BEDEUTUNG DES RISIKOMANAGEMENTS FÜR DIE SICHERHEIT VON SMART GRIDS

Johannes GÖLLNER (1), Christian MEURERS (1), Andreas PEER (1)

Lucie LANGER (2)

Markus KAMMERSTETTER (3)

1) Bundesministerium für Landesverteidigung und Sport, Roßauer Lände 1, 1090 Wien
2) AIT Austrian Institute of Technology GmbH, Safety & Security Department, Donau-City-Straße 1, 1220 Wien
3) Technische Universität Wien, Institute of Computer Aided Automation, Treitlstraße 1-3, 1040 Wien

Kurzfassung:

Die Energieversorgung der Zukunft wird sich fundamental auf den Einsatz von IKT-Systemen stützen. Die damit verbundenen Risiken wirken sich unmittelbar auf die Sicherheit der Energieversorgung aus und stellen neue Bedrohungsbilder in diesem Bereich dar. Im Rahmen des KIRAS-Sicherheitsforschungsprogramms beschäftigt sich das Projekt *Smart Grid Security Guidance (SG)*^{2}, basierend auf einer fundierten Bedrohungs- und Risikoanalyse aus einer gesamtstaatlichen Sicht sowie auf Sicherheitsanalysen von Smart-Grid-Komponenten, mit einer systematischen Untersuchung von Smart-Grid-Technologien in Bezug auf IKT-Aspekte und der Erforschung von entsprechenden Gegenmaßnahmen zur Erhöhung der Sicherheit von IKT-Systemen in der kritischen Infrastruktur „Energie“.

Keywords: Energie, Bedrohung, Sicherheit, Kritische Infrastruktur, Smart Grid

1 Einleitung

Eine drastische Veränderung der Stromnetze ist derzeit im Gange. Konventionelle Wege zur Bereitstellung von Energie durch zentrale Versorger und bisherige Netztechnologien werden in Zukunft nicht mehr ausreichen, um die Energieversorgung unserer Gesellschaft sicherzustellen. Deshalb werden Informations- und Kommunikationstechnologien (IKT) zunehmend angewendet, um beispielsweise eine flexible Integration von Wind-, Solar- oder Biomasse-Energieerzeuger in das vorhandene Stromnetz zu ermöglichen. Diese Integration von Energie-Anbieter, Verbraucher, Erzeuger und Netzbetreiber mittels IKT bilden die Grundpfeiler für *Smart Grids*.

Mit dem zunehmenden Einsatz neuer Smart Grid Technologien entsteht parallel zum Stromnetz ein umfassendes IKT-Netz, dass durch seine große Ausdehnung und vielen Teilnehmer und Zugangspunkte ähnlichen Gefahren ausgesetzt sein wird wie beispielsweise derzeit das Internet. Allerdings wird die allgemeine Energieversorgung von diesem IKT-System abhängig sein, und ähnliche Sicherheitsprobleme wie im derzeitigen Internet hätten fatale Folgen. Potenzielle Bedrohungen reichen von Energiediebstahl durch Stromzählermanipulation, Angriffen auf Kontrollelemente der Netzbetreiber zur Störung des Betriebes bis hin zu großräumigen Abschaltungen des nationalen Stromnetzes beispielsweise aus terroristischen Motiven. Es ist daher unbedingt erforderlich, dass rechtzeitig Maßnahmen zur Gefahrenabwehr getroffen werden. Nur dann ist eine Zukunft für intelligente Stromnetze (Smart Grids) gewährleistet, ohne die Sicherheit der kritischen Infrastrukturen zu gefährden.

Das im Rahmen des Sicherheitsforschungsprogrammes KIRAS durchgeführte Projekt *Smart Grid Security Guidance* - (SG)² - hat das Ziel, solche Maßnahmen auf Basis einer umfassenden Bedrohungs- und Risikoanalyse zu erforschen. Das Projekt untersucht und entwickelt Methoden, Konzepte und Vorgehensmodelle, sowie begleitende Softwarewerkzeuge, um das Risiko durch die beschriebenen Bedrohungen zu minimieren, und die Sicherheit von Smart Grids in Österreich zu gewährleisten. Dazu werden neuartige Ansätze zur Modellierung komplexer IKT-unterstützter Smart Grid Architekturen definiert, und bilden die Grundlage für eine Analyse und Evaluation von primären Angriffsformen und Angriffsflächen, sowie zur Abschätzung von Folgewirkungen.

Diese Architekturmodelle werden im Hinblick auf Bedrohungen und Verwundbarkeiten untersucht, um die effizientesten Schutzmaßnahmen gegen mögliche Angriffe zu ermitteln. Bisher lag der Fokus von Netzbetreibern hauptsächlich auf Ausfallssicherheit ihrer Systeme – bösartige Angriffe, welche durch die fortschreitende Vernetzung der IT-Komponenten innerhalb ihrer Systeme leichter möglich werden, müssen in Zukunft aber ebenso berücksichtigt werden. Ein wichtiges Ergebnis des Projekts wird daher auch ein Katalog von Schutzmaßnahmen sein, um – nach deren Anwendung – die Sicherheit von Smart-Grids gegenüber IKT-basierten Bedrohungen gewährleisten zu können.

Zur realistischen Risikoabschätzung werden Sicherheitsanalysen von Smart Grid Komponenten durchgeführt, um die Bedrohungen und Verwundbarkeiten praktisch bewerten zu können. Da die Absicherung eines intelligenten Stromnetzes sehr komplex ist, werden weiters basierend auf existierenden Lösungen aus dem „allgemeinen“ IT Security Bereich

neue Software-Werkzeuge entwickelt, welche eine effiziente Anwendung der erforschten Richtlinien und Methoden in den speziellen Umgebungen der Energienetzbetreiber unterstützen.

Das Problem der Absicherung der Energieversorgung gegenüber Cyberangriffen ist weltweit ein Thema, und deshalb arbeiten weltweit auch viele verschiedene Organisationen und Unternehmen an Produkten und Lösungen in diesem Bereich. Auch erste Entwürfe von Richtlinien und Maßnahmen finden sich in Ergebnissen der Arbeiten beispielsweise von NIST in den USA und ETSI in Europa. Diese berücksichtigen jedoch keine österreichischen Aspekte, wie lokale Regulierungs- und Marktbedingungen, rechtliche Anforderungen und Netzstrukturen, weswegen diese Richtlinien nicht direkt in Österreich eingesetzt werden können. Die breite Zusammenarbeit von Energienetzbetreiben, staatlichen Stellen die mit dem Schutz kritischer Infrastrukturen betraut sind, Smart Grid Produktherstellern aus der Industrie und Experten im Bereich Informationssicherheit aus dem akademischen und privatwirtschaftlichen Bereich in diesem Projekt gewährleistet eine maximale Einbindung aller bisherigen internationalen und auch nationalen Entwicklungen in diesem Bereich, um darauf aufbauend neuartige, auf nationale Verhältnisse zugeschnittene Maßnahmen zur Realisierung eines zukünftigen sicheren und intelligenten Stromnetzes in Österreich zu erforschen.

2 Das Doppel-Vektoren Modell

Als Basis für die Bedrohungs- und Risikoanalyse dienen zunächst State-of-the-Art-Risikomodelle wie die BSI-Standards und IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik, die in den Bereichen der Informationstechnik und Risikoanalyse bereits ein weites Spektrum an Gefährdungen abdecken. Weiters werden Ergebnisse und Ansätze aus bereits durchgeführten Forschungsprojekten, wie beispielsweise das Doppelvektorenmodell, berücksichtigt.

Die Komplexität von Systemen und die Etablierung einer gemeinsamen Terminologie machen Kategorisierungsmodelle erforderlich, um Systemkomponenten und –elemente klassifizieren zu können. Dieser Ansatz garantiert einen normierten und analytischen Prozess, um Ergebnisse und verschiedene Elemente und Komponenten miteinander vergleichen zu können. Dazu wurde das sogenannte Doppelvektorenmodell auf Basis einer ersten Kategorisierungsebene (Metakategorisierungsebene) im Rahmen des BMLVS-internen Forschungsprojektes „Szenarioplanung und Wissensmanagement im ÖBH“ im Zeitraum 2010 – 2013 durch Johannes GÖLLNER, Klaus MAK, Christian MEURERS, Andreas PEER und Günther POVODEN entwickelt.

Die Kategorisierungs-Systematik des Doppelvektorenmodells ist in der nachfolgenden Abbildung dargestellt.

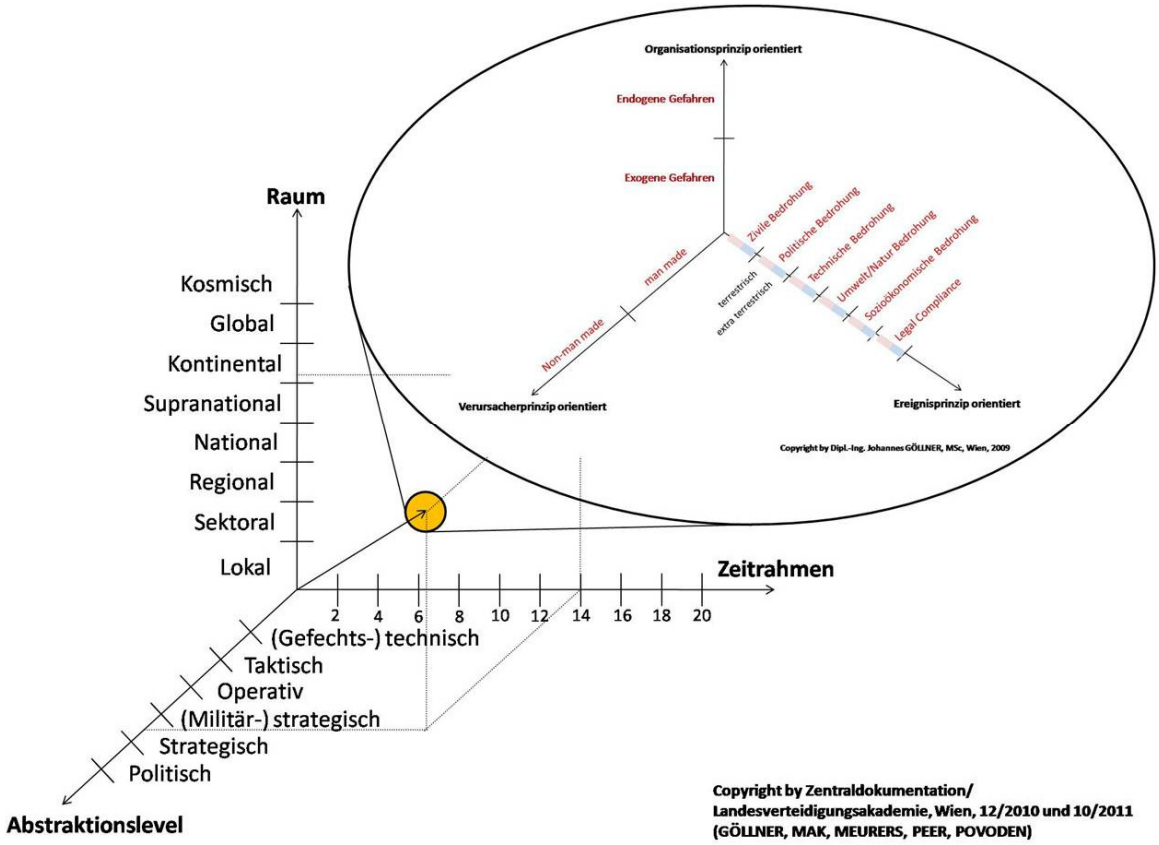

Abbildung 1 - Doppelvektorenmodell

Das Doppelvektorenmodell stellt ein dreidimensionales, mehrstufiges Meta-Klassifikationssystem dar, in dem jedes Element über die vektorale Zuordnung von definierten Eigenschaften und Attributen dargestellt und beschrieben werden kann.

Die erste Ebene unterscheidet die Ordinaten nach zeitlichen und räumlichen Aspekten und bietet einen organisations- bzw. ebenenspezifischen Abstraktionslevel an (politisch, strategisch, militärstrategisch, operativ, taktisch, gefechtstechnisch).

In der zweiten Ebenen wird das Ereignis kategorisiert hinsichtlich des Verursachers und ob Organisationsimmanente Gefahren einwirken oder resultieren. Zusätzlich kann/muss das Ereignis im Rahmen der Ereignisprinzip-Achse, auch unter Berücksichtigung des Ursprunges (terrestrisch, extraterrestrisch), weiter kategorisiert werden.

Das Doppelvektorenmodel bietet somit eine normierte Basis für weitere Analysen.

Nachfolgend sind die einzelnen Vektoren detailliert beschrieben:

- Vektor 1 [1], [2], [3], [4], [5], [6]:
  - Raum
    - Lokal
    - Sektoral
    - Regional

        - National
        - Supranational
        - Kontinental
        - Global
        - Kosmisch
    - Abstraktionslevel
        - (Gefechts-)technisch
        - Taktisch
        - Operativ
        - (Militär-)strategisch
        - Strategisch
        - Politisch
    - Zeitrahmen
        - Sekunde
        - Minute
        - Stunde
        - Tage
        - Wochen
        - Monate
        - Jahre
        - Jahrzehnte
        - Jahrhunderte
- Vektor 2 [7]:
    - Organisationsprinzip-orientiert
        - Exogene Gefahren
        - Endogene Gefahren
    - Verursacherprinzip-orientiert
        - Man-made
        - Non-man-made
    - Ereignisprinzip-orientiert (terrestrisch/extraterrestrisch)
        - Zivile Bedrohung
        - Politische Bedrohung
        - Technische Bedrohung
        - Umwelt/Natur Bedrohung
        - Sozioökonomische Bedrohung
        - Legal Compliance

Das Doppelvektorenmodell wurde in mehreren Anwendungsfällen erarbeitet, weiterentwickelt sowie getestet und stellt die Möglichkeit dar, ereignisrelevanten Inhalt zu dokumentieren und für weitere Analysen abrufbar zu Verfügung zu stellen. Auch lassen sich Muster zu diversen Ereignissen in spezifischen Kategorien damit erkennen, was einen weiteren Mehrwert im Rahmen dieses KIRAS Forschungsprojektes SG^2 darstellt.

3 Der $(SG)^2$-Risikokatalog

Im Rahmen des KIRAS-Projekts Smart Grid Security Guidance – (SG)2 wurde ein Risikokatalog für Smart Grids in Österreich entwickelt, welcher Energieversorgungsunternehmen dabei unterstützen soll, eine Risikoanalyse für ihr System durchzuführen. Ausgehend von der durch CEN-CENELEC-ETSI entwickelten Referenzarchitektur (Smart Grid Architecture Model) [8] wurde zunächst ein IKT-Architekturmodell für österreichische Smart Grids definiert, welches als Grundlage für den Risikokatalog diente.

Dazu wurden die IKT-Architekturen ausgewählter nationaler sowie internationaler Smart-Grid-Projekte auf SGAM abgebildet. In den meisten Fällen wurde bei Einordnung in das SGAM-Modell vorwiegend derjenige Teil des SGAM-Modells belegt, welcher den Domains Distribution, DER und Customer Premises, sowie den Zonen Process, Field und Station entspricht. Die Auswirkungen der Einführung von Smart Grids zeigen sich somit deutlicher im Mittel- und Niederspannungsnetz sowie bei der verteilten Erzeugung, da diese Bereiche bisher einen niedrigen Automatisierungsgrad aufweisen. Ergänzend zu den ausgewählten Pilotprojekten wurden auch Systemarchitekturen nationaler Energieversorgungsunternehmen betrachtet und auf SGAM abgebildet, wobei neben dem aktuellen Stand der Technik auch bereits kurz- bis mittelfristig absehbare Entwicklungen berücksichtigt wurden. Ergebnis dieser Auswertungen war schließlich ein IKT-Architekturmodell, welches die verschiedenen IKT-Komponenten und Kommunikationsverbindungen zwischen diesen aufzeigt. Dieses diente anschließend als Grundlage für den Bedrohungs- und Risikokatalog

Um die Bedrohungs- und Risikoanalyse nicht allzu komplex werden zu lassen, wurden die im Architekturmodell dargestellten Komponenten und Kommunikationsverbindungen zu den folgenden Domänen gebündelt:

- Funktionale Gebäude
- E-Mobilität
- Haushalte
- Erzeugungsanlage Niederspannung
- Erzeugungsanlage Mittelspannung
- Messstellen
- Umspannwerk (Hoch-/Mittelspannung)
- Umspannwerk (Mittel-/Niederspannung)
- Netzbetrieb
- Metering
- Energiehandel

Anschließend wurden, ausgehend von den IT-Grundschutz-Bedrohungskatalogen [9] sowie ergänzenden Dokumenten wie z.B. den einschlägigen BSI-Schutzprofilen [10][11], relevante

Bedrohungen identifiziert. Auf diese Weise entstand eine Liste von etwa 250 Bedrohungen, die jedoch zum Teil unterschiedliche Detaillierungsgrade aufwiesen. Um eine konsistente Darstellung zu erreichen, wurden diese Bedrohungen in weiteren Iterationen teils zusammengefasst und auf den Smart-Grid-spezifischen Kontext zugeschnitten. So entstand letztendlich ein Katalog von 31 Bedrohungen, welche verschiedenen Kategorien zugeordnet wurden. Diese Bedrohungen wurden anschließend im Rahmen des vorhandenen IKT-Architekturmodells evaluiert, d.h. es wurde untersucht, inwieweit die Bedrohungen auf die einzelnen Domänen zutreffen.

Anschließend wurde das Risikopotential dieser Bedrohungen bewertet, indem die Eintrittswahrscheinlichkeit und die Auswirkungen eines erfolgreichen Angriffs geschätzt wurden. Die Einschätzung erfolgte jeweils auf einer Skala von 1 (sehr gering) bis 5 (sehr hoch). Durch Multiplikation der beiden Werte ergibt sich das zu der jeweiligen Gefährdung gehörige Risikopotential. Dabei wurde das Risikopotential bei Werten <5 als „niedrig“, zwischen 5 und 12 als „mittel“ und ab 12 als „hoch“ eingestuft. Insgesamt lässt sich sagen, dass erfolgreiche Angriffe auf die dezentralen Komponenten beim Kunden (d.h. einzelne Haushalte) eine hohe Wahrscheinlichkeit und eher geringe Auswirkungen haben, während es sich bei den zentralen Komponenten v.a. im Netzbetrieb umgekehrt verhält. Zieht man jedoch in Betracht, dass erfolgreiche Angriffsmethoden beispielsweise auf Smart Meter öffentlich werden und sich entsprechend rasch verbreiten, so können die Auswirkungen auch hier gravierend sein und die Stabilität des Energienetzes maßgeblich negativ beeinflussen.

Der $(SG)^2$-Risikokatalog vermag keine individuelle Risikoanalyse eines konkret implementierten Systems zu ersetzen, kann jedoch Energieversorgern als Hilfestellung dienen, um Bereiche mit hohem Risikopotential zu identifizieren und ihre Gegenmaßnahmen hierauf zu fokussieren. Vorschläge zu geeigneten Sicherheitsmaßnahmen werden derzeit im Projekt $(SG)^2$ erarbeitet.

4 Auswertung & Ausblick

Vor allem durch die fortschreitende Transformation bestehender Energienetze zu Smart Grids und der damit verbundenen massiven Integration von Informations- und Kommunikationstechnologien (IKT) stehen Netzbetreiber heute vor der Herausforderung die dadurch entstehenden Risiken adäquat zu bewerten. Erst durch die Risikobewertung können kritische Bereiche identifiziert und in weiterer Folge besser geschützt werden. Diese Risikobewertung kann allerdings nur mittels Detailbetrachtung der bei den Netzbetreibern umgesetzten Systemlandschaft erfolgen. Eine auf die Gesamtarchitektur bezogene Risikobewertung fehlt jedoch häufig. Viele Netzbetreiber stehen daher heute vor dem Problem, zum einen auf keine geeigneten Risikomanagement Methoden im Smart Grid Bereich zurückgreifen zu können und, zum anderen, Risiken in der Smart Grid Gesamtarchitektur nicht erfassen zu können.

Im Gegensatz zu den im EURACOM FP7 Projekt analysierten bestehenden Methoden [13], verfolgt der im KIRAS-Projekt *Smart Grid Security Guidance – $(SG)^2$* entstandene Risikokatalog einen durch die Gesamtarchitektur getriebenen Ansatz. Durch die

architekturelle Bewertung in Bezug auf Risikopotential und Eintrittswahrscheinlichkeit erfolgt für die Netzbetreiber eine innerhalb des Smart Grids architekturbezogene Vorauswahl der bestehenden Risiken.

Durch Kombination der Gesamtarchitektur Risikobewertung mit der detailbezogenen individuellen Risikobewertung ermöglicht die Anwendung des (SG)² Risikokatalogs einen gesamtheitlichen Ansatz.

Sowohl die Gesamtarchitektur wie auch der (SG)² Risikokatalog wurden nicht nur in Abstimmung mit führenden Netzbetreibern und Herstellern entwickelt, sondern auch in mehreren Feedbackrunden mit den Mitgliedern des (SG)² Konsortiums evaluiert und kontinuierlich erweitert. Dadurch kann ein hoher praktischer Nutzungsfaktor gewährleistet werden. Der Hauptnutzen liegt dabei in der Möglichkeit Fragestellungen aus unterschiedlichen Expertendomänen klar formulieren und mittels einzelner Elemente des Architekturmodells gezielt beantworten zu können.

Im Spezifischen fanden folgende Evaluierungsschritte statt:

1. Evaluierung des Gefahrenkatalogs: Um den Gefahrenkatalog zu evaluieren und in Bezug auf seine Praktikabilität und Nähe zu realen Smart Grid Umgebungen zu evaluieren, wurden mehrere Workshops mit Experten aus den Bereichen Netzbetreiber, Hersteller sowie akademischer Forschungseinrichtungen durchgeführt. Im Zuge dieser Workshops wurden weitere Gefahren zum Gefahrenkatalog hinzugefügt, die besonders für die Smart Grid Domäne relevant sind.
2. Evaluierung der Gefahren: Um die jeweiligen Gefahren im Gefahrenkatalog zu evaluieren, wurden diese innerhalb des Architekturmodell von einem Expertenteam aus Netzbetreibern, Herstellern und akademischen Forschungspartnern in Bezug auf deren Kritikalität sowie der Abhängigkeitsverhältnisse geprüft. Die Ergebnisse wurden erneut innerhalb des Konsortiums diskutiert und gemeinsam mit den Netzbetreiben in Enduser-Workshops präzisiert.
3. Evaluierung in Bezug auf Eintrittswahrscheinlichkeiten und Auswirkungen: Im letzten Schritt fand in Bezug auf den Gefahrenkatalog eine Evaluierung der Eintrittswahrscheinlichkeiten und der Auswirkungen statt. Diese Evaluierung wurde im unabhängig von einer durch Experten aus den Bereichen Netzbetreiber, Hersteller und akademischen Forschungspartnern durchgeführt und widerspiegelt jeweils deren Einschätzungen. In einem gemeinsamen Workshop wurden die Ergebnisse schließlich konsolidiert und gemeinsam diskutiert sodass ein breiter Einsatzbereich des resultierenden Gefahren- und Risikokatalogs sicherzustellen.

5 Referenzen

[1] Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung - Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen, Schriftenreihe der National Defence Academy 13/2010, S.7, Vienna, Austria, Feber 2011, ISBN: 978-3-902670-53-3.

[2] Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: Wissensmanagement im ÖBH, Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung - Teil 3.A: Einführung in Szenarioentwicklung und Szenariomanagement-Grundlagen, Szenariotechnik und Szenarioplanung, Schriftenreihe der National Defence Academy 15/2010, S.37, Vienna, Austria, September 2011, ISBN: 978-3-902670-55-7.

[3] Vortrag: Hybridisation of Social Network Analysis in Contxt with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria (Johannes GOLLNER, Christian MEURERS, Andreas PEER, Guenter POVODEN), accepted paper at the 7th Social Network Conference 2011 at the University of Greenwich, London, United Kingdom, accepted: 13.05.2011 by Programme Committee, ppt.-presentation at the Conference 07.07.2011

[4] Vortrag: „Staatliche Sicherheit und Versorgungssicherheit am Beispiel Energie“: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen und deren Interaktionen mit Fokus Energie (Johannes GOLLNER, Andreas PEER), ppt.-Präsentation (Seite 33) iRd World Energy Council-Landesverteidigungsakademie- Symposion am 13.10.2011 an der Landesverteidigungsakademie, Wien.

[5] Vortrag: Soziale Netzwerkanalyse –SNA iRd Wissensmanagement-Forschungsprojektes „Szenarienplanung und WM“ des ÖBH: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen unter Berücksichtigung der SNA (Klaus MAK, Johannes GOLLNER), ppt.-Präsentation (Seite 17+18) iRe geladenen Vortrages Bundeskriminalamt des BMI, November 2011, Wien.

[6] Vortrag/Briefing: Beispiel- und modellhafte Darstellung einer Risikoanalyse (Johannes GOLLNER), ppt.-Präsentation (Seite 16) iRd Raiffeisen Akademie-LG für Bankmanager an der Landesverteidigungsakademie Wien, 27.02.2012, Wien.

[7] Göllner, Johannes, Eigendefinition von 06/2009, Vorlesungspräsentation an der Donau Universität Krems iRd LVA Risikomanagement; Integraler Bestandteil der internen Publikationen und Vortragsreihen der LVAk [3]-[6]

[8] CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, Document for the M/490 Mandate, Version 3.0, 2012

[9] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standards 100-1 bis 100-4, 2008, aktuelle Version erhältlich unter https://www.bsi.bund.de/

[10] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0073), Version 1.2, 2013

[11] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0077), Version 1.0, 2013

[12] FP7 project EURACOM, http://www.eos-eu.com/?Page=euracom