OWISS

OFFSHORE WINDENERGIE - SCHUTZ UND SICHERHEIT

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

# Verbundprojekt: Offshore-Windenergie - Schutz und Sicherheit
# Teilvorhaben: Gefahren für Offshore-Windparks durch Logistik- und IT-Prozesse

**Leitung:** **Matthias Dreyer (ISL)**

**Mitarbeit:** **Berit Böttger, Holger Lüdecke, Wiebke Duhme, Ralf Michael Knischka (ISL)**

**Laufzeit:** **01.01.2015 – 31.12.2017**

**Datum:** **25.04.2018**

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 Ausgangslage

Die Sicherstellung der Stromversorgung an Land und damit Schutz und Sicherheit von Offshore-Infrastrukturen war Gegenstand des Verbundprojekts OWiSS. Als Betrachtungsansatz diente der Status der Offshore-Windenergie im Jahr 2020 in der deutschen Nord- und Ostsee.

Schon seit einigen Jahren wandelt sich die Stromversorgungswelt in Deutschland. Durch die Energiewende will man aus der Atomkraft bis 2022 gänzlich aussteigen und auch die Stromerzeugung aus Kohlekraftwerken, dem heute größten Stromerzeuger in Deutschland, soll deutlich zurückgefahren werden. Die verminderte Stromerzeugung aus den beiden genannten Bausteinen soll durch den Ausbau erneuerbarer Energien aufgefangen werden.

Unsere moderne Gesellschaft basiert auf einer zuverlässigen Energieversorgung. Aus diesem Grund setzt sich die gesamte Stromversorgung aus mehreren Bausteinen zusammen, um bei Ausfall eines Bausteins die verminderte Stromerzeugung durch einen weiteren Baustein abzusichern.

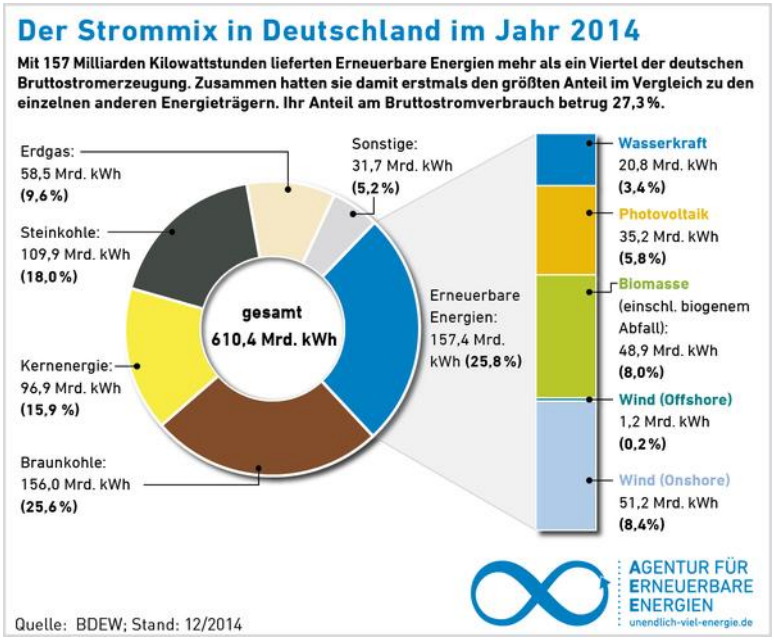



**Abbildung 1: Struktur der Stromerzeugung in Deutschland 2014**[1]

[1] Quelle: Bundesverband der Energie- und Wasserwirtschaft (BDEW); Stand 12/2014

Bis zum Untersuchungsjahr 2020 wird sich der Anteil erneuerbarer Energie nach den aktuellen Ausbauplänen weiter erhöhen: ein Teil davon wird durch den Ausbau der Offshore-Windenergie erreicht.

Da sich die Menge der Stromerzeugung der einzelnen Bausteine in der Zukunft anders verteilen wird (Menge durch Atom- und Kohlekraftwerke vermindert sich, Stromerzeugung durch erneuerbare Energien erhöht sich), ist die Erzeugung aus erneuerbaren Energien vor Bedrohungen und Gefährdungen besonders zu schützen. Jedoch gibt es auch hier Redundanzen, da diese von Jahreszeiten und Wetterbedingungen abhängig sind, so dass die Stromausbeute pro Jahr und Baustein sehr unterschiedlich ausfallen kann. Die Stromerzeugung aus erneuerbaren Energien setzt sich aus folgenden Bausteinen zusammen:

- Windkraft,
- Sonnenenergie,
- Wasserkraft und
- Biomasse.

Die Windkraft liefert mit 52,4 Mrd. kWh bezogen auf die erneuerbaren Energien mit Stand vom 31.12.2014 den größten Beitrag zur Bruttostromerzeugung, wobei auf die Onshore-Windenergie mit 51,2 Mrd. kWh der größte Anteil entfällt (siehe Abbildung 1: Struktur der Stromerzeugung in Deutschland 2014). Die Offshore-Windenergie befindet sich mit einem Anteil von 1,2 Mrd. kWh an der Erzeugung von Windenergie noch in der Aufbauphase. Dieses soll sich jedoch ändern. Der Nachteil: der Ausbau ist sehr teuer und aufwändig; die Wirtschaftlichkeit darf nicht außer Acht gelassen werden, jedoch ist die Energieausbeute auf See sehr viel höher als an Land, da der Wind offshore stärker und dauerhafter bläst als onshore.

Die Inbetriebnahme des ersten Offshore-Windparks in Deutschland erfolgte 2009, alpha ventus mit 12 Windenergieanlagen mit je 5 MW Leistung. Bis 2012 waren bereits insgesamt 308 MW Leistung installiert. Mit Stand 31. Dezember 2014 wurde diese Leistung mit nunmehr rund 1.050 Megawatt in zwei Jahren mehr als verdreifacht[2]. Ziel der Bundesregierung bis zum Untersuchungsjahr 2020 ist eine installierte Leistung von 6.500 MW[3] auf über das Sechsfache von heute, bis zum Jahr 2030 plant die Bundesregierung bereits eine Leistung von 15.000 MW. Zum Ende des Jahres 2017 lag die installierte Leistung Offshore bei rund 5.000 MW. Offshore-Windenergieparks werden in deutschen Gewässern hauptsächlich au-

[2] Quelle: Deutsche Windguard: Status des Offshore-Windenergie-Ausbaus in Deutschland 2014

[3] Quelle: Agentur für Erneuerbare Energien: http://www.unendlich-viel-energie.de/erneuerbare-energie/wind/offshore

ßerhalb der 12-Seemeilen-Zone in der ausschließlichen Wirtschaftszone (AWZ) gebaut. Bereits gebaute, bzw. im Bau befindliche und geplante Offshore-Windenergieparks befinden sich in den Hochseegewässern der Deutschen Nord- und Ostsee.

Das Bundesamt für Seeschifffahrt und Hydrographie (BSH) entscheidet über die Zulassung von Windenergieanlagen in der deutschen Nord- und Ostsee. Es ist zuständig für Antragsverfahren innerhalb der AWZ. Grundlagen für die Errichtung von Anlagen in der AWZ sind das Seerechtsübereinkommen der Vereinten Nationen vom 10. Dezember 1982 (SRUe)[4] und das deutsche Seeaufgabengesetz (SeeAufgG)[5]. Die darauf beruhende Seeanlagenverordnung (SeeAnlV)[6] regelt das Zulassungsverfahren.

Zurzeit (Stand 01/2018) speisen Offshore-Windenergieanlagen mit einer Leistung von 5.387 MW Strom ins deutsche Stromnetz ein; Offshore-Windparks (OWP) mit einer Gesamtleistung von etwa 780 MW befinden im Bau. Bei den noch nicht begonnenen Projekten wurden bereits weitere OWP mit einer Gesamtleistung von rund 1.520 MW genehmigt.

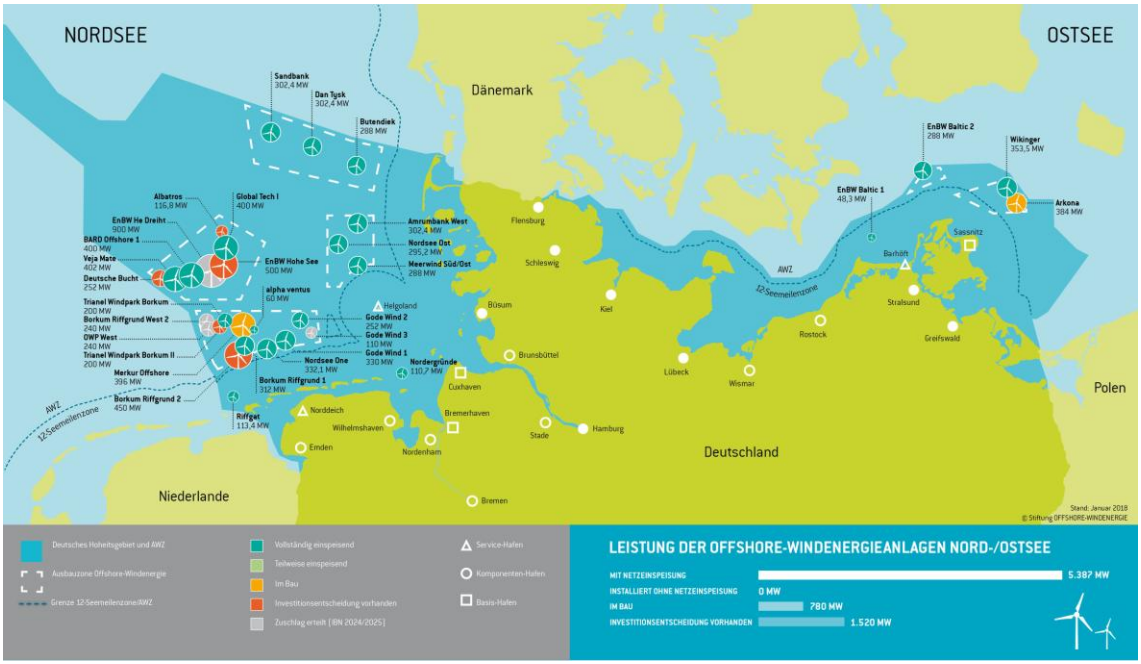



**Abbildung 2: Offshore Windparkkapazitäten in Nordsee und Ostsee**

4 Quellen: http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf (Original in Englisch), am 26.05.2015, http://www.bsh.de/de/Meeresnutzung/Wirtschaft/Windparks/Grundlagen/SrUe.pdf (Übersetzung in Deutsch), am 26.05.2015

5 Quelle: http://www.gesetze-im-internet.de/bseeschg/BJNR208330965.html, am 26.05.2015

6 Quelle: http://www.gesetze-im-internet.de/bundesrecht/seeanlv/gesamt.pdf, am 26.05.2015

Bereits während der Projektlaufzeit ist der Anteil der Stromerzeugung durch Offshore-Windenergie enorm angestiegen und wird auch in Zukunft noch weiter steigen. Aus diesem Grund liegt die Zielsetzung des Projektes OWiSS, nämlich die Identifikation bzw. Neuentwicklung von Maßnahmen zum Schutz und für die Sicherheit deutscher OWP nahe: natürliche, technische oder gesellschaftliche Risiken lassen eine hohe Verletzlichkeit solcher Offshore-Energieerzeugungsanlagen vermuten. OWiSS leistet bezogen auf die Offshore-Windenergie einen Beitrag zur Sicherung einer störungsfreien Energieversorgung von Bevölkerung und Wirtschaft.

# 2 Vorgehensweise

Im Mittelpunkt der Untersuchungen des ISL standen in der Anfangsphase des Projekts logistische und informationstechnische Prozesse während des Betriebs und in Bezug auf weitere Nutzungsmöglichkeiten von Offshore-Infrastrukturen. Im Konsortium wurden zunächst die verwundbarsten Komponenten eines Offshore-Windparks identifiziert – nämlich diejenigen Komponenten, bei deren Ausfall die Bevölkerung ebenfalls von länger anhaltenden Stromausfällen betroffen sein könnte. Auf Basis der identifizierten Komponenten (Umspann- und Konverterplattfomen sowie Export-Seekabel) wurden Überlegungen angestellt, in welcher Weise diese angreifbar sind. Eine akute Angriffsmöglichkeit bietet dabei u.a. die Informationstechnologie. Die Windparks und Plattformen werden per Fernwartungssystem überwacht, die Seekabel sind mit Datenübertragungsmedien ausgestattet, so dass ein Eindringen in das Netzwerk und die Stilllegung bzw. Zerstörung einer Komponente auf verschiedene Arten, auch aus der Ferne denkbar und machbar wären. Auch ein unberechtigtes Eindringen von Personen in Bereiche auf einer Plattform, durch z.B. Wartungs- und Reparaturdienste von Fremdfirmen, scheint möglich.

Im weiteren Verlauf des Projektes wurden die Ursachen für verschiedene Angriffsmöglichkeiten erforscht sowie bereits vorhandene Schutzmaßnahmen geprüft und ggf. Verbesserungsvorschläge bzw. neue Maßnahmen erarbeitet, um Offshore-Windparks vor Angriffen besser zu schützen. Die heute bereits in Betrieb genommenen Offshore-Windenergieparks (OWP) stehen in Sachen IT-Sicherheit auf unterschiedlichstem Niveau. Für die Umsetzung von IT-Sicherheit für OWP gibt es bisher nur wenige Standards. Auch unterliegen die OWP nicht dem seit Juli 2015 geltenden IT-Sicherheitsgesetz, in welchem Verfahren für eine verbesserte IT-Sicherheit definiert sind. Die Möglichkeit, dass durch einen Cyberangriff ganze Windparks oder sogar Cluster von Windparks betroffen sein könnten und dadurch die Energieversorgung von Bevölkerung und/oder Wirtschaft gestört würde, besteht.

Im fortschreitenden Projekt teilten sich die Untersuchungen des ISL bei der Betrachtung der zu ergreifenden und zu bewertenden Maßnahmen in zwei Richtungen auf: Zum einen wurden Möglichkeiten zur Erhöhung der IT-Sicherheit detailliert untersucht. Hier wurde deutlich, dass in Bezug auf Maßnahmen zur IT-Sicherheit eine Vielzahl von Akteuren – vom Anlagenbauer über die Systementwickler, den Übertragungsnetzbetreibern und Direktvermarktern bis hin zum Offshore Windenergiepark (OWP)-Betreiber selbst und deren Sicherheitsfachleuten – unterschiedliche Zuständigkeitsbereiche inne haben und verschiedene Zugriffsrechte auf

OWP und ihre Subsysteme besitzen. Dies erhöht den Bedarf für Maßnahmen zur IT-Sicherheit enorm.

Zusätzlich beschäftigte sich das ISL aber auch mit der Simulation der Auswirkung von Maßnahmen als Einflussfaktor für deren Bewertung. Das hierfür (weiter-)entwickelte Simulationsmodell bildet dabei den laufenden Betrieb eines oder mehrerer OWP ab und trägt zur Ermittlung von Daten für die ökonomische Bewertung präventiver Maßnahmen bei. Zur Simulation von Schadensszenarien aus dem energiewirtschaftlichen Bereich war die betriebswirtschaftliche Expertise des Projektpartners Deutsche Offshore Consult (DOC) die Grundlage für die Modellierung der Maßnahmen in dem Simulationsmodell, um damit Aussagen für vergleichende Bewertungen zu erhalten. Den durch die Simulation ermittelten Kosten (Logistikkosten und entgangene Einspeisevergütung) zur Wiederherstellung der Funktionalität eines OWP im Schadensfall wurden in der ökonomischen Bewertung u.a. die Kosten für eine Umsetzung der untersuchten Maßnahmen gegenübergestellt.

Abschließend wurden im Projekt Planspiele entwickelt, um eine Sensibilisierung für die Prävention in den Bereichen IT Sicherheit und der Energiewirtschaft zu fördern.

OWiSS hatte eine Laufzeit von drei Jahren. Das Teilvorhaben des ISL konnte im Dezember 2017 erfolgreich abgeschlossen werden.

# 3 Analyse von Gefährdungen und Bedrohungen

Die Analyse von Gefährdungen und Bedrohungen mit der Zusammenstellung in einem Gefährdungs- und Bedrohungskatalog bildete die Basis für weitere Untersuchungen. Dazu erfolgte eine Sammlung aller denkbaren Gefährdungen und Bedrohungen durch Recherchen und Befragungen von Fachleuten aus dem Bereich Offshore. Hieraus wurde schließlich nach einer Bewertung ein priorisierter Gefährdungs- und Bedrohungskatalog erstellt. Im Fokus standen dabei Gefährdungen und Bedrohungen, die zu einem Engpass der Stromversorgung in der Bevölkerung führen könnten.

Der Fokus des Instituts für Seeverkehrswirtschaft und Logistik (ISL) im Verbund lag auf möglichen Bedrohungsszenarien

- aus Sicht logistischer Prozesse beim Betrieb von OWPs (Versorgung, Wartung, Reparatur, Repowering), durch Transport von Personen und Material
- aus Sicht von „intelligenten“ Angriffen (z.B. Eingriffe in die Anlagentechnik, die Fernsteuerung oder Eingriffe in sonstige Informations- und Kommunikations-Technik)
- unter Berücksichtigung von weiteren Nutzungsmöglichkeiten von OWPs wie Marikultur (Fischzucht in Windparks) oder Touristik (Windparkausflüge)

sowie auf der Sammlung möglicher durch Sabotage, durch gezielte Angriffe entstehende Schäden und deren Priorisierung aus Sicht des Betreibers bezogen auf die Energieversorgung von Bevölkerung und Wirtschaft.

Ziel im weiteren Projektverlauf war die Entwicklung von neuen bzw. verbesserten Maßnahmenkonzepten zur Abwendung von Bedrohungen und damit zur Sicherstellung der Windparksicherheit unter Einbeziehung bereits vorhandener präventiver und reaktiver Maßnahmen zur Reduzierung möglicher Schwachstellen.

## 3.1 Einführung

### 3.1.1 Komponenten eines Offshore-Windenergieparks

Die einzelnen Windenergieanlagen eines Windparks werden – unabhängig von der Entfernung zur Küste – gebündelt an die zum Windpark gehörende Umspannplattform angeschlossen, die die Transformation des gesammelten Stroms auf ein höheres Spannungsni-

veau zur Minimierung von Verlusten übernimmt. Für den Stromtransport aus der Umspannplattform eines OWP zum Land werden dagegen unterschiedliche Technologien[7] – je nach Entfernung des OWP von der Küste – eingesetzt:

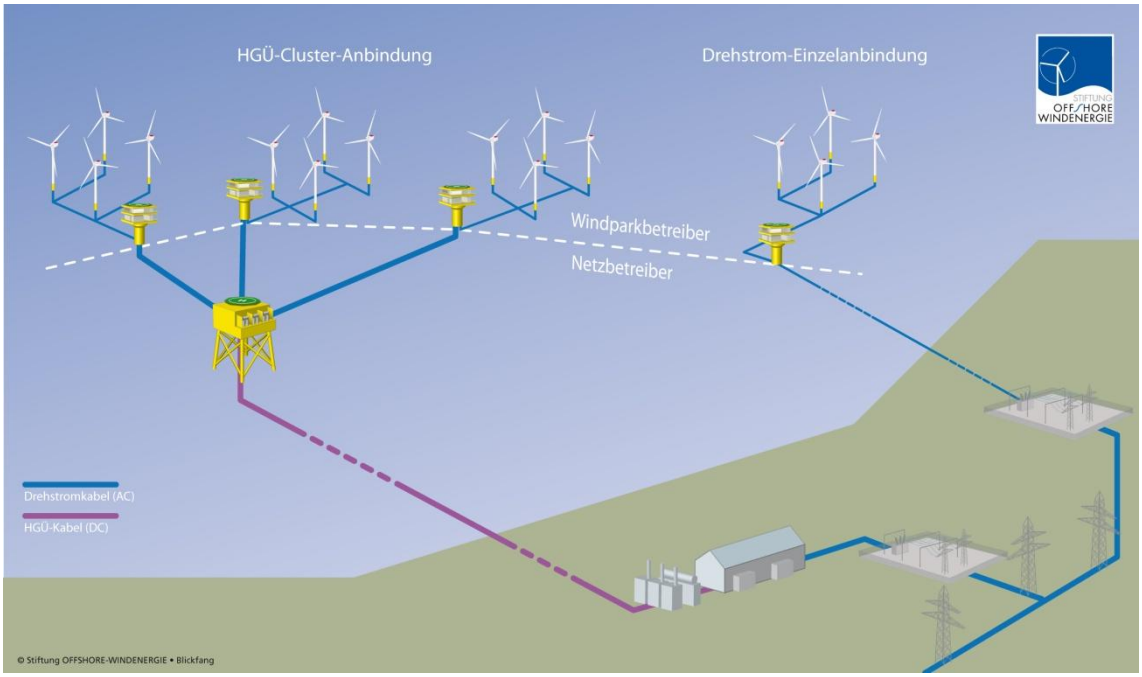



**Abbildung 3: Aufbau eines OWP**

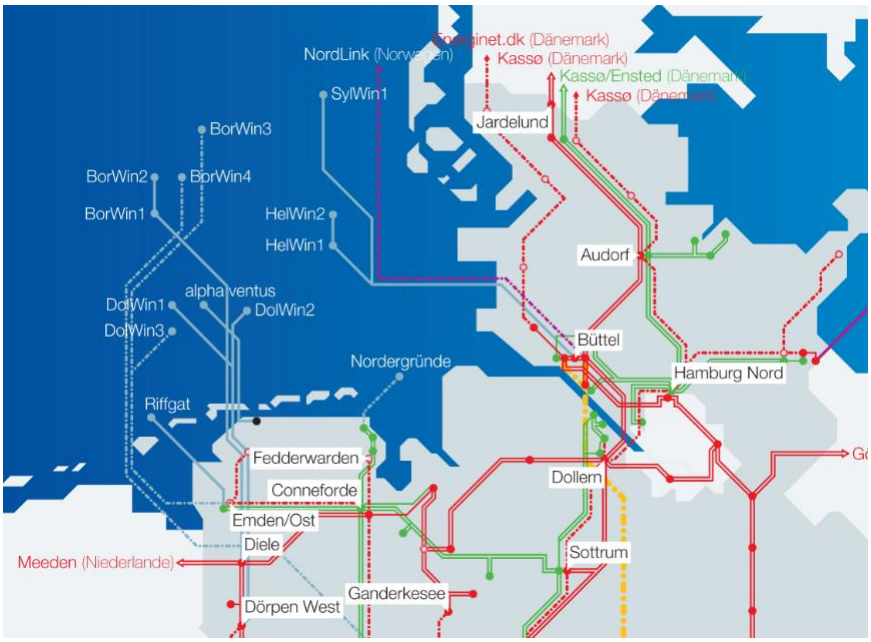
Möglich ist eine direkte Drehstromanbindung der Umspannplattform eines OWP mit dem Land (AC-Netzanbindungssystem), wie man sie hauptsächlich in der Ostsee sowie bei küstennah gelegenen OWP findet oder aber die Bündelung des Meeresstroms per AC-Anbindung zu einer ebenfalls im Meer gelegenen Konverterplattform, in der die Umwandlung des Drehstroms in Gleichstrom erfolgt. Von hier erreicht der gesammelte Strom die Landseite über ein DC-Netzanbindungssystem (HGÜ-Kabel: Hochspannungs-Gleichstrom-Übertragung), da durch diese Technologie zum einen höhere Leistungsmengen transportiert werden können, während gleichzeitig die Stromverluste geringer sind als bei der Übertragung über eine Drehstromanbindung. Diese Clusterbildung von OWP ist damit effizient und hat einen positiven Nebeneffekt: Es wird weniger in die Natur eingegriffen, da weniger Kabel mit Landanschluss in den Meeresboden eingelassen werden müssen.

7 Quelle: ABB Group; Dr.-Ing. Jutta Hanson: Netzintegration von Offshore-Windparks (https://www.vde.com/de/regionalorganisation/bezirksvereine/suedbayern/facharbeit%20regional/akenergietechnik/documents/netzintegration%20offshore%20windpark.pdf)

Der Strom erreicht per Seekabel den nächsten Netzknotenpunkt auf der Landseite, wo er bei der DC-Übertragung zunächst auf 220 kV transformiert und anschließend in das Stromnetz eingespeist wird.

### 3.1.2 Netzanbindung

Die Firma TenneT – und innerhalb der TenneT-Gruppe TenneT-Offshore – ist seit Dezember 2006 aufgrund gesetzlicher Grundlagen für die Netzanbindung der deutschen Offshore-Windparks in der Nordsee verantwortlich. Dazu gehören Konzeption, Planung, Bau und Betrieb von Anschlussleitungen auf See bis zum Netzanschlusspunkt an Land. Mit allen geplanten Infrastrukturprojekten verfügt TenneT insgesamt bis zum Jahr 2020 über eine Übertragungskapazität von acht Gigawatt Strom aus erneuerbarer Energie.




Quelle: TenneT (TenneT, 2018)

**Abbildung 4: Offshore-Netzanbindungen in der Nordsee**

Die Netzanbindung von Windparks in der Ostsee übernimmt die Firma 50Hertz, seit hier 2011 mit EnBW Baltic 1 der erste kommerzielle Windpark in der Ostsee in Betrieb gegangen ist.

### 3.1.3 Vorgehen

Zunächst wurden durch Recherchen, Gespräche und Brainstorming denkbare Bedrohungen und Gefährdungen für einen OWP identifiziert und strukturiert.

Schon 2012 forschte die Deutsche Windguard GmbH im Auftrag der Stiftung Offshore-Windenergie zum Thema Plausibilisierung des Ausfallrisikos von Offshore-Netzen in der deutschen Nordsee[8]. Ziel der Arbeit war die Bewertung des Risikos von durch Schäden verursachten Betriebsunterbrechungen in Offshore-Windparks und der daraus entstehenden Ertragsminderung. Die Deutsche Windguard bezieht sich in ihrer Untersuchung auf die Risikobereiche Onshore- und Offshore-HGÜ-Stationen (Konverterplattformen) und Kabel sowie kombinierte Risiken. Betrachtet wurden ausschließlich Schadensereignisse, die gravierende Ausfallzeiten zur Folge haben könnten.

Die im Rahmen des Projektes durchgeführten Recherchen des Verbundpartners IFAM[9] haben ergeben, dass es für eine allgemeine Gefährdungsanalyse nicht sinnvoll scheint, jedes einzelne Element zu untersuchen, sondern dass eine Betrachtung der leistungsstärksten Systemelemente ausreichend ist. Ein typischer Offshore-Windpark in der Nordsee besteht dabei aus 80 OWEA mit je 5MW installierter Leistung (= 400 MW für den OWP). Der Ausfall einzelner OWEA und sogar der Ausfall eines ganzen Windparks kann auch von anderen Energieträgern aufgefangen werden, indem z.B. Kraftwerke, die mit halber Leistung in Betrieb sind, „hochgefahren“ werden. Die Sicherstellung der Stromversorgung ist nicht gefährdet, da sich die Energieträger gegenseitig durch Redundanzen absichern (müssen). Beispielsweise werden fehlende Stromeinspeisungen der Offshore-Windenergie bei Windflauten, geplanten Abschaltungen von OWEA bei Wartungs- oder Reparaturarbeiten durch andere Stromerzeuger ausgeglichen.

Jedoch ist bekannt, dass plötzliche Totalausfälle kritischer Infrastrukturen zu starken Störungen der elektrischen Netze führen können, die durch entstehende Kettenreaktionen auch Auswirkungen auf die Bevölkerung haben könnten. Die Auswirkungen von Totalausfällen wurden wegen ihrer Bedeutung bereits mehrfach untersucht[10]. Genannt werden in Berichten dazu u.a. ernste Betriebsstörungen von Krankenhäusern, Altenheimen, Notrufzentralen, Verkehrseinrichtungen, Einsatzkräften (Feuerwehr, Polizei, etc.), Versorgung mit Trinkwasser, Treibstoffen, Lebensmitteln, Bargeld, Einschränkung der Kommunikation, Ausfall von Rechner- und IT-Strukturen und vieles mehr. Zu prüfen war also, ob auch ein plötzlicher Abfall in

8 Quelle: Deutsche Windguard GmbH:Plausibilisierung des Ausfallrisikos von Offshore-Netzen in der deutschen Nordsee

9 Quelle: Dr. Jürgen Gabriel, Dr. Karin Jahn; Fraunhofer IFAM; Teilvorhaben: Volkswirtschaftliche und gesellschaftliche Sicht auf die Versorgungssicherheit und Sicherheit der Bevölkerung, AP 110 Analyse möglicher Gefährdungen und Bedrohungen, Teil A, (Entwurf vom 12.05.2015)

10 Quelle: Bericht des BMBF aus 2011 „Innovationen für die zivile Sicherheit: Schutz von Versorgungsinfrastrukturen“: z.B. „Szenarienorientierte Grundlagen und innovative Methoden zur Reduzierung des Ausfallrisikos der Stromversorgung (GRASB)“ und „Intelligente Notstromversorgungskonzepte unter Einbeziehung Erneuerbarer Energien (Smart Emergency Supply System SES2)”

der Stromeinspeisung aus der Offshore-Windenergie, z.B. beim plötzlichen Ausfall eines leistungsstarken Elementes wie einer Konverterplattform und damit eines kompletten OWP-Clusters, eine ebensolche Kettenreaktion auslösen könnte.

Entsprechend der Ergebnisse des Teilprojekts des IFAM[11] sind die leistungsstärksten Elemente ein kompletter Windpark, Umspann- und Konverterplattformen (Offshore- und Onshoreanbindung), Gleichstrom- und Wechselstromkabelverbindungen sowie der Kabelkanal Norderney.

Besonders gefährdet sind auch die Kabelverbindungen zwischen Umspann- und Konverterplattform sowie zwischen Konverterplattform bzw. Umspannplattform und dem Landanschluss. Die Verkabelung innerhalb eines Windparks erfolgt z.B. im Windpark Riffgat redundant (Riffgat), damit im Schadensfall ein Anschluss an die Umspannplattform weiterhin gewährleistet ist. Einheitliche Regelungen gibt es hierfür jedoch nicht.

Ein plötzlicher Totalausfall einer oder mehrerer der o.g. leistungsstärksten Elemente könnte eine Auswirkung auf die Stromversorgung von Bevölkerung und Wirtschaft an Land haben. Aus diesem Grund konzentrierten sich die weiteren Untersuchungen auf diese leistungsstärksten Elemente.

## 3.2 Logistische Prozesse

Soll ein Windpark wirtschaftlich arbeiten, muss dieser möglichst störungsfrei im Betrieb sein. Ein Großteil von Störungen löst jedoch keinen plötzlichen Stromabfall aus, da in der Regel keines der o.g. kritischen, d.h. leistungsstarken Elemente in der Weise betroffen ist, dass es komplett ausfällt. Störungen der Logistik können jedoch erhebliche Kosten verursachen. Fehlende oder defekte Ersatzteile können die Wiederinbetriebnahme einer Anlage empfindlich verzögern. Fallen Anlagen längere Zeit aus, treten deshalb nicht nur Kosten für die Instandsetzung auf, vielmehr kann in dieser Phase kein Strom eingespeist werden, wodurch sich die Einnahmen aus dem betroffenen Windpark empfindlich verringern.

Um mögliche Schäden rechtzeitig zu entdecken und damit längere Ausfallzeiten zu vermeiden, sind regelmäßige Wartungen der Anlagen eines Windparks unvermeidlich. Diese verkürzen außerdem die Reaktionszeiten zur Instandsetzung von Anlagen bei rechtzeitig erkannten Schäden. Gerade für Offshore-Windparks haben Betreiber bereits umfassende Re-

[11] Quelle: Dr. Jürgen Gabriel, Dr. Karin Jahn; Fraunhofer IFAM; Teilvorhaben: Volkswirtschaftliche und gesellschaftliche Sicht auf die Versorgungssicherheit und Sicherheit der Bevölkerung, AP 110 Analyse möglicher Gefährdungen und Bedrohungen, Teil A, (Entwurf vom 12.05.2015)

paratur- und Wartungskonzepte[12] entwickelt, da die Anforderungen für die Sicherstellung eines störungsfreien Betriebs erheblich höher sind als für Windparks an Land.

**Sicherstellung eines störungsfreien Betriebs im Tagesgeschäft**

Um Ausfallzeiten zu minimieren, wird der Windpark mit Hilfe von Überwachungssystemen automatisch und ständig überwacht. Diese elektronischen sog. Condition Monitoring Systeme (CMS) übermitteln laufend physikalische Größen zur Sicherstellung des Betriebs. Bei bestimmten Störungen sind diese Systeme in der Lage, automatisch und selbsttätig zu reagieren, wie z.B. mit dem Abschalten von Anlagen bei zu hohen Windgeschwindigkeiten. Im Falle einer Störung, die vom CMS nicht automatisch behoben werden kann, bietet die Technologie der Fernwartung die Möglichkeit, von der Schaltzentrale an Land aus direkt auf die Steuerungssysteme des Windparks zuzugreifen. Führen diese Vorgehensweisen jedoch nicht zum Erfolg, muss ein Serviceteam vor Ort Störungen beheben. In diesem Fall kann es jedoch ein Problem geben: für einen Einsatz vor Ort müssen bestimmte Wetterbedingungen vorherrschen, damit Servicemaßnahmen überhaupt ausgeführt werden können. Ist der Wind zu stark, die Wellen zu hoch oder kommt dazu noch Nebel auf, wird die Arbeit an den Anlagen für das Serviceteam zu gefährlich und die Maßnahme muss auf ein Gut-Wetter-Fenster verschoben werden.

Fallen Störfälle jedoch in eine längere Schlecht-Wetter-Phase, so hat dies starke finanzielle Auswirkungen für den Betreiber, da sich die Ausfallzeit der Anlage(n) um die erforderliche Wartezeit auf besseres Wetter zum Teil erheblich verlängern kann.

Neben den o.g. Servicemaßnahmen ist eine regelmäßige Sichtungswartung durch das Bundesamt für Seeschifffahrt und Hydrographie (BSH) vorgeschrieben, da eine elektronische Überwachung des Windparks nicht alle Bereiche abdecken kann. Bereiche, wie die Überprüfung der mechanischen Unversehrtheit der Komponenten (z.B. Risse und Korrosion an Rotorblättern und Fundamenten, Kolkbildung), können nur durch Wartungsteams vor Ort sichergestellt werden. Besonders intensiv beansprucht sind die Fundamente und die Rotorblätter. Fundamente werden z.B. durch Tauchroboter auf etwaige Schäden überprüft. Für Wartungsmaßnahmen werden nicht nur sog. Serviceschiffe eingesetzt, auch Hubschrauber kommen vermehrt für den Transport des Serviceteams sowie des benötigten Materials zum Einsatz. Die vorgeschriebenen Sichtungswartungen müssen pro Jahr mindestens ein Viertel

[12] Quelle: OFFSHORE-WINDENERGIE.net: Überblick über die Wartungsarbeiten im Rahmen von Offshore-Windenergie-Projekten (http://www.offshore-windenergie.net/technik/wartung)

aller Anlagen eines Windparks umfassen, d.h. dass jede WEA alle vier Jahre einer Sichtungswartung unterzogen wird.

Eine Bedrohung bzw. Gefährdung von Offshore-Windparkanlagen könnte somit von einzelnen Personen- oder Personengruppen ausgehen, die Wartungs- und Reparaturprozesse vor Ort durchführen. Auch die IT-Anbindung der kritischen Elemente stellt eine Gefahr dar, die aber im Thema IT-Sicherheit detailliert behandelt wird.

## 3.3 IT Sicherheit

In den vergangenen Jahren ist die IT-Sicherheit gegen Cyber-Attacken immer mehr in den Fokus gerückt. Die zunehmende Vernetzung hin zu Industrie 4.0 eröffnet für Unternehmen die kostengünstige Überwachung, Integration und Beschleunigung von Wertschöpfungsprozessen. Sie bietet aber auch Angreifern eine preiswerte und weitestgehend gefahrlose Möglichkeit, kritische Infrastrukturen (KRITIS) zum Stillstand zu bringen.

Generell haben die in der Vergangenheit durchgeführten IT-Angriffe (Stuxnet und Abkömmlinge wie Havex-Trojaner (Gruppe: "Dragonfly", Kampagne: "Energetic Bear" bzw. "Crouching Yeti")) gezeigt, dass diese langfristig und sehr viel subtiler vorbereitet und durchgeführt werden, schwieriger zu analysieren sind und teils über mehrere Jahre unentdeckt bleiben können. Dies ist komplett unabhängig von noch nicht entdeckten Sicherheitslücken, von deren Bestehen man grundsätzlich in jeder Software zunächst ausgehen muss.

Zukünftig sollte davon ausgegangen werden, dass Angriffe durchgeführt werden, die primär nicht das eigentliche Angriffsziel betreffen, sondern vorab sekundäre Ziele kompromittieren, um das eigentliche primäre Ziel zu erreichen. Beispiel: Angriff auf das Quellsoftwareportfolio eines Anlagenherstellers, um Lücken in der Gerätesoftware (Firmware) zu installieren, deren Anlagenbauteile später in den Industrieanlagen verbaut werden, beschreibt diese Methode[13]. Hierdurch wäre ein Angriff von innen heraus durchführbar.

Die deutsche Regierung, das Bundesministerium für Bildung und Forschung (BMBF), das Bundesministerium des Innern (BMI) und auch die Europäische Union (im Programm Horizon 2020) haben daraufhin eine Vielzahl an Forschungsprojekten initiiert, die sich mit der IT- und Cyber-Sicherheit und dem Schutz kritischer Infrastrukturen (KRITIS) beschäftigen.

[13] Quelle: Bundesamt für Sicherheit in der Informationstechnik BSI: Die Lage der IT-Sicherheit in Deutschland 2014

Das ISL betrachtete im OWiSS-Projekt u.a. die IT-Sicherheit in Offshore-Windparks (OWP) und arbeitete u.a. Besonderheiten heraus, die nur die Offshore-Windenergiebranche betreffen.

### 3.3.1 Besondere Bedrohungen und Angriffsmöglichkeiten auf IT-Systeme

Offshore-Windenergieanlagen (OWEA) und -Windparks (OWP) befinden sich fast ausschließlich außerhalb der 12-Seemeilen-Zone (SMZ) in der Ausschließlichen Wirtschaftszone (AWZ), auch 200-Meilen-Zone (370 km) genannt. Sie sind nur zu Wasser und aus der Luft zu erreichen. Die elektrische und netzwerktechnische Anbindung erfolgt über Unterseekabel mit integrierten Glasfaserleitungen (GF-Bündel). Zusätzliche Netzwerkredundanz erfolgt direkt über ein- oder zweifache Satellitenanbindung[14]. Glasfaserleitungen sind abhörsicher, weil sie weder selbst abstrahlen noch durch Strahlung beeinflusst werden können, solange es nicht gelingt, einen Glasfaserpatch an der GF-Leitung zu befestigen oder in das gesamte Seekabel einen Verteiler einzufügen. Weitere Anbindungen erfolgen über Richtfunk.

Satellitenverbindungen (oft Kooperation SES (Société Européenne des Satellites (SES S.A.), Satellit ASTRA 3B, Orbitalposition 23,5° Ost) haben eine hohe Netzwerkverzögerung (mind. 0,5 bis zu 1 Sekunde oder mehr), weil die gesendeten Daten zum und vom geostationären Satelliten über eine lange Distanz (~2x36.000 km) übertragen werden müssen. Digitale Übertragung (Kompression, Verschlüsselung, Kodierungen) vergrößert die Verzögerungszeiten zusätzlich. Satellitenverbindungen sind für die Echtzeitverarbeitung von Daten nicht geeignet. Sie haben eine beschränkte Bandbreite und einen eingeschränkten Datendurchsatz (9,6 KBit/s bis hin zu 155 MBit/s). Der Endkommunikationspunkt Satellit befindet sich unter Kontrolle des Satellitenbetreibers und gehört evtl. einer ausländischen Firma. Die Satellitenkommunikation ist grundsätzlich Ende-zu-Ende verschlüsselt. Inwieweit der Satellitenbetreiber trotzdem Zugriff auf unverschlüsselte Kommunikation hat, ist nicht bekannt. Der andere Endpunkt der Satellitenkommunikation befindet sich als Satellitenantenne auf einer der Plattformen. Die Antenne ist gegen mechanische Zerstörung ggf. unzureichend geschützt und kann somit leicht unterbrochen werden. Satellitenkommunikation kann leicht durch aktive Sender oder schlechte Wetterverhältnisse gestört werden.

In der Nord- und Ostsee werden Unterseekabel bei der Verlegung mindestens 1,5 Meter tief eingespült oder eingefräst, um sie vor mechanischen Beschädigungen durch Anker,

[14] Quelle: Weser Kurier (2015): Maren Beneke: Gut verbunden

Schleppnetze oder anderen Einwirkungen zu schützen. Alle Seekabel sind spannungsführend. Der mechanische Zugang, um das Seekabel zu kompromittieren, ist stark eingeschränkt, jedoch mit entsprechendem Aufwand und Kosten nicht unmöglich. Die Endpunkte, d.h. der Landanschluss oder der Anschluss an die Plattformen sind möglicherweise leichter zugänglich. Inwieweit Personen Zugang zum Netzwerk über nicht verschlossene Anlagenteile einer einzelnen Windkraftanlage bzw. von Plattformen erlangen können, muss geprüft werden.

Auf der Hochseeinsel Helgoland wurde im Jahr 2000 von der Deutschen Telekom ein 113 Meter hoher Funkturm errichtet. Das Turmfundament selbst befindet sich 43 Meter über NN, so dass sich die Gesamthöhe auf etwa 150 Meter über NN summiert. Neben Radio- und Fernsehprogrammen wird der Turm zur Richtfunkanbindung der Windparks Amrumbank West, Meerwind Süd/Ost und Nordsee Ost verwendet. Mit der Einrichtung der Richtfunkverbindungen ist die Bremen Briteline GmbH betraut. Der Turm ist nicht öffentlich zugänglich. Vier Parabolantennen auf dem Turm und in den OWP stellen durch sogenannte Punkt-zu-Punkt-Verbindungen (P2P) in direkter Sichtlinie (Richtfunkstrahl) die zusätzliche Netzwerkanbindung zu den etwa 20 Kilometer entfernten, auf hoher See befindlichen OWP her. Auf Helgoland befindet sich außerdem eine OWP-Betriebsbasis. Sie dient den großen Energiebetreibern zur Steuerung, Regelung und Überwachung der OWP. Die OWP-Betriebsbasis ist ebenfalls per Richtfunk an das Netzwerk angebunden. Die Netzwerkanbindung auf Helgoland kann von Bremen Briteline Mitarbeitern von Bremen aus überwacht werden.

Richtfunk benötigt direkte Sichtverbindung zwischen den beteiligten Systemen, d.h. Sende- und Empfangsantennen müssen in Sichtlinie zueinander ausgerichtet werden. Die Qualität der Netzanbindung ist von den Witterungsverhältnissen - insbesondere der Regendämpfung – abhängig. Die überbrückbare Entfernung der Richtfunkstrecke richtet sich aufgrund der Erdkrümmung nach der Installationshöhe der beteiligten Antennen.

Bemannte Plattformen sind für das Personal mit Netzwerken und Zugang zum Internet ausgestattet. Hieraus lässt sich eine weitere Möglichkeit einer Gefährdung bzw. Bedrohung ableiten.

Industrieanlagen sind empfindlich, wenn das Übertragungsmedium überlastet oder gestört wird. Auf dem 14. IT-Sicherheitskongress des BSI wurde in zwei Vorträgen darauf hingewiesen. Heiko Rudolph von der Firma admeritia GmbH schreibt dazu „Ein [Netzwerk-]Test [im ICS-Umfeld, Anm. d. Verfassers] sollte vorwiegend manuell durchgeführt werden, da schon ein automatisierter Portscan [mittels "Nessus" o.ä. Tools, Anmerk. d. Verfassers] zu erhebli-

chen Beeinträchtigungen oder im Extremfall zum Abschalten eines Systems führen kann“[15]. Erwin Kruschitz von der Firma anapur AG fragte: „Kann die 'Safety' durch Security-Zwischenfälle beeinflusst werden?". Antwort: "Safety kann durch Security-Ereignisse beeinflusst werden. Die nicht gefahrbringende Auslösung des Safety Systems ist denkbar (spurious trip). Dieser Fall kann ohne tiefes Wissen über die Funktion herbeigeführt werden. Für die Herbeiführung eines gefahrbringenden Fehlers oder die Unterdrückung einer Sicherheitsabschaltung ist Information über die Sicherheitsfunktion notwendig. Die Wahrscheinlichkeit ist geringer, der mögliche Schaden jedoch sehr hoch. Der mögliche Angriffsvektor führt über das Engineering System.“[16]. Er verwies außerdem auf den Stromausfall[17] am 02. Mai 2013 in Österreich, bei dem sich ein Steuerungsbefehl eines süddeutschen Erdgasnetzbetreibers für eine Zählerabfrage in das europäische Stromnetz verirrt hatte. Der Erdgasnetzbetreiber stellte diese Abfrage zum Test an alle Komponenten eines neu hinzugefügten Segmentes des regionalen Gasleitungsnetzes in Bayern. Weil Gasnetz und Stromnetz dieselben Steuerungsprotokolle verstanden und mindestens ein Netzübergang des Steuerungsnetzes die Nachricht "An Alle!" (Rundspruchnachricht, sog. "Broadcast") nicht unterband, pflanzte sich die Anfrage ungehindert fort und sorgte dafür, dass der Datenverkehr in diesem Fernwirknetz zu eskalieren begann und "Kreisläufer" in weiteren angeschlossenen Netzen generierte. Diese Nachricht forderte alle beteiligten Geräte auf, zu antworten, was diese auch taten. Informations- und Fernwirknetz wurde durch einen "Paket-Sturm" sich selbst multiplizierender Nachrichten lahm gelegt. Die Netze mussten per Hand aufgetrennt werden, um die "Kreisläufer" zu unterbinden und das Stromnetz wieder kontrollier- und steuerbar zu machen.

Für die Betrachtung der IT-Gefährdungen und -Bedrohungen hinsichtlich Security der kritischen Infrastruktur Offshore-Windenergie spielen Aufwand, Auswirkung und die Gefahr der Entdeckung die entscheidenden Rollen. Kosten und Leichtigkeit eines nicht zu entdeckenden Angriffs schließen bestimmte Angriffe auf einzelne oder mehrere Windkraftanlagen aus. Für einen relevanten Angriff, der tatsächlich eine "Blackout"-Bedrohung darstellt, müssen zentrale Komponenten angegriffen werden, die tatsächlich die Funktionsfähigkeit des gesamten Windparks beeinträchtigen könnten. Hier rücken daher die zentralen Elemente wie Konver-

15 Quelle: admeritia GmbH (2015), Heiko Rudolph: Sicherheitstests von ICS-Anlagen

16 Quelle: anapur AG (2015), Erwin Kruschitz: Security für Safety Systeme. Ein Einblick in die risikobehafteten Zonen der Industrial-Control Systeme

17 Quelle: http://fm4.orf.at/stories/1717900/, am 2. Juni 2015

ter- und Umspannplattformen, Seekabel, Funktürme (Richtfunkstrecken Helgoland) und das ICS in den Blickpunkt.

Ein Angriff auf das Seekabel, um z.B. über die Glasfaserbündel Netzwerkzugriff, Abhörmöglichkeit und bei Bedarf Kontrolle über einen oder mehrere Windparks zu erlangen, wäre nicht ohne Unterbrechung der Stromversorgung oder des laufenden Netzwerkverkehres möglich. Abgesehen davon, ist das Anpatchen (Splicing (Spleiß), Bending (Mikro-Knick mit Clip-On-Koppler) oder berührungsloses Einbringen von Licht und Analyse der Wechselwirkung) an eine Glasfaser nur mit viel Know-How und technischem Equipment zu bewerkstelligen. Unmöglich ist ein solcher Angriff nicht, jedoch bedeutet ein solcher Eingriff in bis zu 50 Metern Wassertiefe an einem stromführenden Seekabel, das pro Meter ca. 50 Kilogramm wiegt, stark ummantelt und zudem noch eingegraben ist, extrem hohen Aufwand mit hohem Risiko einer Entdeckung, der nur von einem Taucher oder U-Boot aus durchgeführt werden könnte.

Grundlage für die weitere Betrachtung waren die vom BSI herausgegebene Empfehlung "Industrial Control System Security - Top 10 Bedrohungen"[18], der Bericht "Die Lage der IT-Sicherheit in Deutschland 2014"[19], das BSI "ICS-Security-Kompendium"[20] und das BSI "ICS-Security-Kompendium - Testempfehlungen und Anforderungen für Hersteller von Komponenten"[21].

18 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktuelles/Analysen/csnews_20120413_IC-Systeme.html, am 5. Juni 2015

19 https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html, am 5. Juni 2015

20 https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Empfehlungen_node.html, am 5. Juni 2015

21 https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Empfehlungen_node.html, am 5. Juni 2015

| Nr. (Nr. alt) | Top 10 2014 | Top 10 2012 |
|---|---|---|
| 1 (2)(3) | Infektion mit Schadsoftware über Internet und Intranet | Unberechtigte Nutzung von Fernwartungszugängen |
| 2 (6) | Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware | Online-Angriffe über Office- / Enterprise-Netze |
| 3 (-) | Social Engineering† | Angriffe auf eingesetzte Standardkomponenten im ICS-Netz |
| 4 (5) | Menschliches Fehlverhalten und Sabotage | (D)DoS Angriffe |
| 5 (1) | Einbruch über Fernwartungszugänge | Menschliches Fehlverhalten und Sabotage |
| 6 (-) | Internet-verbundene Steuerungskomponenten† | Einschleusen von Schadcode über Wechseldatenträger und externe Hardware |
| 7 (10) | Technisches Fehlverhalten und höhere Gewalt | Lesen und Schreiben von Nachrichten im ICS-Netz‡ |
| 8 (-) | Kompromittierung von Smartphones im Produktionsumfeld† | Unberechtigter Zugriff auf Ressourcen‡ |
| 9 (-) | Kompromittierung von Extranet und Cloud-Komponenten† | Angriffe auf Netzwerkkomponenten‡ |
| 10 (4) | (D)DoS Angriffe | Technisches Fehlverhalten und höhere Gewalt |

Legende: †NEU – ‡ENTFALLEN (weil Folgeangriff)

**Abbildung 5: Top 10 der Bedrohungen für Industrial Control Systems**[22]

Grundtenor zur allgemeinen Sicherheit von Industrieanlagen:

- IT-Sicherheit ist zurzeit eher zweitrangig, die Anlage muss laufen, produzieren, bei fast allen Betreibern ist die Handhabung der Sicherheit sehr lax
- generell fehlen Sicherheitsfunktionen in den Anlagen
- es besteht ein Zielkonflikt: Kosten der Sicherheit steht gegen Funktionalität
- Industrieanlagen sind nicht gegen physikalische Angriffe der Übertragungsmedien schützbar (siehe auch Thema Portscan)
- generell zu wenig oder zu flaches IT-Wissen vorhanden
- fragile Produktionslandschaft.

## 3.4 Weitere Nutzungsmöglichkeiten

Nicht nur durch vorsätzliche Angriffe, Naturgewalten und Unfälle sind Bedrohungen und Gefährdungen für einen Windpark denkbar. Auch Offshore-Windenergie ferne Nutzungsmöglichkeiten könnten eine Gefahr für die Sicherheit eines Windparks bedeuten. Zum Schutz eines Windparks gibt das Sicherheitsrahmenkonzept des BMVI vor, einen Windpark durch die Einrichtung einer Sicherheitszone besonders zu schützen. Dieser gedachte Schutzring darf grundsätzlich nicht bzw. nur in Ausnahmefällen befahren werden. Ein Bei-

[22] Quelle: Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland, www.bsi.bund.de

spiel für eine Ausnahme zum Überfahren des Schutzrings ist der von Helgoland ausgehende Windparktourismus, für den auch aktiv geworben wird. Hierbei bekommen Touristen die Möglichkeit, in organisierten Touren per Schiff direkt bis zu einem Windpark zu fahren. Gefahren, die durch den Windparktourismus auftreten könnten, betreffen allerdings lediglich den Windpark Meerwind Süd|Ost. Auch für weitere geplante Windparks wird vermutet, dass diese für einen Besuch von Touristen eher unattraktiv sein werden, da der Aufwand hierfür mit der Entfernung zum Land steigt. Der Informationsbedarf der Touristen wird somit eher durch Offshore-Informationszentren, Wanderausstellungen, Aussichtsplattformen oder Landausflüge, wie die „Tour de Wind“ in Bremerhaven, gedeckt. Ausgewiesene Gebiete für Taucher und Segler nahe der Offshore-Windparks seien aber ebenfalls laut Stiftung Offshore Windenergie denkbar, jedoch noch nicht in Planung.

Viel geforscht wird außerdem im Bereich Marikultur – der Aquakultur im offenen Meer. Dieser sagt man gerade in Deutschland eine Zukunft als Wirtschaftszweig voraus. Heute gibt es zwar noch keine Anlagen mit großem Abstand zur Küste (nämlich in der AWZ), eine Co-Nutzung von Offshore-Windparks wird jedoch von Windparkbetreibern und Züchtern im Bereich Marikultur als denkbar und wünschenswert angesehen, denn Offshore-Windenergieanlagen bieten optimale Verankerungsmöglichkeiten für die Marikultur-Technik in ihren Fundamenten. Doch bis dahin ist noch ein langer Weg, bei dem zunächst eine Vielzahl räumlicher und organisatorischer Hindernisse zu überwinden sind. Denn Bedenken gibt es auf beiden Seiten: Zum einen trägt die Offshore-Branche Sorge, dass die Fundamente durch die zusätzliche Nutzung beschädigt werden können, was Auswirkungen auf die Funktionalität des Windparks haben würde. Die Muschelzüchter geben zu bedenken, dass deren technische Installationen schon durch die vorgeschriebenen Wartungsarbeiten mit Spezialschiffen in Mitleidenschaft gezogen werden könnten. Auch trotz der beschriebenen Argumente gegen eine Bedrohung der Funktionalität eines Windparks können Gefahren durch betriebsferne Nutzung nie ganz ausgeschlossen werden – eine Bedrohung bzw. Gefährdung von Offshore-Windparkanlagen kann immer auch von einzelnen Personen oder Personengruppen ausgehen, die touristische Angebote zu Offshore-Windparks nutzen oder aber in Marikulturprojekte involviert sind. Der Aufwand dafür, einen Schaden an einer Offshore-Infrastruktur willentlich herbeizuführen, der einen plötzlichen Stromabfall zur Folge haben kann, wird jedoch als außergewöhnlich hoch eingeschätzt.

Das Thema Wasserstoffspeicherung ist lange bekannt und gilt als gründlich erforscht –bei der Handhabung von Wasserstoff sind Sicherheitsauflagen zu beachten. Nach einem Gut-

achten[23] des Fraunhofer IWES liegt der Wirkungsgrad bei der Umwandlung Strom – Wasserstoff – Strom bei 34% bis 44%. Sollte Wasserstoff nicht wieder als Strom in das Versorgungsnetz eingespeist werden, könnte ein höherer Wirkungsgrad erzielt werden, weitere Investitionen und Konzepte wären aber erforderlich. Ob Wasserstoff jemals als Energiespeicher in Offshore-Windparks zum Einsatz kommt, ist derzeit noch nicht abzusehen. Sollten aber in Zukunft Offshore-Windparks mit Wasserstoffspeichern geplant werden, so ist dieser als neues Element eines Offshore-Windpark zu betrachten und nicht als weitere Nutzungsmöglichkeit. Im Rahmen von OWiSS wurde das Thema Wasserstoff als Energiespeicher deshalb vom ISL nicht weiter verfolgt.

[23] Quelle: Dr.-Ing. Michael Sterner, M.Sc. Mareike Jentsch, Dipl.-Ing. Uwe Holzhammer (Februar 2011), Energiewirtschaftliche und ökologische Bewertung eines Windgas-Angebotes, Fraunhofer Institut für Windenergie und Energiesystemtechnik (IWES), Kassel, http://www.greenpeace-energy.de/fileadmin/docs/sonstiges/Greenpeace_Energy_Gutachten_Windgas_Fraunhofer_Sterner.pdf

# 4 Ursachen und Maßnahmen

Nicht nur Naturgewalten und Unfälle gefährden OWP, vorsätzliche Angriffe auf einen Windpark sind ebenfalls denkbar.

Zum Schutz eines Windparks gibt das Sicherheitsrahmenkonzept des BMVI vor, einen Windpark durch die Einrichtung einer Sicherheitszone besonders zu schützen. Dieser gedachte Schutzring darf grundsätzlich nicht bzw. nur in Ausnahmefällen befahren werden. Diese 500 Meter Sicherheitszone gilt für alle Fahrzeuge (Ausnahme Behördenfahrzeuge); erlaubt ist das Befahren allerdings bei guter Sicht auch für solche Schiffe ohne besondere Genehmigung, deren Länge kürzer ist als 12 Meter. Eine Seeraumüberwachung ist für alle Betreiber verbindlich. Dieses verlangt das BSH schon vor Genehmigung eines Windparks. Die Überwachung erfolgt per AIS-Kennung. Nicht genehmigten Schiffsverkehr meldet der Betreiber an das Wasser- und Schifffahrtsamt (WSA), welches dann weitere Maßnahmen in die Wege leitet. Die Seeraumüberwachung wurde hauptsächlich vor dem Hintergrund der Gewährleistung der Sicherheit und Leichtigkeit des Schiffsverkehrs verpflichtend, jedoch nicht in erster Linie zur Abwehr von mutwilligen Angriffen. Eine zusätzliche Erkennung per Radar war zwar geplant, ist aber aufgrund einer AIS-Studie nicht weiter verpflichtend, da auch per Radar nicht alles erkennbar ist. Natürlich gibt es aber genehmigte Schiffsbewegungen innerhalb des Windparks durch auftretende Wartungs- und Reparaturmaßnahmen oder aber durch touristische oder Marikulturprojekte. Eine Bedrohung bzw. Gefährdung von Offshore-Windparkanlagen kann immer von einzelnen Personen- oder Personengruppen ausgehen, die zur Wartungsmannschaft oder zum Reparaturteam gehören, die touristische Angebote zu Offshore-Windparks nutzen oder aber in Marikulturprojekte involviert sind. Aus diesem Grund wird z.B. für Mitarbeiter, die Tätigkeiten im Windpark erledigen, ein „People Tracking“ durchgeführt, d.h. vor der Durchführung einer Aufgabe wird geprüft, ob eine Erlaubnis dafür vorliegt (work permit). In der Regel ist nie ein einzelner Mitarbeiter mit einer Aufgabe betraut, sondern immer mehrere Mitarbeiter gemeinsam. Beim Einsatz betriebsfremder Techniker wird die Anwesenheit eines Mitarbeiters des Betreibers angestrebt, ist aber nicht immer möglich. Der Einsatz von z.B. USB-Speichermedien ist im Windpark nicht erlaubt, um unbefugtes Einschleusen von Schadsoftware zu vermeiden. Hier sollte sogar die Möglichkeit der Verwendung von allen externen Datenträgern unterbunden werden. Tagsüber wird der OWP rundum mit Kameras überwacht, um auf unbefugtes Eindringen oder außergewöhnliche Vorkommnisse schnell reagieren zu können. Da unbefugte Personen auf

Anlagen aber nicht zu erkennen sind, werden Kameras oftmals nur im Brandfall aktiviert oder sind nur auf z.B. einen Transformator gerichtet. Nachts ist die Sicht nicht ausreichend, sodass fast nichts erkannt werden kann. Ein unbefugtes Eindringen wird erst dann bekannt, wenn über die installierten Sensoren in den Türen ein Fehler gemeldet wird, denn nach der Norm DIN VDE haben die OWEA als elektrische Betriebsstätten verschlossen zu sein. Gleiches gilt für die Container auf Umspannplattformen. Der Aufwand dafür, einen Schaden an einer Offshore-Infrastruktur willentlich herbeizuführen, der einen plötzlichen Stromabfall zur Folge haben kann, wird aus Gründen der bereits installierten Schutzmaßnahmen sowie der großen Entfernung zum Land als außergewöhnlich hoch eingeschätzt. Eher ist ein IT-fremder Angriff auf eine der Umspann- oder Konverterstationen an Land denkbar. Für den Luftverkehr über einem OWP gibt es allerdings keine Beschränkungen, da die Windenergieanlagen nicht als Industrieanlagen gelten. Über die Luft in einen Offshore-Windpark einzudringen, ist aber nicht ohne außergewöhnlich hohen Aufwand umzusetzen.

Für den Bereich Safety gibt es schon eine Vielzahl gesetzlicher Vorgaben, die zwingend eingehalten werden müssen. Zu den Sicherheitskonzepten, die Betreiber für die Genehmigung ihres Windparks zu erarbeiten haben, gehört u.a. die Definition von Meldeketten, in die die DGzRS (ONRT Offshore Notfallreaktionsteam), das Lagezentrum des Havariekommandos und die Feuerwehr eingebunden sind. Die DGzRS ist dabei nach eigener Aussage zuständig für Rettungen aus Seenot. In der, den Vorträgen beim OWiSS-Treffen mit den assoziierten Partnern nachfolgenden, Diskussion rückte mehr und mehr der Bereich Safety in den Fokus. Hieran erkennt man, dass Safety für Personen und Unternehmen greifbarer ist als der Bereich Security. Am Beispiel „Brand“ kann erklärt werden, dass, unabhängig von der Entstehung des Brandes, mutwillig in einem Security-Fall oder z.B. durch einen Safety-Unfall, Menschenleben im Vordergrund stehen und in beiden Fällen eine Safety-Reaktion, mit den Prioritäten Personen zu schützen, Brand zu bekämpfen, Umweltschäden gering zu halten, ausgelöst wird.

Im Bereich IT – und hier speziell im Security-Bereich möglicher mutwilliger Angriffe – ist man mit der Ausarbeitung von (gesetzlichen) Vorgaben noch längst nicht so weit. Es gibt zwar das IT-Sicherheitsgesetz, jedoch fallen Offshore-Windparks heute noch nicht unter das Gesetz. Es gibt zahlreiche Vorgaben, die z.B. darstellen, wie der Datentransfer und die Netzwerktechnik geschützt werden können. Die ausgearbeiteten möglichen Schutzmaßnahmen gelten im Wesentlichen für die IT-Sicherheit im Allgemeinen. Hier ist ebenfalls zu prüfen, ob eine Anpassung der Anforderungen auf den Sonderfall „Offshore“ erforderlich ist. Zwar

schützt heute jeder seinen Windpark noch nach seinen eigenen Vorstellungen, es ist aber bereits zu erkennen, dass das Bewusstsein für die Gefahr, die von IT-Angriffen ausgehen kann, nicht länger unterschätzt wird. Keiner lässt schon heute unbegrenzten und ungeschützten Zugriff auf seine Netzwerke zu. Die bereits in Betrieb genommenen OWP stehen in Sachen IT-Sicherheit aber auf unterschiedlichstem Level: Sind die einen bereits nach BSI zertifiziert, warten andere mit einer Zertifizierung, bis es einen konkreten Anlass, etwa ein Gesetz oder eine politische Vorgabe gibt. Bei Versicherern stehen die Safety-Thematiken im Vordergrund, Versicherungen zu Cyberrisiken befinden sich in der Anfangsphase.

IT-Sicherheit ist ein sensibles Feld – dies wurde in den letzten Jahren bereits erkannt und vieles wurde bereits getan, erkennbar an eingerichteten Organisationen auf nationaler und europäischer Ebene, geschaffenen Standards und Normen sowie Richtlinien und insbesondere dem IT Sicherheitsgesetz. Aber dieses Feld ist vielfältig und breit – wie auch die Angriffsmöglichkeiten auf Netzwerke und den Datentransfer. Diese gilt es nun so gut wie nur möglich abzusichern und gerade bei kritischen Infrastrukturen einen gewissen Mindestschutz auch verbindlich festzulegen.

Um Aufschluss über das „Soll“ eines effektiven OWP-Schutzes zu erhalten, wurde eine Internet- und Literaturrecherche durchgeführt. Die Recherche bot eine umfangreiche Anzahl von Informationen, die es zu sichten, zu analysieren und zu sortieren galt. Dies war eine z.T. sehr komplexe Aufgabe, da ein Großteil der untersuchten Websites und Dokumente wiederum viele Verweise auf weitere Informationen beinhaltet. Zudem sind viele Konzepte allgemein auf IT-Sicherheit anwendbar und sind nicht speziell für die IT-Sicherheit von Offshore Windpark konzipiert. Die anschließende Befragung von Unternehmen stellte sich aber noch als weitaus mühsamer dar. Die Gespräche mit den Unternehmen kamen oftmals nur schleppend zustande. Dazu noch unterliegen betriebsinterne Konzepte zur OWP-Sicherheit der Geheimhaltungspflicht – nichts darf nach außen dringen, da ansonsten auch mutwillige Angreifer Informationen erhalten könnten. Schon zur Genehmigung eines OWP sind bereits Sicherheitskonzepte zu entwickeln; diese jedoch betreffen in erster Linie Safety-Aspekte. Eine weitere Herausforderung für eine aussagekräftige Informationssammlung bestand darin, dass Aussagen aus Gesprächen aus einer der ausgewählten Branchen sich nicht auf Vorgehensweisen in anderen Unternehmen derselben Branche übertragen lassen, da es sich in der Offshore-Windenergie um eine noch sehr junge Branche handelt, in der weder während der Errichtung noch beim Betrieb standardisierte Prozesse vorherrschen. Die Konkurrenz zwischen den Betreibern ist groß und jeder entwickelt eigene Konzepte und Maß-

nahmenpakete. Unterschiede ergeben sich z.B. aus der Entfernung der Windparks zur Küste, aus der Topologie der Vernetzung der OWEA im Windpark oder Wartungskonzepten.

In der Gefährdungs- und Bedrohungsanalyse wurden mögliche Bedrohungen und Gefährdungen u. a. aus dem IT-Sicherheitsbereich herausgearbeitet, die im weiteren Projektverlauf zu eruieren waren. Hierzu wurde das Gespräch mit verantwortlich Handelnden gesucht. Für Expertengespräche wurden Unternehmen aus den Branchen OWP-Betreiber, Netzanbindungs-Dienstleister, Netzbetreiber, Anlagen-/Bauteile-Hersteller für Offshore-Windparks, Sicherheitsdienstleister sowie Projektentwickler kontaktiert. Für die Interviews wurden Fragenkataloge vorbereitet, die sich im Laufe weiterer Gespräche weiterentwickelt haben.

Von besonderer Bedeutung war es, die Einschätzungen, Ansichten und Erfahrungen von Praktikern zu erhalten, die täglich mit dem Betrieb von WEA, OWP, dem Führen der Leitwarten, dem Einsatz von Material, Schiffen, Personal und der Stromproduktion zu tun haben. In den geführten Interviews wurden die möglichen IT-Bedrohungen und Gefährdungen angesprochen. Hierbei konnten umfassende Erkenntnisse und Einsichten gesammelt werden; nicht nur, ob und inwieweit die theoretisch erarbeiteten Bedrohungen und Gefährdungen überhaupt praxisrelevant sind, sondern auch neue Aspekte, die bisher eher nebensächlich oder gar nicht im Fokus der IT-Sicherheitsbetrachtungen standen.

Es zeigte sich aber, je mehr Interviews abgeschlossen wurden und Vergleichsmöglichkeiten bestanden, leichte Unstimmigkeiten oder Ambivalenzen in den gemachten Aussagen bestanden, die evtl. doch auf noch bestehende Sicherheitslücken schließen lassen. Ein erstes Fazit hieraus lautet: kein Windparkbetrieb gleicht dem anderen.

Die wesentlich genaueren und besseren Informationen wurden nun dazu genutzt, die bisher eher theoretischen Möglichkeiten gegen den praktischen Betrieb zu prüfen und substanzielle Einschätzungen bestehender oder weiterer IT-Sicherheitslücken zu gewinnen.

## 4.1 Maßnahmenangebote

Sind im Bereich Safety bereits viele (gesetzliche) Regelungen und Vorgehensweisen vorhanden bzw. definiert, gibt es im Bereich IT-Security zahlreiche Ansätze, die z.B. darstellen, wie der Datentransfer und die Netzwerktechnik geschützt werden können. Diese ausgearbeiteten möglichen Schutzmaßnahmen gelten im Wesentlichen für die IT-Sicherheit im Allgemeinen und es fehlen möglichst auf die Branche zugeschnittene Maßnahmen.

Die Maßnahmenangebote für IT Security wurden in die Bereiche Organisationen, Gesetze und Richtlinien, Konzepte und Strategien, Normen und Standardwerke unterteilt.

Das BSI ist 1991 mit dem BSI-Errichtungsgesetz zur Förderung der Sicherheit in der Informationstechnik gegründet worden. Maßgeblich initiiert wurden von dem BSI der Umsetzungsplan Kritische Infrastrukturen (UP KRITIS) und die Allianz für Cybersicherheit, über die ein Austausch von relevanten Sicherheitsinformationen erfolgt. Die seit 1993 entstandenen branchenspezifischen Computer Emergency Response Teams (CERT) sind untereinander, in dem CERT Verbund und weltweit in dem Forum of Incident Response and Security Teams (FIRST) vernetzt. In FIRST sind 365 Teams (davon 26 aus Deutschland) aus 77 Ländern beteiligt.[24]

Mit dem am 25. Juli 2015 in Kraft getretenen IT-Sicherheitsgesetz[25] sollen Betreiber besonders gefährdeter Infrastrukturen (sogenannter Kritischen Infrastrukturen) in den Bereichen wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet werden, ihre Netze besser vor Hacker-Angriffen zu schützen. Das Gesetz gilt bereits für Kernkraftwerke und Telekommunikationsunternehmen. In dem IT-Sicherheitsgesetz wurde zunächst nicht die Frage beantwortet, welche weiteren Unternehmen als Kritische Infrastrukturen dem Gesetz unterliegen. Welche weiteren Unternehmen unter das IT Sicherheitsgesetz fallen wurde am 13. Januar 2016 als Referentenentwurf[26] in einer Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom BMI vorgeschlagen und ist am 3. Mai 2016 in Kraft getreten[27]. Demnach unterliegen OWP-Betreiber dem Gesetz, falls die installierte Netto-Nennleistung eines betriebenen Windparks den Schwellenwert von 420 MW übersteigt, wobei jeder Windpark gesondert betrachtet wird. Das ist derzeit nicht der Fall, so dass OWP nicht dem Gesetz unterliegen. Tendenziell werden neue größer ausgelegte Windparks unter das Gesetz fallen.

Die Normenreihe ISO/IEC 27000 wird ständig von den Normungsorganisationen ISO und IEC weiterentwickelt und ist der internationale Standard für die Realisierung eines wirksamen ISMS. In Zusammenarbeit mit Wirtschaftsunternehmen hat das BSI auf Basis ISO/IEC 27001

24 Quelle: https://www.first.org/members/map

25 Quelle: BMI: IT Sicherheitsgesetz (https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf); abgerufen am 24.07.2015

26 Quelle: BMI: Referentenentwurf einer Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vo.pdf),; abgerufen am 13.01.2016

27 Quelle: BMI; Pressemitteilung „Erste Verordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten“; 3. Mai 2016; https://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/05/kritis-vo-tritt-in-kraft.html; abgerufen am 23. Mai 2016

das IT-Grundschutzhandbuch entwickelt und 1994 veröffentlicht. BSI IT-Grundschutz hat sich in der Folge zu einem Standardwerk für das IT-Sicherheitsmanagement in Deutschland entwickelt.

## 4.2 Maßnahmen in den Unternehmen

Bei der Aufnahme der Ist-Maßnahmen wurde der Schwerpunkte auf die Befragung von OWP-Betreibern gelegt. Die OWP-Betreiber agieren zwar in einem Netzwerk mit Dienstleistern, Anlagenherstellern, Netzbetreibern usw., haben aber als Betreiber der Windparks eine zentrale Rolle und sind von Maßnahmen immer betroffen.

OWP-Betreiber haben unbesetzte Sekundär- oder auch Tertiär-Leitwarten an anderen Standorten (z.B. auf Umspann-/Konverterplattform, auf Helgoland oder dem Festland), von denen aus im Fehlerfall die eigenen OWP bedient werden können.

Die OWP sind über eine redundante Datenanbindung erreichbar, per Kabel und per Satellit. Falls Sichtverbindungen bestehen, werden zusätzlich Funkverbindungen eingesetzt.

Der Zugriff auf die Steuerungsebene ist neben den OWP Betreibern auch den Stromnetzbetreibern/Direktvermarktern und Herstellern möglich, z.B. um die Leistung des Windparks einzustellen oder für die Durchführung von Wartungsmaßnahmen. Der Zugriff der Hersteller wird nach dem Ende der Gewährleistungsfrist alternativ von dem Betreiber in Eigenregie übernommen.

Es erfolgt eine Netzwerkteilung und Netzwerksegmentierung, d.h. eine Trennung der technischen von der elektrischen Betriebsführung oder eine Trennung des Office-Netzwerks vom Betriebsnetzwerk.

OWP Betreiber unterliegen nicht dem IT Sicherheitsgesetz. Das IT Sicherheitsgesetz wird von den OWP Betreibern aber eher positiv gesehen. Bezeichnend ist, dass OWP Betreiber Kontakt zu den Organisationen UP KRITIS bzw. der Allianz für Cybersicherheit suchen. Sie versprechen sich davon einen Informations- und Erfahrungsaustausch zu IT-Sicherheitsthemen.

Es kann festgestellt werden, dass die IT-Systemverwalter der OWP-Betreiber die Themen Industrie 4.0 (I4.0) und Internet of Things (IoT), also die Öffnung des Steuerungs- und Regelnetzwerkes zum Office-Netz oder zum Internet, außerordentlich kritisch sehen und diese Techniken aus Schutzgründen ablehnen.

## 4.3 Schwachstellen- und Bedarfsanalyse

Trotz präventiver und reaktiver Maßnahmen bleiben Sicherheitslücken bestehen. Diese Schwachstellen- und Bedarfsanalyse zeigt insbesondere die IT-spezifischen Schwachstellen auf.

Die für die Branche möglichen einsetzbaren Normen und Standardwerke wie z.B. der BSI-Grundschutz oder die Normenreihe ISO/IEC 27000 sind sehr mächtig und kleine sowie mittlere Unternehmen sind mit der Umsetzung von Sicherheitsmaßnahmen mit diesen Standardwerken an der Grenze ihrer Möglichkeiten. Es bestehen keine auf diese Branche zugeschnittenen Standards.

Bei der Errichtung von Offshore-Windparks liegt der Fokus der Sicherheitsmaßnahmen auf Themen wie Brandschutz, Lebensrettung und Notfallmaßnahmen im Safetybereich. Ist das Bewusstsein für den Bereich Security zwar vorhanden, so wird die Security (hier im Besonderen die IT Sicherheit) noch nachgelagert gehandhabt, und eine frühe Einbeziehung der IT-Sicherheit, zumindest auf konzeptioneller Ebene, wäre eine Verbesserung.

Bei Betrieb haben mehrere Beteiligte (OWP Betreiber, Stromnetzbetreiber/Direktvermarkter, Hersteller) Zugriff auf die Steuerungssysteme. Jeder Beteiligte hat mit unterschiedlicher Zuständigkeit nur eine Teilsicht auf das zugängliche Netzwerk.

Eine Herausforderung ist die Detektionsproblematik von Netzwerkanomalien. Um eine Abweichung vom Normalzustand zu erkennen (Anomalieerkennung), ist es wichtig festzulegen, was der annähernd fehlerfreie und unschädliche Normalzustand ist. Diese Grenzwertbereiche oder Grauzonen müssen definiert und ihre Grenzen nachfolgend enger gezogen werden, um möglicherweise neue Angriffe detektieren zu können, die unter dem „Radar“ agieren.

Die Steuerung auf Anlagenebene arbeitet ohne Verschlüsselung, da diese Ebene historisch bedingt keine Schnittstellen nach außen hatte und für einen möglichst schnellen und effizienten Betrieb zu sorgen hatte und hat. Mit der Öffnung der Systeme (Stichwort Industrie 4.0) ergibt sich hier möglicherweise Handlungsbedarf.

Es wurde angemerkt, dass eine gezielte phasenverschobene Fehlschaltung eventuell zu einer Störung des Stromnetzes führen könnte. Indirekte Angriffe wurden als schwer abzuwehren eingestuft, wobei auch der Aufwand für einen derartigen Angriff als sehr hoch eingeschätzt wurde. Unter indirekten Angriffen werden Angriffe verstanden, die z.B. durch das Einschleusen von kompromittierter Hardware eingeleitet werden.

Bei den Betreibern ist die Schärfung des IT Sicherheitsbewusstseins ein Thema. Stichworte sind z.B. der vorsichtige Umgang mit „liegengelassenen USB-Sticks“ oder der Umgang mit Dokumenten als Anlagen im eingehenden E-Mail-Verkehr. Bei sicherheitsrelevanten Prozessen wird das 4-Augen-Prinzip eingesetzt. Eine frühzeitige Berücksichtigung der IT Sicherheit bereits in der Errichterphase ist anzustreben.

# 5 Entwicklung neuer Maßnahmen und Konzepte

Auf Basis der durchgeführten Schwachstellenanalyse wurde festgestellt, dass die existierenden Maßnahmen und Empfehlungen zur Erhöhung der IT-Sicherheit bereits weite Teile zum Schutz von Netzwerken abdecken. Eine Anwendung von diesen Schutzmaßnahmen ist aber in dieser jungen Branche nicht einheitlich geregelt. Sicherheit kostet Zeit und damit Geld und wird deshalb von einigen mehr, von anderen aber weniger intensiv betrieben. Die Sicherheitsforschung in Deutschland wird vorangetrieben, IT-Sicherheit erhält einen immer höheren Stellenwert und viele Unternehmen sind bereits für dieses Thema sensibilisiert.

## 5.1 Maßnahmen für eine verbesserte IT-Sicherheit

In ISO 27001 und im BSI IT-Grundschutzkatalog sind bereits umfangreiche Maßnahmen genannt, die bei stringenter Anwendung die Cyber-Sicherheit erhöhen würden. Die Kapazitäten der OWP-Betreiber sind begrenzt, dennoch sind manche OWP-Betreiber bereits zertifiziert, andere verzichten auf die arbeitsintensive Zertifizierung, versuchen aber in Eigenregie eine möglichst hohe Sicherheitsstufe, z.B. unter Zuhilfenahme der BSI-Grundschutzkataloge oder der ISO 27000 Reihe, mit auf das OWP-Netzwerk zugeschnittenen Maßnahmen zu erreichen.

Diese im BSI-Grundschutz aufgeführten Maßnahmen einzeln zu betrachten, ihre Anwendbarkeit und eine bereits stattfindende Anwendung auf OWP-Betreiber zu prüfen, ist nicht Gegenstand des Projektes, insbesondere weil sich Teile dieses Cybersicherheitsbereiches bereits im Fokus der Betreiber befinden und auch teils gelöst sind.

Die Vorgehensweise für das Ziel, eine Erhöhung der Sicherheit gegen Cyber-Angriffe zu erreichen, besteht darin, die sich aus den Befragungen ergebenden Schwachstellen, die fehlende Netzwerküberwachung in zurzeit nicht sichtbaren Bereichen (Stichwort: „blinde/weiße Flecken"), die sich durchaus auf die Besonderheiten eines OWP beziehen, aber auch auf jede andere KRITIS übertragen werden könnten, eingehender zu betrachten und daraus passende Schlüsse zu ziehen. Die vorhandenen Sicherheitsvorschriften und die bereits bestehende Überwachung und Auswertung im regulären Betrieb eines OWP enthalten bereits geeignete Maßnahmen. Allerdings sind darüber hinaus völlig neue, aber auch seit langer Zeit vorhandene, Verfahren zu etablieren und dauerhaft anzuwenden (siehe auch IT-Grundschutzkatalog, G 2.22 Fehlende oder unzureichende Auswertung von

ten[28]). Die folgend aufgezählten Maßnahmen und Empfehlungen sind daher ausschließlich als Ergänzung zu den bereits bestehenden umfangreichen Sicherheitsmaßnahmen zu verstehen. Die für den OWP-Betrieb verantwortlichen Netzwerk-, Systemadministratoren und ICS/SCADA-Leiter, die sich für eine Befragung zur Verfügung gestellt haben, machten allesamt nach Aussage des für den IT-Teil zuständigen Interviewers, der selbst seit mehr als 20 Jahren im Bereich Rechner- und Netzwerktechnik tätig ist, „einen sehr kompetenten Eindruck mit breitem Erfahrungsschatz“. Für sie stehen Schutz und Sicherheit des OWP-Netzwerkes im Vordergrund ihres Handelns. Übereinstimmend herrscht in der Grundeinstellung ein kritischer Konservatismus gegenüber Innovationen, Stichworte Industrie 4.0 (I4.0) und Internet of Things (IoT), deren Implementierung das Potenzial für eine Erhöhung der Nutzbarkeit bieten, aber die Sicherheitsanforderungen des Netzwerkes aufgrund neuer Möglichkeiten einer Kompromittierung der Anlagen erhöhen. Wachsames und kritisches Personal mit tiefgreifendem Technologieverständnis wird für den Betrieb der Anlagen als unabdingbar erachtet. Ihre Aufgaben können auch bei Einsatz besserer, noch stärker automatisierter Überwachungs- und Meldesysteme mittel- bis langfristig nicht ersetzt werden, weil Netzwerkforensik und Netzwerkanalyse immer eine Beurteilung und Nachprüfung durch Menschen erfordert. Die vorgeschlagenen Maßnahmen – soweit sie zusätzliche Netzwerkgeräte und Analysesoftware betreffen – können deswegen nur als verbessertes und ergänzendes Werkzeug verstanden werden.

Das ISL schlägt zur Verbesserung der IT-Sicherheit die folgenden IT-Maßnahmen vor:

1. Bewusstsein für IT Sicherheit stärken
2. Erhöhung des Netzwerkschutzes
3. Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern
4. Erhöhung der Netzwerksicherheit
5. Firmware als Open Source Software

Um Effekte für eine Verbesserung der IT-Sicherheit zu stärken, werden die folgenden Empfehlungen ausgesprochen:

6. Langfristige Bindung des Personals

[28] BSI (2013); IT Grundschutz; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02022.html, abgerufen am 20. April 2017

7. Entwicklung eines BSI Grundschutz Light

8. IT Sicherheitsgesetz auf OWP-Betreiber erweitern

Im Folgenden werden diese Maßnahmen und Empfehlungen beschrieben.

### 5.1.1 Bewusstsein für IT Sicherheit stärken

Die befragten Netzwerk-/Systemadministratoren und ICS/SCADA-Leiter sind sehr auf die Sicherheit „ihrer" Netzwerke bedacht. Schon aus beruflichen Gründen, mit langjähriger Erfahrung im Bereich IT-Technik und mit Kenntnis der Nachrichten über die täglich berichteten Cyberattacken und Viren-/Trojanerinfektionen, verfügen sie über ein wachsames und gesundes gewachsenes Misstrauen, gern als „Berufsparanoia“ bezeichnet, das es ihnen ermöglicht, Vorsicht gegenüber jeder Art von möglichen äußeren Eingriffen zu üben, seien es die üblichen Schad-E-Mails mit ihren Anhängen und Links oder das Herunterladen und die Installation unbekannter Software: Sie sind von vornherein auf das Erkennen ungewöhnlichen Verhaltens trainiert und vorbereitet.

Ziel ist es, eine Sensibilität für IT-Sicherheit auf „normale“ Anwender zu erweitern und zu festigen. Wünschenswert wären praxisorientierte Schulungen, die den Benutzern verdeutlichen, welche Möglichkeiten die Informationstechnik – aus Sicht eines Angreifers – bietet, Anwender zu überwachen, welche Informationen über das Surfverhalten und die angesteuerten Webseiten gewonnen werden können, dass auch verschlüsselte Verbindungen belauschbar sind oder Tastatureingaben abgefangen und Rechner ferngesteuert werden können. Jedem Anwender muss bewusst werden, dass ein Netzwerk immer in beide Richtungen arbeitet, jede (ausreichend komplexe) Software Fehler hat, ohne geeignete Verschlüsselung jede Information im Klartext auf dem Weg vom Sender zum Empfänger übertragen wird und mitgelesen werden kann. Erst das Aufzeigen der Möglichkeiten, die natürlicherweise jedem erfahrenen Administrator bekannt sind, schafft das gewünschte Bewusstsein und manifestiert die Einsicht bei den Anwendern, mit den eigenen Daten und somit auch mit Unternehmensdaten sehr viel vorsichtiger umzugehen.

Ein praxisorientierter Lehrgang sollte nicht auf die Arbeitsplatzcomputer beschränkt werden - auch sollte vermittelt werden, welche Daten wann und wie häufig durch Smartphones mit jedem Netzwerk (auch dem Internet) ausgetauscht werden. Dies kann so weit gehen, dass den Benutzern gezeigt wird, dass jede Interaktion mit dem Rechner oder dem Smartphone Datenverkehr mit dem Internet erzeugt. Erst dieses Wissen gepaart mit der Erfahrung „am eigenen Leib“ erzeugt Einsicht und von selbst die Erkenntnis zu mehr Vorsicht.

Als Grundsätze sollten gelten:

- Kein Netzwerk ist sicher.
- In dem IT-Netzwerk (hier OWP-Netzwerk) darf es keine unbekannten Geräte und keine unbekannte Kommunikation geben.
- Jede Information ist wichtig und schutzbedürftig.
- Jeder Informationsaustausch ist verdächtig.

Wie bereits weiter oben angedeutet, wird Sicherheit eher als lästig empfunden und dies gern auch auf die Personen übertragen, die für die Sicherheit verantwortlich sind. Sicherheit lässt sich schwer messen. IT-Sicherheit macht sich bemerkbar durch zusätzliche Arbeit oder dadurch, dass die IT-Sicherheit versagt hat. Die Unternehmenskultur sollte den Sicherheitsbereich bzw. die Personen, die damit beauftragt sind, wertschätzen. Dies führt zu einem hoch motivierten Sicherheitspersonal und damit eher zu einem guten Sicherheitssystem auf hohem Niveau.

### 5.1.2 Erhöhung des Netzwerkschutzes

Stichworte wie Internet of Things (IoT), Industrie 4.0 (I4.0) oder Big Data fordern und erfordern eine Öffnung der Industrienetze. Jedoch bewirkt eine Öffnung der Industrienetze eine zusätzlich IT-Sicherheitslücke, die man entweder nicht zulässt oder mit entsprechenden Maßnahmen die IT-Sicherheit verbessert.

Der Netzwerkschutz sollte mit einer durchgehenden Verschlüsselung auf Anlagenebene erhöht werden. Dabei werden nicht nur Informationen besser geschützt, sondern es erfolgt eine Geräteauthentisierung und Geräteauthentifizierung. Innerhalb des Netzwerkes müssen Geräte sich zunächst authentisieren, d.h. sie geben sich dem Netzwerk mit bestimmten Rechten zu erkennen. Anschließend überprüft das Netzwerk die Angaben und authentifiziert das Gerät, d.h. gemäß den Berechtigungen der Zugriffskontrolle mit abgestuften Zugriffsebenen erhält das Gerät in dem Netzwerk erforderliche Zugriffsberechtigungen.

Eine durchgehende Verschlüsselung auf der Anlagenebene erfordert allerdings die Implementierung der Funktionalität in der Hardware. In vorhandenen Anlagen wäre eine Umsetzung aufwändig und mit hohen Kosten verbunden. Wenn also zukünftig im Bereich Offshore-Windindustrie Technologien wie IoT/I4.0 zum Einsatz kommen sollen, müssen die Anlagen der nächsten Generation entsprechend darauf vorbereitet werden.

### 5.1.3 Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern

Ziel dieser Maßnahme ist die Schaffung einer Institution, über die die OWP-Betreiber Informationen über Unregelmäßigkeiten untereinander austauschen. So können meldende OWP diese zentrale Stelle reaktiv über Ereignisse informieren, die im IT-Netzwerk vom Erwarteten abweichen und alle angegliederten OWP können angemessen darauf reagieren bzw. präventiv aktiv werden.

Diese „Institution“ kann eine neue Einrichtung speziell für die OWP-Branche sein oder kann auf bestehenden Informationsnetzwerken aufsetzen, z.B. dem beim BSI angesiedelten Verbund UP KRITIS. Der Bereich Energie ist ein Sektor Kritischer Infrastrukturen in Deutschland, sodass sich die Betreiber aus der OWP-Branche dem UP KRITIS anschließen könnten.

UP KRITIS formuliert seine Ziele wie folgt[29]:

- Förderung der Robustheit von IKT-Komponenten in kritischen Prozessen
- Austausch über aktuelle Vorkommnisse
- Gemeinsame Einschätzung und Bewertung der Cyber-Sicherheitslage
- Erarbeitung gemeinsamer Dokumente und Positionen
- Auf- und Ausbau von Krisenmanagementstrukturen
- Koordinierte Krisenreaktion und -bewältigung
- Durchführung von Notfall- und Krisenübungen
- Gemeinsames Handeln gegenüber Dritten

Teilnehmer des UP KRITIS erhalten Zugriff auf die Produkte des UP KRITIS und auf das Informationsangebot der Allianz für Cyber-Sicherheit mit den darin enthaltenen vertraulichen Inhalten. Alle Teilnehmer des UP KRITIS erhalten die Lageinformationen und Warnmeldungen zur IT-Sicherheit, die vom BSI bereitgestellt werden.

### 5.1.4 Verbesserung der Netzwerksicherheit im OWP

Ziel der Maßnahme ist es, den OWP-Betreibern ein Werkzeug anzubieten, mit dem eine umfassende Überwachung zur Verbesserung der Sicherheit des IT-Netzwerks möglich ist. Derzeit haben unterschiedliche Beteiligte Zugriff auf das OWP-Netzwerk mit unterschiedlichen Zugriffsrechten. Für eine umfassende Überwachung des IT-Netzwerks ist es erforderlich,

[29] BBK, BSI; Zusammenarbeit im Rahmen des UP KRITIS; http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html, abgerufen am 20. Juni 2017

dass eine zentrale Stelle etabliert wird. Den OWP-Betreibern sollte diese Aufgabe der gesamten Netzwerküberwachung zufallen, da sie die zentrale Stelle des gesamten Verbundnetzwerks bilden und nur bei ihnen der gesamte Netzwerkverkehr aus dem Anlagennetz, aus dem eigenen Steuerungs- und Regelnetz und den Netzen der Stromkonzerne und Direktvermarkter zusammenläuft. Nur sie hätten daher die Möglichkeit, den relevanten Netzwerkverkehr zu überwachen und Angriffe, sowohl von innen heraus als auch von außen nach innen, zu erkennen und zu melden.

Der OWP-Betreiber hat auf der Anlage die meisten Netzwerk-Schnittstellen, Netzwerk-Übergänge und Netzwerk-Zugänge, über die Anlage wird die Strommenge des OWP geregelt und der OWP-Betreiber hat das größte Interesse an der Überwachung der Anlage bis in die Anlagenebene. Zusätzlich zum ohnehin schon unter das BSI-Gesetz fallenden Übertragungsnetzbetreiber (ÜNB) bietet die Maßnahme für den OWP-Betreiber ein hohes Potenzial für die Verbesserung der Netzwerk-Sicherheit in Eigenregie. Eine Verbesserung der Netzwerküberwachung (Netzwerkforensik, NIDS/ NIPS – Network Intrusion Detection System/Network Intrusion Prevention System) kann zu einer spürbaren Erhöhung der Netzwerk-Sicherheit in OWP-Netzwerken beitragen. Dennoch muss klar sein, dass es sich um ein Werkzeug handelt, das sich laufend weiterentwickeln bzw. dessen Konfiguration laufend angepasst werden muss, und die gelieferten Informationen des Werkzeugs von Menschen bewertet und ggf. gehandelt werden muss.

Eine verbesserte Netzwerküberwachung ist die Grundlage für eine Erkennung von schädlichem Netzwerkverkehr (Anomalien) und damit zugleich für eine verbesserte Früherkennung und einen möglichen Einsatz wirksamer Abwehrmaßnahmen. Sie deckt Erkennungsbereiche ab, die mit den üblichen, zurzeit am Markt vorhandenen, vorgefertigten Firewall- und (Viren-) Scanner-Gateways und Systemlösungen nicht oder nur sehr schwer erfüllt werden können. Die Netzwerküberwachung setzt „unterhalb“ der Softwarelösungen (Firmware, Virenscanner oder allgemein jedes Programms) an und beschäftigt sich mit der Überwachung der Netzwerkkommunikation auf unterster Ebene, der Überwachung der bei jeder Kommunikation ausgetauschten Netzwerkpakete. Die Netzwerktopologie, Netzwerkprotokolle oder das verwendete Übertragungsmedium (drahtlos/drahtgebunden) spielen dabei für die Überwachung hingegen keine Rolle. Bei dieser Überwachungsart geht es vorrangig nicht um die enthaltene Information in den Paketen, sondern um die übergeordneten Daten (Header-, Meta-Daten, Prüfsummen), die Bestandteil jeder Kommunikation sind wie z.B. die Adressen der Sender und Empfänger einer Nachricht und die verwendete Sprache.

### 5.1.5 Firmware als Open Source Software

Eine Überprüfung des eingesetzten Quellcodes sollte möglich sein. Befindet sich der eingesetzte Quellcode unter einer Open Source Lizenz, hat der OWP-Betreiber mit entsprechender Expertise die Möglichkeit, den Source-Code zu prüfen. Üblicherweise wird der Source-Code aber nicht unter einer Open Source Lizenz stehen. In diesem Fall kann die Prüfung dem Hersteller auferlegt werden.

Grundsätzlich bestehen die folgenden Möglichkeiten:

- Produkte meiden, die in der Hardware Blackboxes verbaut haben.
- Produkte aus der Europäischen Union einsetzen.
- Offenlegung des Quellcodes der Blackbox einfordern.
- Prüfung des Quellcodes der Blackboxes dem Hersteller auferlegen.
- Eine frühzeitige Obsoleszenz durch vertragliche Regelungen vermeiden, falls der Hersteller z.B. nicht mehr verfügbar ist.

### 5.1.6 Langfristige Bindung des Personals

Es wird empfohlen, das Knowhow im Unternehmen zu halten. Dabei ist eine möglichst langfristige Bindung der Mitarbeiter (und damit des Wissens) anzustreben. Damit können zwei Effekte erzielt werden: Einerseits wird das sicherheitsrelevante Wissen im Unternehmen gehalten und stärkt das Knowhow, z.B. Erfahrungen mit Anomalieerkennung und -behandlung, anderseits ergeben sich nach außen hin keine neuen Angriffspunkte, da ein Wissensabfluss von Anlagen- und Netzwerkinterna vermieden wird.

Die Motivation für das und die Identifikation mit dem Unternehmen sollten gestärkt werden, z.B. durch eine Sensibilisierung des IT Sicherheitsbewusstseins und das „Leben“ einer Corporate Identity. Eine stärkere Bindung der Mitarbeiter an das Unternehmen kann auch mit den oben genannten Qualifizierungsmaßnahmen (Maßnahme 1) erreicht werden.

### 5.1.7 BSI Grundschutz Light

Bisher haben nur wenige Unternehmen aus der Branche Offshore-Windenergie den Schritt einer Zertifizierung gewagt, da dieser Schritt als langwierig, kompliziert und teuer betrachtet wird. Aus diesem Grund sollte gerade kleinen und mittleren Unternehmen (KMU) (OWP-Betreiber zählen zu den KMU) der Zugang zu einer Zertifizierung erleichtert werden. Hierfür aber sollte der BSI-Grundschutzkatalog branchenspezifisch zu einer Art BSI Grundschutzkatalog Light abgespeckt werden.

Es wird empfohlen, die große Komplexität des Grundschutzkatalogs zu reduzieren und branchenspezifisch zuzuschneiden. Da in KMU für eine Umsetzung von Zertifizierungsmaßnahmen wenig Personal zur Verfügung steht, könnte damit eine Hürde genommen werden. Eine in einem Interview genannte Dauer von 18 Monaten für einen Zertifizierungsprozess ist für KMU oft nicht akzeptabel.

Auf der CeBIT 2017 in Hannover hat das BSI eine Modernisierung des IT-Grundschutzes vorgestellt[30]. Das Konzept sieht vor, dass für einen modernisierten IT-Grundschutz Profile entwickelt werden. Diese IT-Grundschutz-Profile werden nicht als Vorgabe durch das BSI, sondern durch z.B. Branchenverbände entwickelt und jedes Profil enthält ein Muster-Sicherheitskonzept für ein ausgewähltes Szenario. Das Muster-Sicherheitskonzept „bereitet das Ergebnis mehrerer Prozessschritte der IT-Grundschutz-Vorgehensweise (z.B. Strukturanalyse, Schutzbedarfsfeststellung, Modellierung) und einer Auswahl mehrerer Anforderungen der IT-Grundschutz-Bausteine so auf, dass es als Schablone von ähnlichen Institutionen adaptiert werden kann."

Die Vorgehensweise sieht branchenspezifische Lösungen als „Schablonen für die Informationssicherheit" vor, die als eine nicht verpflichtende BSI Grundschutz Light Version verstanden werden können.

### 5.1.8 IT Sicherheitsgesetz auf OWP-Betreiber erweitern

Seit dem 25. Juli 2015 ist das IT-Sicherheitsgesetz in Kraft[31]. Das Gesetz legt ein dem Stand der Technik entsprechendes Maß an Sicherheitsmaßnahmen fest, das alle vier Jahre einer Evaluation unterzogen wird. Darüber hinaus besteht eine Meldepflicht über IT-Sicherheitsvorfälle an das BSI. Das BSI erstellt aus allen verfügbaren Informationen ein Lagebild, das wiederum den dem Gesetz unterliegenden Unternehmen zur Verfügung gestellt wird, damit entsprechende präventive Schutzmaßnahmen getroffen werden können.

30 BSI, Isabel Münch, Holger Schildt, Birger Klein; 22.03.2017; Modernisierung des IT-Grundschutzes https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/CeBIT_2017_Die_Modernisierung_des_IT-Grundschutzes.pdf;jsessionid=93830CE790F042CB096ABFA485534C80.1_cid360?__blob=publicationFile&v=2; abgerufen am 21. Juni 2017

31 BSI; IT-Sicherheitsgesetz tritt am 25. Juli 2015 in Kraft; https://www.bsi.bund.de/DE/DasBSI/Gesetz/IT-Sicherheitsgesetz.html, abgerufen am 19. April 2017

In dem Referentenentwurf vom 13. Januar 2016[32], in Kraft getreten am 3. Mai 2016[33], wurde festgelegt, welche Unternehmen unter das IT Sicherheitsgesetz fallen. Dort wurde der Schwellenwert pro Windpark auf 420 MW festgelegt. In 2017 erreicht kein Windpark, der in Betrieb ist oder gehen wird, die 420 MW Marke[34]. OWP-Betreiber unterliegen also derzeit noch nicht dem IT-Sicherheitsgesetz.

Ab 2019 ist aufgrund der geplanten Leistung von neuen Windparks damit zu rechnen, dass erste OWP-Betreiber als Betreiber von OWP mit einer Leistung von mehr als 420 MW unter das IT-Sicherheitsgesetz fallen. Ab 2025 ist mit mindestens sechs OWP zu rechnen, die dem IT-Sicherheitsgesetz unterliegen.

Aus den Erfahrungen dieser OWP sollten Rückschlüsse gezogen werden, ob die Grenze 420 MW mittel- bis langfristig Bestand haben sollte oder herabgesetzt wird, um flächendeckend OWP unter das IT-Sicherheitsgesetz zu stellen.

## 5.2 Grenzfälle und Wechselwirkungen

Die Umsetzung einer Maßnahme kann Einfluss auf andere Maßnahmen haben. Die Maßnahme 4 „Verbesserung der Netzwerksicherheit“ per Anomalieerkennung ist eine zentrale Maßnahme, die eine verlässliche Sicherheit in Aussicht stellt. Ein derartiges Werkzeug wird an allen neuralgischen Punkten (Knoten) des IT-Netzwerkes eingesetzt. Es gibt vielversprechende Ansätze für Werkzeuge der Anomalieerkennung.

Die Empfehlung 8 „IT Sicherheitsgesetz auf OWP-Betreiber erweitern“ ist mittel- bis langfristig auf Sinnhaftigkeit zu prüfen. Falls die Maßnahme auf OWP-Betreiber erweitert wird, wäre mit bis dahin bereits umgesetzten Maßnahmen, insbesondere die Maßnahme 3 „Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern“ und die Maßnahme 4 „Erhöhung der Netzwerksicherheit“, eine Basis geschaffen, um den Anforderungen des IT-Sicherheitsgesetzes zu genügen.

Mit einem funktionierenden Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern, sei es als Branchenlösung OWP oder unter dem Dach UP KRITIS, könnte sich bereits eine

[32] BMI; Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI – Gesetz https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/BSI_Kritis_VO.pdf?__blob=publicationFile&v=3, abgerufen am 19. April 2017

[33] BMI (3. Mai. 2016); Pressemitteilung „Erste Verordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten“; https://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/05/kritis-vo-tritt-in-kraft.html; abgerufen am 19. April 2017

[34] Wikipedia (20. April 2017); Liste der Offshore-Windparks; https://de.wikipedia.org/wiki/Liste_der_Offshore-Windparks, abgerufen am 21. April 2017

Kultur der Zusammenarbeit in dem Bereich IT-Sicherheit etablieren. Mit der Umsetzung der Maßnahme zur Netzwerksicherheit per Anomalieerkennung wäre bereits die Basis für Meldeverpflichtungen entsprechend dem IT-Sicherheitsgesetz geschaffen.

Um den erhöhten Informationsbedarf, den Trends wie I4.0 und IoT auslösen, zu stillen, müssen IT-Netzwerke geöffnet werden. Dies führt unmittelbar zu einer Senkung der IT-Netzwerksicherheit. In den durchgeführten Interviews mit Experten herrschte einhelliger Konsens darüber, dass die Implementierung von Innovationen zwar die Nutzbarkeit erhöhen könnten, die Sicherheit des Anlagennetzwerks damit aber möglicherweise gefährdet wird. Hier müssen geeignete Schutzmaßnahmen getroffen werden, mit denen der erforderliche Netzwerkschutz wieder hergestellt wird. Hierzu sind die Maßnahmen 2 „Erhöhung des Netzwerkschutzes“ und 3 „Erhöhung der Netzwerksicherheit“ geeignet. Eine durchgängige Verschlüsselung auf der untersten Anlagenebene laut Maßnahme 2 und die Erhöhung der Netzwerksicherheit per Anomalieerkennung laut Maßnahme 4 sind dazu geeignet, um den Netzwerkschutz trotz geöffneter Netze wieder herzustellen.

Die folgende Grafik zeigt Wechselwirkungen bezogen auf die in OWiSS erarbeiteten IT-Maßnahmen:

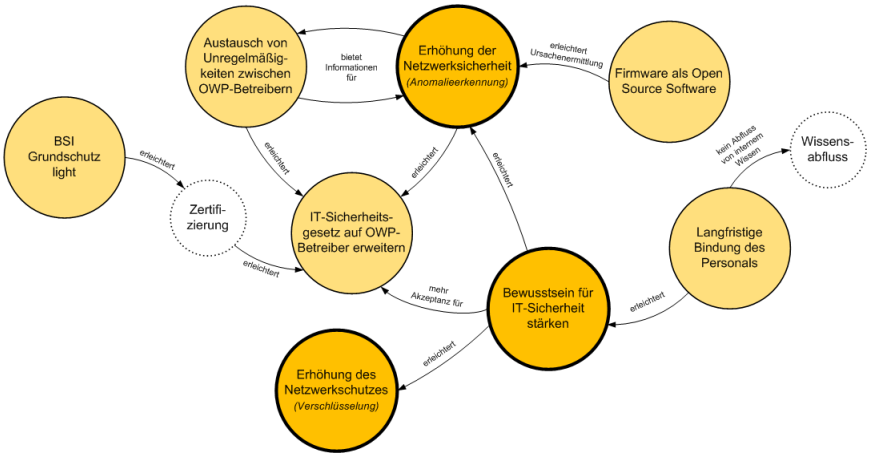



**Abbildung 6: Wechselwirkungen von IT-Maßnahmen**[35]

Die vorgeschlagenen Maßnahmen beeinflussen sich gegenseitig; einige sind sofort umsetzbar, andere z.B. nur nach Gesetzesänderung, einige sind leicht umsetzbar, auch mit unternehmenseigenen Mitteln, andere nicht, da heute noch die Voraussetzungen für eine Umsetzung fehlen. Die vorgeschlagenen Maßnahmen sind betriebsintern einfach und sofort umzusetzen und dienen zeitgleich als Vorbereitung für eine möglicherweise kommende Erweite-

35 Quelle: ISL

rung des IT-Sicherheitsgesetzes sowie für eine Zertifizierung nach einem BSI Grundschutz Katalog in einer sog. Light-Version, sobald diese vorliegt.

Insbesondere wird vom ISL die Maßnahme „Erhöhung der Netzwerksicherheit“ durch Anomalieerkennung so eingeschätzt, dass mit dieser Maßnahme mit relativ wenig Aufwand ein großer Effekt erzielt werden kann.

# 6 Bewertung von Maßnahmen aus ökonomischer Sicht

Im Hinblick auf die zu bewertenden Maßnahmen wird zwischen Maßnahmen für eine verbesserte IT-Sicherheit und Maßnahmen zur besseren Ausfallsicherheit von Offshore-Windparks unterschieden. Zwar liegt der Fokus des ISL auf der Entwicklung von Maßnahmen zur Erhöhung der IT-Sicherheit, präventive und reaktive Maßnahmen zur Verminderung von Schäden wurden jedoch ebenfalls untersucht und bewertet. Diese wurden mittels einer Kosten-Nutzen-Analyse bewertet, wobei Kosten und Nutzen in Geldeinheiten gemessen werden, um eine Vergleichbarkeit und Verrechnung zu ermöglichen.

Problematisch ist die Bewertung von „nicht am Markt gehandelten Gütern, wie beispielsweise Menschenleben, Zeit, Umweltgütern“ sowie bei schwierig einzuschätzendem Nutzen wie Image, Kundenzufriedenheit, Mitarbeiterzufriedenheit, Klimaschutz etc. Dies trifft vor allem auf die Bewertung der IT-Maßnahmen zu. Aufgrund dessen wurden diese Maßnahmen auch nicht mit Hilfe einer Kosten-Nutzen-Analyse (quantitativ) bewertet, sondern auf einer qualitativen Ebene.

## 6.1 Bewertung von Maßnahmen mit energiewirtschaftlicher Bedeutung

Für eine ökonomische Bewertung der energiewirtschaftlich relevanten Maßnahmen, bei denen logistische Prozesse für eine Schadensbehebung notwendig sind, wurde zunächst zur Ermittlung der Kosten ein Simulationsmodell eingesetzt, mit dem unterschiedliche Szenarien von Schadensfällen und deren Beseitigung in ihren Prozessen durchgespielt werden konnten. Die daraus resultierenden Ergebnisse wurden mit Hilfe einer Kosten-Nutzen-Analyse bewertet, um eine Hilfestellung bei der Entscheidung zwischen mehreren Alternativen zu bieten. Nachfolgend wird ein kurzer Überblick über die Kosten-Nutzen-Analyse gegeben sowie die wichtigsten Begrifflichkeiten erläutert.

### 6.1.1 Simulation

Im OWiSS-Projekt wurden präventive und reaktive Maßnahmen (weiter-)entwickelt, so dass Offshore-Windparks ausfallsicherer werden bzw. nach einem Ausfall schneller wieder in Betrieb genommen werden können. Das Simulationsmodell wurde für eine Ermittlung von Logistikkosten und der durch Ausfälle in den Windparks entgangenen Einspeisevergütung eingesetzt. Diese Kosten wurden neben anderen Kostenfaktoren für die Bewertung präventiver

Maßnahmen mit herangezogen. Sowohl für die Abbildung von reaktiven Maßnahmen als auch für die Abbildung von IT-Maßnahmen ist das Simulationsmodell dagegen nicht geeignet.

Der Einsatz des Simulationsmodells ist immer dann sinnvoll, wenn die Ausfalldauer ungewiss und die Ausfallmenge erheblich ist, wie z.B. bei Beschädigung von Exportkabeln oder Ausfall von Großkomponenten von Konverter- und Umspannplattformen. Für den Ausfall oder die Abschaltung von Windenergieanlagen, ganzer Windparks bis hin zu einem kompletten Windparkcluster gibt es vielfältige Ursachen. Einerseits werden über die Sommermonate regelmäßig Wartungsmaßnahmen durchgeführt, da die Wartung jeder einzelnen Anlage in einem 4-Jahres-Rhythmus vom Gesetzgeber vorgeschrieben ist und durch regelmäßige Wartungsmaßnahmen ein weitestgehend ungestörter Betrieb sichergestellt werden soll. Andererseits treten durch Witterung, menschliches oder technisches Versagen Probleme auf, die es zu beheben gilt. Ein Teil dieser Probleme kann zwar bereits von Land aus in der Leitstelle gelöst werden, für andere Probleme muss jedoch ein Spezialschiff für ein Reparaturteam gechartert werden, damit im Windpark die Reparatur durchgeführt werden kann. Im schlimmsten Fall können Großkomponenten ausfallen, die neu gefertigt werden müssen, wodurch ein längerer Ausfallzeitraum verursacht wird, in dem kein Strom produziert werden kann. Hier setzt das im ISL entwickelte Simulationsmodell „OWEA-Service“ an. Das Simulationsmodell dient zur Abbildung einzelner Windparks bis zu einer kompletten Windparklandschaft und simuliert deren Betriebsphase unter Einfluss des Wetters.

Um eine vollständige Bewertung von Maßnahmen durchzuführen, waren neben den durch die Simulation ermittelten Daten weitere Faktoren erforderlich. Die Ergebnisse aus der Simulation sind jedoch ein wichtiger Bestandteil zur Kostenermittlung, da u.a. die Logistikkosten ohne Simulation schwer greifbar sind.

### 6.1.2 Simulation von Maßnahmen mit energiewirtschaftlicher Bedeutung

Da bei einem plötzlichen Ausfall eines Konverters oder eines Exportkabels mit einer Auswirkung für die Bevölkerung gerechnet werden kann, wurde hiermit für uns die Basis für präventive Maßnahmen definiert. Es wurden Verbesserungsvorschläge zur Minimierung der Ausfallzeiten erarbeitet und im Konsortium wurden anschließend die folgenden Maßnahmen für die Abbildung in der Simulation festgelegt. Eine betriebswirtschaftliche Bewertung der abgebildeten Maßnahmen erfolgt neben der vom IFAM durchgeführten energiewirtschaftlichen Bewertung im Anschluss an die Simulation.

Es werden die beiden Szenarien

1. Bauteil Konverter defekt
2. Exportkabel defekt

betrachtet.

Auf die beiden Szenarien werden die beiden vorgeschlagenen Maßnahmen

1. Standardisierung und Lagerhaltung von Großbauteilen sowie
2. Vermaschtes Netz

angewendet.

Für Kabelschäden werden heute bereits Ersatzkabel vorgehalten. Die Standardisierung und Lagerhaltung von Exportkabeln wird mit der Maßnahme 1 abgebildet. Andere Großkomponenten, z.B. der Konverter in Szenario 1, werden nicht auf Lager vorgehalten. Daher wird zusätzlich der Ist-Zustand als Basismodell betrachtet, in welchem das Bauteil Konverter nicht auf Lager vorgehalten wird und im Schadensfall produziert werden muss.

Aus dem Basismodell und den Szenarien kombiniert mit den Maßnahmen ergeben sich insgesamt fünf Alternativen, die im Anschluss an die Simulation zu bewerten sind:

Alternative 1: Szenario 1: Bauteil Konverter defekt
Basismodell: Ist-Zustand
Das Bauteil (der Transformator) muss produziert und ausgetauscht werden. Diese Spezialteile haben in der Regel lange Lieferzeiten; für die Fertigung eines neuen Transformators sind 14-16 Monate anzusetzen. Die Ausfallzeit der Anlage besteht also zum größten Teil aus der Fertigungszeit.

Alternative 2: Szenario 1: Bauteil Konverter defekt
Maßnahme 1: Standardisierung und Lagerhaltung von Großbauteilen
Heute ist man noch nicht in der Lage, Ersatzteile wie z.B. Transformatoren für Konverterplattformen vorzuhalten, da es in der Offshore-Windenergie keine Standardprodukte gibt. Durch Vorhaltung eines Ersatztransformators könnte die Zeit bis zur Reparatur des Konverters erheblich verkürzt werden – ein neuer Transformator kann dann unabhängig von der Reparatur parallel gefertigt und anschließend gelagert werden. Wenn also erreicht werden kann, auch Spezialgroßbauteile zu standardisieren und für den Fall einer Reparatur vorzuhalten, ließen sich die Ausfallzeiten erheblich verringern. In

diesem Fall bliebe lediglich eine Vorbereitungszeit vor Abfahrt des Spezialschiffes zum Konverter. Für den Fall, dass eine Standardisierung in dieser Form auch in Zukunft nicht möglich sein wird, sollte versucht werden, zumindest Basiskomponenten zu standardisieren, die im Schadensfall mit komponentenspezifischen Bauteilen aufgerüstet werden, um zumindest die Herstelldauer deutlich zu verkürzen. In der Simulation wurde eine auf 6 Monate verkürzte Herstelldauer angenommen, um eine Tendenz dafür zu geben, wie stark sich eine solche Verkürzung positiv auswirken könnte. (Alternative 2a: Standardisierung und Lagerhaltung Basiskomponente).

Alternative 3: Szenario 1: Bauteil Konverter defekt

Maßnahme 2: Vermaschtes Netz:

Beim Aufbau eines vermaschten Netzes ist jeder OWP durch eine zusätzliche Kabelanbindung an einen zweiten Konverter angeschlossen. Im Falle eines Konverterschadens werden die angeschlossenen OWP auf „ihren“ Ersatzkonverter umgeswitcht. Da dieser „Ersatzkonverter“ jedoch auf den Stromtransport der bereits angeschlossenen OWP dimensioniert und nicht dafür ausgelegt ist, zusätzlichen Strom von durch einen Konverter- bzw. Kabelschaden betroffenen OWP abzuführen, ist im Schadensfall die Leistung der nun an den Konverter angehängten OWP bei starken Winden zu drosseln, bis Kabel oder Konverter repariert wurden und die OWP ihren Strom über einen erneuten Switch wieder über den Ursprungskonverter ableiten können. Dadurch wird über die gesamte Dauer des Konverterausfalls mit einer verringerten Stromlieferung (erhöhte Stromausfallmenge fließt in die Berechnung der Ausfallkosten ein) gerechnet. Zusätzlich zu einer erhöhten Ausfallmenge ist mit zusätzlichen Investitionskosten für die doppelte OWP-Verkabelung zu rechnen. Die Kostendaten für zusätzliche Verkabelungen lassen sich allerdings nur sehr grob abschätzen und sind deshalb nur als Größenordnung zu verstehen.

Alternative 4: Szenario 2: Exportkabel defekt: Austausch eines Kabelstücks erforderlich

Basismodell: Ist-Zustand: Kabel wird vorgehalten

Die einzige Komponente, die heute schon redundant vorgehalten wird, sind Kabelmeter jedes Typs, der offshore verlegt wurde. Tritt ein Kabelschaden auf, wird von dieser Kabellänge ein entsprechend langes Stück verwendet

und das defekte Kabel hiermit repariert. Trotzdem muss nach der Reparatur eines Kabelschadens das entsprechende Kabel neu gefertigt werden, damit im Falle eines erneuten Schadens wieder eine Ersatzlänge vorrätig ist.
Durch das Vorhalten von Ersatzteilen treten neben den Investitionskosten für das defekte Bauteil auch Kosten für Wartung und Lagerung des Ersatzteils auf. Die Reparatur des Kabels wird in Form einer Omegaschleife durchgeführt. Dabei kann es vorkommen, dass vor der Reparaturmaßnahme für die vorgesehene Fläche auf dem Meeresboden eine Munitionsräumung (UXO) erfolgen muss (Alternative 4a: Ist-Zustand mit UXO).

Alternative 5: Szenario 2: Exportkabel defekt
Maßnahme 1: Vermaschtes Netz [vgl. Alternative 3 bezogen auf die Reaparatur des Exportkabels]
Als Alternative wird die Maßnahme „Vermaschtes Netz“ mit eingeplanter Munitionsräumung gerechnet (Alternative 5a).

### 6.1.3 Simulationsergebnis als Basis für eine ökonomische Bewertung

Aus der Simulation wurden folgende Daten als Eingangsdaten für die Bewertung der unterschiedlichen Szenarien verwendet. Die ermittelten Kostentypen Ausfallkosten, Logistikkosten sowie sonstige Kosten setzen sich wie folgt zusammen:

**Ausfallkosten**

Die Ausfallmenge in GWh wird durch die in der Simulation ermittelte Ausfalldauer in Tagen unter Berücksichtigung der jährlich prognostizierten Volllaststundenzahl und der unterschiedlichen Stromausbeute im Sommer und Winter berechnet. Die Ausfallkosten berechnen sich durch die Multiplikation der Ausfallmenge in GWh mit einer Einspeisevergütung von 3,9 ct./kWh, 14,4 ct./kWh sowie 19,4 ct./kWh zur Ermittlung einer Schadensspanne bei einer definierten Ausfalldauer.

**Logistikkosten**

Die Logistikosten beinhalten die sogenannten Mobilisierungskosten für das Spezialeinsatzfahrzeug sowie dessen Einsatzkosten für die Dauer des Einsatzes.

**Sonstige Kosten**

Je nach Szenario können folgenden Kosten als sonstige Kosten anfallen: Projektengineering, Investitionskosten für das ausgefallene Bauteil, Lagerkosten für ein vorgehaltenes Ersatzbauteil, Wartungskosten für ein vorgehaltenes Ersatzbauteil, Investitionskosten Kabel für

den Anschluss der OWP an einen zweiten Konverter und deren Wartung, Kosten für die Kabelverlegung für den Anschluss der OWP an einen zweiten Konverter. Personalkosten sind nicht explizit aufgeführt.

Die Investitions- und Anschlusskosten für die Verkabelung von OWP an einen zweiten Konverter (vermaschtes Netz) sind ein Schätzwert auf Basis bisheriger Anschlusskosten bereits errichteter OWP. Die Länge der Kabel muss ebenfalls geschätzt werden, was sich sehr auf die Kosten auswirkt.

Die in den sonstigen Kosten enthaltenen Lager- und/oder Wartungskosten für die Alternativen 2, 3, 4 und 5 werden jeweils für 12 Monate berechnet.

In den Kosten für das Spezialschiff sind Personalkosten enthalten. Weitere Personalkosten sind für die Bewertung abzuschätzen. Ebenfalls abzuschätzen sind Veränderungen in den Versicherungskosten, da sich die Ausfallsicherheit der OWP durch die Umsetzung einer der vorgeschlagenen Maßnahmen erhöht.

### 6.1.4 Kosten-Nutzen-Analyse

Im Allgemeinen versteht man unter einer Kosten-Nutzen-Analyse ein Instrument, um zu bestimmen, ob ein Ergebnis – der Nutzen – einer Aktion bzw. Maßnahme den hierfür benötigten Aufwand – die Kosten – rechtfertigt. Wenn davon ausgegangen werden kann, dass Nutzen und Kosten nicht sicher eintreten, werden deren Erwartungswerte, also Nutzen oder Kosten gewichtet mit deren angenommenen Eintrittswahrscheinlichkeiten, verwendet. Im Fall der vorliegenden Bewertung ist letzteres die mögliche Häufigkeit, mit der die beschriebenen Ausfallszenarien eintreten könnten, beispielsweise einmal in 25 Jahren oder alle 10 Jahre. Zudem gibt es in Bezug auf eine Kosten-Nutzen-Analyse einige weitere relevante Entscheidungskriterien: der sogenannte Nettobarwert (Net Present Value (NPV)), die interne Rendite (Internal Rate of Return (IRR)) sowie der Amortisationszeitraum.

In einer der vorgeschlagenen präventiven Maßnahmen wird beispielsweise angenommen, dass ein Transformator als Ersatzteil für einen Konverter hergestellt und eingelagert wird, so dass im Schadensfall die Zeit für die Herstellung des Ersatzteils entfällt und entgangene Einnahmen durch den Stromausfall reduziert werden. Bei dem Kauf des Ersatzteils wird Kapital gebunden, das dann in Form des Ersatzteils und nicht als Geldwert vorliegt und somit nicht zu anderen Zwecken eingesetzt werden kann. Diesen quasi entgangenen Gewinn aus dem ansonsten möglichen „produktiven“ Einsatz des Betrages wird beispielsweise mit kalkulatorischen Zinsen für das gebundene Kapital berücksichtigt. Er gibt damit den Zinssatz wieder,

den ein Investor bei Anlage des Geldes am Kapitalmarkt hätte erzielen können bzw. den er für den Einsatz seines Geldes erwarten kann. Den aus der Abzinsung resultierenden Betrag bezeichnet man als Kapitalwert, Barwert oder Gegenwartswert (Net Present Value (NPV)).

Die interne Rendite bzw. die interne Kapitalverzinsung (Internal Rate of Return (IRR)) und der Amortisationszeitraum sind im Rahmen von Kosten-Nutzen-Analysen ebenfalls von Bedeutung und können als weitere Entscheidungskriterien betrachtet werden. Die interne Kapitalverzinsung ist die Rendite oder Profitabilität eines Projektes – in diesem Fall einer Maßnahme – auf Basis einer diskontierten Cashflow-Analyse. Die interne Kapitalverzinsung (interne Rendite) ist dabei der Zinssatz, der innerhalb einer bestimmten Laufzeit angewandt wird, um einen Kapitalwert (= Barwert oder auch Gegenwartswert) von Null zu erzielen.[36] Der Amortisationszeitraum ist der Zeitraum bis zu dem Zeitpunkt, an dem der Nutzen auf dem Niveau der Kosten liegt, oder dieses übersteigt, d.h. der Zeitraum, in dem sich die Investition rentiert hat.

Im Hinblick auf die Identifizierung des Nutzens wird für die hier durchgeführte Kosten-Nutzen-Analyse der Fokus auf die Vermeidung bzw. Reduzierung von Kosten, die im Schadensfall eintreten, gelegt. Der erwartete Nutzen wird dabei – ebenso wie die Kosten – in Geldeinheiten gemessen, um eine Vergleichbarkeit und Verrechnung zu ermöglichen. Im Hinblick auf die Bewertung der präventiven und reaktiven Maßnahmen sind dabei die sogenannten Opportunitätskosten (auch als Alternativ- oder Verzichtskosten bezeichnet) von Bedeutung. Es handelt sich hier dabei um entgangene Erlöse, die sich dann ergeben, wenn der in den Szenarien prognostizierte Schaden eintritt und keine Maßnahmen ergriffen wurden, um diesen geringer zu halten oder zu vermeiden (Nutzen = vermiedene Einnahmeausfälle; Nettonutzen = vermiedene Einnahmeausfälle abzüglich der dafür anfallenden Kosten). Diese Opportunitätskosten dienen zur Quantifizierung des Nutzens.

### 6.1.5 Vorgehensweise

Zur Definition der für die Kosten-Nutzen-Analyse erforderlichen Kosten wird zwischen zwei Situationen unterschieden:

1. Situation ohne Schadensfall (die strategische Ebene), in der die Maßnahmen zwar umgesetzt wurden, aber nur, um für den Schadensfall vorbereitet zu sein.

[36] Damit ist der interne Zinsfuß oder IRR derjenige Zinssatz, den man bei vollständiger Fremdfinanzierung einer kreditgebenden Bank maximal zahlen kann, damit das Projekt insgesamt gerade noch tragfähig ist. Anders ausgedrückt, ist es aber auch die Kapitalverzinsung, die ein Eigenkapitalgeber für das insgesamt gebundene Kapital erwarten kann. Sind die Kreditzinsen oder die Renditeerwartung des Kapitalgebers höher als der IRR, dann ist das Projekt nicht wirtschaftlich.

2. Die Situation des Schadenseintritts (die taktische Ebene) einschließlich der damit verbundenen Reaktionen bzw. Aktivitäten.

Auf der **strategischen Ebene** wird bestimmt, was zu tun ist, um beispielsweise für die nächsten 25 Jahre vorbereitet zu sein, d.h. die Umsetzung der einzelnen Maßnahmen. Die für diese Ebene relevanten Kostenelemente sind die Investitionskosten bzw. die Anschaffungskosten für Ersatzteile (Transformator, Kabel etc.) und die Kosten für Lagerhaltung und Wartung der vorgehaltenen Ersatzteile. Um die Abschreibung der Kostenelemente beziffern zu können, sind wie die Lebensdauer der angeschafften Ersatzteile und die Häufigkeit der möglichen Nutzung erforderlich.

Für die die **taktische Ebene** sind alle Kosten, die als Reaktion auf einen Schadensfall entstehen, von Relevanz. Diese Kosten wurden aus den Simulationen abgeleitet und sind je nach Jahreszeit (Sommer und Winter) sowie den entgangenen Erlösen auf Basis der unterschiedlichen Vergütungsverträge unterschiedlich. Dabei wurden die Kosten berechnet 1. für den Schadensfall ohne Maßnahme (Ausgangsszenarien) sowie 2. für Kosten, die anfallen, wenn die Maßnahmen ergriffen wurden und der Schadensfall eintritt.

Für beide Ausgangsszenarien und den dazu gehörenden Maßnahmen wurde ein Excel-Modell erstellt. Dieses enthält eine Übersicht über die taktischen Kosten, die im Schadensfall eintreten, differenziert nach Jahreszeit und Vergütungsstufe pro entgangener kWh. In dem Berechnungsmodell werden die strategischen mit den taktischen Informationen kombiniert. Zur flexibleren Berechnung gibt es verschiedene Eingabe- und Auswahlfelder zur Festlegung der Kriterien. Dazu gehört zunächst ein Eingabefeld für kalkulatorische Zinsen für die Verzinsung des gebundenen Kapitals. In der aktuellen Niedrigzinsphase kann man hier von 2% bis maximal 4% ausgehen. Für die vorliegenden Berechnungen wird ein Zinssatz von 2% angesetzt. Dieser wird auch in den Beratungen zur BVWP 2015 empfohlen.[37]

Im Hinblick auf das gebundene Kapital würde man die Abschreibung nutzen, um das im jeweiligen Jahr bzw. das durchschnittliche gebundene Kapital zu errechnen. Das setzt aber voraus, dass über den Einsatz des Investitionsgutes Gewinne entstehen, die das gebundene Kapital stückweise „zurückfließen“ lassen. Das ist hinsichtlich der hier vorgeschlagenen Maßnahmen nicht der Fall, da die angeschafften Ersatzteile ja nur eine Art Versicherung darstellen. Aufgrund dessen werden die kompletten Anschaffungs- und Einlagerungs- bzw.

[37] Wissenschaftliches Expertengespräch zur Methodik der Nutzen-Kosten-Analyse, Berlin, 15.10.2013, unter Leitung von Dr. Gerhard Schulz, Leiter der Unterabteilung Grundsatzangelegenheiten, Investitionspolitik des BMVBS. Forschungsprojekt „Grundsätzliche Überprüfung und Weiterentwicklung der NKA im Bewertungsverfahren der BVWP“ Thema: Diskontierung, Prof. Dr. Thorsten Beckers, TU Berlin - WIP

Wartungskosten über den Gesamtzeitraum als gebundenes Kapital angesehen und entsprechend verzinst.

Ein weiteres Eingabefeld ermöglicht den Restwert des jeweiligen Ersatzteils einzugeben, da es denkbar ist, dass sowohl das Ersatzteil (Transformator) aus Maßnahme 1 als auch der zusätzliche Konverter aus Maßnahme 2 nach Ablauf von 25 Jahren über einen gewissen Restwert verfügen. Beläuft sich beispielsweise der Restwert des – ungenutzten – Transformators nach 25 Jahren auf 40% des Anschaffungspreises, werden nur 60% des Kaufpreises für den Abschreibungszeitraum angesetzt. In den vorliegenden Berechnungen wurde die Kalkulation mit Restwert jedoch nicht berücksichtigt. Um nachträgliche umfangreiche Änderungen zu vermeiden, wurde diese Möglichkeit jedoch im Vorfeld mit einbezogen.

Zusätzlich besteht die Möglichkeit, die Häufigkeit eines Schadensfalles auszuwählen. Da die Berechnung der Kosten und Nutzen auf theoretischer Ebene erfolgt, liegen keine Informationen vor, wann der Schadensfall eintritt. Aus diesem Grund werden sowohl die Kosten im Schadensfall als auch der Nutzen mit der möglichen Häufigkeit des Schadenseintritts – bezogen auf einen bestimmten Zeitraum – multipliziert. Für die Berechnung stehen dabei die folgenden Möglichkeiten zur Verfügung, die in einem entsprechenden Feld ausgewählt werden können.

- 1 Schadensfall innerhalb von 25 Jahren, d.h. eine Häufigkeit von 0,04
- 1 Schadensfall alle 10 Jahre, d.h. eine Häufigkeit von 0,1
- 1 Schadensfall alle 5 Jahre, d.h. eine Häufigkeit von 0,2
- 1 Schadensfall pro Jahr, d.h. eine Häufigkeit von 1

Bei unterschiedlicher Häufigkeit ändern sich die Logistikkosten bzw. die Kosten im Schadensfall insgesamt. D.h. bei dem hieraus resultierenden Nutzen handelt es sich um einen Erwartungswert, da dieser mit der Wahrscheinlichkeit der Eintrittshäufigkeit gewichtet ist. Zudem ist es möglich, die Jahreszeit, in der der Schadensfall eintritt, auszuwählen, da die Logistikkosten zur Schadensbehebung unterschiedlich ausfallen, abhängig von einem Ausfall im Sommer oder Winter. Auch die Höhe der Einspeisevergütung kann ausgewählt werden; diese ist notwendig zur Ermittlung der entgangenen Einnahmen. Sie basiert auf unterschiedlichen Verträgen, wobei die Höhe der Vergütung in erster Linie vom Jahr der Inbetriebnahme der OWEA abhängt. Zur Verfügung stehen dabei 3 Stufen:

- Vergütungsstufe 3,9 ct./kWh

- Vergütungsstufe 14,4 ct./kWh
- Vergütungsstufe 19,4 ct./kWh

Hinsichtlich des Abschreibungszeitraums ist es möglich, 10, 15, 20 oder 25 Jahre auszuwählen. Die vorliegende Analyse wurde jedoch mit einem Abschreibungszeitraum von 25 Jahren gerechnet, da dieser auch den Simulationen zugrunde lag.

Auf der folgenden Seite wird am Beispiel von Szenario 1 und der drei vorgeschlagenen Alternativen der Aufbau des Excel-Modells verdeutlicht. Zugrundegelegt wurden dabei kalkulatorische Zinsen in Höhe von 2%, eine Schadenshäufigkeit von 0,04. Der Schadenseintritt erfolgt im Winter, die Vergütungsstufe beläuft sich auf 3,9 ct./kWh. Für die Bewertungen der Szenarien werden die Ergebnisse differenziert nach verschiedenen Auswahlkriterien in Tabellen zusammengefasst. Die Tabelle zeigt dabei im oberen Bereich die erfassten strategischen Kosten, im unteren Bereich erfolgt die eigentliche Kosten-Nutzen-Analyse unter Einbeziehung der auf der taktischen Ebene erfassten Kosten und entgangenen Erlöse im Schadensfall. Dabei werden im ersten Jahr die vollständigen Investitionskosten (cash flow) aufgeführt, die über einen Zeitraum von 25 Jahren abgeschrieben werden, so dass im zweiten und allen übrigen Jahren das gebundene Kapital bzw. der Restwert aufgeführt werden. Als jährliche Kosten fallen hier die Abschreibungen an. Einbezogen werden weiterhin die jährlichen laufenden Kosten für Lagerhaltung und Wartung, die Kosten im Schadensfall und der erwartete Nutzen (im wesentlichen eingesparte Einnahmeausfälle), die beiden letzteren Positionen jeweils multipliziert mit der Eintrittswahrscheinlichkeit des Schadens.

**SZENARIO 1: Bauteil Konverter defekt**

| | | |
|---|---|---|
| Zinsen (kalkulatorische) | 2% | |
| | Eintragung möglich, sonst leer lassen | |
| Restwert Bauteil | | |
| Restwert Konverter | | |
| Restwert Kabel | | |
| | Eintragung möglich, sonst leer lassen, beläuft sich der Restwert nach 25 Jahren z.B. auf 40% des Anschaffungswertes, wird im letzten Jahr dieser Betrag abgezogen | |
| Strategisch (Kosten, die anfallen, um vorbereitet zu sein) | Die übrigen Kosten wie Lagerhaltung, Wartung werden nicht verändert | |

| | ② | ③ | ④ |
|---|---|---|---|
| **Investitionskosten** | **Standardisierung und Lagerhaltung von Großbauteilen** | **Standardisierung und Lagerhaltung Basis** | **Vermaschtes Netz** |
| **Bauteil** Investitionskosten | 11.000.000 | 11.000.000 | |
| Bauteil Lagerkosten pro Jahr (5.000€/Monat) | 60.000 | 60.000 | |
| Bauteil Wartungskosten pro Jahr (5.000€/Monat) | 60.000 | 60.000 | |
| **Konverter** Investitionskosten | | | |
| Konverter Wartungskosten pro Jahr (5.000€ pro Monat) | | | |
| **Kabel** Investitionskosten | | | 117.200.000 |
| Kabelverlegung | | | 7.435.000 |
| Kabel Wartungskosten (7.083,33€ pro Monat) | | | 85.000 |
| **STRATEGISCHE KOSTEN INSGESAMT** | **11.120.000** | **11.120.000** | **124.720.000** |

| | | |
|---|---|---|
| Häufigkeit des Schadensfalles AUSWÄHLEN | 0,04 | 1 Schadensfall innerhalb von 25 Jahren |
| Eintritt des Schadensfalles (Sommer/Winter) AUSWÄHLEN | Winter | |
| Einspeisevergütung AUSWÄHLEN | 3,9 ct./kWh | |

| | | Standardisierung und Lagerhaltung von Großbauteilen | Standardisierung und Lagerhaltung Basis | Vermaschtes Netz |
|---|---|---|---|---|
| **Bauteil (Trafo)** Investitionskosten | | 11.000.000 | 11.000.000 | 0 |
| Bauteil (Trafo) Lagerkosten pro Jahr (5.000€/Monat) | | 60.000 | 60.000 | 0 |
| Bauteil (Trafo) Wartungskosten pro Jahr (5.000€/Monat) | | 60.000 | 60.000 | 0 |
| **Konverter** Investitionskosten | | 0 | 0 | 0 |
| Konverter Wartungskosten pro Jahr (5.000€ pro Monat) | | 0 | 0 | 0 |
| **Kabel** Investitionskosten | | 0 | 0 | 117.200.000 |
| Kabelverlegung | | 0 | 0 | 7.435.000 |
| Kabel Wartungskosten (7.083,33€ pro Monat) | | 0 | 0 | 85.000 |
| **Investitionskosten insgesamt** | | **11.120.000** | **11.120.000** | **124.720.000** |
| Abschreibungszeitraum AUSWÄHLEN | | 25 | 25 | 25 |
| Häufigkeit des Schadensfalles pro Jahr | | 0,04 | 0,04 | 0,04 |
| **Kosten pro Schadensfall insgesamt** | | **45.109.002,92** | **90.741.788,75** | **103.621.588,04** |
| **Erwarteter Nutzen insgesamt** | | **164.281.325,63** | **118.648.539,79** | **105.768.740,50** |
| **JAHR 1** | **Kapitalkosten/Investition** | **11.000.000** | **11.000.000** | **124.635.000** |
| | Abschreibung Kapitalkosten | 0 | 0 | 0 |
| | Jährliche laufende Kosten | -120.000 | -120.000 | -85.000 |
| | Kosten im Schadensfall (Häufigkeit berücksichtig | -1.804.360 | -3.629.672 | -4.144.864 |
| | Erwarteter Nutzen (Erwartungswert) | 6.571.253 | 4.745.942 | 4.230.750 |
| | Netto-Nutzen | 4.646.893 | 996.270 | 886 |
| | Abgezinster Netto-Nutzen | 4.555.777 | 976.735 | 869 |
| | **Total Cashflow** | **-6.353.107** | **-10.003.730** | **-124.634.114** |
| | **Abgezinster Cashflow** | **-6.228.536** | **-9.807.578** | **-122.190.308** |
| **JAHR 2** | **Gebundenes Kapital/Restwert** | **11.000.000** | **11.000.000** | **124.635.000** |
| | Abschreibung Kapitalkosten | -440.000 | -440.000 | -4.985.400 |
| **ABGEZINSTER NETTO-NUTZEN** (Net Benefit) | | 85.690.247 | 11.705.003 | -96.130.860 |
| **BARWERT (abgezinster Cashflow)** Kapitalwert | | 82.715.985 | 9.261.671 | -122.173.346 |
| **AMORTISATIONSZEITRAUM** | | 2,40 | 12,32 | > 25 |
| **INTERNE KAPITALVERZINSUNG (IKV)** | | 73,1% | 8,6% | Keine IKV |

JAHR 1
•
•
JAHR 25

**Abbildung 7: Vergleichende Kosten-Nutzen-Berechnung der Maßnahmen am Beispiel**

Der Netto-Nutzen ergibt sich aus dem Erwartungswert des Nutzens abzüglich der jährlichen laufenden Kosten sowie den Kosten im Schadensfall. Der in der Tabelle aufgeführte Cash-

flow resultiert aus der Aufsummierung der Kapitalkosten und des erwarteten Nutzens abzüglich der jährlichen laufenden Kosten und der erwarteten Kosten im Schadensfall. Die Aufsummierung dieses jährlichen Cashflows über den Zeitraum von 25 Jahren ergibt den Barwert oder Gegenwartswert. Werden kalkulatorische Zinsen angesetzt, werden diese über den gesamten Zeitraum mit dem entsprechenden Wert abgezinst, ebenso wie der erwartete Netto-Nutzen. Im Falle der Aufsummierung der mit einem Kalkulationszinssatz auf einen Startzeitpunkt abgezinsten Netto-Cashflows der einzelnen Jahre spricht man vom Kapitalwert.

Der Amortisationszeitraum gibt das Jahr an, in dem der abgezinste Cashflow positiv wird. Ist dies über den gesamten Zeitraum von 25 Jahren nicht der Fall, rentiert sich die Maßnahme nicht. In diesem Fall ergibt sich keine, bzw. eine negative interne Kapitalverzinsung, da innerhalb der Laufzeit kein Zinssatz ermittelt werden konnte, um einen Kapitalwert (= Barwert oder auch Gegenwartswert) von Null zu erzielen.

### 6.1.6 Zusammenfassung der Ergebnisse der Bewertung

Die Bewertung der vom ISL vorgeschlagenen IT-Maßnahmen und Empfehlungen wurden auf qualitativer Ebene vorgenommen. Daneben war auch die betriebswirtschaftliche Betrachtung von Szenarien mit logistischem Hintergrund mit Auswirkungen auf die Bevölkerung Aufgabe des ISL.

**Ökonomische Bewertung der simulierten Szenarien**

Basis für eine ökonomische Betrachtung der logistischen Szenarien waren die Ergebnisse aus der Simulation. Mit Hilfe des Simulationsmodells zur Abbildung von logistischen Prozessen während der Betriebsphase von Offshore-Windparks wurde ermittelt, welcher Schaden beim Ausfall von energiewirtschaftlich relevanten Offshore-Komponenten auftreten und welche Kosten für die Wiederherstellung des Ursprungszustandes zu erwarten sind.

Im Szenario 1 „Defekte Konverterplattform“ zeigen die Ergebnisse der Kosten-Nutzen-Analyse, dass die Maßnahme „Standardisierung und Lagerhaltung von Großbauteilen“ – unter der Voraussetzung, dass in der Zukunft eine Standardisierung bei speziellen Großbauteilen denkbar ist – die empfehlenswerteste Maßnahme ist. Sollte eine Standardisierung nicht möglich werden, weil die Großkomponenten im Einzelnen zu speziell sind und eine passgenaue Abstimmung auf z.B. Konverter, Umspanner o.ä. weiterhin nötig ist, so ist zu prüfen, inwieweit die lange Herstellungsdauer für eine defekte Komponente verkürzt werden

kann, indem z.B. eine standardisierte Basiskomponente geschaffen wird, für die im Schadenfall dann die abgestimmten Spezialteile gefertigt und eingebaut werden müssten. Die Simulation erzeugt mit einer auf sechs Monate verkürzte Herstellungsdauer schon deutlich verbesserte Ergebnisse.

Bei einem Schadensfall alle 25 Jahre rechnet sich die Maßnahme „Vermaschtes Netz“ aufgrund der hohen Investitionskosten nur in den beiden höchsten Vergütungsstufen von 14,4 und 19,4 ct./kWh. Wird jedoch die Annahme getroffen, dass in einem Zeitraum von 10 Jahren mindestens ein Schaden dieser Größenordnung auftritt, amortisiert sich diese Maßnahme in allen Vergütungsstufen.

| | Standardisierung und Lagerhaltung von Großbauteilen | Standardisierung und Lagerhaltung Basiskomponente | Vermaschtes Netz *Drosselung 12,5%* | Vermaschtes Netz *Drosselung 40%* |
|---|---|---|---|---|
| 1 Schadensfall innerhalb von 25 Jahren (Häufigkeit 0,04 p.a.) | 3,9 ct./kWh:<br>Nach 2,4 Jahren (W)<br>Nach 1,9 Jahren (S)<br>14,4 ct./kWh:<br>Nach weniger als 1 Jahr<br>19,4 ct./kWh:<br>Nach weniger als 1 Jahr | 3,9 ct./kWh:<br>Nach 12,32 Jahren (W)<br>Keine Amortisation (S)<br>14,4 ct./kWh:<br>Nach 1,82 Jahren (W)<br>Keine Amortisation (S)<br>19,4 ct./kWh:<br>Nach 1,29 Jahren (W)<br>Keine Amortisation (S) | 3,9 ct./kWh:<br>Keine Amortisation<br>14,4 ct./kWh:<br>Nach 7,62 Jahren (W)<br>Nach 7,48 Jahren (S)<br>19,4 ct./kWh:<br>Nach 5,47 Jahren (W)<br>Nach 5,35 Jahren (S) | 3,9 ct./kWh:<br>Keine Amortisation<br>14,4 ct./kWh:<br>Keine Amortisation<br>19,4 ct./kWh:<br>Keine Amortisation |
| 1 Schadensfall innerhalb von 10 Jahren (Häufigkeit 0,1 p.a.) | 3,9 ct./kWh:<br>Nach weniger als 1 Jahr<br>14,4 ct./kWh:<br>Nach weniger als 1 Jahr<br>19,4 ct./kWh:<br>Nach weniger als 1 Jahr | 3,9 ct./kWh:<br>Nach 4,25 Jahren (W)<br>Keine Amortisation (S)<br>14,4 ct./kWh:<br>Weniger als 1 Jahr (W)<br>Keine Amortisation (S)<br>19,4 ct./kWh:<br>Weniger als 1 Jahr (W)<br>Keine Amortisation (S) | 3,9 ct./kWh:<br>Nach 13,77 Jahren (W)<br>Nach 14,06 Jahren (S)<br>14,4 ct./kWh:<br>Nach 2,90 Jahren (W)<br>Nach 2,85 Jahren (S)<br>19,4 ct./kWh:<br>Nach 2,11 Jahren (W)<br>Nach 2,07 Jahren (S) | 3,9 ct./kWh:<br>Keine Amortisation<br>14,4 ct./kWh:<br>Nach 23,95 Jahren (W)<br>Nach 19,14 Jahren (S)<br>19,4 ct./kWh:<br>Nach 15,14 Jahren (W)<br>Nach 12,25 Jahren (S) |

**Abbildung 8: Ergebnisse für das Szenario „Defekte Konverterplattform“**

Dies ist jedoch nur dann der Fall, wenn man von einer maximalen Drosselung der OWP von 12,5% ausgeht. Ist mit einer Drosselung von 40% zu rechnen, ist die Maßnahme kostenseitig nicht zu empfehlen.

Für das zweite Szenario „Defektes Exportkabel“ ist die Maßnahme „Standardisierung und Lagerhaltung von Großbauteilen“ für Exportkabel bereits umgesetzt. Dies bedeutet nicht, das jedes Kabel gleich ist und durch einen standardisierten Kabelstrang ersetzt werden könnte, sondern dass bereits bei Kabelverlegung 10% der verlegten Spezialkabel für einen eventuellen Schadensfall eingelagert werden. Bei der Bewertung wird dieser Ist-Zustand mit der Maßnahme „Vermaschtes Netz“ verglichen.

Für den Vergleich wurden in diesem Szenario zwei unterschiedliche Ausgangslagen definiert: Zum einen wird lediglich die Reparaturzeit des Kabels betrachtet und zum anderen die Reparatur mit einer vorgelagerten Sprengmittel-Räumung (UXO), die in den meisten Fällen

durchgeführt werden muss und die eine Wiederinbetriebnahme des Konverters deutlich verzögert. Beide Szenarien rechnen sich rein kostentechnisch betrachtet nicht bzw. nur unter unrealistischen Bedingungen. In diesem Szenario erscheinen die bereits ergriffenen Maßnahmen – die Vorhaltung von Kabeln – ausreichend, um Schadensfällen zu begegnen.

| | **Vermaschtes Netz** *Drosselung 12,5%* | **Vermaschtes Netz** *Drosselung 40%* |
|---|---|---|
| **1 Schadensfall innerhalb von 25 Jahren (Häufigkeit 0,04 p.a.)** | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Keine Amortisation | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Keine Amortisation |
| **1 Schadensfall innerhalb von 10 Jahren (Häufigkeit 0,1 p.a.)** | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Keine Amortisation | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Keine Amortisation |

| | **Vermaschtes Netz$_{UXO}$** *Drosselung 12,5%* | **Vermaschtes Netz$_{UXO}$** *Drosselung 40%* |
|---|---|---|
| **1 Schadensfall innerhalb von 25 Jahren (Häufigkeit 0,04 p.a.)** | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Nach 24,72 Jahren (nur im Sommer) | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Keine Amortisation |
| **1 Schadensfall innerhalb von 10 Jahren (Häufigkeit 0,1 p.a.)** | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Nach 11,99 Jahren (nur im Sommer)<br>19,4 ct./kWh: Nach 8,42 Jahren (nur im Sommer) | 3,9 ct./kWh: Keine Amortisation<br>14,4 ct./kWh: Keine Amortisation<br>19,4 ct./kWh: Keine Amortisation |

**Abbildung 9: Ergebnisse für das Szenario „Defektes Exportkabel“**

Die Kosten im Schadensfall nach Durchführung der Maßnahme „Vermaschtes Netz“ übersteigen die Kosten bei dem heute bereits gegebenen Zustand. Bei einer vorgelagerten Räumung von Sprengkörpern verringert sich der Kostenunterschied. Je länger die Ausfallzeiten durch eine solche Räumung, desto geringer ist die Kostendifferenz.

Wenn sich durch den Zeitraum für die Sprengkörper-Räumungsarbeiten die Ausfallzeiten in einem solchen Maße erhöhen, dass die Ausfallkosten die Investitionskosten für die Durchführung der Maßnahme übersteigen, rechnet sich die Durchführung dieser Maßnahme aus Kostensicht. Sollte diese Maßnahme aber zur Verringerung von Stromverlusten im Falle eines Konverterausfalls durchgeführt werden, so wäre gleichzeitig auch der finanzielle Schaden im Falle von Kabelschäden verringert. Die Durchführung der Maßnahme ist ebenfalls dazu geeignet, den finanziellen Schaden bei einem Interkonnektorausfall (Offshore-Verbindung zwischen Umspann- und Konverterplattform) zu reduzieren.

Sollte es in Zukunft möglich sein, einen Switch sofort und automatisiert bei Ausfällen durchzuführen, verringern sich Ausfallmenge und Kosten. Ein automatisierter Switch würde die Versorgungssicherheit der Bevölkerung erhöhen, da in Fällen solcher Schäden keine Stromunterbrechung stattfände.

## 6.2 Qualitative Bewertung von IT-Maßnahmen

Wie die ökonomische Bewertung deutlich zeigt, verursacht der Ausfall eines OWP erhebliche Kosten. Dazu gehören Einnahmeausfälle durch entgangene Einspeisevergütungen und die Kosten für die Wiederherstellung der Systeme. Auch bei erfolgreichen IT-Angriffen kann mit erheblichen Schäden gerechnet werden. Diese Angriffe sollen deshalb weitestgehend minimiert und ein Stillstand der OWP damit vermieden werden. Kosten für hierfür benötigte Maßnahmen liegen in wesentlich niedrigeren Bereichen als die der auf energiewirtschaftliche Belange ausgerichteten Maßnahmen. Auch kann ein durch einen erfolgreichen IT-Angriff erzeugter Schaden nicht genau beziffert werden, da nicht abgesehen werden kann, über welchen Zeitraum eine Stilllegung des OWP in Folge eines mutwilligen IT-Angriffs erfolgen wird. Aus diesem Grund soll die Bewertung auch nicht auf quantitativer sondern auf qualitativer Ebene aufzeigen, welche Maßnahmen mit oder ohne Kombination mit anderen Maßnahmen für einen verbesserten Schutz des OWP sorgen.

| Maßnahme | Nutzen | Kosten | Mitarbeiter-zufriedenheit | Image |
|---|---|---|---|---|
| Erhöhung der Netzwerksicherheit | ++ | mittel | ++ | ++ |
| Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern | ++ | mittel | ++ | ++ |
| Erhöhung des Netzwerkschutzes | ++ | niedrig | o | o |
| Bewusstsein für IT-Sicherheit stärken | + | niedrig | + | o |
| Firmware als Open Source Software | + | niedrig | o | o |
| Langfristige Bindung des Personals | + | niedrig | ++ | + |
| BSI Grundschutz Light | ++ | --- | + | + |
| IT-Sicherheitsgesetz auf OWP-Betreiber erweitern | + | --- | o | + |

**Abbildung 10: Kosten und Nutzen der IT-Maßnahmen als qualitative Größen**

Die Maßnahmen sind in der Tabelle nach den entstehenden Kosten sortiert. Die Kosten für die Umsetzung der Maßnahmen „BSI Grundschutz Light“ und „IT-Sicherheitsgesetz auf OWP-Betreiber erweitern“ liegen beim BSI bzw. beim Gesetzgeber.

Die beiden Maßnahmen „Erhöhung der Netzwerksicherheit“ durch Anomalieerkennung und „Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern“ haben den höchsten Nutzen, werden aber auch mit hohen Kosten eingestuft. Würden diese beiden Maßnahmen umgesetzt und eine Zertifizierung nach BSI Grundschutz oder BSI Grundschutz Light mit entsprechend umgesetzter Maßnahme „BSI Grundschutz Light“ erfolgt, würde dafür die Basis geschaffen werden, dass die OWP bereits dem IT Sicherheitsgesetz in wesentlichen Punk-

ten genügen: Die Zertifizierung belegt, dass die OWP den IT Sicherheitsanforderungen für IT Managementsysteme erfüllen, mit der Anomalieerkennung werden Eingriffe in das IT System proaktiv und auf dem neuesten Stand der Technik erkannt. Die Basis für den Austausch von Informationen erfolgt mit der Maßnahme „Austausch von Unregelmäßigkeiten zwischen OWP-Betreibern“, wobei hier auch die Plattform UPKRITIS genutzt werden kann.

Mit dem Ausbau der Offshore Windenergie gewinnt der Bereich eine wachsende Bedeutung und die OWP Betreiber sind gefordert, sich und damit das Gesamtsystem OWP angemessen hinsichtlich IT-Angriffen zu schützen.

# 7 Sensibilisierung für Prävention durch Planspiele

Für die Umsetzung der Maßnahme „Erhöhung der Netzwerksicherheit“ durch Anomalieerkennung, das vom ISL mit der höchsten Priorität zur Erhöhung der IT-Sicherheit belegt hat, wurde ein Planspiel erarbeitet, das dabei unterstützen soll, die betroffene Branche für die Notwendigkeit von präventiven Maßnahmen zur Erhöhung der Netzwerksicherheit zu sensibilisieren. Im Bereich IT-Sicherheit wird der Einsatz einer Anomalieerkennung als eine Maßnahme eingeschätzt, mit der technisch IT-Angriffe erkannt werden können, danach aber von IT-Administratoren eingestuft und bewertet werden müssen. Die Maßnahme ist eine präventive Maßnahme, mit der IT-Angriffe vorab abgewehrt werden könnten.

Der Projektpartner IFAM hat ebenfalls präventive Maßnahmen zu Szenarien definiert, die energiewirtschaftliche Auswirkungen auf die Bevölkerung haben könnten. Obwohl für die Sicherheit der offshore installierten Anlagen schon viele Maßnahmen getroffen werden, können terroristisch motivierte oder mutwillige Angriffe nie vollständig ausgeschlossen werden. Mit geeigneten präventiven Maßnahmen ist es jedoch möglich, den Schaden für die angeschlossenen OWP zu verringern, indem deren Ausfallzeiten verkürzt werden.

Wenn ein Konverter bzw. das an diesen angeschlossene Exportkabel so schwer beschädigt ist, dass der Konverter keinen Strom mehr abführen kann, sind die an den Konverter angeschlossenen OWP ebenfalls betroffen und müssen heruntergefahren werden. Obwohl diese keinen eigentlichen Schaden aufweisen, sind sie ohne geeignete Maßnahmen vom Land abgeschnitten und können bis zur Reparatur des Konverters bzw. des Exportkabels keinen Strom liefern. Dies bedeutet einen erheblichen finanziellen Schaden. Außerdem kann ein plötzlicher Ausfall einer Konverterplattform mit mehreren großen Windparks auch Auswirkungen auf die Stromversorgung der Bevölkerung haben.

Hier soll die präventive Maßnahme „Vermaschtes Netz“ zum Einsatz kommen. Bei einem Konverter- oder Kabelausfall muss ein Umschalten auf einen Ersatzkonverter durchgeführt werden, über den die betroffenen OWP ihren Strom bis zur Reparatur ableiten.

In die Erarbeitung des Planspiels für die präventive Maßnahme „Standardisierung und Lagerhaltung von Großbauteilen“ fließt das Vorgehen mit ein, dass heute bereits Ersatzkabel vorgehalten werden, um Kabelschäden schnell beheben zu können. Für das Szenario mit defektem Exportkabel wurde deshalb eine Übung zum vermaschten Netz vorbereitet. Andere Großkomponenten, z.B. Transformatoren können heute noch nicht auf Lager vorgehalten

werden. Aus diesem Grund wurden für dieses Szenario beide angesprochenen Maßnahmen in einem Planspiel verarbeitet.

Da eine Umsetzung der erarbeiteten Maßnahmen unterschiedliche Zeitrahmen umfasst, aber eine gemeinsame Basis für die Ausgangslage aller Planspiele vorhanden sein soll, wurde das Betrachtungsjahr der Ausgangslagen und der umgesetzten Maßnahmen auf das Jahr 2025 gesetzt.

## 7.1 Sensibilisierung für Prävention in der IT-Sicherheit

Das Planspiel besteht aus insgesamt drei Durchgängen, die unterschiedliche Ausgangslagen aufweisen. Ziel dieser Differenzierung ist es, eine Sensibilisierung für mögliche Gefahren zu erreichen und unterschiedliche Auswirkungen aufzuzeigen, je nachdem, welche Maßnahmen bei Beginn des jeweiligen Szenarios bereits getroffen wurden, um Gefahren abzuwenden und Auswirkungen zu minimieren. Der Ablauf gestaltet sich wie folgt:

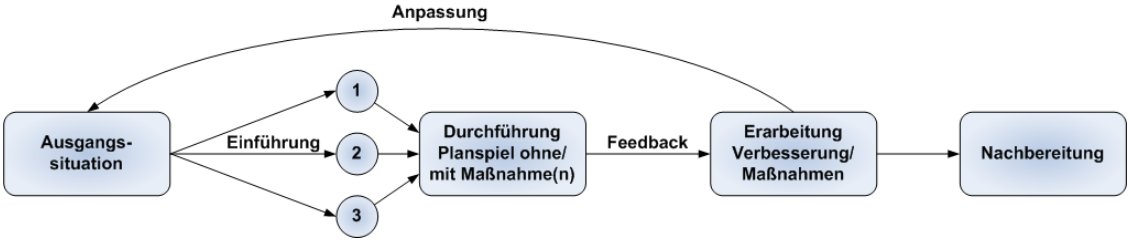



**Abbildung 11: Planspiel zur Sensibilisierung der Teilnehmer für die IT-Sicherheit**

Allen Durchgängen des Planspiels liegt die gleiche Art des Angriffs zugrunde. Dabei handelt es sich um die Kompromittierung einer Standardkomponente (in diesem Beispiel eine Kamera), die auf der Mehrzahl der OWEA verbaut ist und über eine eigene „Intelligenz“ in Form eines Betriebssystems mit allen Fähigkeiten der Netzwerkkommunikation verfügt.

Über ein empfohlenes Update der Firmware dieser Standardkomponente wird der Angriff zeitversetzt implementiert. Dabei soll zeitgleich ein Not-Stopp aller betroffenen OWEA provoziert werden, indem durch eine Fälschung von Messdaten die Steuerung selbst den Stopp auslöst. Um die Einsatzbereitschaft der Angriffssoftware mitzuteilen, sendet die Komponente ein einmaliges kurzes Datenpaket an eine Adresse im Internet, dessen Weg nicht nachvollziehbar ist und das Ziel nicht ausgemacht werden kann.

Das Planspiel beginnt im Jahre 2025. In der Nord- und Ostsee sind 28 OWP in Betrieb. Das entspricht einer Leistung von ca. 11 GW[38]. Weitere 16 OWP befinden sich in der Bauphase bzw. sind geplant. Der für das Planspiel betrachtete fiktive OWP „Windkraft“ ist im Jahr 2019 in Betrieb gegangen.

Beginnend mit einer Situation ohne Umsetzung von präventiven Maßnahmen werden den Teilnehmern nach jeder Planspielrunde Grenzen oder Schwachstellen aufgezeigt sowie mit ihnen über Maßnahmen und Verbesserungen in der Prävention diskutiert. Die erarbeiteten Maßnahmen und Verbesserungen fließen jeweils in die folgende Planspielrunde ein.

Ziel des Planspiels im Bereich IT ist es, Risiken aufzuzeigen, die ohne präventive Maßnahmen bestehen, die Teilnehmer so für Gefahren zu sensibilisieren und mit ihnen Lösungsvorschläge zu erarbeiten. Ziel des Planspiels ist ebenfalls, den Übenden die Auswirkungen eines IT-Angriffs sowie ihre Grenzen in der Schadensabwehr aufzuzeigen, ihnen zu vermitteln, welche Maßnahmen zur besseren Bewältigung einer Krisensituation hilfreich sind, und sie dafür zu sensibilisieren, präventive Maßnahmen zur Absicherung ihrer Netzwerke einzusetzen. Das Planspiel dient nicht dazu, mit den Teilnehmern neue Prozesse zu üben, sondern soll sie über die gespielten Szenarien auf Gefahren hinweisen, die schon abwendbar wären, für die aber ohne Prävention weiterhin ein Risiko besteht.

Die vorgeschlagenen Maßnahmen, wie die Anwendung einer Anomalieerkennung oder der Aufbau eines Informationsnetzwerkes, sind theoretisch schnell umsetzbar. Zwar hat sich das Bewusstsein für IT-Sicherheit bereits gewandelt, allerdings ist nach Einschätzung des ISL zu diesem Thema eine weitere Verbreitung von Informationen bei den Betreibern von Offshore-Windparks notwendig. Ziel ist zunächst die Abwendung eines Schadens nach einem mutwilligen IT-Angriff für den eigenen OWP. Durch den Zusammenschluss aller OWP-Betreiber in einem Informationsnetzwerk steigt die Wahrscheinlichkeit für ein rechtzeitiges Erkennen schädlichen Netzwerkverkehrs, so dass nicht nur der eigene Windpark, sondern der ganze Verbund profitiert.

In dem Planspiel wird das Potenzial in der Verbesserung der Schadensabwehr durch die vorgestellten Maßnahmen deutlich. Die Teilnehmer lernen, dass es mit relativ einfachen Mitteln möglich ist, dieses Ziel zu erreichen.

[38] Quelle: Bundesnetzagentur; Offshore-Netzentwicklungsplan 2025: Bestätigung; 25.11.2016; https://www.netzausbau.de/SharedDocs/Downloads/DE/2025/NEP/O-NEP2025_Bestaetigung.pdf, abgerufen am 27. Juli 2017

## 7.2 Sensibilisierung für Prävention im energiewirtschaftlichen Bereich

Auch im energiewirtschaftlichen Bereich liegt das Ziel der Planspiele in der Sensibilisierung der Teilnehmer für präventive Maßnahmen – hier jedoch zur Erhöhung der Sicherheit von Offshore-Windparks.

In den Vorarbeiten wurden Szenarien beschrieben, in denen den energiewirtschaftlichen Bereich betreffende präventive Maßnahmen einbezogen sind. Die Ausgangslage geht von einer Zerstörung von Großkomponenten, einer Konverterplattform und eines Exportkabels aus. Die entsprechenden präventiven Maßnahmen werden den Teilnehmern in einem zweistufigen Planspiel nahegebracht.

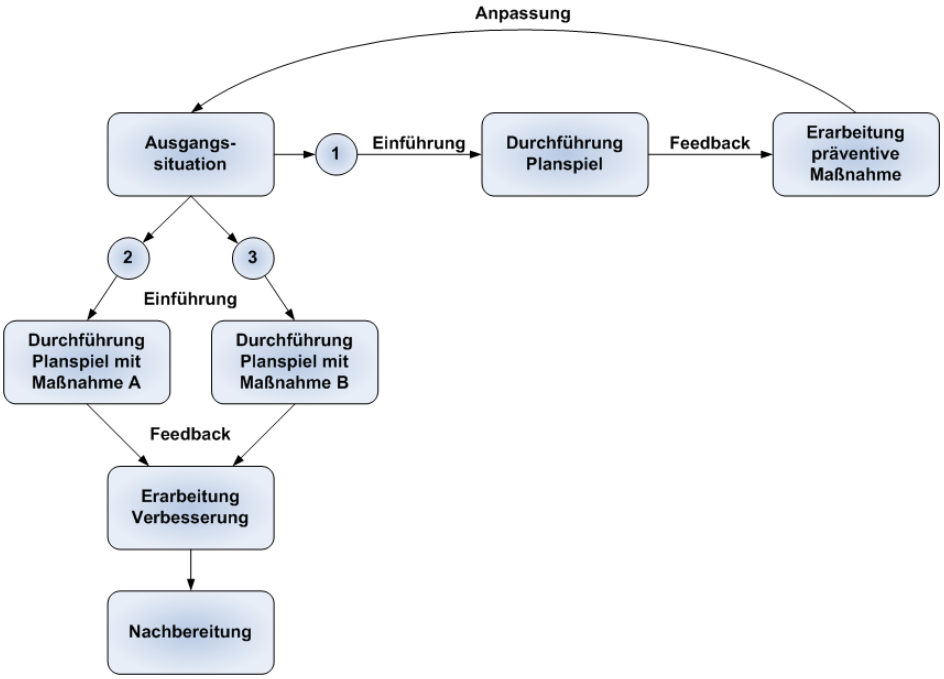



**Abbildung 12: Planspiel zur Sensibilisierung der Teilnehmer für die Sicherheit von OWP**

In der ersten Planspielrunde werden den Teilnehmern die Probleme aufgezeigt, die durch die Zerstörung einer Großkomponente auftreten: Vom möglichen Stromausfall an Land, über die angebundenen OWP, die zwar noch funktionsfähig, aber dennoch betroffen sind und bis zur Wiederherstellung der Großkomponente keinen Strom an Land abführen können, was hohe Ausfallkosten zur Folge hat.

Der Fokus wird für die jeweils zweite Planspielrunde nicht auf das Verhindern der Zerstörung – für die immer ein Risiko besteht – gelegt, sondern auf die Verkürzung der Ausfalldauer der betroffenen OWP. Die durch eine Maßnahme veränderte Ausgangslage im Schadensfall soll

dann in einem zweiten Durchgang durchgespielt und damit die Maßnahme auf ihre Eignung geprüft werden. Maßnahmen zur Verkürzung der Ausfalldauer bewirken veränderte Prozesse, die gemeinsam mit den Übenden in Planspielen durchspielt, anschließend bestätigt oder überarbeitet werden.

In den Planspielen sind über die Darstellung der präventiven Maßnahmen hinaus im Krisenfall weitere Abläufe erforderlich, auf die der Vollständigkeit halber als weitere Drehbücher mit Teilübungen, die für eine Darstellung der gesamten Prozesskette notwendig wären, hingewiesen wird. Die Ausarbeitungen dieser Teilübungen waren jedoch nicht Bestandteil des OWiSS-Projektes.

Heute ist eine Kapazität von mehr als 5.000 MW offshore installiert. Dies ist ein theoretischer Wert, der nur dann erreicht werden kann, wenn alle Anlagen durchgängig unter Volllast laufen. Nach dem Unternehmen Next Kraftwerke GmbH[39], gegründet aus der universitären Forschung, ist „ein Volumen zwischen 2.500 und 3.500 Megawatt Regelenergie“ erforderlich, um „alle Schwankungen im deutschen Stromnetz sicher ausgleichen zu können“. Für die Gewährleistung der Bereitstellung dieser Kapazität sind die Übertragungsnetzbetreibern verantwortlich.

Die Ausbaumenge offshore stellt bei einem Ausfall heute also noch kein Problem dar und könnte mühelos ausgeglichen werden. Jedoch wird die Ausbaumenge steigen und damit werden die Ausgleichsprobleme wachsen. Sollte dann zusätzlich an anderer Stelle ein Problem mit der Stromerzeugung auftreten, kann es passieren, dass ein Ausgleich der fehlenden Strommenge aus dem europäischen Stromnetz nicht ausreicht und in Folge dessen eine Auswirkung auf die Bevölkerung (bis zum flächendeckenden Stromausfall) zu spüren ist. Ein erheblicher finanzieller Schaden wäre eine der Folgen eines solchen Stromausfalls, der durch die Umsetzung einer präventiven Maßnahme zwar nicht vermieden, wohl aber erheblich verringert werden kann. Das Planspiel soll die Übenden deshalb für die Notwendigkeit präventiver Maßnahmen sensibilisieren. Die Durchführung von präventiven Maßnahmen lässt sich jedoch nicht in kurzer Zeit erreichen, sondern geht mit einer langen Planungs- und Durchführungsdauer einher. Aus diesem Grund kann die Übung dazu dienen, die Stromnetzbetreiber schon heute über mögliche präventive Maßnahmen zu informieren und ihnen die hierdurch verbesserte Situation aufzuzeigen.

[39] Quelle: https://www.next-kraftwerke.de/wissen/regelenergie

# 8 Fazit

Im Grünbuch des Zukunftsforums des Deutschen Bundestages[40] wird ein massiver Stromausfall als eines der beiden Schlüsselszenarien für die Bedrohung der zivilen Sicherheit genannt. Das enorme Wachstum in der Offshore-Branche stellt größte Herausforderungen an alle beteiligten Akteure, die diejenigen von Windenergieanlagen an Land bei weitem übersteigen: Die erschwerte Erreichbarkeit durch die Entfernung zum Land sowie die Wetterabhängigkeit bei Reparatur- und Wartungsprozessen wirken sich zudem erschwerend auf die Einhaltung eines reibungslosen Betriebs aus.

Die wachsende Bedeutung der Energieversorgung durch Offshore-Windenergie bedingt die Untersuchung möglicher Bedrohungslagen, welche die Energieversorgung beeinträchtigen könnten. Auf der Sicherstellung der Stromversorgung an Land und damit dem Schutz und der Sicherheit von Offshore-Infrastrukturen lag der Fokus des Verbundprojekts OWiSS. Die Betrachtung aller Sicherheitsaspekte während des Betriebs von OWP sowie der Auswirkung von Schadensfällen auf die Bevölkerung. war ebenfalls Teil des OWiSS-Projektes. Das Teilvorhaben OWiSS-ISL lieferte im Rahmen des Gesamtvorhabens einen signifikanten Beitrag zum Schwerpunkt „Schutz und Sicherheit von Offshore-Infrastrukturen“, da die Analyse, Maßnahmenkonzeption und Simulation und damit die Erprobung der Maßnahmenkonzepte (am Beispiel von logistischen Prozessen) einen Beitrag zur Sicherung der unterbrechungsfreien Energieversorgung von Bevölkerung und Wirtschaft aus regenerativen Energiequellen leistet.

Folgende Ergebnisse konnten im Rahmen des Teilvorhabens OWiSS-ISL erzielt werden:

- Es wurden Konzepte für verbesserte IT-Maßnahmen sowie Empfehlungen für einen erhöhten Schutz von Offshore-Windparks entwickelt. Diese Konzepte sind nicht offshore-spezifisch, sondern können auch auf andere Branchen übertragen werden.

[40] Quelle: Gerold Reichenbach, Ralf Göbel, Hartfrid Wolff, Silke Stokar von Neuforn; Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland; September 2008; http://zoes-bund.de/wp-content/uploads/2015/10/Gruenbuch_Zukunftsforum.pdf, abgerufen am 10. April 2016

- Das eingesetzte Simulationsmodell OWEA-Service (Simulation von Logistikprozessen in einem Offshore-Windpark oder einer Windparklandschaft während der Betriebsphase) wurde im Rahmen des Projektes um spezielle Wartungsprozesse (onshore-/offshore-Service), Offshore-Plattformen und Wohnschiffe, die Priorisierung von Aufträgen, Eingabeparameter wie Volllaststunden und Einspeisevergütung zur Auswertung der Stromausfallmenge/-kosten etc. erweitert und schließlich für die Abbildung der Auswirkungen von Schadensfällen von OWP-Clustern als Basis einer ökonomischen Bewertung von Maßnahmen eingesetzt.
- Für vergleichende Bewertungen von Maßnahmen und deren Alternativen wurde ein im ISL vorhandenes Excel-Kostenmodell für Kosten-/ Nutzenanalysen für die strategische und taktische Ebene weiterentwickelt. Die Ergebnisse der Simulationen flossen als Eingabedaten in das Bewertungsschema ein.
- Es wurden Vorlagen für Drehbücher entwickelt, die der Sensibilisierung der Offshore-Windparkbetreiber für die Durchführung präventiver Maßnahmen (im IT- und energiewirtschaftlichen Bereich) zum Schutz von Offshore-Windparks dienen. Diese bilden eine Grundlage für die Durchführung von Planspielen.