SIEMENS
Ingenuity for life

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

Vortrag Maritimes Cluster Norddeutschland, 12.10.2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	**Vorstellung**	**2**
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	Was ist zu tun?	17
7	Zusammenfassung	38

© Siemens AG 2016

Der Referent

Klaas Eßmüller

Leitung Promotion Factory Automation

klaas.essmueller@siemens.com

Tel. +49 (0)40 2889-8599

Seit 2015	Leitung Promotion Factory Automation, Hamburg
2007-2010	Siemens AG, Promotor industrielle Steuerungstechnik und HMI (Human Machine Interface)
2006	Certification Microsoft Certified Systems Engineer (MCSE)
2000-2007	Siemens AG, Fachberater industrielle Kommunikation, PCbased-Automation und industrielle Steuerungstechnik
1999-2000	Praktikum und Diplomarbeit, Mannesmann Rexroth AG, Lohr am Main
1996-2000	Studium der Elektrotechnik, Fachrichtung Automatisierungstechnik , Fachhochschule Ostfriesland, Emden
1992-1995	Ausbildung zum Datenverarbeitungskaufmann

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	**Ziel des Vortrags**	**4**
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	Was ist zu tun?	17
7	Zusammenfassung	38

© Siemens AG 2016

Was Sie sich merken sollte
Das Defense-in-Depth-Konzept

SIEMENS
Ingenuity for life

Sicherheitsrisiken zwingen zum Handeln

Anlagensicherheit
- Physischer Zugangsschutz
- Prozesse und Richtlinien
- Security Services zum Schutz von Produktionsanlagen

Netzwerksicherheit
- Zellenschutz und Perimeternetzwerk
- Firewalls und VPN

Systemintegrität
- Systemhärtung
- Authentifizierung und Benutzerverwaltung
- Patch Management
- Erkennung von Angriffen
- Integrierter Zugangsschutz in der Automatisierung

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	**Bestandsaufnahme**	**5**
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	Was ist zu tun?	17
7	Zusammenfassung	38

© Siemens AG 2016

Bestandsaufnahme
Elektrische Bestandteile eines Schiffes

SIEMENS
Ingenuity for life

Elektrische „Bestandteile“ eines Schiffes (Auswahl):

▪ Dieselelektrischer Antrieb	- vernetzt
▪ Pumpen	- mit Diagnose-Schnittstelle
▪ Winden	- mit Diagnose-Schnittstelle
▪ Alarm-, Control- und Monitoring-System	- weitreichend vernetzt
▪ Energieversorgung und –verteilung	- vernetzt
▪ HVAC	- vernetzt
▪ Navigation und Ruderanlagen	- vernetzt
▪ Ballast-Systeme	- vernetzt
▪ Wasser-Aufbereitung und Abwasser	- vernetzt
▪ Sensorik z.B. für Treibstoff-Messung	- mit Diagnose-Schnittstelle
▪ …..	

Zusätzlich Offshore-Onshore-Verbindung des gesamten Schiffes

© Siemens AG 2016

Bestandsaufnahme
Elektrische Bestandteile eines Schiffes

SIEMENS
Ingenuity for life

Fragen:

Wissen Sie, was auf den Schiffen verbaut, vernetzt und wie gesichert ist?
Was steuert das Schiff? Was hält es am Leben?
Welche Schnittstellen und Schwachstellen bestehen?

Was hätte der Ausfall oder der Angriff auf ein solches (Teil-)System zur Folge?
Was muss ein Zulieferer beachten zur Betriebssicherheit des Schiffes?

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	**Trends im Bereich IT-Security**	**9**
5	Bedrohungslage	11
6	Was ist zu tun?	17
7	Zusammenfassung	38

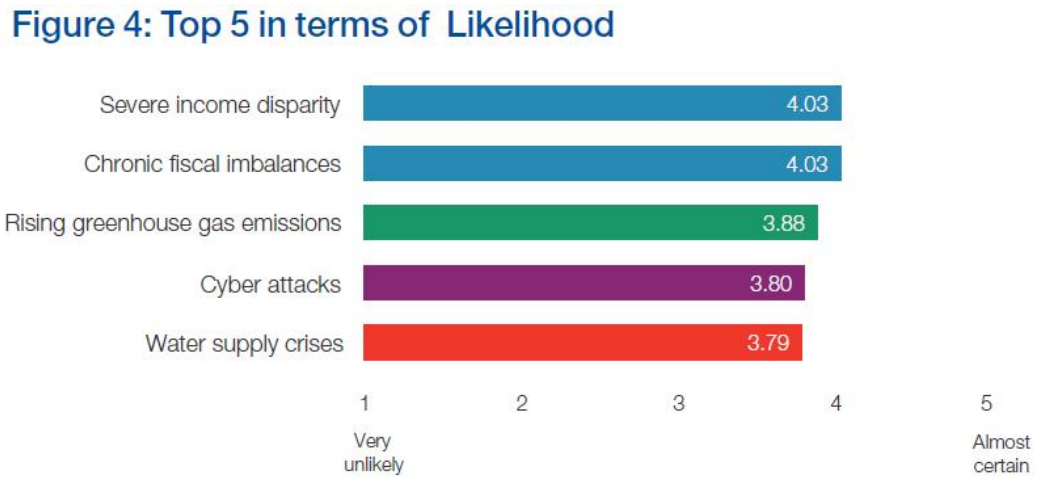
© Siemens AG 2016

Trends im Security-Bereich
Ständige Zunahme der weltweiten Vernetzung

SIEMENS
Ingenuity for life

Trends mit Auswirkungen auf die Security

- Cloud Computing-Ansätze
- **Zunehmender Einsatz von Mobilgeräten**
- **Drahtlostechnologie**
- **Verringerter Arbeitskräftebedarf**
- Smart Grid
- **Weltumspannender Fernzugriff auf Anlagen, Maschinen und mobile Anwendungen**
- **Das "Internet der Dinge"**



Quelle: World Economic Forum, 50 Global Risks

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	**Bedrohungslage**	**11**
6	Was ist zu tun?	17
7	Zusammenfassung	38

© Siemens AG 2016

Industrial Security

Schlagzeilen über aufgedeckte Schwachstellen auf den Titelseiten

SIEMENS
Ingenuity for life

Auch für die Schifffahrt besteht das Risiko, Opfer von sogenannten Cyber-Attacken zu werden – mit erheblichen Folgen.

Auf diese Gefahr weisen die Autoren der neuen Studie zur Schiffssicherheit der Allianz Global Corporate & Specialty SE (AGCS) hin (THB 22. März 2016).

Die Experten führen zur Begründung die zunehmende Verbreitung der elektronische Navigation, aber auch die fortschreitende Automatisierung und digitale Vernetzung in der Schifffahrt an. Damit nehme die Anfälligkeit für kriminell motivierte Hacker-Angriffe deutlich zu – „mit Folgen, die weit über den reinen Datenverlust hin ausgehen“, so die Sicherheitsexperten.

Ihnen liegen verschiedene Erkenntnisse über „einige nennenswerte Cyber-Vorfälle“ vor. Die Fachleute sind auch in der Langfristanalyse besorgt: „Möglicherweise bleiben der Branche nur noch wenige Jahre, um sich gegen das Risiko eines Schiffsverlustes durch eine Cyber-Attacke zu wappnen.“ Kapitän Andrew Kinsey, Senior Marine Risk Consultant, AGCS, stellt dazu fest: „Piraten nutzen bereits Sicherheitslücken aus, um den Diebstahl bestimmter Ladungen in die Wege zu leiten.“ Die dringende Empfehlung der Autoren: „Cyber-Gefahren für die Schifffahrt können nicht hoch genug bewertet werden.“

Quelle: http://www.thb.info/rubriken/maritime-sicherheit/single-view/news/it-piraten-greifen-reedereien-an.html

© Siemens AG 2016

Industrial Security

Schlagzeilen über aufgedeckte Schwachstellen auf den Titelseiten

SIEMENS
Ingenuity for life

Hacker können die Schiffsnavis umprogrammieren

Die Realität sieht anders aus. "Die Vorsorge unserer Kunden gegen Cyberangriffe ist verbesserungsfähig", beklagt sich der Allianz-Manager. Ein Kollege der Ergo-Versicherung sieht das genauso: "Das Problembewusstsein muss sicherlich noch größer werden", sagt Jürgen Heimes, der dort den Transportbereich verantwortet.

Quelle: http://www.welt.de/wirtschaft/article146919521/Cyberkriminelle-attackieren-Containerschiffe.html

Eine andere Gefahr kommt gerade erst ins Blickfeld der internationalen Schifffahrt: Cyberangriffe. Es soll bereits Hackerangriffe auf Schiffe gegeben haben, bisher noch unbestätigt. Angeblich wurden in zwei Fällen die Steuerungsanlagen von Schiffen manipuliert, ein Schaden ist daraus wohl nicht entstanden. Die jüngste Aufmerksamkeit um den Angriff auf den Unterhaltungskonzern Sony durch Computerhacker aus Nordkorea macht es deutlich: Ein Anschlag auf Computer, die zum Beispiel ein Schiff steuern oder das Beladen koordinieren, kann zu einem Totalausfall führen.

Quelle: http://www.welt.de/wirtschaft/article138877895/Der-riskante-Gigantismus-auf-den-Ozeanen.html

© Siemens AG 2016

Industrial Security

Schlagzeilen über Security-Vorfälle mittlerweile auf den Titelseiten

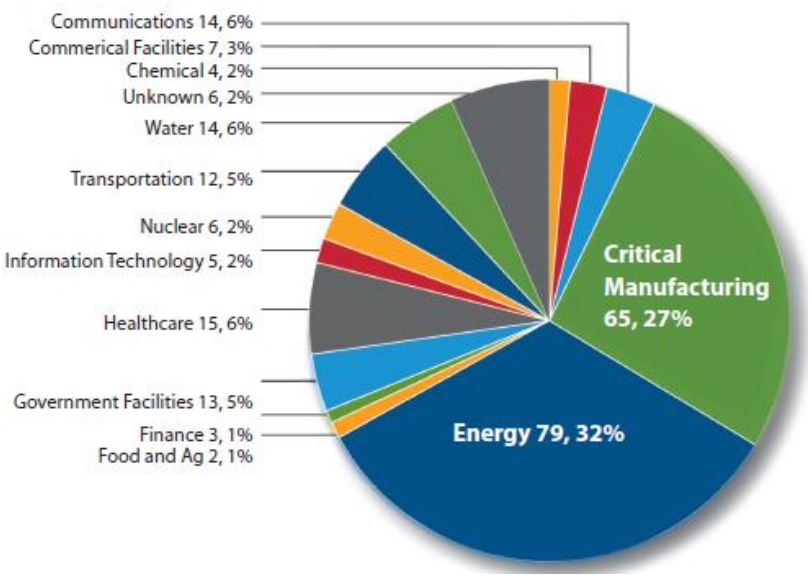
In Sachen Sicherheit Druck auf SCADA-Entwickler notwendig

USA durch Hacker-Angriffe gefährdet

Kraftwerks- und Produktionsanlagen-Software in USA offenbart riskante Sicherheitslücken

Stromnetz im Visier von Hackern

Industrielle Leitsysteme kommen in die Jahre – vermehrte Anfälligkeit für Cyberattacken



Quelle: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

In seinem Fiskaljahr (Oktober 2013 bis September 2014) untersuchte ICS-CERT 245 Angriffe auf Steuerungsrechner in der USA.

12. Februar 2013: „Unsere Gegner suchen nun auch nach Möglichkeiten, unser Energieversorgungsnetz, unsere Finanzinstitutionen und unsere Luftfahrtkontrollsysteme zu sabotieren. Wenn wir die letzten Jahre zurückblicken, müssen wir uns wundern, dass wir angesichts der realen Bedrohung unserer Sicherheit und Wirtschaft nichts unternommen haben. Deshalb habe ich im Laufe dieses Tages eine neue Rechtsverordnung unterschrieben, die unsere Cyber-Abwehr stärken wird… Nun muss der Kongress ebenfalls handeln und dieses Gesetz verabschieden, um unsere Regierung besser in die Lage zu versetzen, unsere Netzwerke zu sichern und Angriffe zu verhindern."

- US President Barack Obama

© Siemens AG 2016

Industrial Security
Cyber-Bedrohungen können an vielen Stellen auftreten

SIEMENS
Ingenuity for life

Cyber-Security-Bedrohungen schaffen Handlungsbedarf

- **Anlagenstillstand z. B. durch Viren oder Malware**
- Verlust von geistigem Eigentum, Rezepturen, …
- **Sabotage an der Produktionsanlage**
- **Manipulation von Daten oder Anwendungssoftware**
- **Unbefugter Einsatz von Systemfunktionen**
- Vorschriften und Normen bezüglich Industrial Security müssen eingehalten werden
  - Vorschriften:
    FDA, NERC CIP, CFATS, CPNI, KRITIS
  - Standards:
    ISA 99, **IEC 62443**

© Siemens AG 2016

SIEMENS
Ingenuity for life

Top 10 Bedrohungen 2014 im Überblick

1. **Infektion mit Schadsoftware** über Internet und **Intranet**
2. **Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware**
3. Social Engineering
4. **Menschliches Fehlverhalten** und Sabotage
5. Einbruch über Fernwartungszugänge
6. **Internet-verbundene Steuerungskomponenten**
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Smartphones im Produktionsumfeld
9. Kompromittierung von Extranet und Cloud-Komponenten
10. (Distributed) Denial of Service Angriffe ((D)DoS Angriffe)

Quelle: BSI-Veröffentlichung zur Cyber-Sicherheit 2014

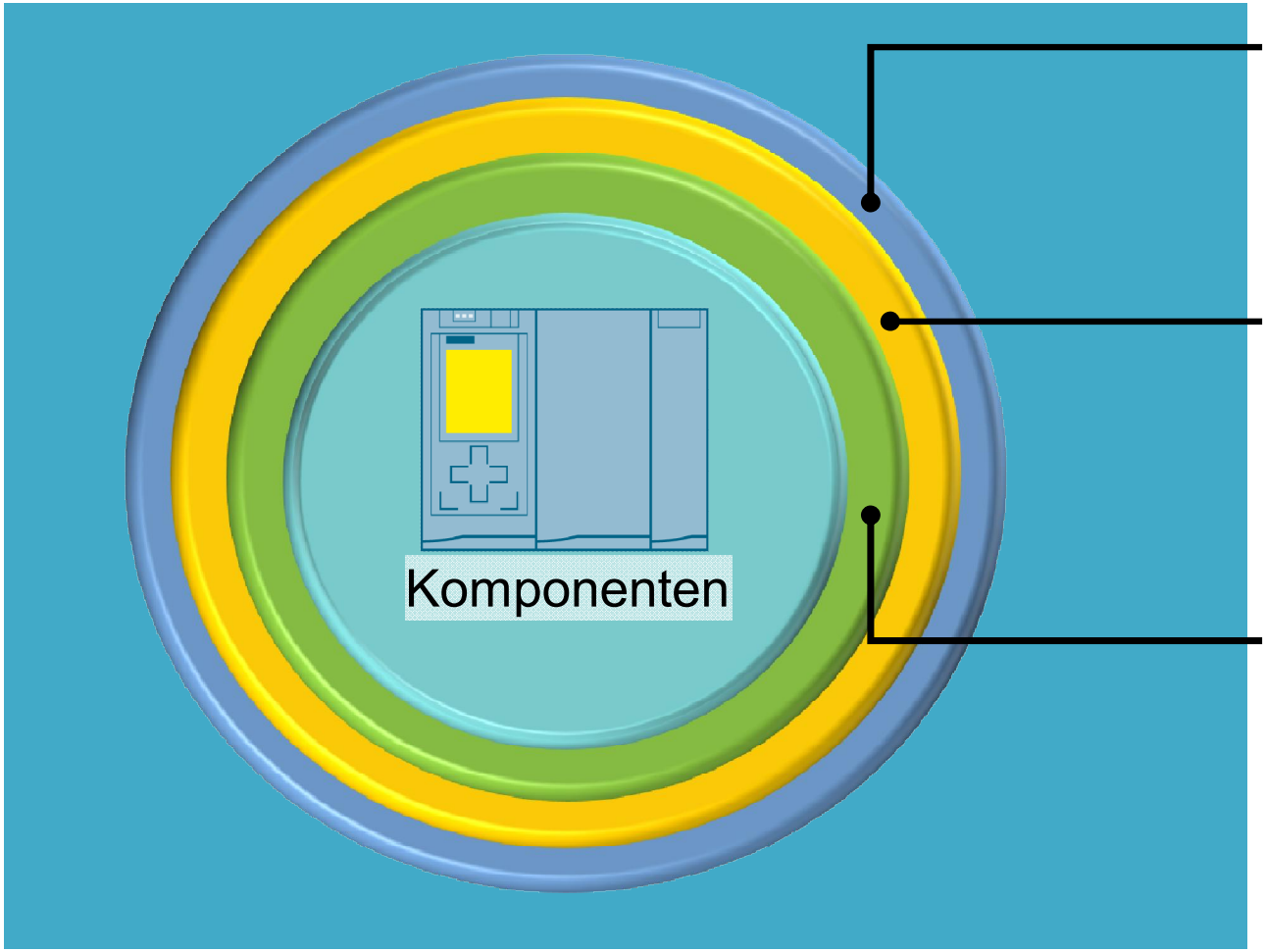
© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	**Was ist zu tun?**	**17**
6.1	Anlagensicherheit	19
6.2	Systemintegrität	23
6.3	Netzwerksicherheit	32
7	Zusammenfassung	38

Defence-in-Depth
Erklärung eines Schlagwortes



Anlagensicherheit
- Verhinderung des physischen Zugangs zu kritischen Anlagenbereichen
- Etablierung eines Security Managementprozesses

Netzwerksicherheit
- Kontrollierte Schnittstellen zwischen Netzwerkteilen z. B. über Firewalls
- Weitere Segmentierung des Netzwerkes

Systemintegrität
- Systemhärtung
- Antivirus- und Whitelisting-Software
- Wartungs- und Updatevorgänge
- Benutzerauthentifizierung für Bediener
- In Automatisierungskomponenten integrierte Zugriffsschutzmechanismen (Makerslist!)

Security-Lösungen im Industriekontext müssen alle Schutzebenen berücksichtigen

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

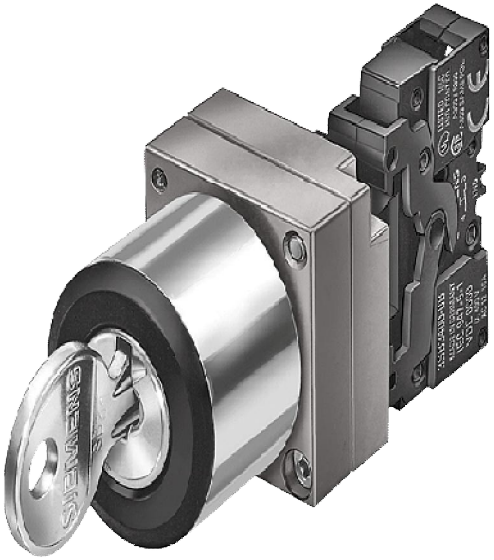
SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	**Was ist zu tun?**	**17**
6.1	**Anlagensicherheit**	**19**
6.2	Systemintegrität	23
6.3	Netzwerksicherheit	32
7	Zusammenfassung	38

Anlagensicherheit…
ganz einfach: physikalischer Zugang

SIEMENS
Ingenuity for life

Ein einfaches Beispiel für Anlagensicherheit…



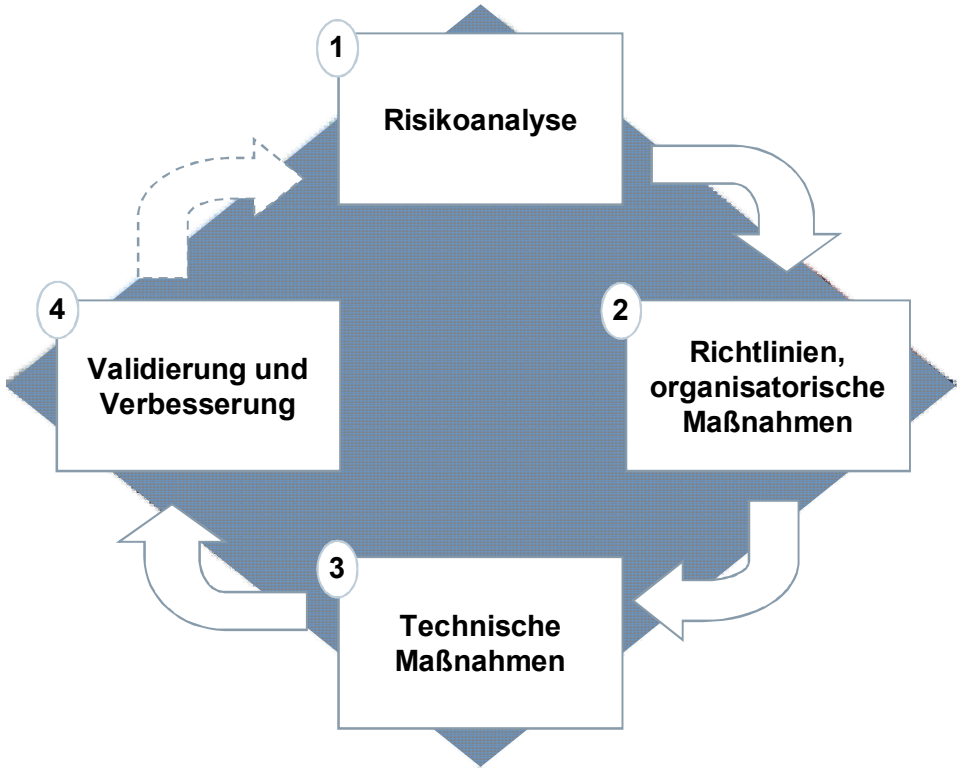
Verhinderung des physischen Zugangs

© Siemens AG 2016

Anlagensicherheit
Security-Management

Security-Management ist eine Schlüsselaufgabe:

- Risikoanalyse mit Definition von Risikominderungsmaßnahmen
- Festlegung von Richtlinien und Koordinierung organisatorischer Maßnahmen
- Koordination technischer Maßnahmen
- Regelmäßige/ereignisabhängige Wiederholung der Risikoanalyse



Security-Management ist unverzichtbar für ein durchdachtes Sicherheitskonzept

© Siemens AG 2016

Anlagensicherheit
Informationsmöglichkeiten

SIEMENS
Ingenuity for life

Wo finde ich Informationen?

- **BSI** (**B**undesamt für **S**icherheit in der **I**nformationstechnik) unter http://www.bsi.bund.de/
- **BSI** (**B**undesamt für **S**icherheit in der **I**nformationstechnik) – „Anforderungen an netzwerkfähige Industriekomponenten“ unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_067.pdf
- **ICS Cert** (Industrial Control Systems – Cyber Emergency Response Team) Alerts („Warnungen“) unter http://ics-cert.us-cert.gov/alerts
- **Siemens Industrial Security** Siemens-spezifische Warnungen unter http://www.siemens.de/industrial-security
- **Und nicht Shodan (https://www.shodan.io) !**

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	**Was ist zu tun?**	**17**
6.1	Anlagensicherheit	19
6.2	**Systemintegrität**	**23**
6.3	Netzwerksicherheit	32
7	Zusammenfassung	38

Industrial Security
IEC 62443-4-1 basierende TÜV SÜD-Zertifizierung

SIEMENS
Ingenuity for life

Zertifizierter Prozeß

- 7 Standorte vom TÜV SÜD nach IEC62443-4-1 zertifiziert
- Entwicklung von Simatic S7-Industriesteuerungen, Simatic Industrie-PCs, Simatic HMI-Geräte zum Bedienen und Beobachten und Sinamics-Antriebe bis zur Engineering-Software TIA (Totally Integrated Automation)-Portal
- Zertifizierung von: Fähigkeiten und Expertise, Sicherheit von Komponenten Dritter, Prozess- und Qualitätssicherung, sichere Architektur und sicheres Design, Schwachstellen-Handhabung bis zum Sicherheits-Update-, -Patch- und -Änderungs-Management

Security by Design

http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/PDF/Presse-Mitteilung_IEC62443_DE.pdf

© Siemens AG 2016

Industrial Security
Systemintegrität durch Achilles Level 2 Zertifizierung

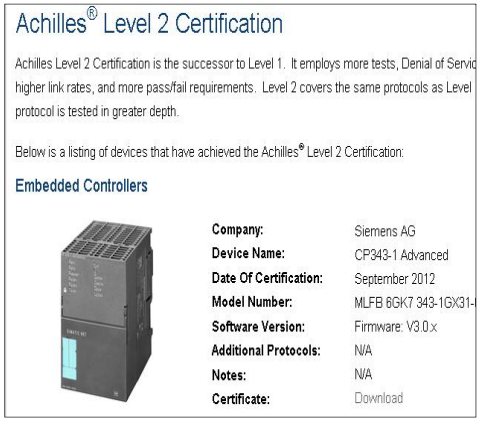
SIEMENS
Ingenuity for life

Achilles-zertifizierte Baugruppen

- Liste zertifizierter Baugruppen: https://www.wurldtech.com/certifications/achilles-communications-certified-products
- Aktuell (Stand: 11.10.2016) 146 Siemens-Produkte mit Achilles Level 2 Zertifizierung

Company:	Siemens AG
Device Name:	SIMATIC S7-1500 CPU 1513-1 PN
Date Of Certification:	May 2013
Model Number:	MLFB 6ES7 513-1AL00-0AB0
Software Version:	Firmware: V1.0.x
Additional Protocols:	N/A
Notes:	N/A
Certificate:	Download

Company:	Siemens AG
Device Name:	SIMATIC S7-1500 CPU 1516-3 PN/DP
Date Of Certification:	May 2013
Model Number:	MLFB 6ES7 516-1AN00-0AB0
Software Version:	Firmware: V1.0.x
Additional Protocols:	N/A
Notes:	N/A
Certificate:	Download



Achilles® Level 2 Certification

Achilles Level 2 Certification is the successor to Level 1. It employs more tests, Denial of Servic higher link rates, and more pass/fail requirements. Level 2 covers the same protocols as Level protocol is tested in greater depth.

Below is a listing of devices that have achieved the Achilles® Level 2 Certification:

Embedded Controllers

Company:	Siemens AG
Device Name:	CP343-1 Advanced
Date Of Certification:	September 2012
Model Number:	MLFB 6GK7 343-1GX31-
Software Version:	Firmware: V3.0.x
Additional Protocols:	N/A
Notes:	N/A
Certificate:	Download

Achilles-Test als Bestandteil des Systemtests

© Siemens AG 2016

Industrial Security

Manipulationsschutz im System SIMATIC S7-1500
(selbstverständlich mit Klassen-Zertifikat)

SIEMENS
Ingenuity for life

Höherer Manipulationsschutz

- Verbesserter Schutz gegen Manipulation der Kommunikation bei Zugriff auf Controller durch digitale Prüfsummen
- Schutz vor Netzwerkangriffen wie Einschleusen gefälschter/aufgezeichneter Netzwerkkommunikation (Replay-Angriffe)
- Geschützte Übertragung von Passwörtern bei Authentifizierung
- Erkennung manipulierter Firmware-Updates durch digitale Signaturen

Schutz der Kommunikation vor unberechtigten Manipulationen für höchste Anlagenverfügbarkeit

© Siemens AG 2016

SIMATIC S7-1518
Die leistungsfähigste CPU von Siemens

SIEMENS
Ingenuity for life

+power +efficiency

Code-Performance
(Analyse von 247 Kundenprojekten)

- 8 mal schneller als die CPU S7-1516
- 4 mal schneller als die CPU S7-319
- 10-12 mal schneller als die CPU S7-319 bei der Verwendung von symbolischer Programmierung

S7-1518 Highlights

Performance

- Bit, Word, Gleitpunkt: 1ns, 2ns , 6ns
- Klemme-Klemme Reaktion: ~160µs
- Kurze Zyklus Zeit: 250µs
- Rückwandbus: 400M Baud

Kommunikation

- PN IRT (V2.3)
- drei PROFINET Schnittstellen mit eigner IP-Adresse
- IPv6 mittels CP 1543-1

Security

- Hacker-Attacken Tests von ENCS (European Network for Cyber Security) blieben ohne Erfolg
- VPN und Firewall mit CP 1543-1
- Security Integrated: Know-How-Schutz, Binding to SMC, Manipulationsschutz, ...

Benutzerfreundlichkeit

- Integrierte Funktionalitäten: z.B. Motion, Trace, …
- Mehrsprachige Vor-Ort Diagnose am Display
- Forcetable und Watchtable direkt auf dem Display

© Siemens AG 2016

Industrial Security
Zugriffsschutz im System SIMATIC S7-1500

SIEMENS
Ingenuity for life

Höherer Zugriffsschutz (Authentifizierung)

- Neue Schutzstufe 4 für CPU-Komplettverriegelung (auch HMI-Verbindungen benötigen Passwort)*
- Granulare Vergabe von Berechtigungsstufen (1-3 mit eigenem PW)
- Für Zugriffe über CPU- und CM-Schnittstelle
- Generelle Projektierungssperre über CPU-Display

Umfassender Schutz gegen unberechtigte Projektierungsänderungen

* Nur in Zusammenspiel mit den SIMATIC HMI Panels möglich

© Siemens AG 2016

SIEMENS
Ingenuity for life

Whitelisting

- Anstatt ausführbare Programme (z.B. „.exe“, „.bat“, „.dll“) bei Start auf Malware zu untersuchen, werden einmalig alle ausführbaren Programme signiert.
- Nach Aktivierung des Whitelisting können nur noch autorisierte Anwendungen ausgeführt werden.
- Es können sichere Update-Quellen (z. B. für Sicherheits-Patches) angegeben werden
- Automatischer Schutz gegen fremden Programmcode (z. B. per USB-Stick) und sog "Zero-Day Exploits"
- Nachrüstung in bestehenden Anlagen möglich
- McAfee Application Control ist auf Verträglichkeit bei diverser SIMATIC Software getestet (s. nächste Seite)

An dieser Stelle: der Support für Windows XP durch Microsoft endete am 08. April 2014

© Siemens AG 2016

SIEMENS
Ingenuity for life

Windows XP

- Auszug aus dem BSI-Dokument „Umgang mit dem Ende des Supports für Windows XP“

Wird ein Altsystem mit nicht mehr unterstütztem Betriebssystem weiter betrieben, so muss dieses besonders gut geschützt werden, um die Sicherheit der gesamten Organisation nicht zu gefährden. Maßnahmen hierfür können beispielsweise sein:

- Verlagerung von allen Programmen, Diensten, Zugängen und Benutzerkonten, die nicht unbedingt auf diesem System laufen müssen, auf andere Systeme mit modernen Betriebssystemen, um die Angriffsfläche zu verkleinern.
- Installation von Schutzmechanismen, wie Application Whitelisting, welche typischerweise auch noch für veraltete Betriebssysteme unterstützt werden, oder die Nutzung der Richtlinien für Softwareeinschränkungen[1].
- Isolierung des Systems so weit wie möglich, idealerweise durch vollständige Trennung vom Rest des Netzes.
- Ist eine Trennung nicht möglich, so sollte das System in ein spezielles Netzsegment platziert, durch möglichst restriktive Firewalls geschützt und mittels Intrusion-Detection-Systemen gesondert überwacht werden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_085.html

© Siemens AG 2016

SIEMENS
Ingenuity for life

Folgende SIMATIC-Produkte wurden erfolgreich auf Verträglichkeit mit McAfee Application Control getestet:

- Step7 Classic
- Step7 im TIA Portal
- PCS7
- WinCC Classic
- WinCC im TIA Portal
- IndustriePCs
- Software-Controller auf Windows-basierend Betriebssystemen

Bitte jeweils die Versions-Abhängigkeiten beachten!

© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	**Was ist zu tun?**	**17**
6.1	Anlagensicherheit	19
6.2	Systemintegrität	23
6.3	**Netzwerksicherheit**	**32**
7	Zusammenfassung	38

Industrial Security
Firewall mit dem CP 1543-1

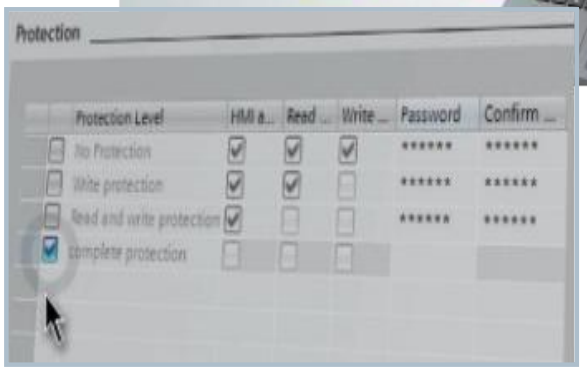
SIEMENS
Ingenuity for life

Höherer Zugriffsschutz (Authentifizierung)

- Neue Schutzstufe 4 für CPU-Komplettverriegelung (auch HMI-Verbindungen benötigen Passwort)*
- Granulare Vergabe von Berechtigungsstufen (1-3 mit eigenem PW)
- Für Zugriffe über CPU- und CM-Schnittstelle
- Generelle Projektierungssperre über CPU-Display

Erweiterter Zugriffsschutz

- über Security CP 1543-1 durch integrierte Firewall und VPN



Umfassender Schutz gegen unberechtigte Projektierungsänderungen

* Nur in Zusammenspiel mit den SIMATIC HMI Panels möglich

© Siemens AG 2016

Industrial Security

Netzwerksicherheit durch Einsatz einer Firewall – Begriffserklärung

SIEMENS
Ingenuity for life

192.168.1.15

Firewall-Regeln

Port		
20	FTP	Kommunikation gesperrt
21	FTP	Kommunikation gesperrt
80	HTTP	**Kommunikation erlaubt**
102	STEP7	Kommunikation gesperrt
119	NTP	Kommunikation gesperrt
666	DOOM	Kommunikation gesperrt

192.168.1.120

Firewall-Regeln

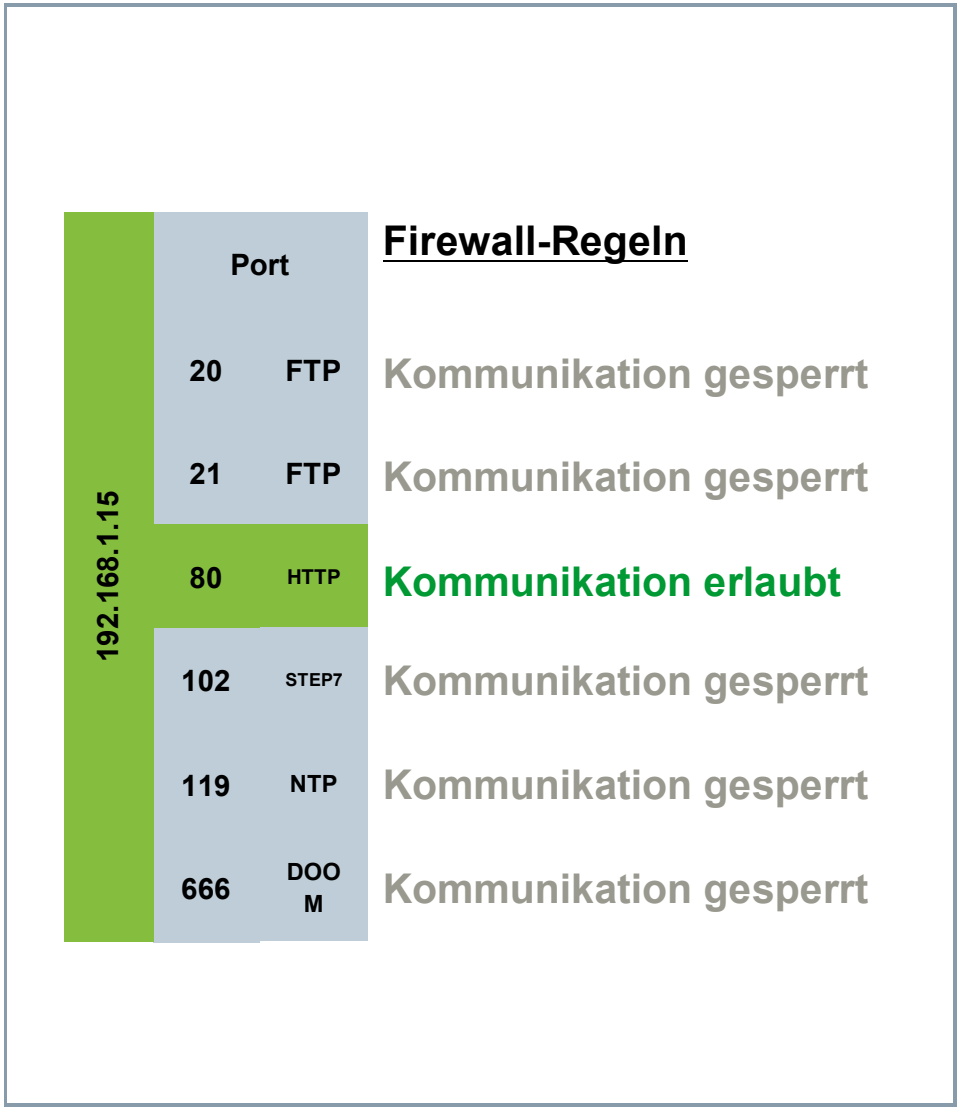
Port		
20	FTP	Kommunikation gesperrt
21	FTP	Kommunikation gesperrt
80	HTTP	**Kommunikation erlaubt**
102	STEP7	**Kommunikation erlaubt**
119	NTP	Kommunikation gesperrt
666	DOOM	Kommunikation gesperrt

© Siemens AG 2016

Industrial Security
Netzwerksicherheit durch Einsatz von Firewalls

SIEMENS
Ingenuity for life

- Durch den Einsatz einer Firewall kann gezielt Kommunikation am Netzwerk blockiert oder erlaubt werden.
- Durch eine Firewall kann Zugriff auf definierte Netzwerkdienste beschränkt werden.
- Vordefinierte Regeln ermöglichen eine sehr einfache Parametrierung der Firewall im TIA Portal für den CP1543-1
- Durch entsprechende Firewall-Regeln kann der Zugriff auf Netzwerkdienste auch auf bestimmte Quell-Adressen beschränkt werden.
- Firewall-Regeln werden zentral im TIA Portal verwaltet.



© Siemens AG 2016

Industrial Security
Netzwerksicherheit durch Einsatz von VPN

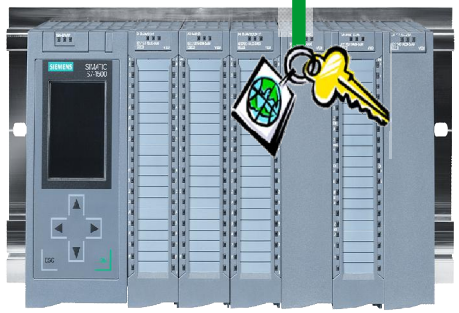
SIEMENS
Ingenuity for life

Zertifikat (=Schlüssel)
alternativ PSK (Pre-shared key) möglich

VPN **Von Ende-zu-Ende verschlüsselte Kommunikation (Tunnel)**

192.168.1.20

192.168.1.15

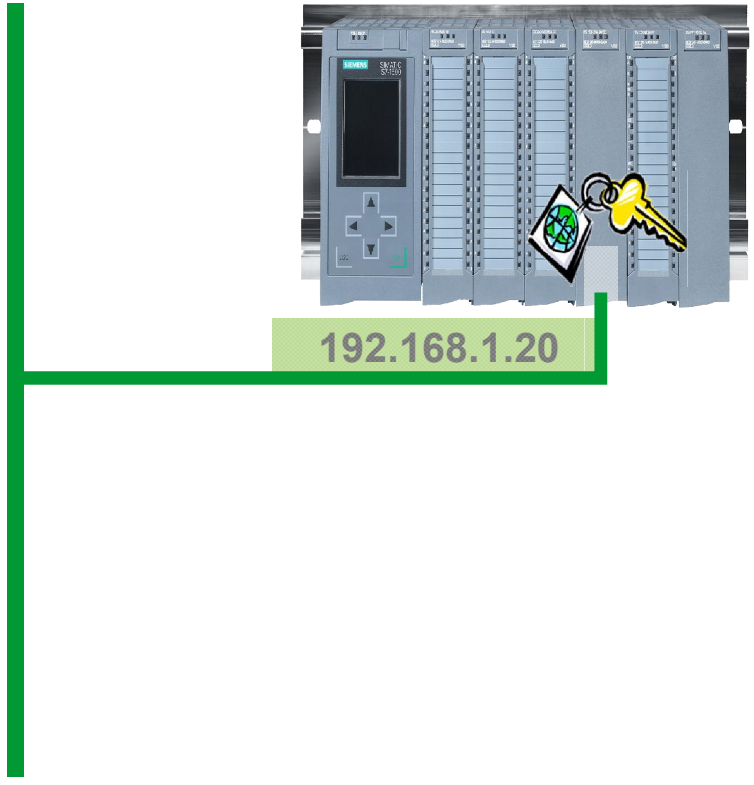


© Siemens AG 2016

Industrial Security
Netzwerksicherheit durch Einsatz von VPN

SIEMENS
Ingenuity for life

- Durch den Einsatz eines VPN (Virtuelles Privates Netzwerk) wird Kommunikation zwischen zwei Teilnehmern verschlüsselt.
- Zur Verschlüsselung kommen sog. Zertifikate oder Pre-shared keys (PSK) zum Einsatz, die automatisch vom TIA Portal generiert werden.
- Der sog. VPN-Tunnel bietet einen gesicherten Kommunikationskanal über ein unsicheres Netzwerk hinweg.
- Nur Teilnehmer mit Zertifikat oder PSK können an der VPN-Kommunikation teilnehmen.
- Ein „Mitlesen“ oder Stören der Kommunikation ist nicht möglich.



© Siemens AG 2016

IT Security auf Schiffen - aktuelle Probleme und mögliche Lösungsansätze

SIEMENS
Ingenuity for life

1	Vorstellung	2
2	Ziel des Vortrags	4
3	Bestandsaufnahme	5
4	Trends im Bereich IT-Security	9
5	Bedrohungslage	11
6	Was ist zu tun?	17
7	**Zusammenfassung**	**38**

© Siemens AG 2016

Zusammenfassung:

- IT-Security betrifft alle Branchen und somit selbstverständlich auch die maritime Industrie
- Der Bedarf nach IT-Security erfordert…
  - …das Umsetzen organisatorischer Maßnahmen beim Reeder, u.a.
  - …das ständige Informieren über Security-Schwachstellen und –Trends bei allen Beteiligten
  - …die Berücksichtigung von IT-Security schon im Entwicklungsprozess und
  - …Planung der Vernetzung unter Security-Gesichtspunkten.

„Emma Mærsk2“ von user:Nico-dk / Nils Jepsen - Eigenes Werk (own photo). Lizenziert unter CC BY-SA 2.5 über Wikimedia Commons
https://commons.wikimedia.org/wiki/File:Emma_M%C3%A6rsk2.jpg#/media/File:Emma_M%C3%A6rsk2.jpg

© Siemens AG 2016

Was Sie sich gemerkt haben sollten
Das Defense-in-Depth-Konzept

SIEMENS
Ingenuity for life

Sicherheitsrisiken zwingen zum Handeln

Anlagensicherheit
- Physischer Zugangsschutz
- Prozesse und Richtlinien
- Security Services zum Schutz von Produktionsanlagen

Netzwerksicherheit
- Zellenschutz und Perimeternetzwerk
- Firewalls und VPN

Systemintegrität
- Systemhärtung
- Authentifizierung und Benutzerverwaltung
- Patch Management
- Erkennung von Angriffen
- Integrierter Zugangsschutz in der Automatisierung

© Siemens AG 2016

Ansprechpartner

Klaas Eßmüller
Leiter Promotion Factory Automation

Lindenplatz 2
20099 Hamburg

Telefon: +49 40 2889 8599
Mobil: +49 1522 256 55 16

E-Mail:
klaas.essmueller@siemens.com

siemens.com/marine

© Siemens AG 2016