Aktuelle Forschung zu kritischen Infrastrukturen

Dr.-Ing. Erich Rome
Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme

Fraunhofer
IAIS

SATW-Fachveranstaltung Cyber-Security, Zürich, 21.4.2016

CIPR Net

Fraunhofer
IAIS

Aktuelle Forschung zu kritischen Infrastrukturen
Agenda

1. Hintergrund
    1. Kritische Infrastrukturen (KRITIS) und deren Schutz
    2. Akteure im „Schutz Kritischer Infrastrukturen“
2. Forschung im „Schutz Kritischer Infrastrukturen“ – Eigene Projekte
    1. CIPcast: Entscheidungsunterstützungssystem für KRITIS-Betreiber
    2. CIPRTrainer: Exploration von Handlungsalternativen für Krisenmanager im Zivilschutz
3. Fazit: Praxiserfahrungen beim Technologietransfer

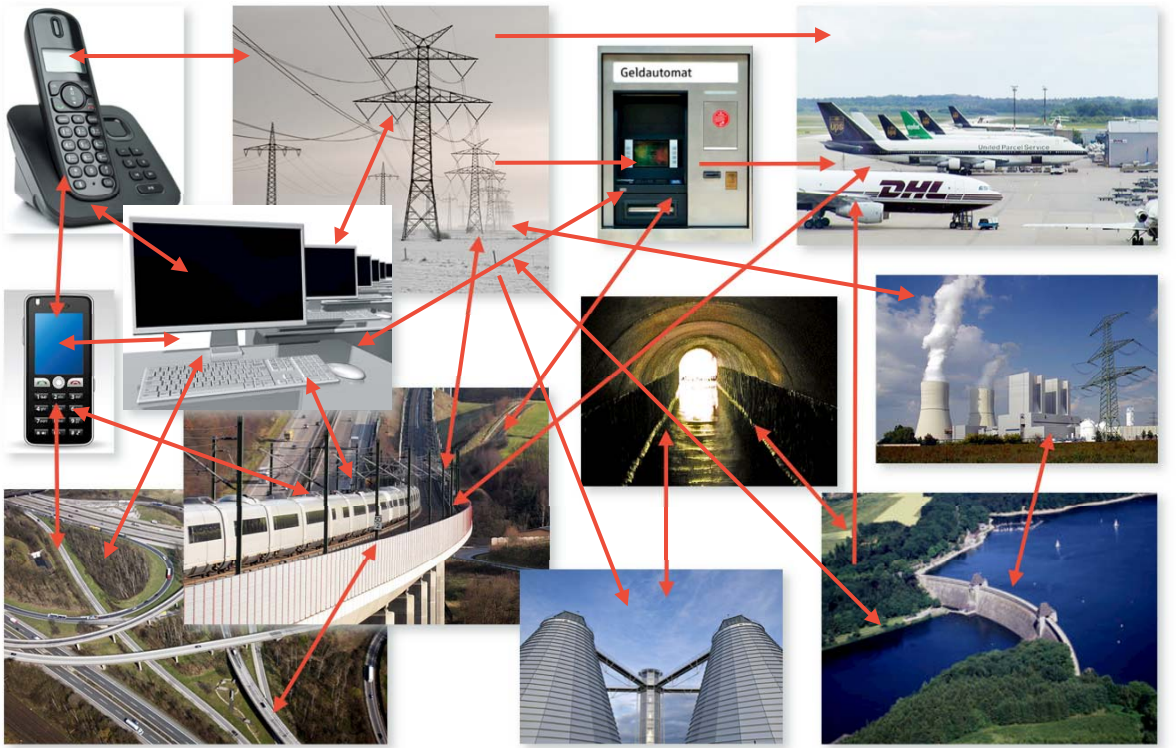
Das System der (Kritischen) Infrastruktur-Systeme

- **Komplex**
- **Wechselseitig abhängig**
- **Teils grenzübergreifend**
- **Verändert sich stetig**

Deutsche KRITIS-Sektoren:

1. **Energie**
2. **Transport & Verkehr**
3. IKT
4. Staat & Verwaltung
5. Medien & Kultur
6. Wasser
7. Ernährung
8. Finanz- & Versicherungswesen
9. Gesundheit

KRITIS: Nationale Definitionen können abweichen (FR:11, USA:17)



Schutz Kritischer Infrastrukturen

Akteure im KRITIS-Schutz

Akteure sind

- EU
- Regierungen und Behörden der Mitgliedsstaaten
- KRITIS-Betreiber
- Bevölkerungsschützer, Katastrophenschützer und ziviles Krisenmanagement
- Forschungsförderer und Forscher (div. EU, national)

KRITIS-Schutz

- EU: EU-Richtline von 2008 zu Europäischen KRITIS
- National: Sektorendefinition, Umsetzungspläne, neue Behörden und Einrichtungen
- Deutschland: UP KRITIS (ÖPP), Änderung der Fachgesetze, Cyber-Abwehrzentrum
- Herausforderung: Welche Elemente einer Infrastruktur sind „kritisch“?

Schutz Kritischer Infrastrukturen

Forschungsthemen und Transfer

Themen KRITIS-bezogener Sicherheitsforschungsprojekte u.a.:

- Risikoanalyse
- Verständnis der wechselseitigen Abhängigkeiten von KRITIS
- Entscheidungsunterstützungssysteme, Informations- und Warnsysteme

Transfer?

- Studie des Centre for European Policy Studies [**CEPS2011**]: ***Critical Infrastructure Protection in the EU*** identifizierte verbliebene Defizite und gab Handlungsempfehlungen
- **Transfer** KRITIS-bezogener Forschungsergebnisse in die praktische Anwendung **blieb in der EU hinter den Erwartungen zurück**
- Wie kann Technologietransfer gelingen?
- Was sind Barrieren für Technologietransfer?

Forschung im Gebiet Schutz Kritischer Infrastrukturen
bei Fraunhofer IAIS

Fördergeber: EU FP6, FP7, H2020, National: BMBF

IRRIIS	Integrated Risk Reduction in Information-based Infrastructure Systems
DIESIS	Design of an Interoperable European federated Simulation network for Critical InfraStructures
EMILI	Emergency Management in Large Infrastructures
VASA	Visual Analytics for Security Applications (BMBF)
HIPOW	Protection of Critical Infrastructure against High Power Microwave Threats
SECRET	Security of Railways against Electromagnetic Attacks
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
PREDICT	Predicting the Domino Effect in Crisis Situations
RESIN	Climate Resilient Infrastructures and Cities

CIPRNet – Critical Infrastructure Preparedness and Resilience Research Network

- Projektart: **Network of Excellence**
- Laufzeit: 48 Monate, 1.3.2013–28.2.2017
- Kofinanziert von FP7
- Fördersumme 6.6 M €
- Nachfolgeaktivität zur Design-Studie DIESIS
- 12 Partner, darunter JRC der EU
- Koordinator Fraunhofer

EU-FP7-Exzellenznetzwerk CIPRNet

Neue Fähigkeiten für Endanwender schaffen

Implementierung neuer **Fähigkeiten** für effektiverer Reaktionen auf Katastrophen, die KRITIS betreffen oder von ihnen ausgehen:

- **CIPcast: Entscheidungsunterstützungssystem mit Mehrwert**
  - Für nationale und multi-nationale Krisenmanager und KRITIS-Betreiber
  - basierend auf der **Integration von Technologien** der CIPRNet-Partner
  - Für Prävention und Störfallreaktion und –wiederherstellung (cold, warm hot phase)
- **CIPRTrainer: »was wäre, wenn…«-Untersuchungen für die Exploration verschiedener Handlungsalternativen**
  - basierend auf KRITIS-Modellierung, -Simulation und -Analyse kombiniert mit »serious gaming«-Methoden
  - Für Ausbildung, Übung und post-mortem-Analyse
- Gemeinsam genutzte Methode zur **Konsequenzanalyse**

EU-FP7-Exzellenznetzwerk CIPRNet

CIPRNet-DSS CIPcast im Einsatz

CIPcast: Entscheidungsunterstützungssystem (DSS) mit Mehrwert

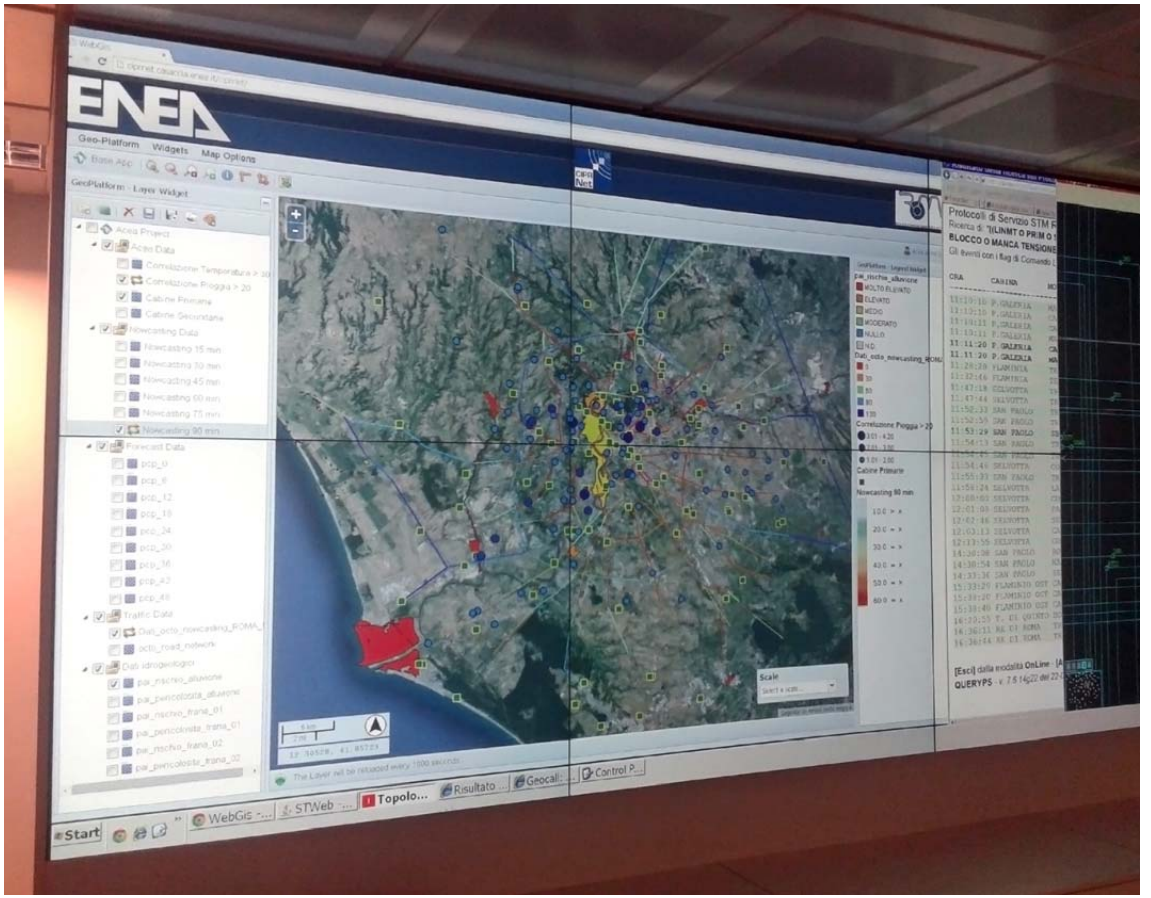
- Funktionalität:
  - Modellierung von KRITIS und ihrer realen Abhängigkeiten
  - Vorhersage von Wetterereignissen und Risiko für Elemente der Strom-, Telekommunikations-, und Trinkwasser-Infrastruktur
  - Empfehlungen für optimalen Einsatz von Reparaturteams
- Transfer an Endnutzer:
  - Prototyp im Einsatz bei römischem KRITIS-Betreiber
  - Kooperationen mit weiteren KRITIS-Betreibern laufen
  - Anfragen vom nationalen Krisenmanagement, den Kommunen Rom und Florenz und der Region Mantua
  - Einsatz beim „Heiligen Jahr“ in Rom

EU-FP7-Exzellenznetzwerk CIPRNet

CIPRNet-DSS im Einsatz

CIPRNet-DSS CIPcast auf LED-Wand im Kontrollzentrum eines Stromnetzbetreibers

(Projektpartner ENEA: Italienische Forschungseinrichtung)



EU-FP7-Exzellenznetzwerk CIPRNet

CIPcast im Einsatz

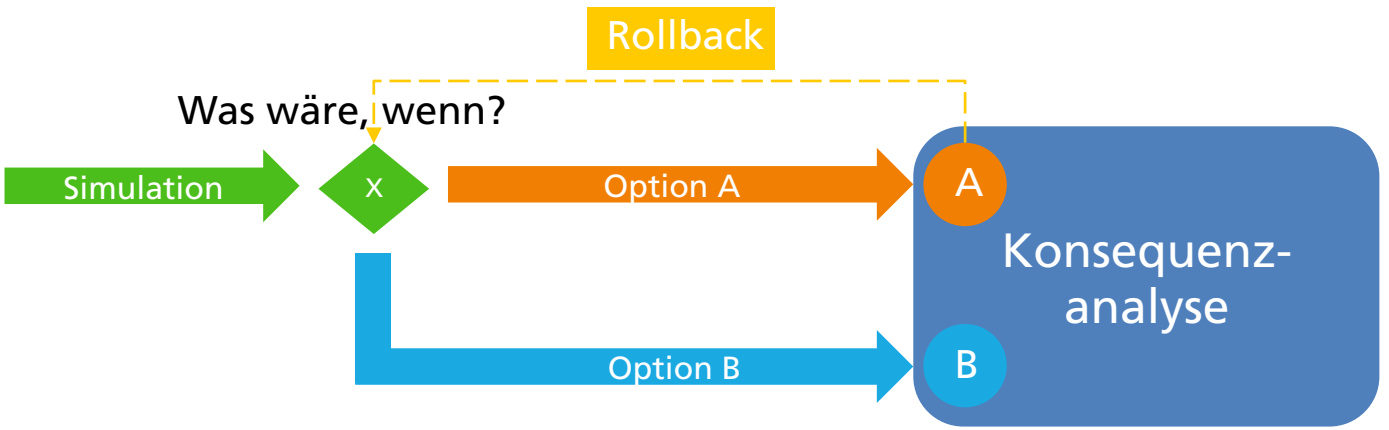
- Basis von CIPcast:
  - Anbindung von Nowcast- und Forecast-Diensten
  - Daten der Elemente des Mittelspannungsnetzes von Rom
  - Wartungsdaten (5 Jahre) der Elemente zeigen, welche Elemente z.B. bei Extremwetter (Hitze, Starkregen) häufig ausfallen
- Durch Forecast kann das Ausfallrisiko eines Elementes in den nächsten Stunden bestimmt werden
- Der Betreiber kann dann das Netz auf den Punkt verschieden konfigurieren
  - Robustere Konfiguration ➜ höhere Impedanz ➜ mehr Strom wird benötigt ➜ höhere Kosten
  - Effizientere Konfiguration ➜ geringere Impedanz ➜ weniger Strom wird benötigt ➜ geringere Kosten

EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: »was wäre, wenn«-Analyse

CIPRTrainer: Trainingssystem für die Exploration verschiedener Handlungsmöglichkeiten

- **»was wäre, wenn …«-Untersuchungen** kombiniert mit **Folgenabschätzungen**
  - Ermöglicht Vergleich verschiedener Szenarienverläufe
  - Ermöglicht Exploration verschiedener Handlungsoptionen ***während*** der Simulation (in der Realität meist nicht möglich)
  - Analyse: Folgen der Wahl von Handlungsoption A und B werden verglichen (Konsequenzanalyse: welche war die bessere Wahl?)

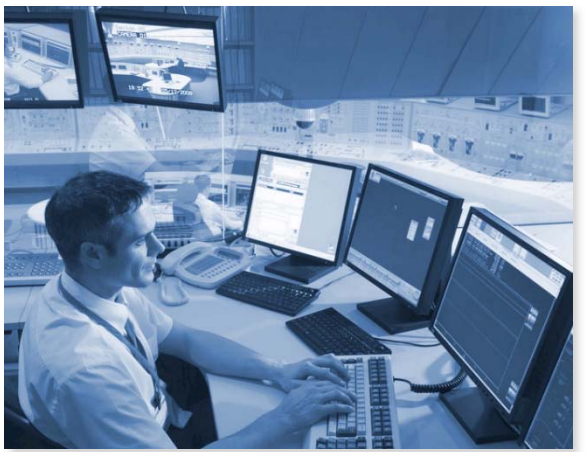


EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: »was wäre, wenn«-Analyse

- Motivation
  - Verhalten von KRITIS im Krisenfall ist meist eine unbekannte Größe
  - Bedeutung von KRITIS für Gegenmaßnahmen und Notfallplanung ist oft nur teilweise bekannt (insufficient awareness)
  - Verfahren zur Folgenabschätzung (consequence analysis) sind noch schwach entwickelt

- Geeignet für
  - *Post-mortem*-Analysen realer Schadensereignisse
  - Ausbildung / Training von Krisenstabspersonal: Lageführungspersonal und Entscheider



EU-FP7-Exzellenznetzwerk CIPRNet

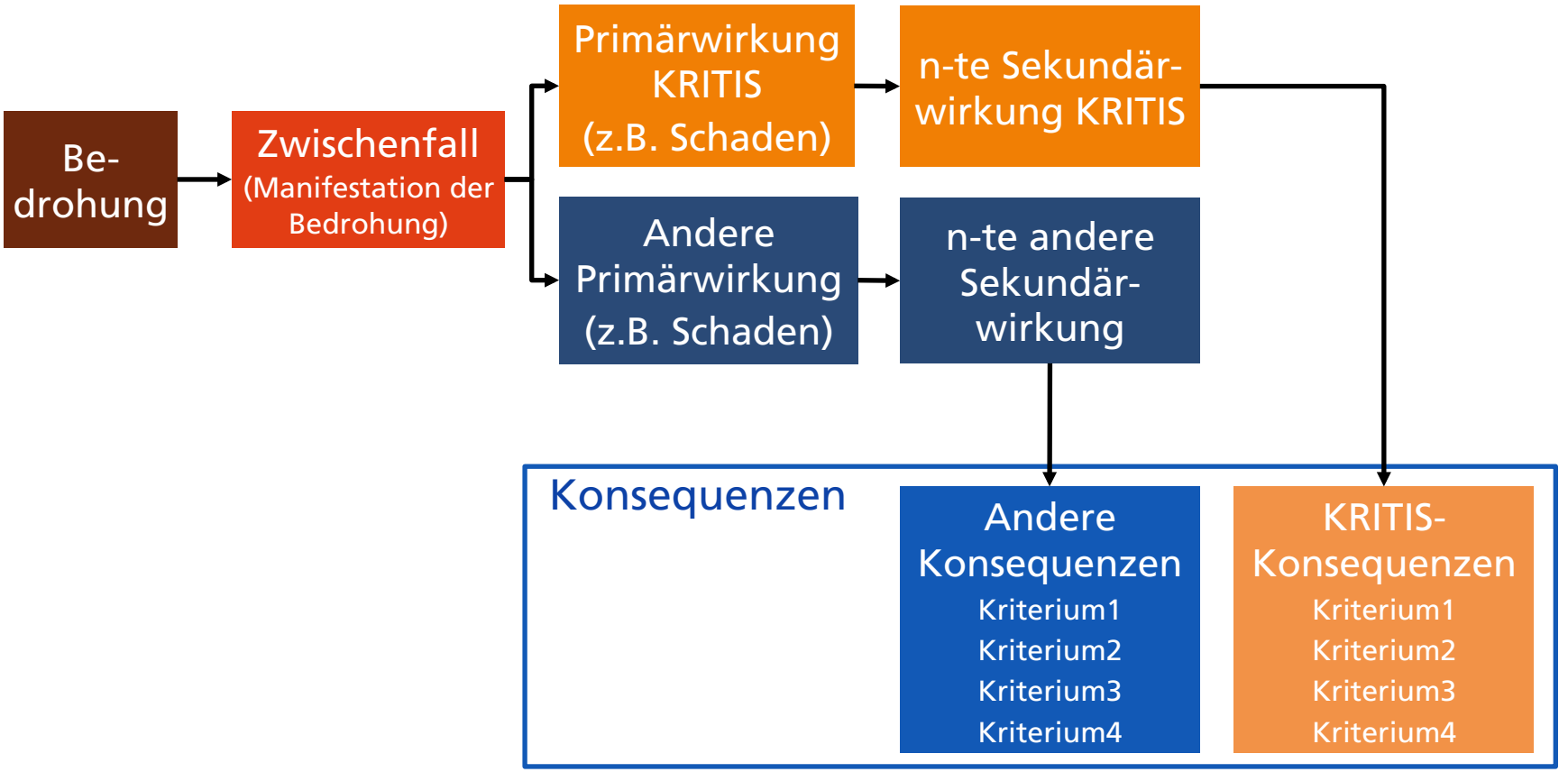
Technische Basis der »was wäre, wenn«-Analyse

- Modellierung von Krisenszenarien
  - Infrastrukturen und ihre Abhängigkeiten
  - Vorfälle (Angriffe, technisches Versagen, Extremwetterereignisse, …)
  - Aktionen: Vorbereitungsmaßnahmen, Gegenmaßnahmen, …
  - Ereignisketten
- Verfahren zur Abschätzung von Wirkungen und Konsequenzen, basierend auf
  - Sozio-ökonomischen Daten
  - Schadensmodellen
- Simulation der Krisenszenarien
- GIS-basierte grafische Benutzungsschnittstelle

EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: »was wäre, wenn«-Analyse

Schema der Konsequenzanalyse in CIPRNet



EU-FP7-Exzellenznetzwerk CIPRNet

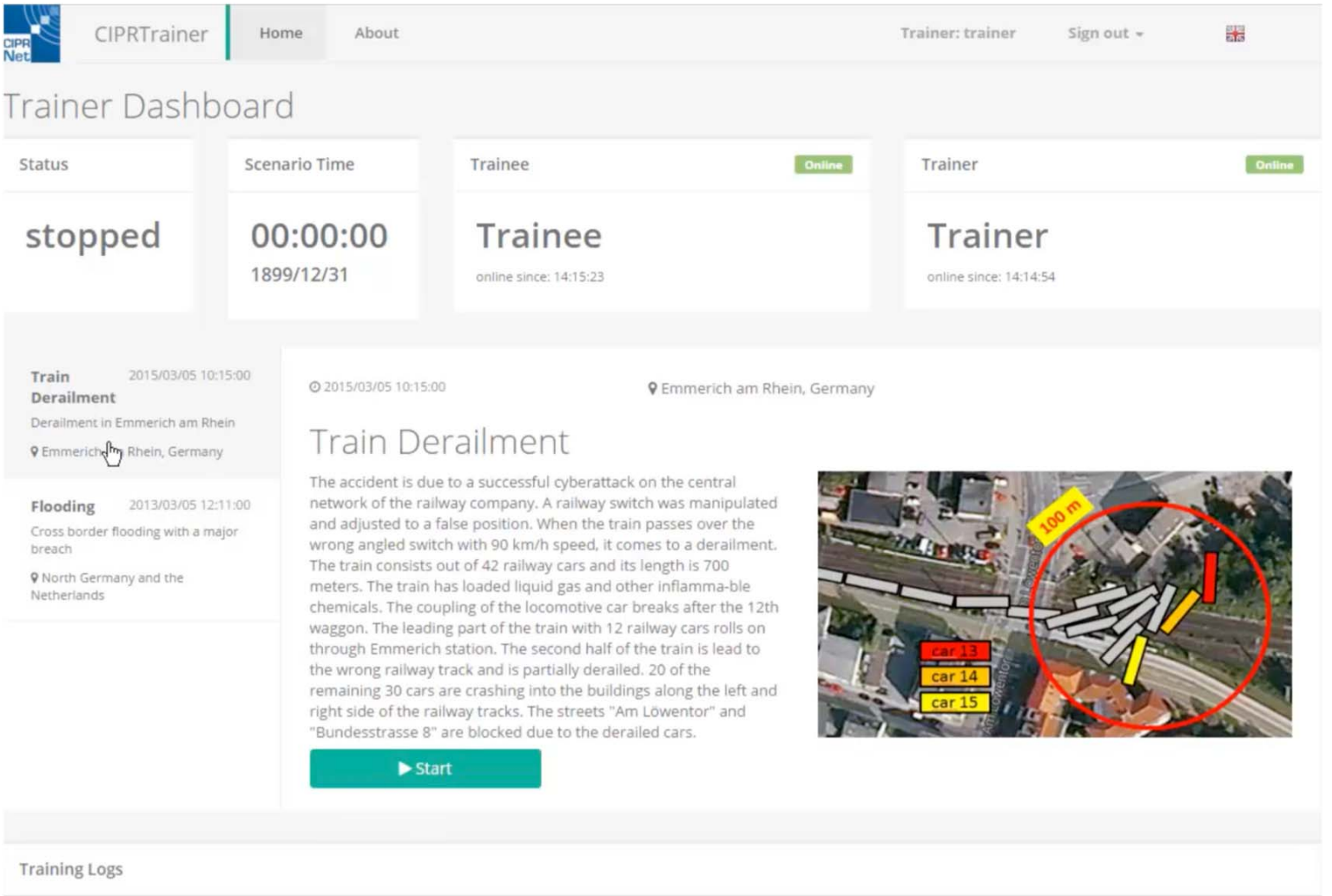
CIPRTrainer-Beispiel

Szenario: Entgleisung eines Güterzuges im deutsch-niederländischen Grenzgebiet

- Angenommene Ursache:
  - Cyber-Angriff auf ein Stellwerk; Weiche wird verstellt während der Güterzug sie überfährt
- Angenommene Wirkungen:
  - Auslaufende Chemikalien, Brände von Chemiewaggons
  - Giftige Rauchwolken führen zur Sperrung einer nahen Autobahn und zur Sicherheitsabschaltung von Datenzentren hinter der Grenze
  - Schäden an Bahn-Infrastruktur, Betuwe-Linie gesperrt, weiträumige Zugumleitungen
  - Chemikalien in der Kanalisation führen zu einer Explosion, die Teile des Strom- und des Telekommunikationsnetzes zerstört

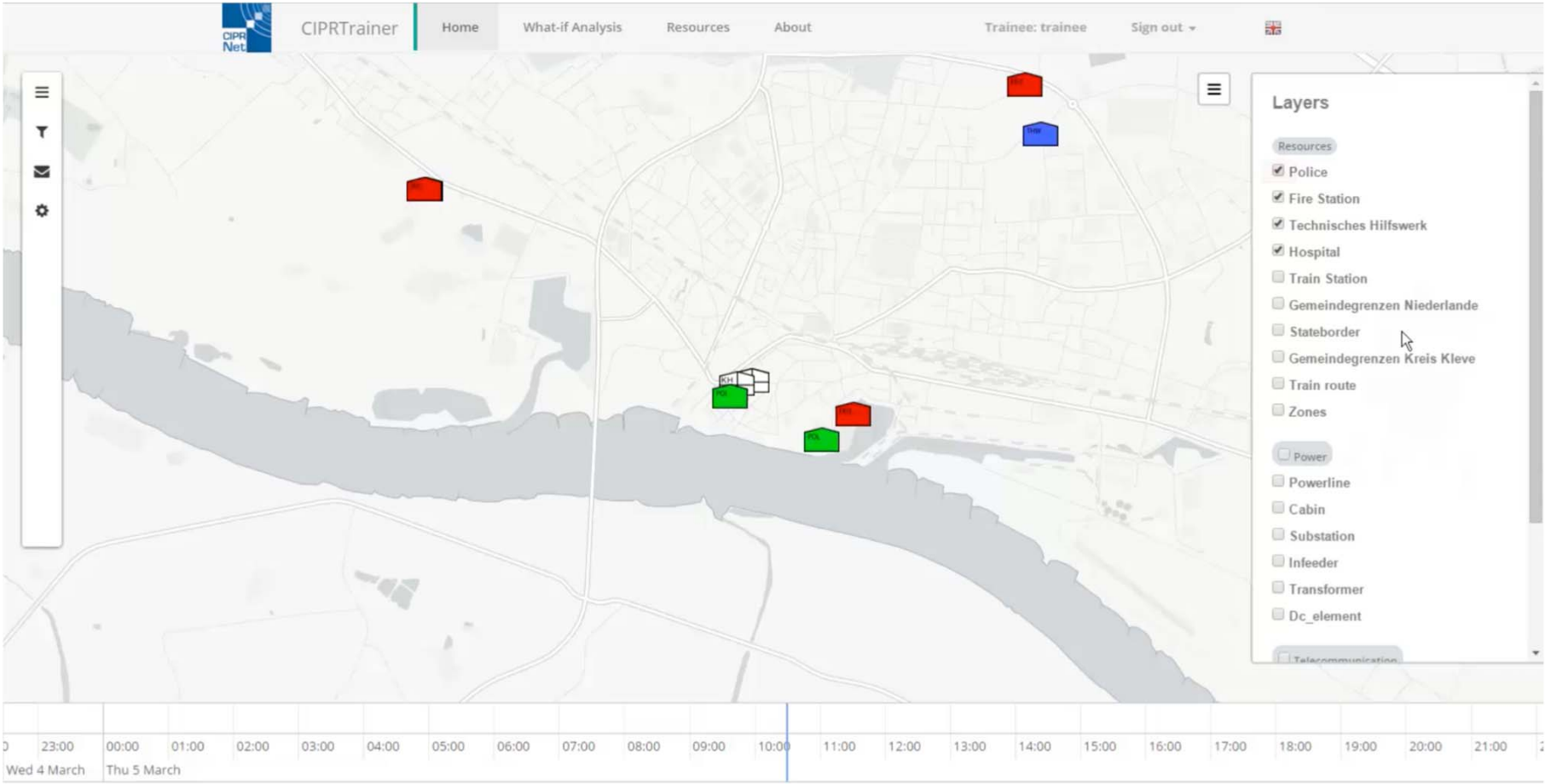
EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: Trainer view



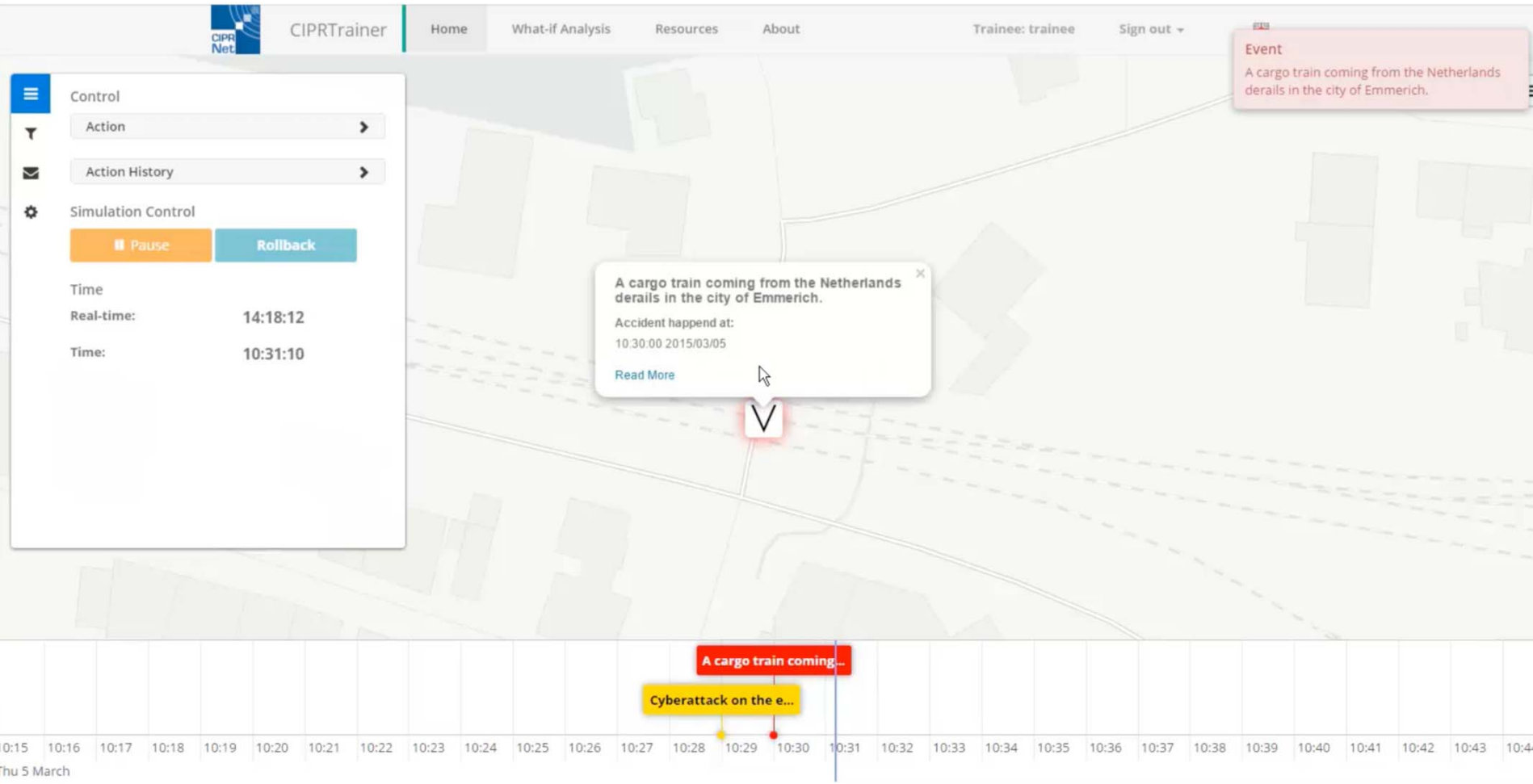
EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: Trainee view / GIS layers



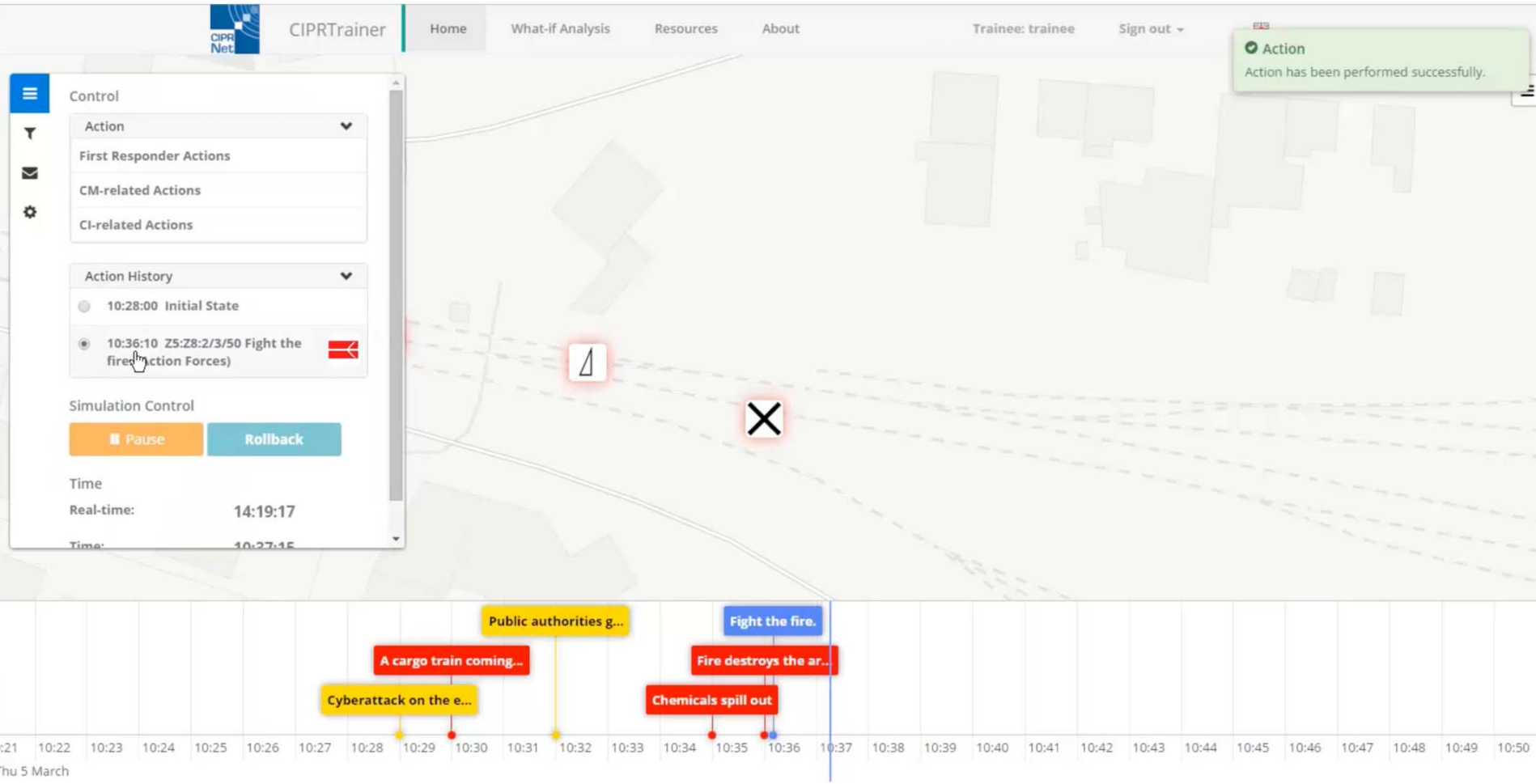
EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: Derailment event



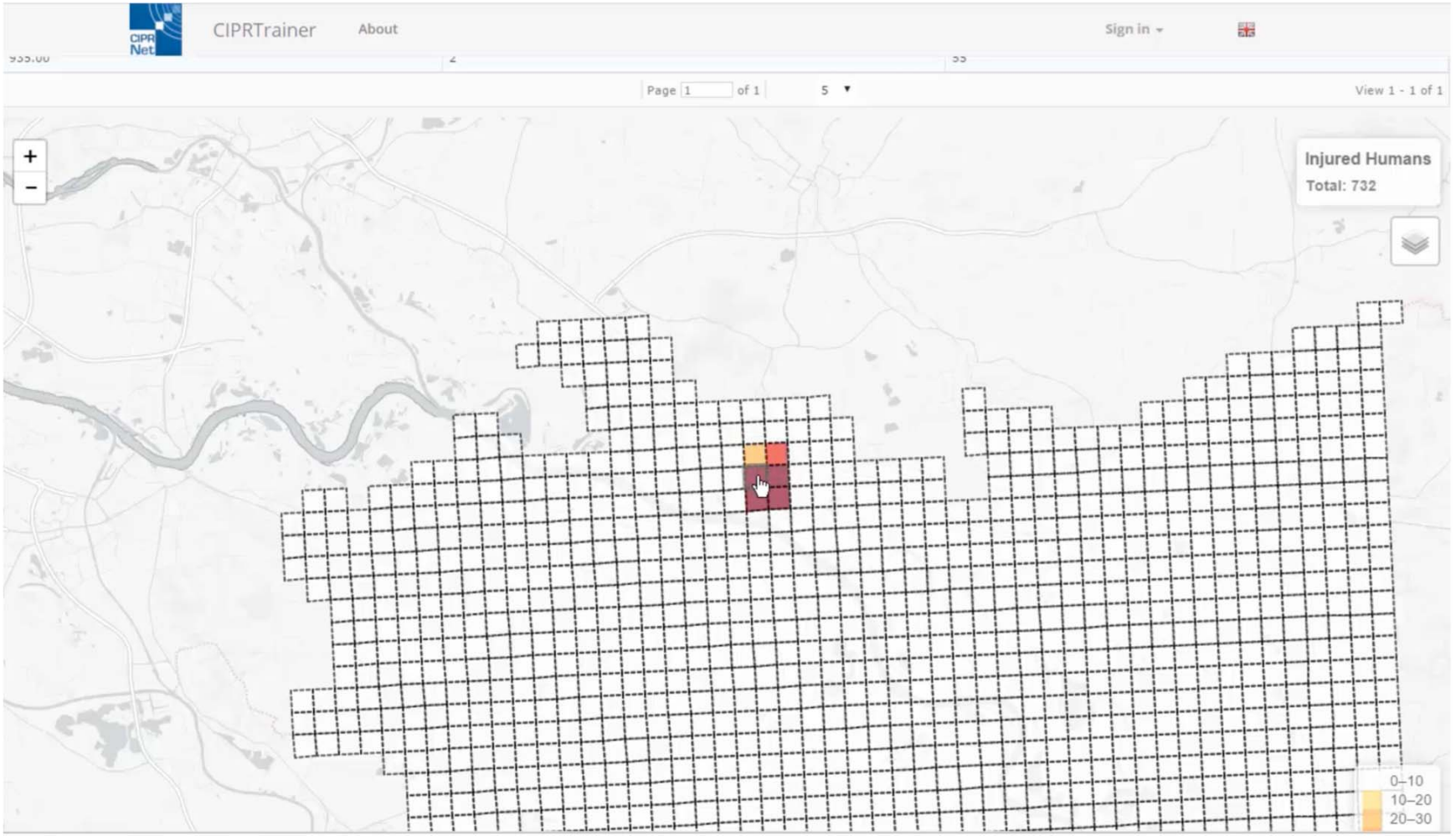
EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: Ausführung von Aktionen



EU-FP7-Exzellenznetzwerk CIPRNet

CIPRTrainer: Darstellung von Konsequenzen



EU-FP7-Exzellenznetzwerk CIPRNet

Transfer: Zusammenarbeit mit Experten und Endnutzern

- Im Konsortium:
  - Internationaler Eisenbahnerverband UIC
  - Deltares: Wasser-Forschungsinstitut (Flutmodelle)
  - Spezialisten für Cyber-Sicherheit, Telekommunikations- und Stromnetze
- Externe Experten und Endnutzer bei CIPcast
  - Strom-, Telekommunikations- und Trinkwassernetzbetreiber
  - Nationale und regionale Krisenmanagementbehörden
- Externe Experten bei CIPRTrainer
  - Ausbildungszentrum des französischen Krisenmanagements
  - Ausbildungszentrum des deutschen Krisenmanagements
  - Feuerwehrleute

Fazit
Technologietransfer KRITIS

- Trotz einzelner Erfolge: Inhärente Probleme des Forschungsgebietes sind
  - Vulnerabilitäten, die aus Sicherheitsgründen nicht öffentlich gemacht werden dürfen
  - Daraus resultieren Vorbehalte der KRITIS-Betreiber gegenüber der KRITIS-Forschung
- Zusammenarbeit mit KRITIS-Betreibern erfordert Vertrauensbildung
- Einführung von (innovativer) Technologie zum KRITIS-Schutz wird einfacher, wenn ein geldwerter Zusatznutzen identifiziert werden kann
  (Anderes Beispiel: Chemosensoren im Trinkwassernetz)
- Krisenmanagement im Bevölkerungs- und Katastrophenschutz ist affiner zum praktischen Einsatz von Forschungsergebnissen als KRITIS-Betreiber

Fazit
Technologietransfer KRITIS

- Einige Zutaten zum erfolgreichen Transfer:
  - Einfach zu handhabende Lösungen
  - Im täglichen Betrieb einsetzbar
  - Geldwerter Zusatznutzen
- Probleme beim Einsatz von Forschungsprototypen:
  Wartung, Kosten, Kandidat für „Tool-Friedhof“?
- Lösung? Zentrum für Technologietransfer, Know-how, und Unterstützung – VCCC
- Benötigte Kapazitäten:
  - Forscher, die in einem multidisziplinären Umfeld arbeiten können und den dafür benötigten „Mindset“ mitbringen
  - Forscher, die die KRITIS-Sicherheitsproblematik verstehen und verantwortungsvoll mit den gewonnenen Erkenntnissen umgehen (Veröffentlichungen)

Disclaimer

Parts of this presentation were derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreements no 312450.

Danke für Ihre Aufmerksamkeit!

www.predict-project.eu

www.resin-cities.eu

www.ciprnet.eu

www.cipedia.eu (online CIP glossary)

PREDICT

RESIN
CLIMATE RESILIENT CITIES AND INFRASTRUCTURES

CIPR Net

Fraunhofer IAIS

Literaturreferenzen

Publikationen

LUIIJF2015a Luiijf E., Klaver M., Governing Critical ICT: **Elements that Require Attention**, European Journal on Risk Regulation, Volume 6 (2015), Issue 2, July/August 2015, p. 263-270

KOZIK2015a Kozik R., Choras M., Flizikowski A., Theocharidou M., Rosato V., Rome E., **Advanced services for critical infrastructures protection**, Journal of Ambient Intelligence and Humanized Computing, Springer Berlin Heidelberg, ISSN 1868-5137, volume 6, issue 6, p. 783-795, December 2015

LUIIJF2015b Luiijf E. **Cyber (In-)security of Industrial Control Systems: A Societal Challenge**, in: F. Koornneef and C. van Gulijk (Eds.): SAFECOMP 2015, LNCS 9337, pp. 7–15, 2015

KOZIK2015a Kozik R., Choras M., Holubowicz W., Renk R., **Increasing Protection and Resilience of Critical Infrastructures – Current challenges and approaches**, in Proc on Critical Infrastructures Preparedness: Status of Data for Resilience Modelling, Simulation and Analysis (MS&A), ESReDA Workshop, Wroclaw, 28th–29th May 2015

TOFANI2015 Tofani A., Di Pietro A., Lavalle L., Pollino M., Rosato V., Alessandroni S., **CIPRNet Decision Support System: Modelling Electrical Distribution Grid Internal Dependencies**, in Proc on Critical Infrastructures Preparedness: Status of Data for Resilience Modelling, Simulation and Analysis (MS&A), ESReDA Workshop, Wroclaw, 28th–29th May 2015

ROME2014 Rome, E., Langeslag, P., Usov, A., **Federated Modelling and Simulation for Critical Infrastructure Protection**, in: D'Agostino, G., Scala, A. (eds), Network of Networks: the last Frontier of Complexity, Springer, Cham Heidelberg, (2014)

BURZEL2014 Burzel, A., Hounjet, M., Becker, B., di Pietro, A., Pollino, M., Rosato, V., Tofani, A., **Towards a decision support system for consequence analysis of flooding on critical infrastructure**, 11th International Conference on Hydroinformatics, New York, USA

FORMI2014 Formicola V., Di Pietro A., Alsubaie A., D'Antonio S., Martí J.R., **Assessing the Impact of Cyber Attacks on Wireless Sensor Nodes that Monitor Interdependent Physical Systems**, Critical Infrastructure Protection, Springer Berlin Heidelberg, Vol. VIII, pp.213-229, 1st January 2014

ALSU2014 Alsubaie A., Alutaibi K., Martí J.R., Di Pietro A., and Tofani A., **Resources Allocation in Disaster Response using Ordinal Optimization Based Approach**, IEEE Canada International Humanitarian Technology Conference (IHTC 2014), Montreal, 1st–4th June 2014

ROME2009 E. Rome, S. Bologna, E. Gelenbe, E. Luiijf, V. Masucci (2009): **DIESIS - Design of an Interoperable European Federated Simulation Network for Critical Infrastructures**. In: Proceedings of the 2009 SISO European Simulation Interoperability Workshop (**ESIW '09**), Simulation Councils, Inc., San Diego, CA, USA, ISBN 1-56555-336-5, pp. 139–146. Conference: Istanbul, Turkey, July 13-16, 2009

Literaturreferenzen

Sekundärliteratur

LUIIJF2010 H.A.M. Luiijf, A.H. Nieuwenhuijs, M.H.A. Klaver, M. van Eeten, E. Cruz (2010): **Empirical Findings on Critical Infrastructure Dependencies in Europe**. International Journal of System of Systems Engineering 2010 - Vol. 2, No.1 S. 3–18

LUIIJF2009 H.A.M. Luiijf, M.H.A. Klaver (2009): **Insufficient situational awareness about Critical Infrastructures by Emergency Management**, In: Symposium on C3I for Crisis, Emergency and Consequence Management IST-086 / RSY-019, May 2009, Bucharest, Romania, NATO RTO, RTO-MP-IST-086, paper 10

NIEUW2008 A.H. Nieuwenhuijs, H.A.M. Luiijf, M.H.A. Klaver (2008): **Modeling Critical Infrastructure Dependencies**. in: IFIP International Federation for Information Processing, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi, (Boston: Springer), November 2008

LUIIJF2005 H.A.M. Luiijf, M.H.A. Klaver (2005): **International Interdependency of C(I)IP in Europe (Internationale Verflechtung von C(I)IP in Europa)**. In: B.M. Hämmerli, S. Wolthusen (Eds), *Proceedings of CIP Europe 2005 - Critical Infrastructure Protection*, GI CIS Forum, Bonn, Germany, 19 September 2005

BROWN2010 T. Brown (2008): **Infrastructure Dependency Indicators**, In Wiley Handbook of Science and Technology for Homeland Security, Wiley

BMI2009 BMI (Hrsg., 2009): **Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)**, Berlin, Juni 2009

NPSI2005 Bundesministerium des Innern (Hrsg., 2005): **Nationaler Plan zum Schutz Kritischer Infrastrukturen**, Berlin, Juli 2005

BSK2005 Bundesministerium des Innern (Hrsg., 2005): **Schutz Kritischer Infrastrukturen – Basisschutzkonzept**, Berlin, 2005.

UPK2005 Bundesministerium des Innern (Hrsg., 2005): **Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen**, Berlin, 2005

OECD2008 OECD, **Protection of 'Critical Infrastructure' and the role of investment policies relating to national security,** May 2008

EU2008 European Commission, **Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment to improve their protection**

CEPS2011 A. Renda, B.M. Hämmerli (2011): **CEPS Task Force Report Protecting Critical Infrastructure in the EU.** Centre for European Policy Studies, Brussels

Links

www.cipedia.eu

www.predict-project.eu

www.resin-cities.eu

www.ciprnet.eu

www.secret-project.eu

www.va-sa.net

www.hipow-project.eu

www.diesis-project.eu

www.irriis.org

www.emili-project.eu