GAI NetConsult GmbH— Am Borsigturm 58 — 13507 Berlin — www.gai-netconsult.de — Tel: 030/417898-0

Project Basecamp – ein drastischer Weckruf für die Leittechnik

Dr. Stephan Beirer (GAI NetConsult GmbH)

Februar 2012 Sonderdruck aus Security *Journal* #59

Mitte Januar fand in Miami Beach, USA die auf Leit– und Automatisierungstechnik spezialisierte S4-Sicherheitskonferenz statt. Diesmal wurde auf der Tagung eine schier unüberschaubare Zahl von Sicherheitslücken in Industrie-Steuerungen veröffentlicht – was anschließend zu heftigen Kontroversen über das Sicherheitsniveau in der Leittechnik führte.

Die S4-Konferenz – mit vollem Namen *SCADA Security Scientific Symposium* – ist die führende Fachveranstaltung zur IT-Sicherheitsthematik für Leit- und Steuerungstechnik und die industrielle IT [1]. Jedes Jahr trifft sich im sonnigen Miami Beach / Florida der kleine Kreis der SCADA-Sicherheitsexperten, um sich über aktuelle Schwachstellen, neue Angriffsmethoden und Gegenmaßnahmen auszutauschen. Der Teilnehmerkreis umfasst sowohl Sicherheitsforscher, Berater, und Vertreter von Behörden als auch Systembetreiber sowie Sicherheitsverantwortliche von Leittechnik- und Komponentenherstellern aus den Bereichen der Industrie, Energieversorgung und Verkehrsleittechnik. Neben den Vorträgen stand deshalb insbesondere auch der fachliche Austausch zwischen den Konferenzbesuchern im Vordergrund.

Weites Themenspektrum

Auch in diesem Jahr wurden auf der S4-Konferenz mehrheitlich Vorträge zu technischen Themen präsentiert, die sich an ein Fachpublikum richteten und die auf die komplexen Spezifika der industriellen Steuerungstechnik und ihrer Sicherheitsprobleme ausführlich eingingen. So stellte der Stuxnet-Experte Ralph Langner weitere Details seiner Reverse-Engineering-Analysen vor, die mit nahezu an Sicherheit grenzender Wahrscheinlichkeit zeigen, dass das Angriffsziel des Wurms wie schon seit Längerem vermutet das Steuerungssystem der Zentrifugen der iranischen Urananreicherungsanlage in Natanz war. Der Microsoft-Sicherheitsforscher Suha Can zeigte, wie mit dem frei erhältlichen Microsoft-Tool EMET (Enhanced Mitigation Experience Toolkit, [2]) auch schwer zu patchende Leitsystem-Anwendungen nachträglich so gehärtet werden können, dass Standard-Angriffe gegen immer noch für die Leittechnik typische Schwachstellen wie Buffer oder Heap Overflows deutlich schwerer auszuführen sind. Ein großer Vorteil von EMET ist, dass damit aktuelle Schutztechnologien wie DEP (Dynamic Data Execution Protection) oder ASLR (Mandatory Address Space Layout Randomization) auch im Nachhinein für Anwendungen einsetzbar sind, selbst wenn der Hersteller diese bei der Quellcodeübersetzung nicht aktiviert hatte.

Sean McBride vom US-amerikanischen Dienstleister Critical Intelligence präsentierte eine ernüchternde statistische Analyse der in den letzten Jahren öffentlich bekanntgewordenen Sicherheitsschwachstellen in Leittechnik - und Automatisierungssystemen. Ein Ergebnis seiner Auswertung war, dass die Zahl der veröffentlichen Sicherheitslücken enorm zugenommen hat: so wurden bei dem auf industrielle Steuerungssysteme spezialisierten Informationsdienst ICS-CERT in den zehn Jahren von 2001 bis 2010 insgesamt 149 Schwachstellen gemeldet – bis Ende 2011 hatte sich diese Zahl dann in nur einem Jahr auf 364 Sicherheitslücken mehr als verdoppelt. Für weniger als die Hälfte dieser Lücken waren Anfang 2012 Sicherheitspatches verfügbar, besonders bedenklich hierbei ist zudem, dass laut McBrides Angaben das ICS-CERT festgestellt hat, das 60% der von den Herstellern veröffentlichten Patches die jeweilige Lücke gar nicht zuverlässig schlossen. Da nicht alle Lücken vom ICS-CERT erfasst bzw. veröffentlicht werden, ist bezüglich der Schwachstellenzahl von einer weitaus größeren Dunkelziffer auszugehen, insbesondere da in McBrides Auswertung noch nicht die 665 (!) Schwachstellen enthalten sind, die von den beiden ebenfalls an der S4-Konferenz anwesenden Sicherheitsexperten Terry McCorkle (Boeing) und Billy Rios (Google) im Rahmen eines „Freizeit-Projekts" im Herbst 2011 gefunden wurden [3]. Neben der klassischen Leittechnik war auch das zukünftige Smart Grid auf der Konferenz ein Thema, so stellte die GAI NetConsult den aktuellen Stand des deutschen Smart Metering Protection Profiles vor, das einen wichtigen Grundbaustein zu Absicherung des Smart Grids darstellt [4,5].

Application Whitelisting

Ein auf der diesjährigen S4-Konferenz intensiv diskutiertes Thema war das sog. Application Whitelisting. Es handelt sich dabei um ein Schadsoftwareschutzkonzept, bei dem im Gegensatz zum traditionellen pattern-basierten Ansatz („Blacklisting") auszuführender Programmcode nicht mit Mustern bekannter Schadsoftware verglichen wird. Stattdessen werden nur als vertrauenswürdig bekannte Programme und Code zur Ausführung zugelassen, welche zuvor über die sogenannte Whitelist freigegeben worden sind. Gerade im Leittechnik-Umfeld, wo auf Grund der sehr hohen Verfügbarkeitsanforderungen ein klassischer, pattern-basierter Virenschutz wegen der Gefahr von Fehlalarmen (False Positives) nur schwer einsetzbar ist, ist Applica-

tion Whitelisting eine interessante Alternative. Insbesondere kann beim Whitelisting auf die aufwendigen Funktionsprüfungen verzichtet werden, die beim Blacklisting nach jedem Pattern-Update notwendig sind, und die die Häufigkeit von AV-Pattern-Updates (und somit die Wirkung des Schadsoftwareschutzes) im Prozesstechnikbereich häufig stark reduzieren. Dr. Sebastian Obermeier von ABB Corporate Research und Andrew Ginter von Waterfall Security Solutions präsentierten zwei Vorträge, in denen sie sich beide mit der Effektivität von Whitelisting-Lösungen und Methoden zur Umgehung dieser Schutzmechanismen beschäftigten. Während Ginter sich mit allgemeinen Ansätzen zur Aushebelung des Whitelistingschutzes durch Software-Interpreter wie Perl oder TCL befasste, stellte Dr. Obermeier eine vergleichende Studie des ABB-Forschungszentrums vor. Hier wurden drei verschiedene Whitelisting-Lösungen, die auf unterschiedlichen technischen Ansätzen beruhen, getestet. Leider ist ABB durch strikte Vertraulichkeitsvereinbarungen mit den Herstellern der Whitelisting-Software gebunden, so dass die Ergebnisse nur in anonymisierter Form vorgestellt werden durften. Neben der Fragestellung, ob die Whitelisting-Software mit ABB-Produkten kompatibel ist wurde auch die Effektivität des Schutzes untersucht, insbesondere ob Whitelisting den klassischen Virenschutz und ein Patchmanagement vollständig ersetzen kann. Das ABB-Forschungsteam fand in allen getesteten Produkten Möglichkeiten, die Schutzfunktion auszuhebeln oder zu umgehen. Insbesondere zeigte die Untersuchung laut Dr. Obermeier das Application Whitelisting kein Ersatz für ein umfassendes Patchmanagement sein kann. Auch die in den Produkten enthaltenen zusätzlichen Speicherschutz-Funktionen konnten nicht alle Angriffe gegen ungepatchte Sicherheitslücken abfangen, weshalb die Installation von Sicherheitsupdates immer noch notwendig bleibt. Auch wenn die Whitelisting-Lösungen erwartungsgemäß keinen hundertprozentigen Schutz bieten konnten, scheinen sie aber trotzdem eine sinnvolle Alternative zu einem pattern-basierten Schadsoftwareschutz für Leitsystemkomponenten darzustellen.

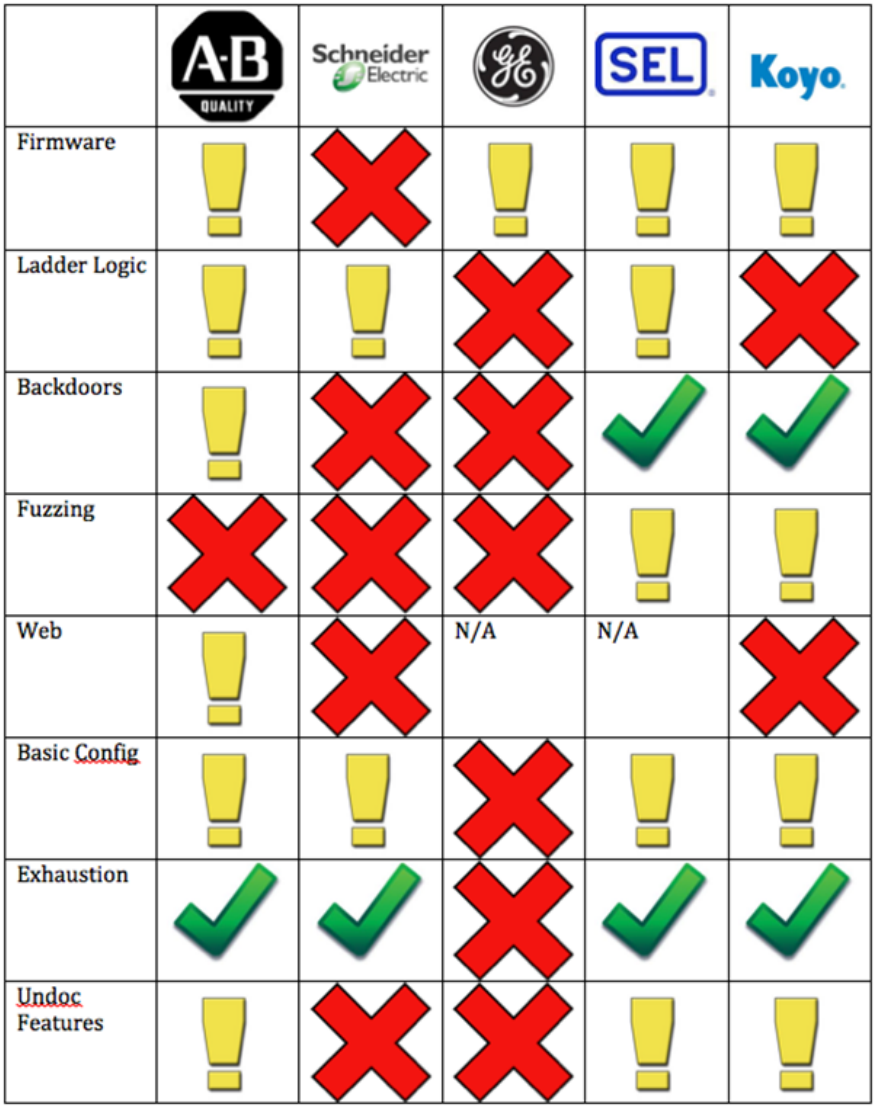

Abbildung-1: Überblick über die Ergebnisse von Project Basecamp (X: einfach auszunutzende Schwachstelle, !: Schwachstelle vorhanden und vermutlich ausnutzbar, ✓: Kein Problem festgestellt; mit freundlicher Genehmigung von Dale Peterson, Digital Bond)

Project Basecamp

Mit großer Spannung wurde von allen S4-Teilnehmern der erste Vortrag des zweiten Konferenztages zum sog. „Project Basecamp" erwartet. Der Konferenzveranstalter Dale Peterson, Geschäftsführer des renommierten, auf SCADA-Sicherheit spezialisierten Beratungsunternehmens Digital Bond hatte für dieses Projekt mehrere Sicherheitsexperten gebeten, sieben verschiedene SPSen (Speicherprogrammierbare Steuerungen) und Automatisierungskomponenten unterschiedlicher Hersteller einer Reihe von Sicherheitstests zu unterziehen. Die Ergebnisse dieser Untersuchung wurden exklusiv auf der S4-Konferenz veröffentlicht. Um die befürchteten juristischen Schwierigkeiten im Vorfeld der Veröffentlichung zu vermeiden wurden die Komponentenhersteller vorab weder über die untersuchten Produkte noch über die Testergebnisse informiert. Deshalb waren Sicherheitsexperten verschiedener Hersteller angereist, um sich vor Ort zu informieren – sicherlich in der Hoffnung nur den Mitbewerb und nicht die eigenen Produkte auf

der Liste der geprüften Systeme zu finden.
Das vom Digital-Bond-Mitarbeiter Reid Wightman, einem international anerkannten SCADA-Sicherheitsspezialisten, geleitete Projekt hatte die folgenden Steuerungskomponenten untersucht:

- Control Microsystems SCADAPack
- General Electric D20ME
- Koyo / Direct LOGIC H4-ES
- Rockwell Automation / Allen-Bradley ControlLogix
- Rockwell Automation / Allen-Bradley MicroLogix
- Schneider Electric Modicon Quantum
- Schweitzer SEL-2032

Es handelt sich dabei um Automatisierungskomponenten, die in der industriellen Produktion und in der Energieversorgung, vor allem in Nord- und Südamerika und in Asien eingesetzt werden.

Wightmans Vortrag dauerte zwei Stunden und zeichnete ein mehr als deutliches Bild vom Stand der Softwarequalität der im Bereich der Leittechnik eingesetzten Produkte – Wightman sprach wortwörtlich von einem „Blutbad". Alle getesteten Komponenten wiesen eine schier unüberschaubare Vielzahl von unterschiedlichen Schwachstellen auf. Die SCADA Pack-Komponente wurde durch die ersten einfachen Tests bereits so in Mitleidenschaft gezogen, dass hier keine weitere Untersuchung möglich war und keine Testergebnisse präsentiert werden konnten.
Die identifizierten Sicherheitslücken umfassen ein weites Spektrum von Schwachstellentypen, im Folgenden deshalb nur ein grober Überblick:

- undokumentierte, fest einprogrammierte und nicht deaktivierbare Standardnutzer
- ungeschützte Passwortübertragung über das Netzwerk
- unauthentisierter Schreibzugriff auf Firmware und SPS-Programmierung
- unauthentisierter Zugriff auf SPS-Funktionen
- unauthentisierter Vollzugriff auf den Arbeitsspeicher der Komponenten
- Buffer-Overflows
- Replay-Schwachstellen in den genutzten Netzwerkprotokollen
- Cross-Site-Scripting (XSS) und Session-Hijacking in den zur Parametrierung genutzten Web-Interfaces
- eine Vielzahl von Denial-of-Service-Schwachstellen

Über die genannten Sicherheitslücken lassen sich die Controller bei einem Netzwerkzugriff nahezu beliebig manipulieren, z.B. ist es möglich die Komponenten neu zu starten oder zu stoppen, den SPS-Speicher auszulesen und zu beschreiben, den Programmablauf innerhalb der SPS abzuändern und umzuprogrammieren sowie die Ein- und Ausgänge der SPS zu manipulieren. Ebenso können die Komponenten auf sehr einfache Art zum Absturz gebracht werden.
Es handelt sich hierbei sowohl um Programmier- und Implementierungsfehler aber auch um grundlegende Design- und Architekturschwächen. Während ein Hersteller einen Implementierungsfehler durch ein Firmware-Update beheben kann, ist dies bei einer De-sign-Schwäche häufig nicht einfach möglich, ohne Inkompatibilitäten zu verursachen. Besonders deutlich wird dies bei den von Wightmans Team aufgedeckten Schwachstellen in dem von den Rockwell-Komponenten genutzten Protokoll EtherNet/IP (*EtherNet Industrial Protocol*), die es beispielsweise erlauben die Controller über das Netzwerk in den STOP-Modus zu versetzten. Dies ist im Automatisierungsumfeld besonders kritisch, da hierdurch der durch die Steuerung geregelte Prozess schlimmstenfalls in einen unkontrollierten Zustand geraten kann. Da das EtherNet/IP-Protokoll als Quasi-Standard von ca. 150 weiteren Herstellern (z.B. Wago, HIMA, ABB, Yokogawa, Pilz, Phoenix Contact, Honeywell) ebenfalls genutzt wird, ist von den identifizierten Sicherheitslücken sehr wahrscheinlich auch eine Vielzahl anderer Geräte betroffen. Es dürfte schwer werden, die Design-Schwächen in einer neuen EtherNet/IP-Protokoll-version zu beheben, da hier vermutlich tiefgreifende Änderungen am Protokoll und eine entsprechende umfassende Abstimmung im zuständigen Normungsgremium ODVA (Open DeviceNet Vendor Association) notwendig sind.

Abbildung-2: Schneider Electric Modicon Quantum SPS, in der Mitte der Ethernet-Controller (Bild: S. Beirer, GAI NetConsult)

Heftige Kritik

Für verschiedene im Rahmen von „Project Basecamp" identifizierte Sicherheitslücken hat Digital Bond während der Konferenz und in den folgenden Tagen Angriffscode, sog. Exploits veröffentlicht. Unter anderem sind Module für das Angriffs- und Si-

cherheitstesttool Metasploit verfügbar. Hierfür und für die Tatsache, dass die Hersteller vor dem S4-Vortrag nicht über die gefundenen Schwachstellen informiert wurden und somit keine Gelegenheit hatten, Patches zu entwickeln wurde Dale Peterson von verschiedenen Seiten teilweise heftig kritisiert. Es sei unverantwortlich die Lücken der Controller, die auch in den Kritischen Infrastrukturen wie der Energieversorgung genutzt werden, überhaupt zu publizieren.

Abbildung-3: General Electric D20ME Steuerung (Bild: S. Beirer, GAI NetConsult)

Peterson wies die Kritik in seiner Auftaktrede und im persönlichen Gespräch zurück. Er begründete die Durchführung des Projekts damit, dass die grundsätzlichen Schwachstellen von SPSen, Safety- und Automatisierungskomponenten den Herstellern und Sicherheitsspezialisten seit mehr als 10 Jahren bekannt seien und das für die geprüften Produkte einige der jetzt veröffentlichten Schwachstellen bereits vor mehreren Jahren an die Verantwortlichen gemeldet wurden. Trotzdem hat es bisher nahezu keine Fortschritte bei der Absicherung der Komponenten gegeben. Besonders deutlich wurde dies nach der Veröffentlichung der Siemens S7-Schwachstellen auf der BlackHat-Konferenz durch Dillon Beresford in 2011 [6]. Hier beschränkte sich die Reaktion der meisten Experten und vieler Anwender darauf, die – zu großen Teilen bis heute nicht behobenen - massiven Sicherheitslücken als ein Übel anzusehen, das für Industrie-Komponenten üblich sei und mit dem man wohl leben müsse.

Peterson verglich die Situation mit der Veröffentlichung des „Fire-Sheep"-Tools im Jahre 2010. Mit Hilfe dieses einfach zu bedienenden Browser-AddOns können nicht hinreichend gesicherte Web-Anmeldeinformationen von Nutzern abgefangen werden, wenn diese dasselbe LAN- bzw. WLAN-Segment nutzen. Die zu Grunde liegende Schwachstelle war seit mehreren Jahren bekannt, aber erst nach der Veröffentlichung des Tools stellten populären Webdienste wie Hotmail, Twitter, WindowsLive oder Facebook ihre Anmeldeportale auf das verschlüsselte HTTPS-Protokoll um, wodurch die Sicherheitslücke behoben wurde. Peterson hofft, dass für die Leit- und Automatisierungstechnik ein ähnlicher Effekt eintritt. Anwender und Betreiber sollen erkennen welche massiven Lücken in den von ihnen eingesetzten Produkten vorhanden sind - und wie einfach diese ausgenutzt werden können. Nur so könnten die Hersteller dazu gebracht werden, seit langem bekannte Schwachstellen zu beheben, um spürbare Fortschritte auf dem Gebiet der SCADA-Sicherheit zu erzielen.
Eine Analyse der bisher veröffentlichten Exploit-Module zeigt, dass die ausgenutzten Schwachstellen wie beispielsweise das Auslesen eines unverschlüsselten Firmware-Passwords über TFTP so grundlegender Natur sind, dass ein durchschnittlicher Angreifer mit normalem IT-Security Knowhow durch Nutzung des Exploits bis auf den reinen Zeitgewinn keine wesentlichen Vorteil hat. Die Lücke lässt sich auch ohne das Exploitmodul mit einem TFTP-Client einfach finden und ausnutzen. Ebenso lässt sich die Funktionsweise eines anderen veröffentlichten Exploits, mit dem ein STOP-Befehl an eine EtherNet/IP-Komponente gesendet werden kann durch eine einfache Analyse des Netzwerkverkehrs zwischen dem im Internet verfügbaren Konfigurationstool und einem Controller in kürzester Zeit nachvollziehen.
Es ist prinzipiell davon auszugehen, dass ein motivierter Angreifer sich die Kenntnis über die im Project Basecamp identifizierten Schwachstellen durch eine entsprechende Analyse in kurzer Zeit selbst verschaffen kann – und das eine Vielzahl der jetzt veröffentlichen Schwachstellen den hieran interessierten Kreisen bereits seit Langem bekannt ist. Die Befürchtung, dass mit Hilfe der durch Project Basecamp veröffentlichten Exploits nun massenhaft Steuerungen von Nachahmungstätern auf Script-Kiddie -Niveau angegriffen werden, ist aber allein schon deshalb unbegründet, weil die Komponenten normalerweise nicht ungeschützt im Internet betrieben werden. Ein Angreifer muss deshalb zunächst einmal die üblichen Schutzmaßnahmen wie beispielsweise eine Firewall überwinden. Fehlen diese aber, so ist dies eine grobe Fahrlässigkeit des verantwortlichen Betreibers – zum Beispiel, wenn die Steuerungen von niederländischen Küstenschutz-Flutwehren ungeschützt im Internet zugänglich sind [7].

Keine Entwarnung in Sicht

In Hinblick auf die häufig kritischen Einsatzfelder der genannten Komponenten ist es schwer nachvollziehbar, dass bekannte Lücken und Probleme nicht öf-

fentlich diskutiert werden sollten - geschweige denn, dass sie nicht behoben werden. Gerade weil es sich um sensible Komponenten handelt, dürfen Anwender und Betreiber es nicht mehr länger hinnehmen, dass die nachweisbar vorhandenen massiven Sicherheits- und Stabilitätsprobleme nicht beseitigt werden. Gerade im Umfeld der Leit- und Steuerungstechnik müssen die gleichen wenn nicht sogar höhere Maßstäbe angelegt werden, wie sie in anderen Branchen üblich sind. Es sollte deshalb den Verantwortlichen durchaus zu denken geben, wenn auf renommierten Sicherheitskonferenzen wie dem „Kaspersky Threatpost Security Analyst Summit" das Sicherheitsniveau im SCADA-Bereich öffentlich als „lächerlich" bezeichnet wird [8] oder wenn das Fachpublikum einer anderen Konferenz bei der Vorstellung von Sicherheitslücken wiederholt in schallendes Gelächter ausbricht [3]. Auch unter einem optimistischen Blickwinkel ist es aber leider kaum zu erwarten, dass hier zeitnah eine umfassende Verbesserungen der Situation eintritt, gerade auch in Hinblick auf die langen Investitions- und Entwicklungszyklen und die langfristigen Einsatzzeiträume der betroffenen Systemtechnik. Im Gegenteil, berücksichtigt man die immer weiter zunehmende Vernetzung der Systeme und Komponenten, ist hier zunächst sogar mit einer weiteren Zunahme des Risikos zu rechnen. Sowohl Betreiber aus Industrie, Energieversorgung und Verkehrsleittechnik und die System- und Komponentenhersteller werden sich deshalb darauf vorbereiten müssen, dass in Zukunft immer häufiger Schwachstellen in kritischen Komponenten publiziert werden und das Gefährdungspotential mit jeder Veröffentlichung weiter ansteigt. Folgeprojekte zum Project Basecamp sind bereits von Digital Bond und anderen Sicherheits-Forschern angekündigt – dann werden vermutlich auch Komponenten und Anwendungen europäischer Hersteller dabei sein.

Referenzen

[1] www.digitalbond.com/s4

[2] support.microsoft.com/kb/2458544/de

[3] www.irongeek.com/i.php?page=videos/derbycon1/mccorkle-and-rios-100-bugs-in-100-days-an-analysis-of-ics-scada-software

[4] H. Diening: Sicherheit im Smart Metering, **Security** *Journal* #55, GAI NetConsult GmbH

[5] www.gai-netconsult.de/download/security/events/S4/SmartMeterGatewayPP.pdf

[6] S. Beirer: Tanzende Affen und andere Schwachstellen in SIMATIC S7-Steuerungen, **Security** *Journal* #56, GAI NetConsult GmbH

[7] www.rnw.nl/english/bulletin/sluices-pumping-stations-bridges-poorly-protected

[8] threatpost.com/en_us/blogs/state-scada-security-laughable-researchers-say-020312