

18. Dezember 2025

Positionspapier

Zwischen Beitrag und Belastbarkeit: Realistische Wege zur Integration der Offshore Windbranche in die maritime Sicherheitsarchitektur

1. Zweck des Dokuments

Dieses Papier spiegelt die gemeinsame Haltung der Mitglieder des BWO zu möglichen sicherheitsrelevanten Anforderungen im maritimen Raum wider. Es soll Behörden und Politik einen realistischen Einblick geben, welche Systeme, Daten und Abläufe in Offshore-Windparks bereits heute bestehen - und welche Bedingungen erfüllt sein müssen, damit zusätzliche sicherheitspolitische Erwartungen künftig rechtssicher, verhältnismäßig und wirtschaftlich planbar umgesetzt werden können.

Die Inhalte basieren auf einer branchenweiten Umfrage in der Mitgliedschaft des BWO, sowie auf den Beratungen in den BWO-Fachausschüssen Security und Betrieb. Ziel dieses Dokuments ist es, frühzeitig Transparenz zu schaffen, praktische Umsetzbarkeit einzuschätzen und einen strukturierten Dialog über Rollen, Verantwortlichkeiten und technische Schnittstellen aufzusetzen.

Die Branche signalisiert ausdrücklich Bereitschaft, an Lösungen mitzuwirken und bestehende Strukturen konstruktiv einzubringen. Gleichzeitig ist entscheidend, dass neue Anforderungen **gemeinsam entwickelt, klar mandatiert und orientiert an einem Security-by-Design-Ansatzes** ausgestaltet werden – mit verlässlichen rechtlichen und finanziellen Rahmenbedingungen. Ein Security-by-Design-Ansatz meint im Rahmen dieses Papiers keine starre technische Vorgabe, sondern wird als Orientierungsrahmen verstanden. Da viele Offshore-Windparks bereits bestehen, bedeutet dies, Sicherheitsbelange frühzeitig in Planungs- und Betriebsprozesse einzubeziehen und den Wissenstransfer zwischen Branche und Behörden kontinuierlich zu organisieren und zu institutionalisieren. Auf diese Weise können bestehende Branchenerfahrungen in der Datenverarbeitung in rechtssichere und wirtschaftlich tragfähige Lösungen einfließen. Diese praxisnahe Sicherheitsplanung setzt voraus, dass regulatorische Unklarheiten vermieden und bestehende rechtliche Verpflichtungen – insbesondere DSGVO-Bestimmungen - beachtet werden. Zudem gilt für luftfahrtbezogene Safety-Strukturen und Einsatzdaten ein besonderer Schutz, der klare Abgrenzungen gegenüber sicherheitspolitischen Anwendungen erfordert. Nur sofern diese Aspekte angemessene Berücksichtigung finden, können zusätzliche Sicherheitsmaßnahmen wirksam, zügig und dauerhaft in den Betrieb integriert werden, ohne bestehende Investitions- und Planungssicherheit zu gefährden.

Bereits in der Stellungnahme des BWO zum KRITIS-Dachgesetz wurde betont, dass klare Zuständigkeiten und transparente Verfahren unabdingbar sind. Diese Klärung ist bisher nicht vollständig erfolgt und erschwert eine rechtssichere Planung für die Branche. Das vorliegende Papier soll daher auch dazu beitragen, diese Lücken offen zu benennen und eine praxisorientierte Weiterentwicklung des Regelungsrahmens anzustoßen.

2. Ausgangslage: Sicherheitsforderungen im Wandel

Obwohl das KRITIS-Dachgesetz auf eine Stärkung der Resilienz kritischer Infrastrukturen zielt, bleiben wesentliche Fragen zur rechtlichen Zuständigkeit und insbesondere zum zulässigen Umfang von Betreibermaßnahmen offen. Nicht abschließend geregelt ist, welche Aufgaben im Zuständigkeitsbereich staatlicher Sicherheitsbehörden liegen und welche durch Betreiber unterstützend erbracht werden dürfen. Dies betrifft insbesondere aktive Schutzmaßnahmen wie beispielsweise in Bezug auf die Gefährdung durch Drohnen. Mangels klarer gesetzlicher Leitplanken bleibt offen, was Betreiber dürfen und was nicht – eine Lücke, die voraussichtlich auch durch das KRITIS-Dachgesetz nicht geschlossen wird. Diese Rechtsunsicherheit führt zu Begrenzungen in Planung, Investition und Sicherheitsmanagement innerhalb der Branche.

Die Umsetzung maritimer Sicherheitsanforderungen im Offshore-Kontext befindet sich angesichts geopolitischer Entwicklungen in einer Phase konzeptioneller und regulatorischer Weiterentwicklung. Die Offshore-Wind-Branche erkennt ihre sicherheitspolitische Rolle als Betreiber kritischer Infrastruktur an und teilt das Ziel, maritime Resilienz weiter zu stärken. Gleichzeitig zeigt die Perspektive der Branche, dass Sicherheit im Offshore-Bereich nur wirksam und dauerhaft tragfähig gestaltet werden kann, wenn technische, regulatorische und insbesondere wirtschaftliche Realitäten zusammengeführt werden.

Vor diesem Hintergrund erachtet die Branche eine regulatorische und technische Ausgestaltung, orientiert an einem Security-by-Design-Ansatz, als notwendig. Dieser Ansatz geht über eine reine Abfrage bestehender Systeme oder Daten hinaus und umfasst die gemeinsame Entwicklung passgenauer Prozesse, Schnittstellen und Governance-Strukturen, sowohl in staatlichen Behörden als auch in den

Betreiberunternehmen. Ziel ist es, Sicherheitsanforderungen so zu gestalten, dass sie praktikabel, interoperabel und anschlussfähig an bestehende Betriebsprozesse sind.

Auch hier besteht nach Einschätzung des BWO weiterhin eine Regelungslücke hinsichtlich klarer Zuständigkeiten zwischen staatlichen Sicherheitsinteressen und privater Betriebsverantwortung. In der BWO-Stellungnahme zum KRITIS-Dachgesetz wurde bereits darauf hingewiesen, dass Sicherheitsaufgaben, die kernstaatliche Funktionen berühren – wie Radar- oder Drohnenüberwachung – nicht an Betreiber ausgelagert werden dürfen. Solange diese Grenzziehung nicht rechtssicher erfolgt, läuft die Umsetzung neuer Sicherheitsanforderungen Gefahr, unverhältnismäßig zu werden oder staatliche Aufgaben faktisch zu privatisieren. Ein strukturierter Wissenstransfer ermöglicht es, betriebliche und technische Erfahrungen der Branche frühzeitig in die Behördenarbeit einzubringen und neue Anforderungen realistisch zu gestalten. Security-by-Design heißt für uns damit vor allem: Frühzeitige Koordination und gegenseitiges Verständnis über operative Grenzen und das Erfordernis klarer rechtliche Rahmenbedingungen.

Ein solcher Weg kann Vertrauen schaffen - nicht nur in Zielsetzung und Verfahren, sondern auch in Verantwortlichkeiten und späterer Anwendung. Die Ergebnisse der Branchenumfrage und Ergebnisse der Diskussionen in der Fachgruppe des BWO zeigen, dass vorhandene Kompetenzen, etablierte Betriebsprozesse und bestehende Systeme wertvolle Orientierungspunkte bieten. Gleichzeitig wurde deutlich, dass Vertrauen kein Ausgangspunkt ist, sondern Ergebnis eines transparenten, kontinuierlichen und strukturierten Austausches. Wenn Betreiber und Behörden gemeinsam an Konzepten zur Lagebilderstellung und Sicherheitsarchitektur arbeiten, entsteht ein gegenseitiges Verständnis für Anforderungen, Restriktionen und Risiken - und damit eine Grundlage für tragfähige Lösungen.

Sicherheit muss dabei ganzheitlich gedacht werden: als Zusammenspiel staatlicher Sicherheitsinteressen, betrieblicher Umsetzbarkeit und wirtschaftlicher Tragfähigkeit. Unklare Kostentragung, potenzielle Nachrüstverpflichtungen oder fehlende Planungssicherheit stellen ein Risiko nicht nur für laufende Projekte, sondern auch für künftige Investitionen dar und wirken unmittelbar auf die Investitions- und Standortattraktivität. Diese Aspekte müssen im Prozess der Konzeptentwicklung von Beginn an mitgedacht und adressiert werden.

Der BWO versteht sich hierbei als vermittelnde Struktur und Ansprechpartner, um praktische Erfahrungen der Betreiber, technische Anforderungen sowie sicherheitspolitische Ziele zusammenzuführen und in einen konstruktiven Arbeitsprozess zu überführen - transparent, fachlich abgestimmt und mit Blick auf ein standortförderndes Ergebnis.

3. Bestehende Fähigkeiten und verfügbare Technik der Betreiber

Dieses Kapitel fasst die bestehenden technische Möglichkeiten der Betreiber zusammen. Es zeigt, dass bereits vielfältige Strukturen vorhanden sind, die prinzipiell geeignet sind, einen Beitrag zu behördlichen Sicherheitsinteressen zu leisten. Gleichzeitig macht die Branche deutlich, dass gerade hier eine klare Regulatorik erforderlich ist, die festlegt, welche Daten und Systeme zu welchem Zweck genutzt werden dürfen – und wer für die daraus resultierenden Betriebskosten verantwortlich ist. Die Frage der Zweckbindung und die Diskussion über mögliche Nutzungskonzepte können nicht ohne eine parallele Klärung der Finanzierungs- und Interessenlage geführt werden. Aus Sicht des BWO bedarf es hier einer offenen, strukturierten und rechtlich verbindlichen Abstimmung, damit ein ausgewogenes Verhältnis zwischen Sicherheitsinteressen, betrieblicher Machbarkeit und wirtschaftlicher Tragfähigkeit gewahrt bleibt.

3.1. Schiffsverkehr und Betriebsüberwachung

Die Betreiber verfügen flächendeckend über technische Systeme zur maritimen Lageüberwachung, insbesondere AIS-Tracking und CCTV. Ergänzend dazu unterhalten viele Unternehmen Seeraumbeobachtungs-Strukturen, die Schiffsbewegungen aktiv überwachen und operative Lagebilder führen. Diese Fachstrukturen gelten aus Sicht der Branche als geeignete Ansprechpartner für die Analyseeinheiten des Maritimen Sicherheitszentrums. Während einige Betreiber die erhobenen Daten bereits speichern, sehen andere Potenzial für eine nutzungsabhängige Speicherung, sofern Rechtsgrundlagen, Zuständigkeiten und Speicherfristen eindeutig definiert sind. Radarbasierte Systeme sind derzeit vereinzelt vorhanden. Die Diskussion über eine mögliche Nachrüstung führt jedoch zu Verunsicherung - weniger

hinsichtlich der Technologie selbst, sondern im Hinblick auf die Datenverarbeitung, Auswertung und die Verantwortlichkeit für daraus abgeleitete Maßnahmen. Der BWO empfiehlt daher, zunächst gemeinsam die Zwecke, Anforderungen (z. B. Reichweite, Auflösung), Prozesse sowie die Finanzierung zu definieren, um Planungssicherheit hinsichtlich künftiger CAPEX- und insbesondere OPEX-Folgen zu gewährleisten.

3.2. Kommunikation und Einsatzkoordination

Rund um die Uhr besetzte Leitstellen sind in der Branche etabliert und nutzen VHF-Funk, Mobilfunk, digitale Plattformen sowie teilweise Satellitenkommunikation. Zudem kommen verbreitete IT-gestützte Funksysteme wie TETRA oder PMR zum Einsatz. Eine Integration in staatliche Kommunikationsarchitekturen erscheint grundsätzlich möglich, sofern Rollen, Meldewege und technische Standards gemeinsam festgelegt werden. Zu berücksichtigen ist dabei, dass Leitstellen-Strukturen bei international tätigen Unternehmen häufig nicht ausschließlich in Deutschland angesiedelt sind und bereits heute in europäischen Verbänden arbeiten. Aus Sicht der Branche wäre es daher sinnvoll, auch staatlicherseits eine europäisch abgestimmte Lösung zu verfolgen, um Effizienz, Interoperabilität und Reaktionsfähigkeit sicherzustellen. Eine grenzüberschreitende Zusammenarbeit wird als wesentliche Voraussetzung für einen kohärenten maritimen Sicherheitsansatz gesehen und dürfte auch auf Behördenseite Zustimmung finden.

3.3. Wetter- und Umweltbeobachtung

Daten zur Wetter- und Umweltbeobachtung werden in Offshore-Windparks teils im Minutenraster erhoben. Erfasst werden dabei beispielsweise Windrichtung und -geschwindigkeit, Sichtweiten, Niederschlagsmengen, Seegang sowie Luft- und Wassertemperatur. Ergänzend hierzu werden weitere Umweltmonitoringdaten gesammelt, darunter teilweise Avifauna-Beobachtungen oder Monitoringprogramme zum Vogelzug. Eine sicherheitsbezogene Nutzung dieser Datensätze wäre grundsätzlich denkbar, setzt jedoch eine klare Zweckbindung, eindeutige Verantwortlichkeiten und datenschutzrechtliche Rahmenbedingungen voraus. Aus Sicht der Branche ist eine frühzeitige und strukturierte Abstimmung erforderlich, da Kosten, technische Umsetzung und Governance-Fragen nur dann effizient planbar sind. Eine nachträgliche Integration sicherheitsrelevanter Funktionen in bestehende Systeme wäre hingegen technisch aufwendig, finanziell belastend und organisatorisch schwer realisierbar und könnte bestehende Sensibilitäten rund um Datenhoheit und Vertrauensschutz zusätzlich verstärken. Die gemeinsame Entwicklung solcher Anforderungen mit den jeweiligen Fachstellen der Betreiberunternehmen würde daher Vertrauen fördern und eine tragfähige Grundlage für eine konstruktive Zusammenarbeit zwischen Behörden und Wirtschaft bilden. Ein Ansatz nach dem Prinzip „Security by Design“ trägt damit in angemessenem Verhältnis zur Stärkung von Resilienz und Sicherheit im maritimen Raum bei.

3.4. Notfallmanagement und Havarie

Alle Betreiber verfügen über dokumentierte Notfallprozesse, digitale Einsatznachverfolgung sowie etablierte Schnittstellen zu Rettungskräften. Diese Strukturen sind historisch gewachsen und dienen primär der **Safety**. Zur Steuerung werden u. a. CIM, HEMS, Notfallleitstelle sowie Betriebsleitstellen genutzt. Einsatzzeiten, Positionen und Einsatzverläufe werden protokolliert und in der Regel bis zu fünf Jahre gespeichert. Diese Prozesse und Systeme sind bewusst nicht auf **Security** ausgerichtet und sollten weiterhin klar getrennt betrachtet werden. Gleichzeitig kann die gewachsene operative Praxis wertvolle Hinweise liefern, wie Kommunikationsarchitekturen, Rollenmodelle und interoperable Schnittstellen in der Praxis funktionieren und wie sie - ohne bestehende Abläufe zu überlagern - künftig für Security-Fragestellungen übertragen werden können.

Die konzeptionelle Weiterentwicklung zukünftiger Security-Strukturen kann sich daher an der etablierten Zusammenarbeit zwischen Staat und Unternehmen im Safety-Bereich orientieren. Ein frühzeitiger, strukturierter Austausch ermöglicht es, vorhandene Mechanismen gezielt zu übertragen, Doppelstrukturen zu vermeiden und potenzielle Herausforderungen im Security-Kontext von Beginn an auszuschließen. Aus Sicht der Branche ist es sinnvoll, diesen Prozess zeitnah aufzusetzen und insbesondere die einschlägigen Fachstellen innerhalb der Betreiberunternehmen einzubeziehen, um realistische, interoperable und dauerhaft akzeptierte Lösungen zu entwickeln.

3.5. IT-/OT-Systeme und Cybersecurity

Betreiber nutzen bereits Systeme zur strukturierten Darstellung maritimer Lagebilder, darunter AIS-basierte Tracking-Software, GIS-Umgebungen, SCADA-Infrastrukturen oder spezialisierte Lagebildlösungen. Technische Schnittstellen zur Weitergabe dieser Daten an Dritte existieren derzeit nicht; insbesondere eine Übertragung an staatliche Systeme ist aktuell weder technisch vorgesehen noch organisatorisch implementiert. Die Ergebnisse der Branchenumfrage zeigen, dass bisher keine standardisierte Datenweitergabe an externe Empfänger erfolgt und hier ein hohes Maß an Sensibilität besteht.

Sollten künftig interoperable Lösungen geschaffen werden, müssten Architektur, technische Standards, Rollenverteilungen sowie Cybersecurity- und OT-Schutzanforderungen konzeptionell neu definiert werden. Aus Sicht der Branche sollte hierfür wieder einem Security-by-Design-Ansatz gefolgt werden, um Governance, Datenflüsse, Schutzmechanismen und Schnittstellen frühzeitig mitzudenken, statt sie nachträglich in bestehende Systemlandschaften integrieren zu müssen. Ein zentrales Element betrifft dabei die Frage, wie eine solche Schnittstelle über die gesamte Laufzeit eines Offshore-Projekts betrieben werden soll und wie die damit verbundenen OPEX-Kosten langfristig getragen werden. Dies berührt unmittelbar die Themen Zuständigkeiten, Finanzierung und die Definition des konkreten Zwecks, dem potenzielle Security-Maßnahmen dienen sollen.

Damit mögliche Schnittstellenmodelle praxistauglich, interoperabel und akzeptiert werden, ist aus Sicht der Branche erforderlich, diese nicht rein administrativ vorzugeben, sondern gemeinsam mit den einschlägigen Fachstellen in den Betreiberunternehmen zu entwickeln - orientiert an realen Betriebsprozessen, regulatorischen Anforderungen und einem klar begründeten sicherheitspolitischen Mehrwert. Dabei kann sich die Branche allenfalls eine Form eines Monitoring-Zugriffs auf festgelegte Parameter vorstellen, nicht aber einen steuernden oder permanenten Echtzeitzugriff von außen. Ein solches Vorgehen würde operative Abläufe und Verantwortlichkeiten überschneiden und ist technisch wie regulatorisch nur unter klar definierten Rahmenbedingungen vertretbar. Dabei stellt sich im Besonderen die Frage, ob alternative Lösungsansätze existieren, die als milderes, aber gleichermaßen geeignetes Mittel in Betracht kommen könnten.

4. Datenschutz- und Governanceanforderungen

Mit Blick auf Governance und Datenschutz identifiziert die Branche vier sensible Datenkategorien: (1) personenbezogene Daten, (2) Betriebsdaten, (3) visuelle Überwachungsdaten (z. B. CCTV) und (4) IT-/OT-Systeminformationen. Eine Weitergabe solcher Daten an staatliche Stellen erfordert eine eindeutige Rechtsgrundlage, definierte Datenkategorien, abgestimmte Verantwortlichkeiten sowie transparente Lösch- und Aufbewahrungsregelungen. Für alle oben beschriebenen Systeme und Prozesse gilt dabei, dass deren Einsatz und Weiterentwicklung nur gelingen kann, wenn Governancefragen und technische Schnittstellen Hand in Hand entwickelt werden.

Vor diesem Hintergrund hält die Branche einen regelmäßigen, strukturierten Austausch zwischen Behörden und Betreiberunternehmen für erforderlich. Ziel sollte sein, Erwartungen, operative Anforderungen und Schutzbedarfe frühzeitig abzugleichen und so gemeinsam tragfähige, praxistaugliche und sicherheitskonforme Schnittstellenmodelle zu entwickeln. Ein solcher kooperativer Ansatz stärkt Vertrauen, erhöht Planungssicherheit und minimiert das Risiko späterer, technisch aufwendiger und kostenintensiver Anpassungsprozesse. Er ermöglicht zudem, Security-Anforderungen so zu gestalten, dass sie in bestehende Betriebs- und OT-Strukturen integrierbar sind, ohne Safety-Prozesse oder Betriebsabläufe zu beeinträchtigen.

5. Kooperationswille der Branche

Die abschließende Frage der Umfrage bezog sich darauf, ob Betreiber grundsätzlich bereit wären, sich an einem vertieften Austausch mit staatlichen Stellen - etwa im Rahmen eines Besuchs oder strukturierten Dialogformats mit dem Maritimen Sicherheitszentrum - zu beteiligen. Diese Frage wurde von allen teilnehmenden Unternehmen beantwortet und zeigt eine grundsätzliche Bereitschaft, sich aktiv einzubringen. Einige Rückmeldungen erfolgten unter Vorbehalt und verweisen nochmals auf Themen, die bereits an verschiedenen Stellen benannt wurden: die Notwendigkeit klarer Rahmenbedingungen, definierter Zuständigkeiten, transparenter Governance- und Datenschutzregeln sowie eines belastbaren

Verständnisses von Zweck, Datennutzung und erwarteten Ergebnissen. Gleichzeitig wurde hervorgehoben, dass ein solcher Austausch nur dann nachhaltig wirksam sein kann, wenn er strukturiert, vertrauensbasiert und als gemeinsamer Entwicklungsprozess verstanden wird, bei dem Betreiber frühzeitig eingebunden werden. Die Ergebnisse deuten damit eindeutig darauf hin, dass Beteiligungsbereitschaft vorhanden ist - vorausgesetzt, zentrale Fragen werden vorab geklärt und die Zusammenarbeit erfolgt auf Augenhöhe.

6. Fazit

Die Offshore-Wind-Branche bekräftigt ihr Interesse an einer konstruktiven Zusammenarbeit mit Sicherheitsbehörden und ist bereit, bestehende Fähigkeiten, Daten und Systeme zur Weiterentwicklung maritimer Resilienz einzubringen. Dieses Signal zeigt, dass Betreiber ihre Verantwortung als Teil der kritischen Infrastruktur anerkennen und aktiv an Lösungsansätzen mitwirken möchten. Voraussetzung hierfür sind jedoch klare rechtliche Rahmenbedingungen, definierte Zuständigkeiten sowie ein transparenter und verstetigter Prozess zur Abstimmung technischer, organisatorischer und datenschutzrechtlicher Anforderungen.

Gleichzeitig machen die Rückmeldungen deutlich, dass die Bereitschaft zur Mitwirkung in der Branche untrennbar mit Fragen der Finanzierung und der langfristigen Planbarkeit verknüpft ist. Unklare Kostenregelungen, potenziell verpflichtende technische Nachrüstungen und zusätzliche laufende OPEX-Belastungen stellen ein erhebliches wirtschaftliches Risiko dar - sowohl für bestehende Assets als auch für Investitionen in neue Projekte. Dies betrifft nicht nur Betreiber, sondern die gesamte Investitionsstruktur des Sektors. Vor diesem Hintergrund sind ein hinreichender Bestandsschutz und ein frühzeitig definierter Rahmen erforderlich, um die langfristige Finanzierbarkeit sowie die Verlässlichkeit des Standortes Deutschland zu sichern.

Die Umfrage zeigt, dass Betreiber bereit sind, vorhandene Systeme, Daten und Expertise zu teilen – gleichzeitig aber erwarten, dass praxiserprobte Seeraumbeobachtungs-, Safety-Prozesse und bestehende IT/OT-Architekturen als Grundlage für spätere Security-Lösungen einbezogen werden. Dass dies bislang nicht systematisch erfolgt, wurde wiederholt als unverständlich gewertet. Ein frühzeitiger, strukturierter Austausch schafft nicht nur Transparenz, sondern ist aus Sicht der Branche eine wesentliche Voraussetzung für Vertrauen - und Vertrauen wiederum ist gestaltbar, wenn Betreiber und damit der BWO als Branchenvertretung aktiv in die Erarbeitung eines Lagebildkonzepts eingebunden werden. Für die Weiterentwicklung sicherheitsrelevanter Strukturen wird daher ein **Security-by-Design-Ansatz** als zielführend erachtet. Nur wenn Anforderungen gemeinsam definiert, Schnittstellen gemeinsam gestaltet und Governance-Fragen frühzeitig geklärt werden, entsteht eine Lösung, die sowohl staatlichen Sicherheitsinteressen als auch den wirtschaftlichen Realitäten einer kapitalintensiven, langfristig geplanten Infrastruktur gerecht wird. Dieses Vorgehen bietet die Chance, Akzeptanz zu sichern, Effizienz zu erhöhen und einen Sicherheitsrahmen zu schaffen, der nicht als zusätzliche Belastung, sondern als gemeinsame Weiterentwicklung der maritimen Sicherheitsarchitektur verstanden wird.

Die Branche ist bereit, diesen Weg mitzugehen - partnerschaftlich, transparent und planbar.

Kontakt

Philipp Jakobi
Leiter Betrieb und Security
Bundesverband der Windenergie Offshore e.V.
Spreeufer 5
10178 Berlin
p.jakobi@bwo-offshorewind.de

Lobbyregister: R000252