POINT OF RESOLUTION
DEFENSE & INFRASTRUCTURE SECURITY

51.3397° N 12.3731° E
LEIPZIG · GERMANY

WHITE PAPER

METHODISCHE GRUNDLAGE DER POINT OF RESOLUTION · POR-WP-2026-001

KRITISCHE INFRASTRUKTUR · LAGEKLÄRUNG · ENTSCHEIDUNGSUNTERSTÜTZUNG

Von der Risikoanalyse zur Lageklärung

Ein entscheidungsorientierter Ansatz für komplexe Lagen in kritischen Infrastrukturen

KERNAUSSAGE

Das zentrale Defizit komplexer Infrastrukturlagen liegt häufig nicht im Fehlen einzelner Methoden, Datenquellen oder Technologien, sondern in ihrer fachlichen, organisatorischen und zeitlichen Trennung. Entscheidungsorientierte Lageklärung setzt deshalb beim Informationsbedarf an und integriert geeignete Evidenzquellen so lange, bis die verbleibende Unsicherheit einer belastbaren Entscheidung nicht mehr entgegensteht.

POINT OF RESOLUTION
Risk Intelligence · Technical & Engineering Analysis · Monitoring · Decision Support
White Paper POR-WP-2026-001 | Version 1.1 | 22. September 2026

DOKUMENTENKOPF

GEGENSTAND	Methodische Herleitung und Beschreibung entscheidungsorientierter Lageklärung als operativer Prozess zwischen Risikoerkennung, Lageverständnis und Entscheidung in kritischen und verteidigungswichtigen Infrastrukturen.
REIHE	White Paper · POR-WP-2026-001
STAND	22. September 2026
VERSION	1.1
DOKUMENTTYP	White Paper · methodische Grundlage
KLASSIFIZIERUNG	Public
AUSSAGEEBENE	Methodisch · operativ · organisatorisch
QUELLENBASIS	ISO · IEC · EU · KRITISDachG · BBK · CISA · NIST · JRC · DWA · ODNI · Fachliteratur · POR
SPRACHE	Deutsch, mit englischem Abstract
UMFANG	34 Quellen · 5 Abbildungen · 3 Tabellen · 2 Anhänge
STATISTIK	Keine Ereignis- oder Fallstatistik

ZITIERVORSCHLAG

POINT OF RESOLUTION: Von der Risikoanalyse zur Lageklärung. Ein entscheidungsorientierter Ansatz für komplexe Lagen in kritischen Infrastrukturen. White Paper POR-WP-2026-001, Version 1.1, Stand 22.09.2026, Leipzig.

HINWEIS ZUR VERWENDUNG

Dieses White Paper ist eine fachliche Arbeitsgrundlage und keine Rechtsberatung, behördliche Einstufung oder Zertifizierung. Die beschriebenen Konzepte ersetzen keine gesetzlich vorgeschriebenen Risikoanalysen, Resilienzpläne, Sicherheitsprüfungen oder fachtechnischen Nachweise. Sicherheitskritische Detailanalysen sind kontextbezogen, rechtlich geprüft und nach Need-to-know durchzuführen.

SICHERHEITSGRENZE DIESER PUBLIKATION

Diese Darstellung benennt bewusst keine objektspezifischen Schwachstellen, Angriffspfade, Zugriffstechniken oder Umgehungsmethoden. Die Anwendungsbeispiele sind konstruiert und beschreiben keine realen Vorgänge.

VERSIONSHISTORIE

Version 1.0 | 21.09.2026 | Erstfassung
Version 1.1 | 22.09.2026 | Quellenkorrektur, Präzisierung Normstatus, Abb. 4 und Abschnitt 3.5

HERAUSGEBER

Ingo Zimmer, POINT OF RESOLUTION, Haferkornstraße 15, 04129 Leipzig

ZUM AUTOR

Ingo Zimmer ist Founder & Mission Director von POINT OF RESOLUTION und Inhaber von THE MALAMUTE – Bar, Consulting & Engineering, beide Leipzig. Er war fünfzehn Jahre im militärischen Nachrichtenwesen der Bundeswehr tätig, mit mehreren Auslandseinsätzen. Fachlich arbeitet er an der Zustandserfassung und dem Monitoring linearer und unterirdischer Infrastruktur, unter anderem an Hangsicherungs- und Entwässerungssystemen an Schieneninfrastruktur, und hat dafür eigene Monitoring- und Detektionssysteme entwickelt. Er entwickelt und leitet Qualifizierungsprogramme für Betreiber und Ausführende kritischer Infrastruktur, unter anderem für das Bahn- und Straßenumfeld, mit Schwerpunkten auf Kanalinspektion, Zustandsbewertung von Entwässerungsanlagen, Datenqualität und digitalen Zwillingen sowie Arbeitssicherheit. Dazu gehört ein gemeinsam mit der SAG Akademie Darmstadt entwickelter Online-Meisterkurs für den Rohr-, Kanal- und Industrieservice. Seine Seminare zur Zustandserfassung von Entwässerungssystemen behandeln sowohl das geltende Merkblatt DWA-M 149-5 als auch den Entwurf DWA-A 149-5.

INHALT

Abstract

Kritische Infrastrukturen sind sozio-technische Systeme, deren Funktionsfähigkeit aus dem Zusammenwirken physischer Anlagen, digitaler Systeme, betrieblicher Prozesse, Menschen, Organisationen und externer Abhängigkeiten entsteht. Die zu ihrer Analyse verfügbaren Methoden – Risikomanagement, Resilience Engineering, Monitoring, Fernerkundung, Situation Awareness, Early Warning und strukturierte Analyseverfahren – sind fachlich entwickelt, werden jedoch überwiegend getrennt angewandt. Dieses White Paper leitet her, dass das daraus entstehende Defizit nicht im Fehlen von Methoden oder Daten liegt, sondern im Fehlen eines gemeinsamen Entscheidungsbezugs, und leitet als analytische Synthese vier Mechanismen ab, die diese Trennung begünstigen können: divergierende Problemdefinitionen, inkompatible Systemgrenzen, unterschiedliche Zeitraster und das Fehlen einer gemeinsamen Bewertungssprache. Vorgeschlagen wird entscheidungsorientierte Lageklärung als verbindendes Arbeitsprinzip. Ausgangspunkt ist nicht die verfügbare Technologie, sondern die anstehende Entscheidung und die für sie fehlende Information. Daraus ergibt sich ein iterativer Prozess aus sieben Phasen, eine getrennte Führung von Erkenntnisstatus und Confidence sowie ein vorab definiertes, in der Regel asymmetrisches Entscheidungskriterium. Der Ansatz ersetzt weder regulatorische Pflichten noch fachtechnische Prüfungen; er ist als operative Ergänzung zwischen Risikoerkennung, Lageverständnis und Entscheidung konzipiert. Ziel ist nicht Informationsvollständigkeit, sondern Resolution: ein Erkenntnisstand, der eine verantwortbare menschliche Entscheidung trotz verbleibender Unsicherheit ermöglicht. Das White Paper ist ein Arbeitsmodell und benennt prüfbare Nutzenannahmen sowie Bedingungen, unter denen einzelne Annahmen oder Bestandteile verworfen oder angepasst werden müssten.

Schlagwörter: Kritische Infrastruktur, Lageklärung, Entscheidungsunterstützung, Resilienz, Evidenzfusion, Unsicherheit, Frühwarnung, KRITIS-Dachgesetz

Abstract (English)

Critical infrastructures are socio-technical systems whose performance emerges from the interaction of physical assets, digital systems, operational processes, people, organizations, and external dependencies. The methods available to analyze them — risk management, resilience engineering, monitoring, remote sensing, situation awareness, early warning, and structured analytic techniques — are professionally mature but are largely applied in isolation. This white paper argues that the resulting deficit lies not in missing methods or missing data, but in the absence of a shared decision reference, and derives four mechanisms as an analytical synthesis that can sustain this separation: diverging problem definitions, incompatible system boundaries, mismatched time scales, and the lack of a common assessment language. It proposes decision-oriented situation resolution — the systematic conversion of an unclear situation into decision-relevant knowledge — as a connecting working principle. The starting point is not the available technology but the pending decision and the information it lacks. This yields an iterative seven-phase process, separate tracking of evidence status and confidence, and a decision criterion that is defined in advance and is typically asymmetric. The approach replaces neither regulatory obligations nor technical inspections; it is designed as an operational layer between risk identification, situational understanding, and decision. The objective is not completeness of information but resolution: a state of knowledge sufficient for accountable human decision-making despite residual uncertainty. The white paper presents a working model and identifies testable benefit assumptions as well as conditions under which individual assumptions or components would have to be rejected or revised.

Keywords: critical infrastructure, situation resolution, decision support, resilience, evidence fusion, uncertainty, early warning, CER Directive

Executive Summary

Die Auswertung verdichtet sich auf sechs Punkte, die für Betreiber, Behörden und technische Verantwortliche unmittelbar handlungsleitend sind.

01 Das Defizit liegt in der Verknüpfung, nicht in den Methoden.

Ingenieurwissenschaftliche Zustandsbewertung, Risikomanagement, Monitoring, Fernerkundung, Resilience Engineering und lagebezogene Analyse liefern jeweils belastbare Erkenntnisse. Aktuelle Reviews zeigen jedoch weiterhin Fragmentierung bei der Resilienzbewertung, Defizite in der sozio-technischen Integration und uneinheitliche Behandlung von Unsicherheit und Entscheidungsbezug. Das daraus abgeleitete Integrationsproblem ist ein fehlender gemeinsamer operativer Bezugspunkt.

02 Mehr Daten erzeugen nicht automatisch mehr Lageverständnis.

Datenquellen unterscheiden sich in zeitlicher Auflösung, räumlicher Abdeckung, Messunsicherheit, Aktualität und semantischer Eindeutigkeit. Ein System kann technisch einwandfrei exakt die falsche Größe erfassen. Hinzu kommt der Preis unstrukturierter Signalvermehrung: Mit der Zahl der Fehlalarme sinkt die Reaktionsbereitschaft – ein Effekt, den die Alarmnormen der Prozessindustrie mit Leistungskennzahlen messbar gemacht haben.

03 Die Entscheidung ist der Ausgangspunkt, nicht das Werkzeug.

Entscheidungsorientierte Lageklärung beginnt mit der Frage, welche Entscheidung ansteht, welche Optionen bestehen, wer verantwortlich ist und bis wann entschieden sein muss. Erst daraus werden Informationsanforderungen und konkurrierende Hypothesen abgeleitet, und erst danach wird das geeignete Mittel gewählt. Diese Werkzeugagnostik schließt das Ergebnis ein, dass vorhandene Daten ausreichen.

04 Erkenntnisstatus und Confidence sind getrennt zu führen.

Der Erkenntnisstatus beschreibt, wie weit eine lagebezogene Aussage innerhalb des Verarbeitungsprozesses fortgeschritten ist – SIGNAL, VERIFIED, ASSESSED, DECISION RELEVANT. Die Confidence beschreibt dagegen die Belastbarkeit der jeweiligen Bewertung. Die getrennte Führung verhindert, dass eine verifizierte Beobachtung mit einer bereits belastbaren Erklärung verwechselt wird, und schafft eine gemeinsame Bewertungssprache zwischen den Fachbereichen.

05 Das Entscheidungskriterium wird vorab definiert und kann asymmetrisch sein.

Vollständige Gewissheit ist in komplexen Systemen nicht erreichbar; zusätzliche Aufklärung kostet Zeit, Geld, Betriebsbelastung und erzeugt gegebenenfalls neue Risiken. Deshalb wird vor Beginn der Informationsgewinnung dokumentiert, welcher Evidenz- und Confidence-Stand für die konkrete Entscheidung als ausreichend gelten soll. Erreicht ist dieser Decision Threshold, wenn die verbleibende Unsicherheit innerhalb der festgelegten Toleranz liegt und zusätzliche realistisch beschaffbare Information die Wahl zwischen den Handlungsoptionen voraussichtlich nicht entscheidungsrelevant verändern würde. Das Kriterium hängt unter anderem von Reversibilität, Schadenspotenzial und Fehlerkosten in beide Richtungen ab und kann deshalb asymmetrisch sein.

06 Der Ansatz ist ein Arbeitsmodell mit benannten Grenzen.

Er ersetzt weder die Feststellung gesetzlicher KRITIS-Betroffenheit noch Risikoanalysen, Resilienzpläne oder fachtechnische Prüfungen, und eine dokumentierte Lageklärung ist kein Compliance-

Nachweis. Seine Einzelbausteine sind fachlich abgesichert, die Integrationslogik ist plausibel und indirekt gestützt, die konkrete Ausgestaltung eine Arbeitskonvention. Kapitel 10 trennt die Kernannahme des Modells von prüfbaren Teilannahmen und benennt Kriterien, anhand derer sie empirisch bestätigt, angepasst oder verworfen werden können.

1. Ausgangslage und Problemstellung

1.1 Kritische Infrastruktur als sozio-technisches System

Die Funktionsfähigkeit kritischer Dienstleistungen entsteht nicht aus einzelnen Anlagen, sondern aus dem Zusammenwirken mehrerer Schichten: physische Assets, digitale Steuerungs- und Kommunikationssysteme, betriebliche Prozesse, qualifiziertes Personal, organisatorische Zuständigkeiten sowie externe Lieferketten und Dienstleistungen. Jede dieser Schichten besitzt eigene Fehlermodi, eigene Zeitkonstanten und eigene Zuständigkeiten. Eine Störung entsteht selten in einer Schicht allein; sie wird typischerweise dort kritisch, wo eine Abweichung eine Schicht- oder Zuständigkeitsgrenze überschreitet.

Rinaldi, Peerenboom und Kelly unterscheiden vier Abhängigkeitstypen, die für die Lagebeurteilung unterschiedliche Konsequenzen haben [5]. Physische Abhängigkeit liegt vor, wenn ein System ein materielles Produkt eines anderen benötigt – die Pumpe die elektrische Energie, das Notstromaggregat den Kraftstoff. Geografische Abhängigkeit entsteht durch räumliche Nähe ohne funktionale Kopplung: zwei unabhängige Kabelstrecken in derselben Trasse sind funktional redundant, geografisch aber nicht. Cyberbezogene Abhängigkeit besteht dort, wo ein System auf Informationen aus einem anderen angewiesen ist, etwa Leittechnik auf Telemetrie. Logische Abhängigkeit schließlich entsteht über Markt-, Vertrags- oder Verhaltensmechanismen, ohne physische oder informationstechnische Verbindung.

Diese Typologie ist nicht akademisch. Sie erklärt, warum Redundanzkonzepte im Papier belastbar wirken und in der Lage versagen: Redundanz wird meist gegen physische Abhängigkeit ausgelegt, während geografische und logische Kopplungen unbewertet bleiben. Das BBK beschreibt in gleicher Richtung zunehmende Interdependenzen und fordert im All-Gefahren-Ansatz die gemeinsame Betrachtung natürlicher, technischer und vorsätzlicher Gefahren [4]. Auch der CISA Infrastructure Dependency Primer behandelt Abhängigkeiten zwischen Infrastruktursystemen ausdrücklich als eigenständigen Analysegegenstand [31].

Daraus folgen drei methodische Konsequenzen.

Erstens kann ein Asset technisch normgerecht sein, während die von ihm getragene Dienstleistung hochgradig verwundbar ist – weil die Verwundbarkeit außerhalb der Systemgrenze liegt, innerhalb derer geprüft wurde. Konformitätsnachweise und Resilienzaussagen sind deshalb nicht dasselbe.

Zweitens besitzt eine identische technische Abweichung unterschiedliche Bedeutung, je nach Funktion, Redundanzlage, Betriebsphase und äußerer Situation. Eine Verformung im zulässigen Toleranzbereich ist in der Regelbetriebsphase ein Wartungshinweis; dieselbe Verformung bei ausgefallener Parallelanlage, während einer Hochwasserlage oder kurz vor einer Sperrpause ist eine Entscheidungsfrage. Ein Messwert wird also erst im Kontext entscheidungsrelevant – und dieser Kontext liegt regelmäßig außerhalb des Messsystems.

Drittens verhalten sich diese Systeme nicht linear. Rückkopplungen können Störungen dämpfen oder verstärken; Kaskaden können sich über Kopplungen fortpflanzen, die in einer isolierten Komponentenbetrachtung nicht offensichtlich sind. Reviews zu interdependenten Infrastrukturen fordern deshalb ausdrücklich, sozio-technische Dimensionen, den vollständigen Resilienzzyklus sowie Validierung und Unsicherheitsanalyse stärker in Bewertungsmodelle zu integrieren [13]. Resilienz erscheint damit weniger als statische Eigenschaft einzelner Komponenten, sondern als dynamische Fähigkeit eines Systems, Störungen zu antizipieren, ihnen zu widerstehen, sich anzupassen und Funktionen wiederherzustellen.

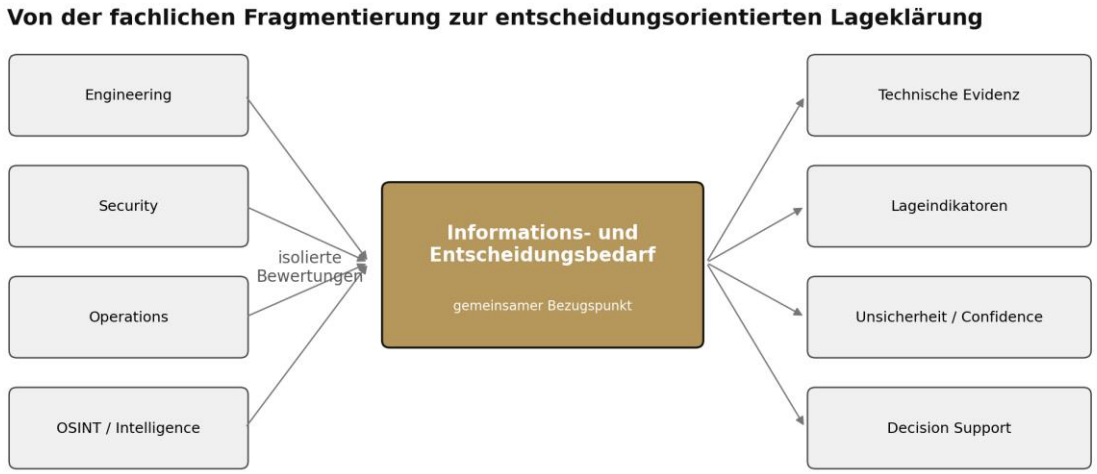

Abbildung 1: Fachliche Einzelperspektiven werden über den konkreten Informations- und Entscheidungsbedarf integriert. Eigene Darstellung.

1.2 Warum mehr Daten nicht automatisch mehr Lageverständnis erzeugen

Digitalisierung, IoT-Sensorik, Fernerkundung und Datenplattformen erhöhen die verfügbare Datenmenge erheblich. Ein besseres Lageverständnis folgt daraus nicht automatisch, weil Datenquellen sich in mindestens fünf Eigenschaften unterscheiden, die unabhängig voneinander schlecht sein können: zeitliche Auflösung, räumliche Abdeckung, Messunsicherheit, Aktualität und semantische Eindeutigkeit – also die Frage, ob überhaupt die Größe gemessen wird, die für die Fragestellung relevant ist.

Der letzte Punkt verdient besondere Aufmerksamkeit. Ein System kann mit hoher Abtastrate, kalibrierter Messkette und lückenloser Historie exakt die falsche Größe erfassen. Die Daten sind dann technisch einwandfrei und für die anstehende Entscheidung wertlos. Ein Dashboard erzeugt in diesem Fall hohe Informationsdichte, ohne die entscheidungsrelevante Frage zu beantworten – und suggeriert zugleich Beobachtbarkeit, wo keine besteht.

Hinzu kommt der Preis unstrukturierter Datenvermehrung. Mit der Zahl der Signale wächst die Zahl der Fehlalarme; mit den Fehlalarmen sinkt die Reaktionsbereitschaft. Alarmmüdigkeit ist keine Personalschwäche, sondern die vorhersehbare Folge eines Systems, das Signale erzeugt, ohne sie zu priorisieren. Die Prozessindustrie adressiert diesen Effekt sowohl normativ als auch über Branchenleitfäden: IEC 62682 beschreibt einen Lebenszyklusansatz für das Management von Alarmsystemen. Konkrete Benchmarkwerte zur Bedienerbelastung – etwa weniger als ein Alarm je zehn Minuten im stationären Betrieb und weniger als zehn Alarme in den ersten zehn Minuten nach einer Anlagenstörung – stammen aus der EEMUA-191-/ISA-18.2-Praxis und sind als empirische Orientierungswerte, nicht als universelle Grenzwerte, zu verstehen [27]. Bezeichnend ist, dass diese Kennzahlen nicht die Datenqualität betreffen, sondern die Aufnahmefähigkeit des Menschen am Ende der Kette. Ein Monitoringkonzept, das diesen Effekt nicht einkalkuliert, kann seine Lagefähigkeit trotz formal wachsender Datenbasis verschlechtern.

Die eigentliche Herausforderung verschiebt sich damit von Datenerfassung zu Selektion, Kontextualisierung und Bewertung. Maßgeblich ist nicht, ob eine Information vorhanden ist, sondern ob sie eine definierte Hypothese stützt oder schwächt, eine entscheidungsrelevante Unsicherheit reduziert, einen Trend sichtbar macht oder eine konkrete Handlungsoption verändert. Für komplexe Lagen ist deshalb ein informationsökonomischer Ansatz erforderlich: Beschafft wird nur jene zusätzliche Information, deren

erwarteter Erkenntniswert die Entscheidung tatsächlich verbessert – gemessen an Zeit, Kosten, operativer Belastung und den Risiken, die die Erhebung selbst erzeugt.

LEITSATZ

Nicht die verfügbare Technologie definiert die Mission. Der Informationsbedarf definiert, welche Technologie, Expertise oder Datenquelle überhaupt erforderlich ist.

1.3 Begriffliche Abgrenzung: Risiko, Gefährdung, Lage, Lageklärung

Die Begriffe werden in Praxis und Literatur uneinheitlich verwendet, weshalb sie für dieses White Paper festgelegt werden.

Gefährdung bezeichnet ein Ereignis, einen Zustand oder eine Einwirkung mit Schadenspotenzial, unabhängig davon, ob ein konkretes System tatsächlich betroffen ist. ISO 31000 fasst Risiko auf einer bewusst übergeordneten Ebene als Auswirkung von Unsicherheit auf Ziele [1]. Für dieses White Paper wird diese Definition nicht ersetzt, sondern für kritische Infrastrukturen tiefer operationalisiert: Risiko bezeichnet hier die mögliche Auswirkung von Unsicherheit auf definierte betriebliche, sicherheitsbezogene, regulatorische oder gesellschaftliche Ziele, analysiert über Gefährdung, Exposition, Verwundbarkeit, relevante Abhängigkeiten und Folgen. Diese Größen sind damit keine konkurrierende Risikodefinition, sondern die analytischen Dimensionen, mit denen die abstrakte ISO-Definition für konkrete Infrastrukturszenarien zerlegt und prüfbar gemacht wird.

Diese Vertiefung ist für die Lageklärung notwendig, weil die organisationsübergreifende Definition der ISO bewusst offenlässt, über welchen Wirkmechanismus Unsicherheit in einem konkreten Infrastruktursystem auf Ziele wirkt. Für eine operative Analyse muss jedoch unterscheidbar sein, welche Gefährdung betrachtet wird, welche Funktion exponiert ist, welche Verwundbarkeit oder Abhängigkeit die Wirkung vermittelt, welche Folgen relevant sind und an welcher Stelle die Unsicherheit liegt. Erst diese Zerlegung erlaubt es, Informationslücken, Beobachtungsgrößen und Entscheidungsbedarf gezielt miteinander zu verknüpfen.

Lage bezeichnet demgegenüber den gegenwärtigen, beobachteten Zustand eines Systems einschließlich der auf ihn einwirkenden Umstände; ihr Zeitbezug ist real. Lageklärung (englisch: situation resolution) ist der Prozess, in dem eine unklare Lage durch gezielte Informationsgewinnung und Bewertung so weit aufgeklärt wird, dass eine konkrete Entscheidung verantwortbar getroffen werden kann.

Der Unterschied zwischen Risikoanalyse und Lageklärung ist damit kein terminologischer, sondern ein zeitlicher und ein adressatenbezogener: Die Risikoanalyse beantwortet, was geschehen könnte und wie darauf vorzubereiten ist. Die Lageklärung beantwortet, was gegenwärtig geschieht, wie belastbar diese Aussage ist und welche Handlungsoption sie trägt.