infrastruktur wurde die ifak-Software anschließend auf Airbus-Knoten übertragen. Auf der Mission-Critical-Seite umfasste der Aufbau auf Airbus Node 4 unter anderem eine ifak-KVM mit Datenquelle, Attack Injector und MQTT-Publisher sowie RabbitMQ und Tenzir. Auf der durch eine Datendiode getrennten Non-Mission-Critical-Seite

wurden auf Airbus Node 5 Tenzir und ein Kubernetes-Cluster für die ifak-Anomalieerkennung mit RabbitMQ-Broker, AMQP-Consumer, *libcosim*-Co-Simulator, Proxy-FMU-Service und Alarmdetektor betrieben. Die Kopplung der Komponenten erfolgte über MQTT beziehungsweise AMQP. Damit wurden Messdaten aus der geschützten Domäne rückwirkungsfrei zur verteilten Simulation und Auswertung übertragen, manipulierte Füllstandssignale mit den Vorhersagen des digitalen Zwillings verglichen und erkannte Abweichungen als Alarm bereitgestellt.

Die Integration bestätigte zugleich, dass neben der eigentlichen Software insbesondere die konsortialweite Abstimmung von IP-Adressen, Kubernetes- und Tenzir-Konfigurationen sowie weiteren Infrastrukturdetails entscheidend ist. Im Final Review konnte die durchgängige Lösung von der Datenerfassung über die knotenübergreifende Simulation bis zur Anomalieerkennung dargestellt werden. Damit wurde der in HAP 1 definierte Tanksystem-Anwendungsfall auf der gemeinsamen Infrastruktur technisch nachvollzogen und die Verteilung und Orchestrierung der Simulationskomponenten nachgewiesen.

Mit der Integration der digitalen Zwillinge, der Prozessdatenerfassung, des Ist-/Soll-Vergleichs und der Alarmierung in den ifak-Laboraufbau sowie anschließend in die TSN-basierte Partnerinfrastruktur wurde der vorgesehene Beitrag zu AP 5.2 realisiert. Die reproduzierbare Störungseinprägung, der Vergleich der Erkennungsverfahren und der durchgängige Nachweis im finalen Demonstrator setzen zugleich den vorgesehenen ifak-Beitrag zur Evaluation in AP 5.3 um.

7 Wichtigste Positionen des zahlenmäßigen Nachweises

Die Gesamtkosten für dieses Vorhaben betrugen 317.216,37 Euro. Die wesentlichen Positionen des zahlenmäßigen Nachweises entfielen auf Personal-, Reise- und Materialkosten. Den größten Anteil stellten die Personalkosten mit 96,6% dar. Eingesetzt wurden insbesondere wissenschaftliches Personal sowie wissenschaftliche Hilfskräfte. Diese wirkten unter anderem an der Entwicklung Machine-Learning-basierter Verfahren zur Anomalieerkennung sowie an der Erstellung von Simulationsmodellen für Kubernetes- und Docker-basierte Deployments mit.

Die Reisekosten entstanden insbesondere durch die projektinterne Koordination, die Verbreitung der Projektergebnisse sowie die Evaluierung durch den Projektträger. Die Materialaufwendungen dienten dem Aufbau eines Abschlussdemonstrators, bestehend aus mehreren PCs und entsprechender Netzwerktechnik.

Die verwendeten Mittel entsprechen im Wesentlichen den geplanten Kosten.

8 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Das Vorhaben RESISTANT adressierte die zunehmenden Anforderungen an die Cybersecurity stark vernetzter und softwarebasierter Avioniksysteme. Insbesondere die Nutzung digitaler Zwillinge zur kontinuierlichen Überwachung sicherheitsrelevanter Systemzustände, deren verteilte Ausführung sowie die zuverlässige Bewertung von Abweichungen zwischen realem und simuliertem Verhalten waren zu Projektbeginn nicht durch unmittelbar einsetzbare Standardlösungen abgedeckt. Die hierfür erforderlichen Forschungs- und Entwicklungsarbeiten waren daher notwendig, um die technische Machbarkeit der vorgesehenen Ansätze zu untersuchen und prototypisch nachzuweisen.

Die Arbeiten des ifak konzentrierten sich auf die Handhabung, Verteilung und Synchronisation digitaler Zwillinge, die KI-gestützte Anomalieerkennung sowie die teilautomatisierte Erstellung von FMU-basierten Simulationsmodellen. Hierzu wurden bestehende Methoden und Softwarekomponenten weiterentwickelt und für die Anforderungen einer verteilten, sicherheitsorientierten Avionikumgebung angepasst. Insbesondere die knotenübergreifende Co-Simulation mit Proxy-FMU und FMU-Boot-System, die Verfahren zur Bewertung von Abweichungen zwischen Prozess- und

Simulationsdaten sowie die periodische Synchronisation von digitalem Zwilling und physikalischem Prozess erforderten eigenständige Entwicklungs- und Integrationsarbeiten.

Die Angemessenheit der geleisteten Arbeiten zeigte sich im schrittweisen Vorgehen von der Anforderungsanalyse über Laboraufbauten und prototypische Implementierungen bis zur Integration in die gemeinsame TSN-basierte RESISTANT-Infrastruktur. Die entwickelten Komponenten wurden anhand des Tanksystem-Anwendungsfalls erprobt und zu einer durchgängigen Verarbeitungskette von der Datenerfassung über die verteilte Simulation bis zur Anomalieerkennung und Alarmierung zusammengeführt. Auch die Untersuchung unterschiedlicher KI-Verfahren und die Entwicklung der FMU Factory dienten unmittelbar den im Vorhaben definierten wissenschaftlich-technischen Zielen.

Die gegenüber der ursprünglichen Planung erforderliche kostenneutrale Verlängerung des Projekts war insbesondere durch den erhöhten Abstimmungs- und Integrationsaufwand innerhalb der gemeinsamen Infrastruktur begründet. Die zusätzlichen Arbeiten waren erforderlich, um die entwickelten Komponenten auf den Partnerknoten zusammenzuführen und den Gesamtdemonstrator funktionsfähig umzusetzen. Eine Änderung der Projektziele war damit nicht verbunden.

Unter Berücksichtigung der erzielten Ergebnisse, des erfolgreichen Nachweises der verteilten Co-Simulation und Anomalieerkennung sowie der Integration in den RESISTANT-Gesamtdemonstrator kann eingeschätzt werden, dass die durchgeführten Arbeiten für die Erreichung der Projektziele notwendig und in Umfang und Ausgestaltung angemessen waren. Die eingesetzten Mittel standen dabei in einem sachgerechten Verhältnis zu den durchgeführten Forschungs-, Entwicklungs- und Integrationsarbeiten.

9 Nutzung und Verwertung der Ergebnisse

Die im Vorhaben RESISTANT erzielten Ergebnisse erweitern die Kompetenzen des ifak insbesondere in den Bereichen digitale Zwillinge, verteilte Co-Simulation, KI-basierte Anomalieerkennung und automatisierte Erstellung von Simulationsmodellen. Als Forschungsinstitut liegt die Verwertung dabei nicht in der Entwicklung eigener Produkte, sondern vor allem im Wissenstransfer sowie in der Nutzung der Ergebnisse für weitere Forschungs- und Entwicklungsprojekte und Kooperationen mit Industriepartnern.

Besonderes Potenzial besitzen die entwickelten Methoden zur verteilten Ausführung und Synchronisation FMI-basierter digitaler Zwillinge. Die gewonnenen Erkenntnisse und Softwarebausteine können auch außerhalb der Avionik, beispielsweise in der industriellen Automatisierung oder bei anderen vernetzten cyber-physischen Systemen, für Machbarkeitsstudien und prototypische Entwicklungen eingesetzt werden. Gleiches gilt für die untersuchten KI-Verfahren zur Anomalieerkennung, die sich auf Fragestellungen der Zustandsüberwachung, Fehlerdiagnose und Angriffserkennung übertragen lassen.

Mit der FMU Factory wurden zudem neue Ansätze zur Nutzung lokal betriebener Sprachmodelle für die teilautomatisierte Erstellung von Simulationsmodellen untersucht. Die dabei gewonnenen Erfahrungen zu generativer KI, Human-in-the-Loop-Verfahren und dem Schutz vertraulicher Anlagendaten bieten weitere Anknüpfungspunkte für zukünftige Forschungs- und Transferprojekte.

Der Wissenstransfer erfolgt außerdem über wissenschaftliche Veröffentlichungen, Vorträge, die Betreuung akademischer Arbeiten sowie die Mitarbeit des ifak in Fach- und Normungsgremien. Insgesamt stärken die Projektergebnisse die wissenschaftlich-technische Kompetenz des ifak an der Schnittstelle von Simulation, digitalen Zwillingen, KI und Cybersecurity und bilden eine Grundlage für weiterführende Forschungs- und Industriekooperationen.

10 Bekannt gewordener Fortschritt bei anderen Stellen

Während der Laufzeit wurden generative Sprachmodelle (GPT) allgemein verfügbar. Dies wirkte sich unmittelbar auf AP 3.2 aus, dessen Konzept die Nutzung dieser Technologie für die Quellcodeerzeugung aufgriff. Da Sprachmodelle kein physisches Verständnis der beschriebenen Objekte besitzen, blieb die Einbeziehung von Ingenieurinnen und Ingenieuren erforderlich, was zur Human-in-the-Loop-Architektur mit grafischem Knoteneditor führte. Um Betriebsgeheimnisse zu wahren, wurden ausschließlich lokal im Intranet betreibbare Modelle eingesetzt; die Eignung verfügbarer Modelle wurde regelmäßig anhand von Benchmarks und eigener empirischer Tests überprüft. Die im weiteren Verlauf bekannt gewordenen Reasoning-Modelle und Vision-Language-Modelle änderten die prinzipielle Methodik nicht, zeigen aber Ansatzpunkte für künftige Weiterentwicklungen auf. Darüber hinaus wurden im Rahmen der laufenden Recherche keine Forschungsergebnisse Dritter bekannt, die eine Anpassung der Arbeiten erfordert hätten.

11 Veröffentlichungen, akademische Arbeiten und Wissenstransfer

Wissenschaftliche Veröffentlichung:

> Bibilewela P. P. M. Pathirathna, Mario Thron, Cheng Xin: Comparative Analysis of SOM-WMVFTS and BSOM-WMVFTS in High-Dimensional Multivariate Time Series Forecasting. 11th IFAC Conference on Manufacturing Modelling, Management and Control (MIM 2025), Trondheim, Norwegen, 30.06.–03.07.2025. Elsevier B. V. (ISSN 2405-8963), DOI: 10.1016/j.ifacol.2025.09.404.

Die Veröffentlichung behandelt im Projekt untersuchte Verfahren zur Vorhersage multivariater Zeitreihen und deren Nutzung als Grundlage für die datenbasierte Anomalieerkennung.

Akademische Arbeit:

> Bibilewela P. P. M. Pathirathna: Detecting Manipulation Attacks in Industrial Systems: Exploring the Combination of Self-Organizing Maps and Other AI Techniques. Otto-von-Guericke University Magdeburg, Masterarbeit.

Die Arbeit untersuchte KI-basierte Verfahren zur Erkennung von Manipulationen und unterstützte zugleich den Transfer der Projektergebnisse in die akademische Ausbildung.

Weitere Ergebnisverbreitung und Wissenstransfer:

Die Projektergebnisse wurden zudem im Rahmen der Abschlussveranstaltung des Verbundvorhabens vorgestellt und mit den Projektpartnern sowie weiteren fachlich interessierten Akteuren diskutiert. Darüber hinaus flossen Erkenntnisse aus RESISTANT in Gespräche mit Unternehmen und Forschungspartnern im Rahmen der Anbahnung weiterer Forschungs- und Entwicklungsprojekte ein. Dabei wurden insbesondere mögliche Übertragungen der entwickelten Ansätze zu digitalen Zwillingen, verteilter Co-Simulation, KI-basierter Anomalieerkennung und automatisierter Modellerstellung auf weitere industrielle Anwendungsfelder diskutiert.

Literaturverzeichnis

[1] MonIKA: MonIKA-Projektkonsortium (2014): Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung (MonIKA). Abschlussbericht. BMBF-Verbundvorhaben, Projektlaufzeit 01.03.2012–28.02.2014. URL: https://edocs.tib.eu/files/e01fb15/839012829.pdf (abgerufen am 2026-08-31).

[2] IMMUNE: Institut für Automation und Kommunikation e. V. (ifak) (o. J.): IMMUNE – Selbstverteidigende Netzwerke für resiliente Industrie 4.0. Forschungsprojekt, Förderkennzeichen 20X1719D, Projektlaufzeit 2018–2021. URL: https://www.ifak.eu/de/projekte/immune (abgerufen am 2026-08-31).

[3] TALIA: Tietz, V.; Lüttig, B.; Annighöfer, B. (o. J.): TALIA – Technologie, Prozesse und digitale Dienstleistungen für Anwendungen in Kabine- und Avioniknetzwerken auf einer generischen Rechnerplattform. Teilvorhaben: Qualifizierbare Metamodellierung und adaptive Integrierte Modulare Avionik. Schlussbericht. Universität Stuttgart, Institut für Luftfahrtsysteme, Förderkennzeichen 20D1907E. DOI: 10.34657/31357. URL: https://doi.org/10.34657/31357 (abgerufen am 2026-08-31).

[4] PAFA-ONE: Souza Alcantara Queiroz, S.; Brunner, M.; Schulz, B.; Reinhart, J.; Kühn, J.-P.; Annighöfer, B. (2025): PAFA-ONE – Plug&Fly Avionics: Grundlagen für eine sichere und qualifizierbare Selbstorganisation. Schlussbericht. Universität Stuttgart, Institut für Luftfahrtsysteme. URL: https://oa.tib.eu/renate/items/81985675-0cb4-4af0-803e-293a54eeca40/full (abgerufen am 2026-08-31).

[5] Ergenç, D.; Fischer, M. (2023): DELIA – Distributed, Extendable, Lightweight, open, reliable, servIce-oriented Architecture for next-gen mobility. Abschlussbericht des Teilprojekts der Universität Hamburg. Universität Hamburg, Fachbereich Informatik, Rechnernetze (NET), Förderkennzeichen 16KIS0941, 31.01.2023. URL: https://edocs.tib.eu/files/e01fb24/187806360X.pdf (abgerufen am 2026-08-31).

[6] AMQP: OASIS (2012): OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0. OASIS Standard, 29.10.2012. URL: https://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf (abgerufen am 2026-08-31).

[7] MQTT: OASIS (2019): MQTT Version 5.0. OASIS Standard, 07.03.2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf (abgerufen am 2026-08-31).

[8] FMI: Modelica Association Project FMI (2024): Functional Mock-up Interface Specification, Version 3.0.2. Modelica Association, 27.11.2024. URL: https://fmi-standard.org/docs/3.0.2/ (abgerufen am 2026-08-31).

[9] Bibilewela P. P. M. Pathirathna, Mario Thron, Cheng Xin: Comparative Analysis of SOM-WMVFTS and BSOM-WMVFTS in High-Dimensional Multivariate Time Series Forecasting. 11th IFAC Conference on Manufacturing Modelling, Management and Control (MIM 2025), Trondheim, Norwegen, 30.06.–03.07.2025. Elsevier B. V. (ISSN 2405-8963), DOI 10.1016/j.ifacol.2025.09.404.

[10] Molinía, D.; Madani, K. (2022): Bsom: A two-level clustering method based on the efficient self-organizing maps. In: 2022 International Conference on Control, Automation and Diagnosis (ICCAD), 1–6. DOI: 10.1109/ICCAD55197.2022.9853931. URL: https://doi.org/10.1109/ICCAD55197.2022.9853931 (abgerufen am 2026-08-31).

[11] dos Santos, M.C.; Guimar˜aes, F.G.; de Lima e Silva, P.C. (2021): High-dimensional multivariate time series forecasting using self-organizing maps and fuzzy time series. In: 2021 IEEE

International Conference on Fuzzy Systems (FUZZ-IEEE). IEEE, 1–6. DOI: 10.1109/FUZZ45933.2021.9494496. URL: https://doi.org/10.1109/FUZZ45933.2021.9494496 (abgerufen am 2026-08-31).

[12]Kohonen, T. (1982): Self-organized formation of topologically correct feature maps. Biological Cybernetics, 43, 59–69. DOI: 10.1007/BF00337288.

Abbildungsverzeichnis

Abbildung 1: Ursprünglicher Gesamt-Terminplan des Verbundprojekts RESISTANT 5

Abbildung 2: Informationszonen in modernen Flugzeugen (Quelle: Airbus)..... 10

Abbildung 3: Co-Simulator als Orchestrator zur Steuerung verteilter Simulationsmodelle 11

Abbildung 4: Prinzip der verteilten Co-Simulation..... 11

Abbildung 5: Anomalieerkennung (unten, rot) mit einer Kombination aus neuronalen Netzen und Fuzzy-Logik 13

Abbildung 6: Wahl der vermuteten abhängigen Variablen..... 13

Abbildung 7: Einstellung der Modellparameter. 13

Abbildung 8: Webanwendung zur FMU-Erzeugung mit Netzwerk-Editor 14

Abbildung 9: FMU-Codegenerierung mit LLM, Knoteneditor und Human-in-the-Loop 14

Abbildung 10: Labordemonstrator..... 15

Abkürzungen

Abkürzung	Erklärung
AMQP	Advanced Message Queuing Protocol
AP	Arbeitspaket
BSOM	Bi-level Self-Organizing Map
DELIA	(Forschungsprojekt, aus dem die RESISTANT-Knotenarchitektur hervorging)
Docker	Container-Plattform für portable Softwarepakete
FMI	Functional Mock-up Interface
FMU	Functional Mock-up Unit
GPT	Generative Pre-trained Transformer
HAP	Hauptarbeitspaket
ifak	Institut für Automation und Kommunikation e.V.
IABG	Industrieanlagen-Betriebsgesellschaft mbH
IP	Internet Protocol
IT	Informationstechnologie
KVM	Kernel-based Virtual Machine
LLM	Large Language Model
LSTM	Long Short-Term Memory
LuFo	Luftfahrtforschungsprogramm
MQTT	Message Queuing Telemetry Transport
OPC	OLE for Process Control
PID	Proportional-Integral-Derivative (Regler)
SOM	Self-Organizing Map
TSN	Time-Sensitive Networking
UHH	Universität Hamburg
UST	Universität Stuttgart
WMVFTS	Weighted Multivariate Fuzzy Time Series