ENDBERICHT

SMARTMETERIDS

Intrusion Detection in einer Smart Metering Infrastruktur

FFG Projektnummer	843805	**eCall Antragsnummer**	4152268
Kurztitel	SmartMeterIDS	**FörderungsnehmerIn**	Fachhochschule St. Pölten ForschungsGmbH
Bericht Nr.	1	**Berichtszeitraum**	1.6.2014 – 31.3.2016
Bericht erstellt von	Paul Tavolato		

Inhaltsverzeichnis

ENDBERICHT 1
1 Ziele und Ergebnisse 3
2 Arbeitspakete und Meilensteine 6
2.1 Übersichtstabellen 6
2.2 Beschreibung der im Berichtszeitraum durchgeführten Arbeiten 7
2.2.1 AP 1: Auswahl eines Beschreibungsverfahrens 7
2.2.2 AP 2: Definition des formalen Modells der Smart Meter Infrastruktur 8
2.2.3 AP 3: Untersuchung und Berücksichtigung der Datenschutz-Aspekte 17
2.2.4 AP 4: Definition der technischen Überwachungsparameter und –regeln 18
2.2.5 AP 5: Entwicklung der Richtlinien und organisatorischen Maßnahmen zur Überwachung 24
2.2.6 AP 6: Überprüfung der Regeln im Pilotprojekt 26
2.2.7 AP7: Proof-of-concept Implementierung des IDS 26
2.3 Änderungen im Projektverlauf 31
3 Projektteam und Kooperation 32
4 Wirtschaftliche und wissenschaftliche Verwertung 33
5 Erläuterungen zu den Kosten 35
6 Projektspezifische Sonderbedingungen und Auflagen 36
7 Meldungspflichtige Ereignisse 37

1 Ziele und Ergebnisse

- Wurden die dem Förderungsvertrag zugrunde liegenden Ziele erreicht? Sind diese Ziele noch aktuell bzw. realistisch? (Achtung: Änderungen von Zielen erfordern eine Genehmigung durch die FFG)
- Vergleichen Sie die Ziele mit den erreichten Ergebnissen.
- Beschreiben Sie „Highlights“ und aufgetretene Probleme bei der Zielerreichung.

Ziel des Projekts war die Erforschung und Entwicklung eines Verfahrens zur laufenden automatischen Überwachung einer Smart-Meter-Infrastruktur während des Betriebs, um mögliche Angriffe erkennen und geeignete Gegenmaßnahmen ergreifen zu können. Dieses Ziel sollte durch einen White-Listing Ansatz erreicht werden, der verschiedene Ebenen der Kommunikation im Smart Meter Netzwerk umfasst. Außerdem sollte eine Proof-of-Concept Implementierung eines solchen Systems realisiert werden. Dieses Ziel konnte erreicht werden: Es wurde im Rahmen eines formalen Modells des Smart Meter Netzwerks auf zwei unterschiedlichen Ebenen Regeln des Normalverhaltens des Netzwerks ermittelt und für die Überwachung der Einhaltung dieser Regeln wurde ein Intrusion Detection System als Proof-of-Concept implementiert und im Rahmen realer Daten aus dem operativen Betrieb eines Projektpartners, der Wels Strom GmbH, überprüft. Zudem wurden die Aspekte des Datenschutzes, die im Zusammenhang mit dem Betrieb eines derartigen Systems auftreten, untersucht und liegen in Form eines Datenschutzberichts vor. Ein weiteres Ziel war die Entwicklung organisatorischer Richtlinien und Maßnahmen, die im Rahmen bestehender Sicherheitszertifizierung wie ISO 271001 durch den Betrieb von Smart Meter Netzwerken erforderlich werden.
Die Zeile bezüglich Datenschutz und organisatorischer Richtlinien und Maßnahmen konnten voll erreicht werden. Auch das Hauptziel, die Entwicklung eines Überwachungssystems samt Proof-of-Concept Implementierung konnte erreicht werden.
Eine kleine Einschränkung stellt die Beschränkung auf zwei Ebenen der Überwachung dar. Ursprünglich waren drei Ebenen geplant: Die unterste Ebene sollte Regeln auf der syntaktischen Ebene der verwendeten Protokolle erstellen und überwachen, auf der mittleren Ebene standen die Befehlsfolgen, die im Smart Meter Netzwerk übertragen werden, im Mittelpunkt und auf der obersten Ebene sollten Verbrauchsdaten auf ihre Plausibilität überprüft werden.
Die unterste Ebene – Erstellung und Überwachung von Regeln auf der syntaktischen Protokollebene – musste als nicht realisierbar zurückgestellt werden, da es nicht möglich war, die dafür unbedingt notwendigen technischen Detailinformationen über die tatsächlich verwendeten proprietären Protokolle mit verhältnismäßigem Aufwand zu beschaffen. Mit diesen Informationen wird von den Herstellerfirmen aus Sicherheitsgründen sehr restriktiv

umgegangen. Auch der Hinweis auf ein Forschungsprojekt machte es nicht möglich, einfach (und vor allem ohne hohen finanziellen Aufwand) an diese Informationen zu gelangen. Das Projekt hat allerdings gezeigt, dass das keine allzu große Einschränkung darstellt. Einerseits sind diese Informationen sehr produktspezifisch und können daher kaum produktübergreifend verwendet werden (was dann wieder nicht im Sinne eines auf Allgemeingültigkeit abzielenden Forschungsprojekts ist) und andererseits sind auch die Aussagen auf dieser Ebene nur bedingt im Sinne einer Sicherheitsüberwachung auswertbar.
Das Projekt hat sich daher vor allem auf die mittlere Ebene konzentriert, auf der eine detaillierte Betrachtung der Befehlsfolgen möglich ist, die eine ausreichend detaillierte Möglichkeit zur Definition des Normalverhaltens eines Smart Meter Netzwerks bieten. Die Regeln für das Normalverhalten des Systems (der Kommunikation im Smart Meter Netzwerks auf Befehlsebene) wurden mit Hilfe von Verfahren des automatischen Lernens (Machine Learning) ermittelt und einer empirischen Prüfung unterzogen. Das hat unter anderem auch den Vorteil, dass ein eventuell geändertes Kommunikationsverhalten des Systems auf Grund geänderten Nutzerverhaltens oder auf Grund geänderter organisatorischer Rahmenbedingungen beim Netzbetreiber (Verwendung anderer Hardware- oder Software-System, andere Auslese- oder Abrechnungsintervalle und Ähnliches mehr) kein Problem mehr darstellt, da in einem solchen Fall nur die Lernphase des Systems wiederholt werden muss, um neue, auf das geänderte Kommunikationsverhalten des Systems abgestimmte Regeln zu ermitteln.
Die dritte Ebene, die Ebene der Verbrauchsdaten wurde ebenfalls in Betracht gezogen und entsprechende Auswertungen und Vergleich wurden vorgenommen. Allerdings liegen in Bezug auf die Vorhersage dieser Daten (und dem Vergleich mit tatsächlich verbrauchten Werten) bereits sehr viele Forschungsergebnisse vor, die direkt umsetzbar sind. Daher wurde dieser Bereich zwar untersucht und entsprechende Modelle entwickelt, von einer Umsetzung im Rahmen der Proof-of-Concept Implementierung wurde jedoch abgesehen, da es auf Grund bereits existierender Lösungen wissenschaftlich nicht ergiebig gewesen wäre.

Als Highlights des Projekts ist die Erforschung und Entwicklung einer Methode der laufenden Überwachung eines Smart Meter Netzwerks anzusehen. Die Methode basiert auf einem White-Listing-Ansatz. Aus Netzwerkdaten eines normal operativen Netzwerks (das nicht einem Angriff ausgesetzt ist) werden mit Hilfe von Methoden des automatischen Lernens (Machine Learning) Muster abgeleitet, die das Normalverhalten des Netzwerks möglichst gut beschreiben. Diese Muster werden dann zur Überwachung des laufenden Betriebs eingesetzt. Der aktuelle Netzwerkwerkverkehr wird mit den Mustern abgeglichen. Kommt es zu einer Diskrepanz, die über einer bestimmten Schwelle liegt, wird ein Alarm ausgelöst. Zusätzlich wurden Vorgangsweisen im Rahmen des organisatorischen Sicherheitskonzepts definiert, wie mit solchen Alarmen weiter zu verfahren ist.

Als Ergebnis des Projekts liegt Folgendes vor:

1) Ein Simulationsmodell eines Smart Meter Netzwerks, das zum Durchspielen verschiedener Szenarien eingesetzt werden kann. Damit können beispielsweise Szenarien mit unterschiedlichen Konfigurationen getestet werden und der in diesen Konfigurationen – unter Annahme bestimmter Parameter – entstehende Netzwerkverkehr kann beobachtet und analysiert werden.
2) Ein Programm, das aus gegebenen Netzwerkverkehrsdaten mit Hilfe von Algorithmen des maschinellen Lernens Muster ableitet, die das (Netzwerk-) Verhalten des Systems beschreiben.
3) Ein Programm, das aktuellen Netzwerkverkehr als Input nimmt und ihn mit diesen Mustern vergleicht; dabei wird ein Abweichungsprofil erstellt. Überschreiten die Abweichungen einen bestimmten Grenzwert (der in Abhängigkeit von der tatsächlichen Situation individuell festgelegt werden muss), wird ein Alarm ausgelöst.
4) Ein organisatorisches Rahmenmodell für Sicherheitsmaßnahmen in einem Unternehmen, das ein Smart Meter Netzwerk betreibt.
5) Ein Gutachten zu den Datenschutzaspekten, die beim Betrieb eines Smart Meter Netzwerks zu beachten sind. Das Gutachten bezieht auch die europäische Datenschutz-Grundverordnung (DSVG) mit ein und beachtet auch – so weit möglich – Anforderungen, die sich aus dem neuen europäischen Datenschutzrechtsrahmen ergeben werden, der 2018 rechtswirksam werden wird.

2 Arbeitspakete und Meilensteine

2.1 Übersichtstabellen

- Erläuterung: Die Tabellen sind analog zum Förderungsansuchen aufgebaut Basistermin: Termin laut Förderungsansuchen bzw. laut Vertrag gültigem Projektplan Akt. Planung: Termin laut zum Zeitpunkt der Berichtslegung gültiger Planung.

AP Nr.	Arbeitspaket Bezeichnung	Fertig-stel-lungs-grad	Basistermin		Aktuell		Erreichte Ergebnisse / Abweichungen
			Anf.	Ende	Anf.	Ende	
1	Auswahl eines Beschreibungs-verfahrens	100%	6/14	7/14	10/14	11/14	Die eigentliche Arbeit am Projekt hat auf Grund von Verzögerungen beim Start des Pilotprojekts bei den Projektpartnern erst am 1.10.14 begonnen (es wurde die entsprechende kostenneutrale Verlängerung genehmigt).
2	Definition des formalen Modells der Smart Meter Infrastruktur	100%	8/14	10/14	12/14	2/15	
3	Untersuchung und Berücksichtigung der Datenschutz-Aspekte	100%	6/14	12/14	10/15	3/16	Da dieses AP unabhängig von den anderen ist, konnte über die zeitliche Einbettung frei verfügt werden. Grund für die Verschiebung war, dass die neue EU Datenschutz-Grundverordnung, die Anfang 2016 erlassen wurde, noch mit einbezogen wurde.
4	Definition der technischen Überwachungs-parameter und –regeln	100%	9/14	2/15	1/15	6/15	
5	Entwicklung der Richtlinien und organisatorischen Maßnahmen zur Überwachung	100%	2/15	7/15	6/15	3/16	Die Fertigstellung der Ausarbeitung der Policies beim Projektpartner eww/ITandTEL wurde zum Projektende hin verschoben, um auch letzte Ergebnisse der technischen Entwicklung miteinbeziehen zu können
6	Überprüfung der Regeln im Pilotprojekt	100%	9/15	10/15	1/16	2/16	
7	Proof-of-Concept Implementierung des IDS	100%	5/15	11/15	8/15	3/16	
8	Projektmanagement	100%	6/14	11/15	10/14	3/16	Verzögerung bei der Erstellung des Abschlussberichts

Tabelle 1: Arbeitspakete

Meilen-stein Nr.	Meilenstein Bezeichnung	Basis-termin	Akt. Planung	Meilen-stein er-reicht am	Anmerkungen zu Abweichungen
1	Modell definiert	31.8..2014	28.2.2015	28.2.2015	
2	Technische Überwachungsparameter und -regeln definiert	31.12.2014	31.5.2015	31.5.2015	
3	Policies fertig	31.5.2015	31.10.2015	31.3.2016	Die Fertigstellung der Ausarbeitung der Policies beim Projektpartner eww/ITandTEL wurde zum Projektende hin verschoben, um auch letzte Ergebnisse der technischen Entwicklung miteinbeziehen zu können
4	Projektabschluss	30.9.2015	31.3.2016	20.6.2016	Verzögerungen bei der Erstellung des Abschlussberichts

Tabelle 2: Meilensteine

2.2 Beschreibung der im Berichtszeitraum durchgeführten Arbeiten

- Beschreiben Sie die im Berichtszeitraum durchgeführten Arbeiten, strukturiert nach den Arbeitspaketen.
- Konnten die Arbeitsschritte und –pakete gemäß Plan erarbeitet werden? Gab es wesentliche Abweichungen?
- Die Beschreibung beinhaltet ebenso eine allfällige Änderung der angewandten Methodik (Achtung: Änderungen an der Methodik und wesentliche Änderungen im Arbeitsplan erfordern eine Genehmigung durch die FFG!).

2.2.1 AP 1: Auswahl eines Beschreibungsverfahrens

In diesem Arbeitspaket wurden Beschreibungsverfahren untersucht, die für die formale Definition einer Smart Meter Infrastruktur geeignet sind. Prinzipiell kommen dafür Modelle aus der Logik, aus dem Bereich der formalen Sprachen, aus der Statistik und aus dem Bereich der Simulation in Frage. Um zu einer fundierten Entscheidung zu kommen, wurde zunächst eine detaillierte Analyse der Datenströme in Smart Meter Netzwerken vorgenommen. Dabei wurden die wesentlichen in diesem Bereich verwendeten Protokolle untersucht.
Die Ergebnisse dieser Datenstromanalysen sind im technisch-wissenschaftlichen Bericht, im

Anhang 1 „Datenstrom-Analysen in Smart Meter Netzwerken“ zusammengefasst.
Auf Grund dieser Ergebnisse wurde eine Simulation als geeignetes Verfahren für die formale Beschreibung des Smart Meter Netzwerks ausgewählt. Die Simulation hat zudem den Vorteil, dass neben den Analysen tatsächlicher Datenströme auch absichtlich irreguläre Datenströme untersucht werden können, die im Normalbetrieb nur selten auftreten. Es können also Einbrüche (Intrusions) simuliert werden, um auch solche Situationen nicht nur theoretisch sondern auch praktisch untersuchen zu können.

2.2.2 AP 2: Definition des formalen Modells der Smart Meter Infrastruktur

Modell - Simulation

Als abstraktes Modell einer Advanced Metering Infrastruktur wurde eine Multi-Agenten-basierte Simulation gewählt. Ein großer Vorteil dieses Ansatzes liegt darin, dass ein breites Spektrum von relevanten Systemverhalten darin abgebildet werden kann und dass Szenarien erzeugt werden können, die im regulären Betrieb nicht nachzustellen sind. Ein weiterer großer Vorteil ist die Generierung von Testdaten. Eine der größten Herausforderungen bei der Erstellung eines allgemein gültigen Modells stellen dabei die unterschiedlichen Entwicklungen und Umsetzungen unter den Hersteller dar.

MASON

Basis der Simulation ist das MASON Multiagent Simulation Framework. Dieses Framework wurde in einem speziellen Design erstellt, um eine große Anzahl von Agenten effizient auf einem einzelnen Rechner zu unterstützen. Die Funktionen von teilnehmenden Geräten in der Simulation wurden von den im Open Smart Grid Protokoll (OSGP) definierten Operationen abgeleitet. Das OSGP ist eine ergänzende Spezifikation zur Darstellung eines Models von am Smart Grid beteiligten Geräten, wie Smart Meter, Datenkonzentratoren und Kommunikations-proxies.

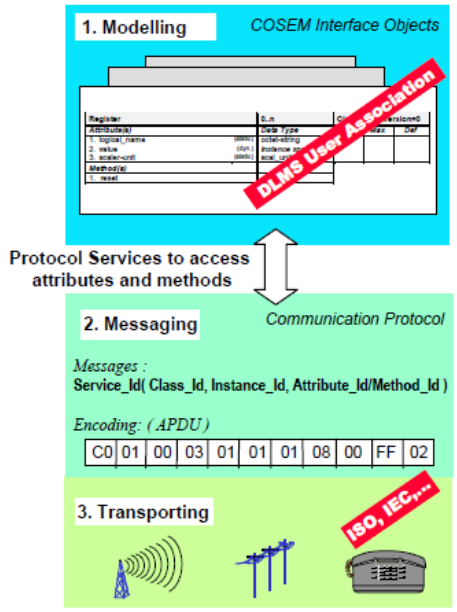
openMUC

Alternativ wurden andere, bereits bestehende Bibliotheken oder Spezifikationen betrachtet und getestet. Eine betrachtete Lösung ist das openMUC[1] Framework. openMUC enthält im Wesentlichen ein Java Framework für die Entwicklung und Implementierung von individuellen Monitoring- und Kontrolllösungen im Kontext von Smart Grid Komponenten. Die Java Bibliothek umfasst dabei folgende Kommunikationsstandards: IEC 61850, IEC 60870-5-104, DLMS/COSEM, M-Bus, IEC 62056-21, ASN.1 und SML. Die Software selbst verspricht einen kleinen Fußabdruck zu hinterlassen, da sie für embedded Umgebungen entworfen wurde. Die Implementierung ist zu 100% in Java und läuft auf allen gängigen Betriebssystemen (Linux,

[1] https://openmuc.org/

Windows, Mac) und CPU Architekturen (Intel und ARM).

openMUC enthält auch die Open Source Java Bibliothek jDLMS für die Kommunikation mit Smart Meter, die das DLMS/COSEM (Device Language Message specification/COmpanion Specification for Energy Metering) Protokoll standardisiert in IEC62056, verwendet. DLMS/COSEM ist ein objektbasiertes Protokoll, das speziell dafür entworfen wurde, unter Verwendung von verschiedenen darunterliegenden Protokollen einen generischen Weg zum Austausch von Daten zu ermöglichen. Zurzeit ermöglicht DLMS/COSEM die Kommunikation via HDLC (High-Level Data Link Control) über eine serielle Verbindung oder über TCP/IP und UDP/IP.



DLMS/COSEM

Die Spezifikation von DLMS/COSEM[2] wurde in den so genannten kolorierten Büchern beschrieben. Das blaue Buch enthält das COSEM Meter Objektmodel und das Objekt-Identifikationssystem. Beschrieben wird ein 3-stufiger Ansatz: Beginnend bei der Modellierung der Geräte und der Abdeckung dieser Geräte mit den verfügbaren Schnittstellen. Dabei werden generische Bausteine verwendet, um Funktionen zu beschreiben. Dieses Modell erlaubt jedoch keine internen oder implementierungsspezifischen Funktionen. Der zweite Schritt umfasst die Kommunikationsdienste und Protokolle zum Abbilden der Elemente des Datenmodells in Application Protocol Data Units (APDU). Der dritte Schritt enthält die Services und Protokolle für den Transport über einen Kommunikationskanal. Die Schritte zwei und drei werden im Green Book beschrieben. Das Yellow Book beschreibt Konformitätstests.

Das Blue Book enthält auch die Relation zu den OBIS Objekten. OBIS Kennzahlen dienen zur eindeutigen Identifikation von Messwerten und werden auch beim Datenaustausch zwischen den Geräten verwendet. Dabei gibt es definierte Codes für allgemein verwendete Einträge, die hauptsächlich Messwerte enthalten, daneben aber auch Eigenschaften von Messgeräten beschreiben.

[2] http://www.dlms.com

Dateneinheit	Schicht	Funktion	DLMS/COSEM
Daten	Applikation	Verarbeitung für die Applikation	jDLMS, Gurux Applikation
	Präsentation	Ent-/Verschlüsselung, maschinenabhängige Daten in maschinenunabhängige Daten konvertierten	COSEM
	Session	Interhost Kommunikation, Session Management unter den Applikationen	DLMS
Segment	Transport	End-to-End Verbindung, Flusskontrolle,	DLMS
Packet	Netzwerk	Logische Adressierung, Path determination	
Frame	Data Link	Physische Adressierung	HDLC oder IEC 62056-47
Bit	Physical	Medium, Signal und Binärübertragung	Serial, TCP/IP

Tabelle 1 DLMS/COSEM nach OSI

jDLMS

jDLMS implementiert diese wesentlichen Bestandteile und charakterisiert logische Geräte als einen Bestandteil von physischen Geräten. So kann ein physisches Gerät über mehrere logische Geräte verfügen. Server und Client benötigen nun Adressen, um eindeutig identifiziert werden zu können. Eine solche Adresse besteht aus der physikalischen Adresse eines Gerätes und aus der Adresse des logischen Gerätes. Die Adresse eines Clients hängt aber auch mit der Art der Kommunikation zusammen und besteht aus zumindest einem Byte. Dieses Byte entscheidet darüber, welche Objekte gelesen oder geschrieben werden können und für welche eine Authentifikation notwendig ist. Ein spezieller Identifikator ist hierbei der Wert 16, der den öffentlichen Client repräsentiert und für die wenigsten Rechte ohne Authentifikation steht. Objekte innerhalb eines Gerätes können auf zwei verschiedene Arten adressiert werden. Die empfohlene Art ist die Adressierung über den logischen Namen eines Objektes, dem OBIS Code, einer 6 Byte lange Zahl die eindeutig identifizierbar unter allen Smart Meter Geräten ist. Die zweite Art der Adressierung enthält eine 2 Byte lange Adresse und soll nur dann zur Anwendung kommen, wenn dies über die logische Adresse nicht möglich ist. Nachdem die Verbindung zu einem Gerät aufgebaut wurde, erfolgt die Kommunikation nach dem Request-Response Modell. Der Client sendet eine Anfrage nach einer spezifischen Aktion und nachdem die Anfrage bearbeitet wurde, erhält diese die entsprechende Antwort. Obwohl die Datenrepräsentation am Gerät objektbasiert gestaltet ist, ist der Zugriff nur in einem Attribut basierten Weg möglich. Eine Anfrage muss folgende drei Attribute beinhalten:

die Class ID, die Adresse des Objektes und eine Attribut ID. Ein Beispiel hierfür wäre der Zugriff auf die aktuelle Zeit eines Gerätes:

- Class ID: 8 (Clock class)
- Logical Name: [0, 0, 1, 0, 0, 255] (Current time)
- Attribute ID: 2 (Data)

Gurux

Ein weiteres Open Source Projekt, das sich DLMS als Schwerpunkt gesetzt hat, ist Gurux[3]. Gurux bietet Programme und Bibliotheken an, um darauf aufbauend ein Automated Meter Reading (AMR) System zu entwickeln. Die Verbindung zum Smart Meter kann dabei, ähnlich wie bei jDLMS, über TCP/IP, Terminal oder serielle Verbindung aufgebaut werden.

Eines der Tools, das von Gurux angeboten wird, ist die Gurux Device Suite. Die darin enthaltene Funktion des Device Publishers bietet Herstellern die Möglichkeit, Profile für physische Geräte anzulegen und für die Community zur Verfügung zu stellen. Mit Hilfe des Gurux Device Editors können die Templates verändert und an die eigenen Ansprüche angepasst werden. Der Gurux DLMS Director ist die Implementierung der Kommunikation mit den DLMS/COSEM Geräten und deckt folgende Standards ab:

- IEC 62056-21 Direct local data exchange
- IEC 62056-42 Physical Layer Services and Procedures for Connection-Oriented Asynchronous Data Exchange
- IEC 62056-46 Data link layer using HDLC protocol
- IEC 62056-47 COSEM transport layers for IPv4 networks
- IEC 62056-53 COSEM application layer
- IEC 62056-61 OBIS Object identification system
- IEC 62056-62 Interface objects

GuruxAMI kann als transparentes Gateway zwischen einer Applikation und einem Gerät fungieren. Mit dieser Funktion kann zum Beispiel eine Terminal-Verbindung durch eine GPRS Verbindung ersetzt werden und eine bestehende Head-End Applikation kann weiterhin vom Gerät lesen, ohne Änderungen am bestehenden System vorzunehmen.

iCube

Eine weitere Implementierung von DLMS/COSEM Kommunikationslösungen bietet icube[4] an. Neben Funktion, die denen von jDLMS und Gurux sehr ähnlich sind, gibt es eine ausführliche theoretische Beschreibung [1] von DLMS und der Kommunikation. Hinzu kommt ein Tool namens OBISHelper, womit es möglich ist, OBIS Codes mit deren Beschreibung zu codieren und decodieren (siehe Abbildung 1: OBIS Helper [2]). icube bietet weiters noch eine Beschreibung der sicherheitsrelevanten Funktionen von DLMS an bzw. deren

[3] www.gurux.fi

[4] http://www.icube.ch/

Implementierung in das Framework.

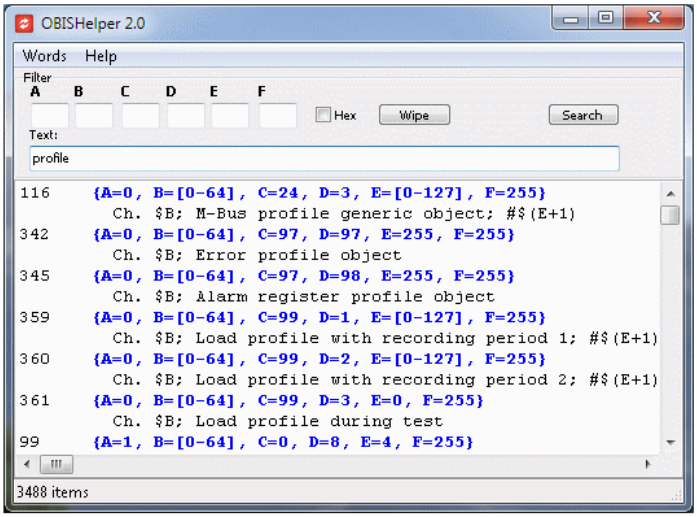


Abbildung 1: OBIS Helper [2]

Eine alternative zu DLMS/COSEM ist der vom amerikanischen Institut für Standards ausgestellte Standard ANSI C12.19 in Verbindung mit ANSI C12.22.
Aus den Datenblätter der im Projekt verwendeten Geräte geht hervor, dass ISKRAemeco Geräte den DLMS/COSEM Standard verwenden, die amerikanischen Hersteller von Echelon sich eher an ANSI C12.19 bzw. C12.22 halten.
Ein Projekt, das sich mit der Kontrolle für die anfallenden Stromkosten beschäftigt, ist volkszaehler.org[5]. volkszaehler.org ist ein freier intelligenter Stromzähler im Selbstbau, bei dem die anfallenden Stromprofile unter der Kontrolle des Nutzers verbleiben. Die Daten des Volkszaehlers sind nicht duch den Versorger auslesbar. Der Volkszaehler besteht aus 4 Modulen: Messen, Übertragen, Speichern und Auswerten. Die Messung des Stromverbrauchs erfolgt zB. über einen Hutschienenzähler mit S0-Schnittstelle oder mittels eines Smart Meters, der über eine optische Schnittstelle ausgelesen wird, auch alte Ferrariszähler oder Gaszähler können abgetastet werden. Die Übertragung erfolgt mit einem IR-Schreib-Lesekopf, einem Ferrariszähler-Lesekopf einem Reed-Kontakt (bei Gaszählern) oder einfach dem S0-Ausgang, die leitungsgebunden an ein folgendes LAMP-System angeschlossen werden. Ausgewertet wird mittels des LAMP Systems. Das kann ein Embedded-Computer (Raspberry PI, Banana Pi, Cubieboard, IOmega iConnect, Seagate Dockstar, SheevaPlug oder andere) oder auch eine Software (VM) auf einem normalen PC [3] sein.

Interessant sind auch Informationen über die verwendete Smart Meter Language. Hier ist

[5] http://volkszaehler.org/

festzuhalten, dass Echelon Zähler nicht den OBIS, sondern ANSI C12.18/19 verwenden. [4]

OSGP

Die wesentlichen Teile von OSGP sind Definitionen der Services. Diese Services werden im Folgenden aufgeführt:

Time-OfUseCalendar

Time-Of Use Calendar ermöglichen es den Energieversorgern, verschiedene Tarife zu unterschiedlichen Tageszeiten anzuwenden. Der Verbrauch wird für jeden Tarif separat aufgezeichnet.

Es werden bis zu 4 verschiedene Tarife unterstützt. Es können Pläne für Wochentage, Samstage, Sonntage und Feiertage jeweils für 4 verschiedene Jahreszeiten konfiguriert werden. Zudem können 15 Feiertage vorgegeben werden.

Pending Tables

Pending Tables ermöglichen es, Konfigurationsänderungen an vielen OSGP Geräten gleichzeitig aktiv zu schalten. Pending Tables werden im Voraus auf die einzelnen Geräte geschrieben, sie werden aber erst zu einem bestimmten Zeitpunkt (Trigger Date/Time) wirksam.

Es gibt Pending Tables unter anderem für den Kalender

Load Profile

Jedes OSP Gerät muss ein Lastprofil mit bis zu 16 Werten pro Messung aufzeichnen können. Diese Messungen erfolgen periodisch in festgelegten Intervallen.

Demand Metering

OSGP Geräte bieten verschiedene Methoden, um den maximalen Energiebedarf (und nicht den gesamten Verbrauch) über einen bestimmten Zeitraum zu ermitteln. Wenn dabei zusätzlich Mittelwerte verwendet werden, haben kurze Spitzen keine Auswirkungen.

Steuerausgänge

OSGP Geräte können über 2 Steuerausgänge verfügen. Der erste ist als Lasttrenner vorgesehen (Abschaltung bei Überschreitung einer maximalen Leistung oder Remote-Abschaltung), der zweite kann über einen Kalender oder Tarif geschalten werden.

Impulseingänge

Impulsausgänge von Gas- oder Wasserzählern können an OSGP Geräte angeschlossen werden. Der Zählerstand wird dann an den Data Concentrator übermittelt.

MBusundMEP

OSGP Geräte können 2 zusätzliche Kommunikationsports haben:

- Einen M-Bus Port, an den bis zu 4 Geräte angeschlossen werden können.
- Einen Multipurpose Expansion Port (MEP), über den Daten gelesen, bestimmte

Konfigurationen geschrieben sowie Methoden aufgerufen werden können.

Zugriff auf Tabellen

Es gibt Befehle für vollständiges sowie teilweises Lesen und Schreiben von Tabellen. Diese Unterscheidung ist notwendig, da jede Nachricht (inklusive Befehl) max. 144 Bytes groß sein darf. Zudem werden beim partiellen Lesen max. 84 Bytes und beim partiellen Schreiben max. 75 Bytes der jeweiligen Tabelle verarbeitet.

Lesen

Fullreadrequest:0x30 <table ID>

`Partial read request`: 0x3F < table ID> <offset> <count>

Werden mehr Bytes als vorhanden angefordert, dann wird mit Antwort mit 0 aufgefüllt und kein Fehler zurückgegeben.

`Response`: <nok>|<ok> <count> <data>

Schreiben

`Full write request`: 0x40 <table ID> <count> <data>

`Partial write request`: 0x4F <table ID> <offset> <count> <data>

Werden mehr Bytes übergeben als Platz in der Tabelle ist, dann werden die überschüssigen Bytes ignoriert und kein Fehler zurückgegeben.

Werden weniger Bytes übergeben als Platz in der Tabelle ist, dann werden nur die übergebenen Bytes überschrieben und kein Fehler zurückgegeben.

`Response`: <nok>|<ok>

Rückgabewerte

Die möglichen Rückgabewerte sind <ok> und <nok>.

<nok> steht dabei für einen der folgenden Rückgabewerte:

<nok> = <sns> | <onp> | <iar> | <bsy> | <dig> | <seq> | <inc> | <ica>

Response code	Responsevalue	Definition
<ok>	0x00	Acknowledge
<err>	0x01	Error
<sns>	0x02	Service Not Supported
<isc>	0x03	Insufficient Security Clearance
<onp>	0x04	Operation Not Possible
<iar>	0x05	Inappropriate Action Requested
<bsy>	0x06	Device Busy
<isss>	0x0A	Invalid Service Sequence State
<dig>	0x0B	Digest Error
<seq>	0x0C	Sequence Number Error
<inc>	0x0E	Incompatible Error
<ica>	0x0F	Interface Change

Neben den Services gibt es in OSGP auch detaillierte Definitionen zu den verwendeten Tabellen. Die in OSGP definierten Tabellen werden in folgende Gruppen eingeteilt:

1. Konfiguration
2. Informationen zum Gerät, dessen Status und dem Versorger
3. Uhrzeit, Datum und Kalender
4. Messwerte zum Stromverbrauch und Energienetz
5. Steuerausgänge
6. Verlauf und Ereignisprotokoll
7. Aufruf und Rückgabe von Methoden
8. Transaktionsmanagement
9. Warteschlangen
10. Pending Tables
11. Herstellerspezifische Tabellen
12. Testmodus
13. MBus und MEP Konfiguration

Lontalk

LonTalk Funktionen:

Das Format der PPDU (Physical Protocol Data Unit oder Frame) und NPDU (Network Protocol Data Unit oder Paket) ist immer gleich. Jedes Paket enthält das Feld *PDU Fmt*. Der Wert dieses Felds legt fest, welche Art von PDU (Protocol Data Unit) transportiert wird und dementsprechend welcher Service von LonTalk gewährleistet wird.

Network Layer

APDU (Application Protocol Data Unit) in NPDU gekapselt

- Unacknowlegded Unicast, Multicast und Broadcast
- Zustellung mit Wahrscheinlichkeit $p \leq 1$
- Keine Paketwiederholung, Empfangsbestätigung oder Segmentierung
- Natürliche Ordnung der Nachrichten bleibt bestehen

Transport Layer

TPDU (Transport Protocol Data Unit) in NPDU gekapselt, TPDU enthält wiederum APDU

- Reliable Multicast und Unicast
- Zuverlässige Zustellung nach dem Best-Effort-Prinzip (max. Anzahl an Wiederholungen)
- Erkennung von Duplikaten
- Vergabe von Transaktionsnummern um die Ordnung von ausgehenden Nachrichten zu gewährleisten

sowie

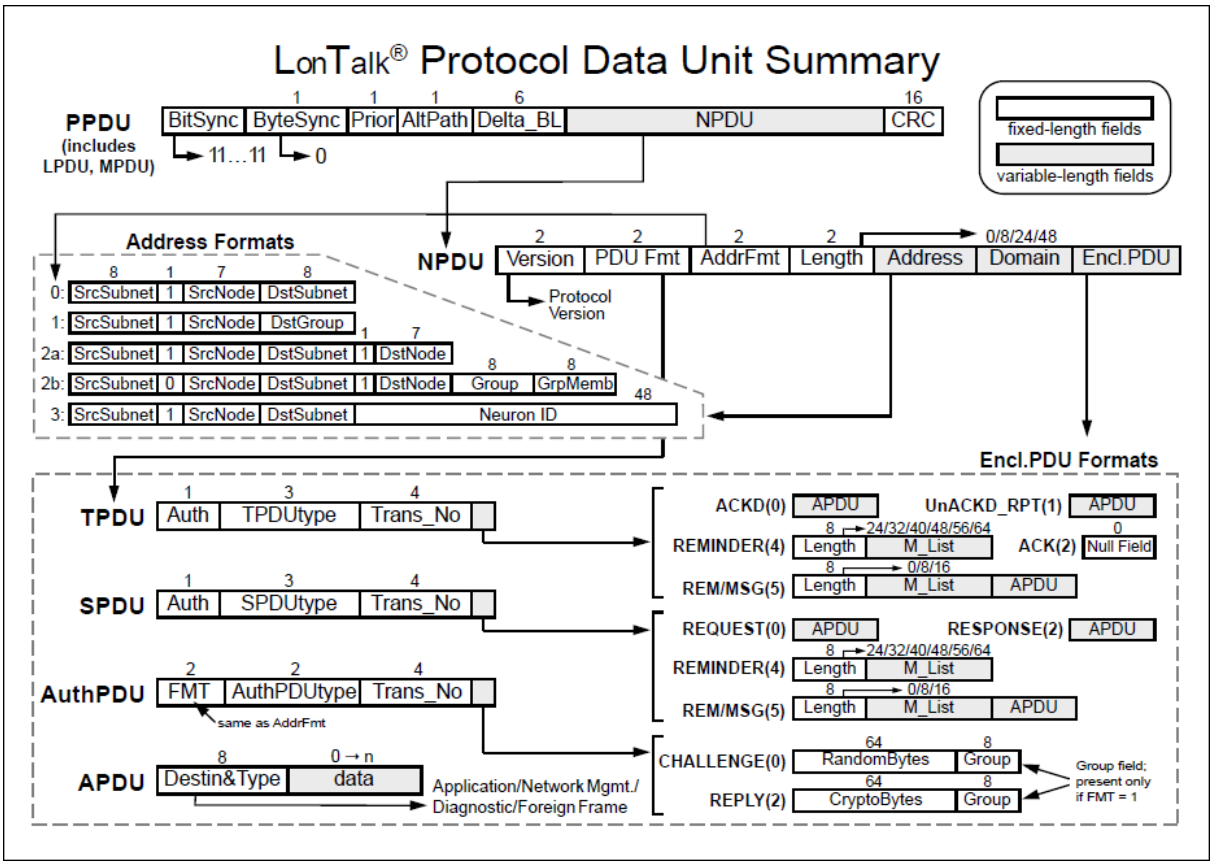
- Unacknowlegded-Repeated Multicast und Unicast
- Keine Bestätigungen erwartet

- Nachricht wird immer max. Anzahl an Wiederholungen mal gesendet

Session Layer

SPDU (Session Protocol Data Unit) in NPDU gekapselt, SPDU enthält wiederum APDU

- Request-Response Service, ähnlich Remote Procedure Calls
- Nicht idempotente Transaktionen werden maximal einmal ausgeführt
- Eine Transaktion gilt als idempotent genau dann wenn die Antwort > 1 Byte ist



Authentifizierung kann bei Transport und Session Layer Protokollen angefordert werden. Der Client muss das *Auth* Bit setzen, um eine authentifizierte Transaktion zu starten. Der Server sendet daraufhin eine Challenge zum Client. Der Client berechnet eine Transformation über die Challenge, ursprüngliche APDU und Schlüssel und schickt diese an den Server. Dieser vergleicht es mit seinem eigenen Ergebnis. Stimmt es überein, gilt die Transaktion als authentifiziert.

Verwendung in OSGP

OSGP verwendet den Request-Response Service des Session Layers von LonTalk. Die folgenden Werte für das Feld *destin_type* wurden spezifiziert:

Wert	Zweck
0x00	Ongoing Operation Messages (z.B. Tabellen lesen)
0x04	Kann für Abwärtskompatibilität genutzt werden
0x45	ADD (Automated Device Discovery) Proxy Message (ausgehend)
0x4A	ADD Proxy Message (eingehend)
0x49	ATM (Automated Topology Management) Query ID
0x48	Antwort auf ATM (Automated Topology Management) Query ID
0x47	ATM Respond to Query
0x46	Antwort auf ATM Respond to Query

Die grau hinterlegten Nachrichten dienen alle der automatischen Erkennung und Verwaltung der OSGP Gerätetopologie. Dieses ATM (Automated Topology Management) genannte Feature bietet unter anderem:

- Automatische Zuordnung von Geräten zu einem DC (Data Concentrator) bei Installation und Topologieänderungen
- Automatische Identifizierung von Testpunkten

ATM ADD nutzt die folgende LonTalk Domain: 0x7A3340F1BCD2.

2.2.3 AP 3: Untersuchung und Berücksichtigung der Datenschutz-Aspekte

Zweck dieses Arbeitspakets war es, die datenschutzrechtlichen Aspekte von Intrusion Detection in einem Smart Meter System zu betrachten und die dabei auftretenden datenschutzrechtlichen Fragestellungen zu formulieren. Fragen der Datenverwendung und der Datensicherheit von personenbezogenen Daten bei Smart Meter Systemen und welche Einwirkungen darauf beim Einsatz von IDS entstehen können, stehen dabei im Vordergrund. Zu diesem Zweck wurde ein externer Experte – Dr. Kurt Einzinger – mit der Ausarbeitung dieses Arbeitspakets beauftragt

Ausgehend von der bestehenden und in Entwicklung befindlichen österreichischen und europäischen Gesetzeslage wurden die datenschutzrechtlichen Problemstellungen der Datenverwendung bei einem Smart Meter System dargestellt und analysiert. Als Referenzanwendung wurde der Einsatz von Smart Meter Systemen bei den Projektpartnern Wels Strom GmbH und Elektrizitätswerk Wels AG (ITandTEL) angenommen, da der dort geplante Einsatz von Intrusion Detection Systemen als typisch für derartige Systeme angesehen werden kann.

Wir befinden uns zurzeit in einer datenschutzrechtlichen Umbruchphase. Mit der erfolgten

politischen Einigung über den Inhalt der europäischen Datenschutz-Grundverordnung (DSGV) zwischen der Europäischen Kommission, dem Parlament und dem Rat steht der Weg frei für eine Umgestaltung des Datenschutzrechts in Österreich. Bis 2018 müssen die derzeit geltenden Bestimmungen an die DSGV angepasst werden, da diese ab dann vollinhaltlich in Österreichisches Recht übergeht. Das heißt, dass in der Zwischenzeit die bisherigen Bestimmungen nach wie vor gelten, dass man aber schon ein Auge auf die DSGV haben sollte und deren Vorschriften mitberücksichtigen muss.

Das Ziel des Projekts ist die Erforschung und Entwicklung eines Verfahrens zur laufenden automatischen Überwachung einer Smart-Meter-Infrastruktur während des Betriebs. Daher ist zu klären, inwieweit die datenschutzrechtlichen Bestimmungen der dabei zu beachtenden Gesetze (DSG 2000, TKG 2003, EU-Verordnung 611/2013, DSGV) zur Anwendung kommen und welche Möglichkeiten es gibt, ein Intrusion Detection System (IDS) für ein Smart Meter System datenschutzkonform zu betreiben.

Da im Datenfluss zwischen Smart Meter, Netzbetreiber, IT- Firma, Stromanbieter und Intrusion Detection System (IDS) personenbezogene Daten enthalten sind, und auch personenbezogene Daten für das IDS verwendet werden, stellt sich einerseits die Frage nach deren gesetzlicher Grundlage und andererseits müssen alle datenschutzrechtlichen Bestimmungen dabei eingehalten werden.

Unmittelbar vor der Rechtswirksamkeit des neuen europäischen Datenschutzrechtsrahmens (2018) müssen hierbei sowohl die derzeitige österreichische Datenschutzrechtslage als auch die neue europäische Datenschutz-Grundverordnung (DSGV) in Betracht gezogen werden.

In der Untersuchung wird besonders auf die Natur des Intrusion Detection Systems und die damit verbundenen Fragestellungen eingegangen. Da davon ausgegangen werden muss, dass im Intrusion Detection System für das Smart Meter System auch personenbezogene Daten verwendet werden, müssen alle datenschutzrechtlichen und Datensicherheits-Vorschriften eingehalten werden.

Der ausführliche Bericht über dieses Arbeitspaket findet sich im technisch-wissenschaftlichen Bericht, Anhang SmartMeterIDS – Untersuchung und Berücksichtigung der Datenschutzaspekte.

2.2.4 AP 4: Definition der technischen Überwachungsparameter und –regeln

Anforderungen an ein MDM (Meter Data Management) System

Das Ziel eines IDS (Intrusion Detection System) für ein Smart Meter Data Management System ist es, auf Grund anormalen Verhaltens eines Gerätes einen nicht definierten Zustand zu erkennen und zu melden. Wichtige Eigenschaften dabei sind die Verhaltensmuster des Smart Meters und des Systems, das die Steuerung und Verwaltung der Zähler über hat, in diesem Fall das Meter Data Management System. Diese Eigenschaften beschreiben die wichtigste

Schicht in der Analyse.
In einer weiteren Analyse werden auf einer höheren Schicht die Verbrauchswerte analysiert. Geplant war die Analyse einer weiteren Schicht, die Informationen über den Zustand des Netzwerks auf unterer Ebene bereitstellt. Da die dafür erforderlichen Definitionen der auf dieser Schicht verwendeten Protokolle das Monitoring von Power Line Communication (PLC) nicht bzw. nur mit unvertretbarem Aufwand beschafft werden konnten, wurde dieser Punkt nicht weiter verfolgt.
Um ein Smart Meter IDS betreiben zu können, ist es notwendig relevante Daten zur Verfügung zu haben und mit einem standardisiertem Verfahren darauf zugreifen zu können. Welche Informationen diese Daten beinhalten sollen und auf welche Art der Zugriff erfolgen kann, wird im Folgenden beschrieben. Es können sich Erläuterungen ergeben, die für ein Meter Data Management System selbstverständlich sind, aber aus Sicht eines IDS trotzdem erwähnt werden müssen.

Inhalt der Daten

Vorerst sei zu erwähnen, dass alle Vorbereitungen und Arbeiten unter der Verwendung von OSGP getroffen wurden. Während DLMS/COSEM konforme Geräte dem objektorientieren Modell folgen, benutzt OSGP REST. Jeglicher Datenaustausch unter OSGP erfolgt über Tabellen, wie zum Beispiel Geräte Status, Events, Logs etc. Daher ist das IDS auf OSGP konforme Geräte ausgerichtet, schließt aber andere Protokolle oder Technologien nicht aus.
Um die Information aus den Daten extrahieren zu können, muss ein Gerät klar identifizierbar sein. Die Unterscheidung hat mittels einer statischen, einzigartigen ID, die abhängig vom Gerät ist, zu erfolgen. Eine Beziehung zum Kunden ist technisch nicht relevant. Die Informationen, die über ein Gerät verfügbar sein sollen, sollen aus verschiedenen Datenquellen bezogen werden und in einem zentralen System (dem MDM) gesammelt werden. Zu den Datenquellen zählen das MDM selbst, alle im Netzwerk und auf der Strecke zum Zähler beteiligten Netzwerkgeräte sowie der Zähler.
Die Information, die im MDM ihren Ursprung hat, enthält die Befehle, die an ein Gerät abgesendet werden. Diese Befehle können entweder ad hoc oder auf regelmäßiger Basis abgesendet werden. In weiterer Folge sollen Log Informationen von allen im Netzwerk beteiligten Geräten an das MDM gesendet und gespeichert werden. Im MDM soll eine Bestätigung im Falle einer positiven Abarbeitung erfolgen oder ein Status wie zum Beispiel „wartend“ abgespeichert werden, sollte noch keine positive Abarbeitung erfolgt sein. Im Falle einer negativen Abarbeitung soll diese auch vermerkt sein. Alle Logeinträge haben mit mindestens einem dazugehörigen Zeitstempel zu erfolgen, wobei die kleinste Einheit eine Sekunde darstellt. Genauere Zeiteinheiten erhöhen den Detailgrad der Logeinträge und Unterscheidbarkeit und sind daher anzustreben. Informationen eines Logeintrages müssen über eine einzigartige, wiedererkennbare Typeninformation verfügen. Events der gleichen Art

müssen somit mit derselben Bezeichnung versehen werden, unabhängig vom Gerät bzw. Hersteller und dürfen sich nur durch Geräte ID oder Zeitstempel unterscheiden. Zur Konsolidierung der Daten sollen Events, die den gleichen Zweck verfolgen, abhängig vom Hersteller oder einem verwendeten Protokoll jedoch eine andere Bezeichnung haben, im MDM System unter derselben Bezeichnung abgespeichert werden.
Zur Analyse der Verbrauchswerte wird ein 15 minütiger Intervallwert benötigt, der entweder den Zählerstand oder den Verbrauch innerhalb des Intervalls wiedergibt.
Zusätzlich zu den oben genannten Eigenschaften ist die Information über den Zustand des Netzwerks von großer Bedeutung. Verfügbare Informationen von Netzwerkschnittstellen müssen dabei denselben Anforderungen wie jenen der Zähler gerecht werden. Eine Konsolidierung von Statusmeldungen verschiedener Technologien soll auch hier angestrebt werden, ist jedoch nicht so bedeutend wie bei Smart Meter Geräten.

Zugriff auf Daten

Zur automatisierten Verarbeitung der Daten ist es notwendig, auf standardisierte Weise auf die Daten zuzugreifen. Die zu bevorzugende Schnittstelle ist ein Zugriff auf die Datenbank des MDM aus dem IDS direkt. Um hierbei eine Beeinflussung oder gar eine Störung des produktiv verwendeten Systems zu verhindern, soll eine Replikation der Datenbank zur Verfügung stehen, auf die zugegriffen werden kann.
Eine – allerdings nicht anstrebenswerte – Alternative ist der Zugriffe auf exportierte Dateien, etwa in Form von Excel. Dies würde zu einem Mehraufwand führen und so die Benutzerfreundlichkeit erheblich einschränken.

Konfigurationsanpassung

Da die Standard-Einstellung der Smart Meter hauptsächlich das Ziel verfolgen, die Qualität des Stromes zu überprüfen und zu garantieren, mussten Änderungen der Konfiguration vorgenommen werden. Die Konfiguration kann auf verschiedenen Ebenen verändert werden, wobei gerade erweiterte Funktionen, die im normalen Betrieb nicht zur Geltung kommen, an Bedeutung gewinnen. Um auffälliges Verhalten überhaupt erst zu erkennen, musste somit die Granularität der Logeinträge angehoben werden, um Abseits von bereits vordefinierten Störungs- oder Manipulationsalarmen Unstimmigkeiten definieren und erkennen zu können.
Die Konfigurationsanpassung betrifft ausschließlich das Eventlog. Die Eventlogkonfiguration lässt sich in Status- und Alarm-Events unterteilen. Durch Änderung der Status-Konfiguration ist es weiters möglich, den Zugriff auf Standard- und herstellerspezifische Tabellen sowie die Aufrufe von Standard- und Herstellerprozeduren aufzuzeichnen.

SEMLogAnalyser

Der SEMLogAnalyser ist das zentrale Programm des Intrusion Detection Systems. Es ist ein Programm zum Erkennen von anormalen Verhalten im Kontext von Smart Meter Netzwerken.

Es enthält sowohl das Extrahieren von zuvor exportierten Daten als auch das Erlernen normalen Verhaltens und das Generieren von Regeln. Als Basis dienen Daten aus dem SEM System, einem proprietären System, das für die Verwaltung von Geräten und die Verrechnung benutzt wird.

Die gesamten Daten können in mehrere Ebenen unterteilt und analysiert werden. Diese Daten enthalten Informationen über das Netzwerk und alle teilnehmenden Geräte sowie die wesentlichen Daten eines Energie Management Systems – die Verbrauchsdaten. Mittels verschiedener Verfahren, abhängig von der betrachteten Schicht, werden Regeln erstellt, die den geordneten und korrekten Ablauf des Verhaltens beschreiben. Später werden diese Regeln verwendet, um Anomalien im System zu erkennen und zu melden, damit weitere Schritte eingeleitet werden können. Ein weiterer Vorteil des Systems besteht auch darin, dass die vielen generierten Logeinträge, die oftmals für den bearbeitenden Mitarbeiter undurchsichtig erscheinen, an einer zentralen Stelle ausgewertet und interpretiert werden.

Schichten

Auf der obersten Schicht befindet sicher der Information Layer. Dabei werden die übermittelten metrologischen Daten in der Form von Lastprofilen interpretiert. Mittels statistischer Verfahren werden auf Basis vergangener Werte Prognosen über zukünftige Werte erstellt und mit dem tatsächlichen Verbrauch verglichen. Über empirische Methoden werden zum einen Schwellwerte ermittelt, die eine Abweichung vom normal definierten Verhalten beschreiben und es werden durch Kumulation der Daten anderer, vergleichbarer Verbraucher besondere Ereignisse erkannt und später nicht als Abweichung vom Normalverhalten prognostiziert.

Auf der zweiten Schicht wird das Verhalten aller sich im Netzwerk befindlichen Geräte analysiert. Dabei gilt den aufgerufenen Befehlen sowie die Ausführung und Initiierung von Funktionen die größte Bedeutung. Unter Beobachtung der zeitlichen Zusammenhänge können so Abfolgen, Sequenzen und Sammlungen von Ereignissen analysiert und definiert werden. Die erstellten Regeln werden auf deren Plausibilität, so weit wie möglich und nachvollziehbar, überprüft und beschreiben den normalen Ablauf immer wieder auftretenden Aktionen.

Auf der dritten Schicht wird das zur Datenübertragung und Netzwerkmanagement verwendete Protokoll analysiert. Ziel dieser Analyse ist die Definition eines Subsets um die Funktionen auf die notwendigsten einzuschränken und die Komplexität zu vermindern.

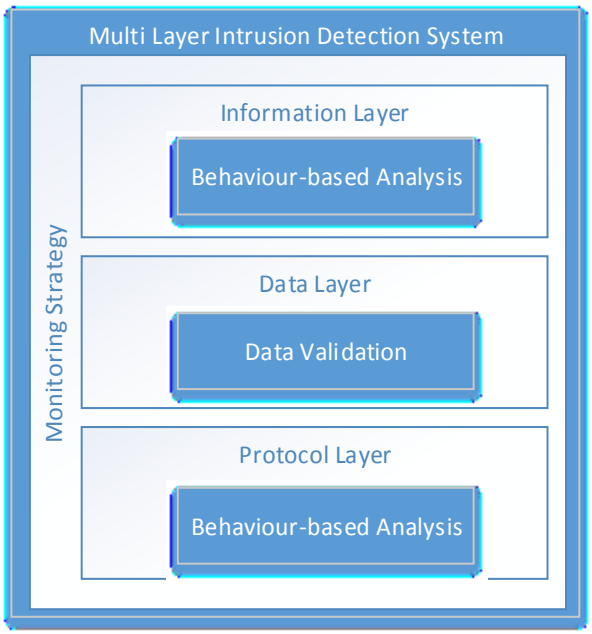


Abbildung 2: Schichten des IDS

Information Layer

Am Information Layer wurden die Verbrauchsdaten betrachtet. Ziel war die Analyse dieser Daten, um zu Normalverbrauchsprofilen zu kommen. Diese Normalverbrauchsprofile können dann laufend mit den Verbrauchsdaten verglichen werden, um eventuelle Abweichungen im laufenden Betrieb zeitnah feststellen zu können. Es wurden entsprechende Auswertungen vorgenommen, um statistisch Verbrauchsprofile zu erzeugen. Dabei wurde zwischen Gewerbebetrieben und Privathaushalten unterschieden, da diese doch sehr unterschiedliche Verbrauchsprofile aufweisen. Die ermittelten Profile stellten sich als sehr ähnlich zu vorhanden Profilen heraus, die von Elektrizitätsunternehmen zum Zwecke der Produktionsplanung erstellt werden. Die entsprechenden Daten finden sich im Anhang des technisch-wissenschaftlichen Berichts.

Protocol Layer

Wie weiter oben bereits erwähnt, konnten Analysen auf dieser Ebene nicht durchgeführt werden, da die dafür notwendigen Detail-Informationen über das proprietäre PLC-Protokoll nicht beschafft werden konnten. Daher wurde auf diese Ebene verzichtet.

Data Layer

Das Projekt konzentrierte sich auf den Data Layer, da hier die wichtigsten und gegenüber Angriffen auch anfälligsten Informationen, nämlich die Befehle zur Steuerung des Smart Meter

Netzwerks zu finden sind. Im folgenden werden die Details der Analyse dieses Layers beschrieben.

Datenextraktion – manuelle Exporte

Die Datenextraktion geschieht beim SEMLogAnalyser über zuvor exportierte Event-, Befehl- und Ergebnislogs. Beim Start des Programmes muss dabei eine Datei in einem Verzeichnis gewählt werden, in der sich die Logdateien befinden. Aus Gründen der einfachen Verarbeitung wird eine Namenskonvention getroffen, Eventlogs werden unter *events.xls*, Ergebnisse unter *results.xls* und Befehle unter *commands.xls* gespeichert. Vor allem beim Exportieren von Eventlogs ist darauf zu achten, dass gesammelte Events (Groupoccurs) aufgelöst werden und jeder Event einzeln sichtbar ist.

Die Information, die über die Events verfügbar ist, wird auf die wesentlichsten und notwendigsten Einträge minimiert, so dass über die verschiedenen Arten von Events ähnliche oder vergleichbare Informationen verfügbar sind. Konkret werden die Events auf folgende Daten beschränkt:

- Root: Information über die Herkunft des Events
- Type: Aussagekräftige Kurzbeschreibung
- AddInfo1: Zusätzliche Information
- AddInfo2: Zusätzliche Information
- Timestamp: Wesentlicher Zeitstempel

Gerade beim Zeitstempel ist es sehr wichtig, sollten mehrere für einen Eintrag vorhanden sein, dass der aussagekräftigste, im Zusammenhang mit anderen Informationen verwendet wird. So ist z.B. bei einem Log Event aus dem Smart Meter die Zeit, in der eine Aktion ausgeführt wurde, die wesentliche verfügbare Information, nicht die Zeit in der das Log Event an den Server übertragen wurde (was auch verfügbar wäre).

Bewertungssystem

Um die Häufigkeit des Vorkommens sowie die Länge und andere aussagekräftige Parameter einer Regel bewerten zu können, wird mittels einer Formel ein Wert für eine Regel ausgerechnet, der mit einer Zahl, dem Rating, zum Ausdruck bringen soll, wie sinnvoll und effizient eine Regel ist.

Das Rating besteht aus der Kumulation zweier Ratings, das erste ist eine statische Bewertung, die am Anfang des Prozesses, in der Phase der Erstellung der Regel, festgelegt wird. Die zweite Bewertung hängt von der Häufigkeit des Vorkommens während der Überprüfungszeit, also im Echtbetrieb, ab. Die dynamische Bewertung soll in diesem Zusammenhang aber nur Aussagen über die Qualität, die Anzahl des Auftretens, treffen und nicht Regeln verifizieren, so dass zum Beispiel Regeln, die über die Zeit nicht mehr auftreten, aus dem Ruleset verschwinden. Dies hat zum Zweck, dass durch das unbeaufsichtigte Lernen keine Situation des False-Learnings entsteht. Die Bewertungen der Regeln sollen auch Aufschluss über die Sinnhaftigkeit der definierten Log Aktionen geben.

2.2.5 AP 5: Entwicklung der Richtlinien und organisatorischen Maßnahmen zur Überwachung

Ausgehend von bestehenden internationalen Normen (z,B, ISO 270001) werden Richtlinien (Policies) definiert, die während des operationalen Betriebs einzuhalten sind. Diese Richtlinien sind insbesondere auch für eventuelle Ausnahmesituationen auszulegen: Wie ist vorzugehen, wenn das automatische Überwachungssystem anormale Vorkommnisse meldet; welche Maßnahmen sind einzuleiten, welche Verantwortlichkeiten sind zu berücksichtigen. Auch Schulungsmaßnahmen können Teil der Richtlinien sein; ebenso die periodische Überprüfung bestimmter Vorgaben.
Im Allgemeinen wird in betroffenen Unternehmen bereits ein ISMS (Information Security Management System) in Kraft sein. Dieses gilt es entsprechend den neuen Anforderungen, die durch die Einführung und den Betrieb einer Smart Meter Infrastruktur entstehen, zu erweitern.
Die folgende Tabelle zeigt die Roadmap, die zur Erarbeitung der entsprechenden Maßnahmen und Richtlinien im Rahmen des gegebenen ISMS erarbeitet wurde.

Der detailliert ausgearbeitete Maßnahmenkatalog liegt als Dokument von 55 Seiten vor. Er wurde vom Projektpartner eww ausgearbeitet, wobei auf die konkreten betrieblichen Rahmenbedingungen Bezug genommen wurde, um die praktische Umsetzbarkeit garantieren zu können. Aus diesem Grund enthält die Ausarbeitung firmenspezifische Details, die der Geheimhaltung unterliegen. Daher kann dieser Maßnahmenkatalog nicht öffentlich zugänglich gemacht werden und ist in diesem Bericht nicht enthalten.

Dokument	Beschreibung	Relevant für Smart Meter
ISMS Policy	ISMS Policy	Policy - Teil der eww Gruppe
Informations- und Anwendungslandkarte	Alle relevanten Anwendungen im Kontext von Smart Meter	In der aktuellen Projektphase kennen wir nur einen Teil der Anwendungen, weil wesentliche Ausschreibungen noch nicht erfolgt sind. Diese Darstellung ist als Draft
Passwort Anweisung	Anweisung, welche sicherstellen, dass die Kennworte bei dem Smart Meter Systemen dem Stand der Technik erstellt werden. Weiters Anweisungen, die den Umfang mit den kritischen Passwörtern sicherstellen.	Relevant
Change-Management	Einteilung aller System-Änderungen in unterschiedliche Kategorien und zugeordnete Maßnahmen	Relevant
Partner Management	Der Umgang mit externen Partnerunternehmen, um die ISMS-Ziele der Policy sicherstellen zu können.	Relevant
Configuration Management und Release Mgt.	Informationssystem über die Systemconfiguration und die relevanten Systemstände	Relevant
Incident-Management	Behandeln aller Vorfälle im Kontext Smart Meter	Relevant
Anweisung öffentliche Systeme	Anweisungen, welche permanent den Zugriff auf kritische Infrastrukturen von Aussen überprüfen und absichern.	Relevant
Anwendung Kryptographische Maßnahmen	Anweisung, wie und in welchem Maße kryptographische Maßnahmen eingesetzt werden	Relevant - Abhängig von der PKI
Datenklassifikation	Klassifikation aller Daten im Zusammenhang von Smart Meter	Relevant, mit Aussage über Auftraggeber einzelner Datenbestände
Capacity Management	Capacitymanagement	Phase II
Notfall-Bewältigung	Alle Maßnahmen zum verhindern und behandeln eines	Phase II - Einbinden in unternehmensweites Notfall-Mgt
Continuity Management	Maßnahmen zur Sicherstellung, dass auch in einem Notfall die wichtigsten Prozesse aufrechterhalten werden können.	Phase II - Einbinden in unternehmensweites Notfall-Mgt
Krisen-Management	Abbildung der Smart Meter Anweisungen im unternehmensübergreifenden Krisenmanagement	Phase II - Einbinden in unternehmensweites Notfall-Mgt

2.2.6 AP 6: Überprüfung der Regeln im Pilotprojekt

Die Überprüfung der durch maschinelles Lernen gewonnenen Regeln im Rahmen des Pilotprojekts zum Einsatz von Smart Metern beim Konsortialpartner Wels Strom wurde auf zwei Ebenen durchgeführt:

1) Einerseits auf dem Information Layer: Die gewonnen Verbrauchsdaten wurden sowohl mit historischen Daten aus Wels als auch mit allgemein verfügbaren Daten aus vergleichbaren Städten verglichen. Der Vergleich ergab, dass bereits existierende Vorhersagemodelle für den Verbrauch eine ausreichende Vorhersagequalität auf einem relativen hohen Konzentrationsniveau besitzen und eine Vorhersage auf individuellerer Basis (einzelne Haushalte) nicht sinnvoll möglich ist, weil die Variationen des Verbrauchs auf individueller Ebene zu stark variieren. Es kann daher nur auf einer aggregierten Basis – entweder durch Zusammenfassung mehrerer Haushalte oder durch zeitliche Aggregation – eine für Anomalie-Erkennung brauchbare Aussage ermittelt werden. Da derartige Vorhersagen allerdings bereits vorliegen und für andere Zwecke verwendet werden, wurde auf eine Implementierung verzichtet. Sie hätte wissenschaftlich gesehen keine neuen Ergebnisse oder Einsichten gebracht.
2) Auf dem Data Layer: Hier werden die Befehle zur Steuerung des Netzwerkverkehrs übermittelt. Daher wurde dieser Ebene die meiste Aufmerksamkeit gewidmet. Die durch maschinelles Lernen aus Netzwerkdaten des Pilotprojekts ermittelten Regeln wurden auf laufenden Netzwerkverkehr angewandt, um zu prüfen, ob eine effiziente Erkennung von Anomalien möglich ist. Die Vergleiche ergaben zufriedenstellende Ergebnisse, waren aber dahingehend eingeschränkt aussagekräftig, da im beobachteten Zeitraum keine Anomalien aufgetreten sind. Das war auf Grund der Tatsache, dass es sich um tatsächliche Daten aus dem Pilotprojekt der Wels Strom handelte natürlich absehbar – es ist im Beobachtungszeitraum eben kein Angriff auf das Netz durchgeführt worden bzw. auch sonst kein besonderer Vorfall eingetreten. Um auch Anomalien testen zu können, wurde auf Daten aus der Simulation zurückgegriffen, die am Beginn des Projekts durchgeführt wurden. Diese Teststellungen ergaben ebenfalls ein positives Ergebnis: Absichtlich eingebaute Anomalien in den Befehlsfolgen wurden erkannt und entsprechende Warnungen vom System generiert.

2.2.7 AP7: Proof-of-concept Implementierung des IDS

Die Proof of Concept Implementierung stellt das Resultat aller gesammelten Erkenntnisse und Vorarbeiten dar. Das System besteht dabei aus zwei wesentlichen Komponenten. Die erste Komponente beschäftigt sich mit dem Lernen des Systemverhaltens und der Erstellung von Regeln, die mit der zweiten Komponente regelmäßig Überprüfungen durchführt. Um die Effizienz von Regeln ständig zu verbessern soll es möglich sein, aus dem Abschnitt der kontinuierlichen Überprüfung

Regeln zu adaptieren, hinzuzufügen oder zu entfernen.

Anforderungen an ein IDS System

Die aus den Anforderungen eines MDM Systems abgeleiteten Schnittstellen und der dadurch produzierte Output definieren gleichzeitig den Input und somit die Schnittstelle zum Input des IDS Systems.

Ziel ist es, die optimierte Datenquelle einzubinden und die Daten zu verarbeiten. Optimiert bedeutet in diesem Zusammenhang, dass durch Änderungen der Konfiguration der Geräte weitere Daten, die für die Auswertung von großer Bedeutung sind, konzentriert im System abgespeichert werden. Das IDS darf in keiner Phase der Überprüfung den produktiven Ablauf stören oder beeinflussen.

Die anzuwendenden Regeln, die den normalen Ablauf beschreiben, sollen entweder aus einem XML File eingelesen werden, oder aus der Datenbank selbst, die aus einem sicheren Betrieb heraus erzeugt und befüllt wird. Diese Regeln sollen mit markanten Merkmalen, wie die Häufigkeit, Länge oder Vorkommen versehen werden, um einen Benutzer, der sich nicht in der Tiefe mit der Materie beschäftigt, die Möglichkeit zu geben, eine Regel zu überprüfen und bewerten. Dabei spielt die Präsentation und Visualisierung der Regeln eine wesentliche Rolle.

Bewertung von Regeln

Die Bewertung der Regeln wird beeinflusst von der Anzahl der Vorkommen, der Länge (Anzahl von Ereignissen), sowie der vergangenen Zeit zwischen den einzelnen Ereignissen. Dabei soll die Gewichtung der einzelnen Faktoren immer die Gesamtheit aller Regeln in die Bewertung miteinbeziehen.

Die Wertung einer Regel beginnt bei 0 und endet bei 1, wobei 0 für die schlechteste Bewertung und 1 für die bestmögliche Bewertung steht. Jeder der 3 in die Bewertung mit einfließenden Teile hat einen gleich großen Anteil und somit einen maximalen Einflussfaktor von einem Drittel.

Der erste Faktor, der bei der Berechnung in Betracht gezogen wird, ist die Länge der Regel, ausgedrückt in der Anzahl der Aktionen, die eine Sequenz beschreiben. Als Basis zur Berechnung dient die durchschnittliche Länge aller Regeln. Dies setzt also voraus, dass zuerst alle Regeln erstellt werden, ehe diese bewertet werden können. Entspricht die Länge der Regel der durchschnittlichen Länge oder darüber hinaus, so wird der Wert 1/3 vergeben; kürzere Längen werden anteilig abgezogen.

Der zweite Faktor, der zur Berechnung des Ratings herangezogen wird, ist die Frequenz der vorkommenden Aktionen innerhalb einer gewissen Zeit. Diese Zeit ist entweder die Dauer einer Regel, beginnend von der ersten bis zur abschließenden Aktion oder, wenn diese Zeit 0 ist (weil die Regel aus nur einer Aktion oder mehreren Aktionen zur selben Zeit besteht), wird das Intervall zur Berechnung herangezogen, das während der Lernphase als maximale Dauer zwischen den Aktionen innerhalb einer Regel definiert wurde. Die Frequenz beschreibt die Aktionen pro Sekunde in einer Regel und wird mit 1/3 der Gesamtbewertung gewichtet.

Der dritte Faktor lässt sich aus der Häufigkeit des Auftretens der Regel während des Beobachtungszeitraums berechnen. Dazu ist es notwendig ein „Cleaning“ der Regeln durchzuführen. Bei diesem Vorgang werden gleiche Regeln aggregiert und ab diesem Zeitpunkt wird die verstrichene Zeit zwischen den Aktionen außer Acht gelassen. Gleiche Regeln können so erkannt und aggregiert werden; außerdem kann ermittelt werden, wie oft eine Regel in der Lernphase vorkommt. Dieser Wert wird wieder relativ zum durchschnittlichen Auftreten berechnet und ergibt ebenfalls 1/3 der Gesamtwertung. Dieser Wert kann später in der Phase des Überprüfens Aufschluss darüber geben, ob das Verhältnis des Vorkommens von Regeln im Echtbetrieb mit dem Vorkommen während der Übungsphase übereinstimmt. Dieser Teil übernimmt den Part des kontinuierlichen Lernens, da hier Erfahrungswerte einfließen, ohne den Ausgangspunkt zu verändern.

Umfeld

Die Implementierung des Systems erfolgte im Netzwerk des Konsortialpartners Wels Strom auf einem virtuellen Windows Server auf dem eine Replikation der Datenbank des SEM Systems liegt. Durch diese Konstellation war eine möglichst wirklichkeitsnahe Realisierung der Proof-of-Concept Implementierung möglich. Der Replikationsvorgang soll einmal täglich erfolgen und eine später definierte kontinuierliche Überprüfung anstoßen oder zumindest in zeitlichen Zusammenhang stehen. Der Grund für Replikation ist, dass auf die Datenbank selbst zwar nur lesend zugegriffen wird, jedoch im Vorhinein nicht bekannt ist, welche Auswirkungen das Auslesen der Datenbank auf die Performance des Systems hat. Daher wird, um die Verfügbarkeit des SEM Systems zu gewährleisten und um ein Beeinflussen des SEM Systems selbst auszuschließen, eine im Datenbanksystem implementierte Replikationsmethode verwendet. Um einen möglichst sauberen und einfachen Zugriff auf die Datenbank zu gewähren, liegt es nahe als Programmiersprache für die Proof-of-Concept Implementierung C# zu verwenden.

Datenbank

Daten, die für die Erstellung der Regeln verwendet werden, werden aus der Datenbank NES_Core bezogen. In dieser Datenbank befinden sich sämtliche Informationen, die für die Erstellung der Regeln notwendig sind. So findet man etwa in der Tabelle CommandHistory alle Einträge über Kommandos, sowie deren dazugehörige Geräte, Seriennummern und Kommando-IDs. Die dazugehörigen Informationen über die Kommandos selbst finden sich in der Tabelle Commands, welche in der Datenbankabfrage miteinander verknüpft werden. Informationen über Events finden sich in ähnlichem Format in der Tabelle EventHistory, dazugehörige Informationen in der Tabelle EventDefinitions. Resultate werden in der Tabelle Results abgespeichert, dazugehörige Informationen befinden sich in der Tabelle Commands. Jeder Eintrag in den Logtabellen (CommandHistory, EventHistory, Results) hat einen dazugehörigen zweiten Eintrag. Der Erste Eintrag enthält die Zeit, in der eine Aktion gestartet wird, der zweite, dazugehörige Wert enthält

einen Zeitstempel, wann die Aktion verarbeitet wurde.

Datenextraktion – Export Files

Für das Erstellen von Regeln können alternativ, wie beim SEMLogAnalyser auch, die aus dem SEM exportierten Excel-Dateien verwendet werden. Dafür gibt es einen eigenen Modus, der in der Konfigurationsdatei aktiviert werden muss. Zusätzlich müssen die Dateinamen für die Events, Commands und Results angegeben werden.

Datenextraktion – Datenbank

Da bei manuellem Export der Daten, so wie es beim SEMLogAnalyser der Fall ist, vom System nicht alle vorhandenen Informationen exportiert werden, gibt es den zweiten Weg der Datenextraktion über die Datenbank selbst. Hierbei wird in der Konfiguration der Zugriff auf die Datenbank konfiguriert.

Erstellung von Regeln

Der erste Schritt, um Regeln zu erstellen, ist die einheitliche Repräsentation derselben. Dafür werden aus dem SEM Daten von verschiedenen Orten (Tabellen) herangezogen. Diese Datensätze enthalten unterschiedliche Einträge, die auf öfter vorkommende Variable reduziert und später als Parameter für den Vergleich herangezogen werden. Diese Daten enthalten:

- Zähler Events:
  Type, **Priority**, **TimeStamp**, StoredTimeStamp, **Status**, **StatusTimeStamp**, GroupCount, GroupOccurence
- Zähler Ablesungen:
  Type, Source, SourceType, Tariff, Value, Unit, **Time**, Validity, ValidityFromMeter, WasExported, MeteringPointId
- Zähler Ergebnisse:
  Type, Time, StroedTime, Status, StatusTime
- Zähler Befehle:
  Type, **Status**, StatusDetail, **StatusTime**, **Priority**, StroedTime, User

Bei der Extraktion der Daten werden diese vereinheitlicht, sodass folgende Attribute von jedem Eintrag übrig bleiben:

- Root: Bezeichnung der Datenquelle
- ID: Eindeutige Bezeichnung
- Action: Aussagekräftige Kurzbeschreibung
- Time: Zeitstempel
- AI: zusätzliche Information

All diese Informationen werden aus den verschiedenen Tabellen der Datenbank zusammengesammelt und in zeitlicher Reihenfolge geordnet. Danach wird innerhalb einer vordefinierten Zeitspanne (Δt) nach zusammengehörigen Events gesucht. Wenn innerhalb von Δt ein neuer Event hinzukommt, wird dieses als Action zur Regel hinzugefügt; dieser Vorgang wiederholt sich so lange, bis nach Ablauf von Δt keine Events mehr auftreten. Danach wird eine

neue Regel begonnen und der Vorgang wiederholt sich. Nachdem so alle Events innerhalb der Lernphase abgearbeitet und in Regeln zusammengefasst wurden, wird das Ruleset bereinigt. Gleiche Regeln werden zusammengefasst und der Counter (der Zähler in dem festgehalten wird, wie oft eine Regel in der Lernphase vorkommt) wird erhöht. Dieser Counter wird später für die Bewertung der Regeln miteinberechnet.
Die Regeln werden danach in einem XML Format exportiert, damit sie nachher für das Pattern Matching in standardisierter Form zur Verfügung stehen.

Pattern Matching – Sequenz Analyse

Bei der Sequenz Analyse wird ein XML Rule File eingelesen, das zuvor in einer Lernphase erstellt wurde. Daraus werden die Regeln in die programminterne Liste von Regeln konvertierte, die danach das Pattern Matching steuern.
Als Basis für das Pattern Matching werden für ein bestimmtes Gerät anhand der Device ID aus der Datenbank über eine gewissen Zeitspanne Logeinträge, aus denselben Tabellen wie beim Erlernen der Regeln, extrahiert und in eine Liste gespeichert.

Scoreboard

Das Ergebnis einer Evaluation wird in einem Scoreboard gespeichert. Dieses Scoreboard enthält statistische Werte über den Prozess der Sequenzanalyse. Die ersten beiden Werte sind die Summen der Hits, wie oft Regeln der überprüften Sequenz zugewiesen werden konnten, und die Summen der Counts, wie oft Regeln während der Lernphase vorgekommen sind. Für jede einzelne Regel kann somit berechnet werden, wie groß der Anteil der Regel an der gesamten Anzahl der Regeln der Lernphase ist, sowie wie oft einzelne Regeln während der Überprüfungsphase angewendet wurden. Die Kumulation dieser Werte ergibt den RatioValue, beziehungsweise unter Berücksichtigung der Bewertungen einzelner Regeln den RatedRatioValue.
Das Scoreboard wird im Anschluss an die Überprüfung an die in der Konfigurationsdatei definierte E-Mail Adresse versandt. Diese Aktion ist al Alarmierung im Sinne der Intrusion Detection zu sehen.

2.3 Änderungen im Projektverlauf

Im Rahmen des Projektverlaufs wurden drei Änderungen notwendig, die aber alle nur zeitliche Auswirkungen hatten und nicht budgetrelevant waren.

1) Der Projektstart hat sich um 4 Monate gegenüber dem Projektvertrag verzögert. Grund dafür war, dass das Pilotprojekt zur Smart Meter Einführung beim Konsortialpartner Wels Strom gegenüber den Planungen, wie sie zur Zeit der Antragstellung bestanden haben, verschoben wurde. Da das Projekt teilweise auf Daten aus diesem Pilotprojekt angewiesen war, wurde bereits frühzeitig – nämlich beim Kickoff-Meeting Anfang Juni 2014 – darauf reagiert und das gesamte Projekt um 4 Monate nach hinten verschoben. Diese Maßnahme war aus Sicht des Projektmanagements sicherlich einfacher und sinnvoller als das Projekt zwischendurch zu unterbrechen.
2) Das Arbeitspaket 3 – Untersuchung und Berücksichtigung der Datenschutz-Aspekte – wurde innerhalb des Projekts verschoben. Ursprünglich am Beginn des Projekts vorgesehen wurde das Arbeitspaket erst ganz am Ende des Projekts durchgeführt. Grund dafür war die Tatsache, dass im Zeitraum des Projekts gerade die letzten Diskussionen zur EU Datenschutz-Grundverordnung geführt wurden, die dann Anfang 2016 erlassen wurde. Diese wesentlichen Grundvoraussetzungen, die spätestens 2018 auch auf die österreichische Gesetzeslage Auswirkungen haben werden, konnten damit noch einbezogen werden. Da dieses Arbeitspaket unabhängig von den anderen ist, konnte über die zeitliche Einbettung frei verfügt werden.
3) Das Arbeitspaket 5 – Entwicklung der Richtlinien und organisatorischen Maßnahmen zur Überwachung – wurde einerseits später begonnen und andererseits zeitlich ausgedehnt. Die Fertigstellung der Ausarbeitung der Policies beim Projektpartner eww/ITandTEL wurde zum Projektende hin verschoben, um auch letzte Ergebnisse der technischen Entwicklung miteinbeziehen zu können. Da es keine Abhängigkeiten von anderen Arbeitspaketen gab, war diese Änderung problemlos abzuwickeln.

Eine letzte kostenneutrale Verschiebung des Abgabetermins für den Endbericht um 3 Wochen ergab sich durch Verzögerungen bei der Übermittlung von Daten zwischen den Konsortialpartnern.

3 Projektteam und Kooperation

- Gibt es wesentliche Veränderungen im Projektteam (interne Schlüsselmitarbeiter und Drittleister)?
- Bei Konsortialprojekten: Beschreiben Sie die Zusammenarbeit im Konsortium.
- Gehen Sie auf Änderungen in der Arbeitsaufteilung ein. Gibt es Auswirkungen auf die Kosten- / Finanzierungsstruktur und die Zielsetzung?

Es gab keine Änderungen bei den Konsortialpartnern; auch der im Antrag genannte Drittleister hat im geplanten Ausmaß am Projekt teilgenommen.
Die Zusammenarbeit der Konsortialpartner ist durchwegs konfliktfrei verlaufen und hat sehr zum Erfolg des Projekts beigetragen. Die geplante Zuteilung der Arbeitspakete ist im Wesentlichen eingehalten worden und die unterschiedlichen Rahmenbedingungen der Konsortialpartner haben zu den erhofften Synergieeffekten geführt. Die FH St. Pölten und die Wels Strom GmbH haben vereinbart, einen neuen Projektantrag einzureichen (der mittlerweile auch genehmigt und direkt im Anschluss an dieses Projekte begonnen wurde).
Einzelne personelle Änderungen im Projektteam sind den aktuellen Erfordernissen und Fluktuationen geschuldet. Das Kernteam blieb bei allen drei Projektpartnern gegenüber dem Antrag allerdings unverändert. Im Verlauf des Projekts wurden im Wesentlichen zusätzliche Personen eingesetzt, die zur Unterstützung des Kernpersonals herangezogen wurden.

4 Wirtschaftliche und wissenschaftliche Verwertung

- Beschreiben Sie die bisherigen Verwertungs- und / bzw. Weiterverbreitungsaktivitäten. Ist eine Verwertung möglich?
- Listen Sie Publikationen, Dissertationen, Diplomarbeiten sowie etwaige Patentmeldungen, die aus dem Projekt entstanden sind, auf.
- Welche weiterführenden F&E-Aktivitäten sind geplant

Verwertungsaktivitäten:
Die organisatorischen Richtlinien zur Umsetzung von Sicherheitsmaßnahmen beim Betrieb von Smart Meter Netzwerken werden bei den Konsortialpartnern eww und Wels Strom in den laufenden Betrieb übernommen. Dabei wurden auch die Datenschutzaspekte berücksichtigt, die im Rahmen des Projekts erarbeitet wurden. Die für IT zuständige Abteilung in der eww, ITandTel, kann diese Projektergebnisse auch direkt und indirekt im Rahmen ihrer Beratungstätigkeit verwerten. In Bezug auf das Überwachungssystem ziehen die Konsortialpartner Wels Strom und eww eine Weiterentwicklung der Proof-of-Concept Implementierung in Betracht, um sie einerseits im eigenen Unternehmen (Wels Strom) einzusetzen bzw. um auch ein Produkt zu erstellen (eww).

Weiterverbreitungsaktivitäten:
Die Ergebnisse dieses Projekts wurden auch bei diversen wissenschaftlichen Veranstaltungen vorgetragen. Zu nennen ist bisher ein Beitrag von Lang-Muhr, C., Schrattenholzer, M., Tavolato, P. mit dem Titel „Multi-Layer Agent-Based Simulation of Network Behaviour in Advanced Metering Infrastructures“, der am 3rd International Symposium for ICS & SCADA Cyber Security Research, 2015 gehalten wurde und den Proceedings dieser Tagung veröffentlicht wurde. Ein weiterer wissenschaftlicher Fachbeitrag mit dem Titel „Anomaly Detection in Smart Meter Networks“ ist gerade in Ausarbeitung. Weitere Vorträge wurden bei internen Seminaren etwa an der Universität für Technik und Ökonomie in Budapest oder an der FH St. Pölten gehalten. Weitere Vorträge sind in nächster Zeit geplant.

Im Zusammenhang mit den Unterrichtstätigkeiten an der FH St. Pölten wurden verschiedene Teilaspekte des Projekts in der Lehrveranstaltung „Forschungswerkstatt“ bearbeitet und entsprechend dokumentiert. Das Projekt und die dabei gewonnen Erkenntnisse haben wesentlich zum Aufbau des Forschungsschwerpunkts Industrial Security am Department für Informatik an der FH St. Pölten beigetragen. Auch eine Bachelorarbeit mit dem Thema „Developing a Set of Best Practices for Smart Meter Rollout related to Cyber Security Measures” ist entstanden.

Weiterführende F&E-Aktivitäten:
Auf Grund von Informationen über das Projekt SmartMeterIDS konnte eine Zusammenarbeit mit der

Firma Siemens AG Österreich eingeleitet werden, die sich für die Projektergebnisse interessiert. Als weiterführendes Forschungsprojekt hat die FH St. Pölten mit den Konsortialpartnern Siemens AG Österreich und Wels Strom im Herbst 2015 das Projekt „Substation Security - Anomalie-Erkennung in Automatisierungsnetzen in der Energieverteilung“ bei der FFG im Rahmen der 2. Ausschreibung Energieforschung eingereicht, das Ende 2015 genehmigt wurde (Projekt-Nr. 853660, KLI.EN Nr. KR15EF0F12654). Die Arbeit an diesem Projekt wurde per 1.4.2016 (also direkt nach Ende dieses Projekts) aufgenommen.

5 Erläuterungen zu den Kosten

- Die Abrechnung ist als eigene Datei im Excel-Format hochzuladen. Die Verwendung der im eCall zur Verfügung gestellten Vorlage ist verpflichtend. Beachten Sie den Kostenleitfaden: www.ffg.at/kostenleitfaden bzw. Ausschreibungsdokumente
- Abweichungen vom Kostenplan sind an dieser Stelle zu beschreiben und zu begründen.
- Ist mit Änderungen am Kostenplan bis zum Projektende zu rechnen? Wenn ja, erläutern Sie diese. (Achtung: Größere Änderungen sind genehmigungspflichtig) (www.ffg.at/Kostenumschichtungen)

Es gab keine wesentlichen Abweichungen hinsichtlich des Kostenplans. Nicht im Antrag vorgesehen war nur der Ankauf eines U20 USB Network Interface – PL20 Channel zum Betrag von € 169,77. Dieses Gerät dient zur Aufzeichnung des Netzwerkverkehrs, der über PL (Powerline, dh das Stromnetz) übertragen wird. Dieser Ankauf war notwendig, um im Rahmen der Proof-of-Concept Implementierung des Intrusion Detection Systems entsprechende Tests durchführen zu können.

6 Projektspezifische Sonderbedingungen und Auflagen

- Gehen Sie auf projektspezifische Sonderbedingungen und Auflagen (laut §6 des Förderungsvertrags) ein, sofern diese im Förderungs- bzw. Werkvertrag vereinbart wurden.

Keine

7 Meldungspflichtige Ereignisse

Gibt es besondere Ereignisse rund um das geförderte Projekt, die der FFG mitzuteilen sind (siehe auch Richtlinien – Anhang zu 5.3., 5.3.5), z.B.

- Änderungen der rechtlichen und wirtschaftlichen Einflussmöglichkeiten beim Förderungsnehmer
- Insolvenzverfahren
- Ereignissen, die die Durchführung der geförderten Leistung verzögern oder unmöglich machen
- Weitere Förderungen für dieses Projekt

Keine