»iReduce«

Intelligente Interdependenz-gesteuerte Alarmflut-Reduktion in KRITIS

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2023	**Status**	laufend
Projektstart	01.01.2025	**Projektende**	31.12.2027
Zeitraum	2025 - 2027	**Projektlaufzeit**	36 Monate
Keywords	Intelligentes Alarm-Management in KRITIS; Operational Technology Monitoring (OTM) / Verkehrsüberwachung & -Steuerung / IoT (Internet-of-Things) / System-of-Systems (SoS); Semantic Knowledge Representation / Discovery / Evolution; Signal (inductive) /		

Projektbeschreibung

Die immense Flut an Meldungen, die durch omnipräsente Überwachungs- und Steuerungstechnologien (aka. "Operational Technology, OT") in kritischen Infrastrukturen (KRITIS) von Energie über IKT bis zu Verkehr laufend ausgelöst wird, stellt eine zentrale Herausforderung des effizienten und sicheren Betriebs solcher Infrastrukturen dar [4][7][10]. Beispielsweise werden im Zuge der Verkehrsüberwachung und -steuerung des österreichischen hochrangigen Straßennetzes (2.249 km/166 Tunnel) pro Stunde im "Normalbetrieb" mehr als 10.000 Meldungen generiert, wobei sich diese Flut an Meldungen in Ausnahmesituationen durch Unmengen von (Alarm)-Meldungen (i.F. "Alarmflut") vervielfacht. Diese Herausforderungen werden durch KRITIS-inhärente Eigenschaften wie Heterogenität, Dezentralisierung und Evolution weiter potenziert [15], was zwangsläufig zu einer isolierten, d.h. ausschließlich auf einzelne OT-Objekte (z.B. Sensoren/Aktoren) fokussierten, Sichtweise führt [16], da die wechselseitigen Abhängigkeiten zwischen OT-Objekten ("OT-Interdependenzen") und deren Semantik gemeinhin oft weder bekannt sind noch maschinell verarbeitbar vorliegen [16]. Dies erschwert eine intelligente Verarbeitung der Alarmflut und in weiterer Folge deren Reduktion [1][4][7][9], sodass betriebsverantwortliche Personen (aka. Operator:innen) mit der herausfordernden Aufgabe konfrontiert sind, manuell, unter Zeitdruck zusammenhängende Problemlagen zu erkennen und einzuschätzen, um so schlussendlich dennoch lebens- und umweltrettende Entscheidungen treffen zu können [1][2][3][4][9][12].

Das Projekt »iReduce« trägt diesen zentralen Herausforderungen Rechnung, indem Basistechnologien zur Interdependenz-gesteuerten Alarmflut-Reduktion realisiert werden, die den Kernbaustein für ein intelligentes Alarmmanagement in KRITIS bilden (KIRAS-Ausschreibungsschwerpunkt 3.1.9). Damit wird die Basis geschaffen, den zentralen Herausforderungen eines effizienten & sicheren Betriebs von KRITIS aufgrund der aktuell vorhandenen Alarmflut umfassend entgegenzuwirken und Operator:innen adäquat und nachhaltig in ihrem Tagesgeschäft aber v.a. auch in Ausnahmesituationen zu unterstützen.

Als zentrales Ergebnis werden funktionale Kernkomponenten, in Form praxisnaher Show Cases exemplarisch für die KRITIS-Domäne der Verkehrsüberwachung und -steuerung umgesetzt, komplettiert durch die Erforschung der konzeptionellen

Voraussetzungen und technischen Rahmenbedingungen sowie einem entsprechenden Geschäftsmodell zu deren Nutzbarmachung für KRITIS. Im Besonderen soll »iReduce« durch entsprechende generische Konzepte die Voraussetzungen für eine möglichst breite Anwendbarkeit in verwandten KRITIS-Domänen schaffen, um so einen Schritt hinsichtlich der Vision einer nachhaltigen und umfassenden Stärkung von KRITIS im Allgemeinen zu setzen.

Der methodische Ansatz folgt dem "Human Centered Design Process", indem das Projektergebnis unter Einbeziehung von Endbenutzer:innen kontinuierlich konkretisiert wird, wobei Nachhaltigkeit und adäquate Evaluierung mittels Benutzer:innenstudien in Kooperation mit (teils über LoIs assoziierten) Bedarfsträger:innen und Unternehmen aus unterschiedlichen KRITIS-Bereichen sichergestellt werden. Das interdisziplinäre Konsortium vereint ein breites Spektrum an Kompetenzen aus Wirtschaft und Wissenschaft mit anwendungsnahem Wissen von KRITIS-Bedarfsträger:innen, im Besonderen aber auch von betriebsverantwortlichem Personal, das als Bedürfnisträger:innen und Ideen-/Lösungsbringer:innen fungiert.

Abstract

The immense flood of messages that is constantly produced by omnipresent monitoring and control technologies (aka. Operational Technology, OT) in critical infrastructures (CIs), ranging from Energy and IKT to traffic, represents a substantial challenge for efficient and safe operation [4][7][10]. For example, in the course of traffic monitoring and control on Austria‘s highways, stretching 2,249 km and covering 166 tunnels, more than 10,000 messages are generated per hour even in “normal operation”, with this flood of messages multiplying in exceptional situations due to vast numbers of (alarm) messages (henceforth “alarm flood”). These challenges are further exacerbated by CI-inherent properties such as heterogeneity, decentralization, and evolution [15]. This inevitably leads to an isolated view, i.e., one that focuses exclusively on individual OT objects (e.g., sensors/actors) [16], since the mutual dependencies between OT objects (“OT interdependencies") and their semantics are generally often neither known nor capable of being processed by machines [16]. This hampers an intelligent processing of the alarm flood and subsequently to reduce it[1][4][7][9], so that human operators are confronted with the challenging task of manually identifying and assessing critical situations under time pressure, ultimately being able to make decisions that save lives and the environment [1][2][3][4][9][12].

The »iReduce« project addresses these central challenges by realizing basic technologies for the exploration of semantic OT interdependencies, which form the core building block for intelligent alarm management in CIs and thus enable a continuous and dynamic reduction of alarm floods (KIRAS-Ausschreibungsschwerpunkt 3.1.9). This creates the basis for comprehensively counteracting the central challenges of efficient and safe CI operation due to the current alarm floods and to provide human operators with adequate and sustainable support in their day-to-day business, and, above all, in exceptional situations.

As a central result, functional core components will be implemented as practical show cases for the CI domain of traffic monitoring and control, completed by research into the conceptual requirements and technical prerequisites as well as a corresponding business model for their exploitation in CIs. In particular, »iReduce« is intended to put forward appropriate generic concepts to enhance their possible applicability to related KRITIS domains in order to take a step towards the vision of a sustainable and comprehensive strengthening of CIs in general.

The methodological approach follows the "Human Centered Design Process" in which the project result is continuously

concretized bythe involvement of end users, ensuring sustainability and adequate evaluation in cooperation with demand carriers (some associated via LoIs) and companies from different CI domains. The interdisciplinary consortium combines a wide range of competencies from business and science with the applied knowledge of CI demand carriers, but in particular also from human operators who act as need providers and idea/solution providers.

Projektkoordinator

- Universität Linz Institut für Telekooperation

Projektpartner

- Autobahnen- und Schnellstraßen- Finanzierungs-Aktiengesellschaft
- Cloudflight Austria GmbH
- FH OÖ Forschungs & Entwicklungs GmbH
- team Technology Management GmbH
- Universität für künstlerische und industrielle Gestaltung Linz