

DER FEIND IN MEINER ANLAGE



RISIKEN IM UMFELD DES INDUSTRIELLEN IOT AM BEISPIEL VERTEILTER ENERGIESYSTEME

Dr. Ingo Hanke, SMA Solar Technology AG



IMPORTANT LEGAL NOTICE



This presentation does not constitute or form part of, and should not be construed as, an offer or invitation to subscribe for, underwrite or otherwise acquire, any securities of SMA Solar Technology AG (the "Company") or any present or future subsidiary of the Company (together with the Company, the "SMA Group") nor should it or any part of it form the basis of, or be relied upon in connection with, any contract to purchase or subscribe for any securities in the Company or any member of the SMA Group or commitment whatsoever.

All information contained herein has been carefully prepared. Nevertheless, we do not guarantee its accuracy or completeness and nothing herein shall be construed to be a representation of such guarantee.

The information contained in this presentation is subject to amendment, revision and updating. Certain statements contained in this presentation may be statements of future expectations and other forward-looking statements that are based on the management's current views and assumptions and involve known and unknown risks and uncertainties. Actual results, performance or events may differ materially from those in such statements as a result of, among others, factors, changing business or other market conditions and the prospects for growth anticipated by the management of the Company. These and other factors could adversely affect the outcome and financial effects of the plans and events described herein. The Company does not undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise. You should not place undue reliance on forward-looking statements which speak only as of the date of this presentation.

This presentation is for information purposes only and may not be further distributed or passed on to any party which is not the addressee of this presentation. No part of this presentation must be copied, reproduced or cited by the addressees hereof other than for the purpose for which it has been provided to the addressee.

This document is not an offer of securities for sale in the United States of America. Securities may not be offered or sold in the United States of America absent registration or an exemption from registration under the U.S. Securities Act of 1933 as amended.

1

Industrielle IoT in verteilten Energiesystemen

2

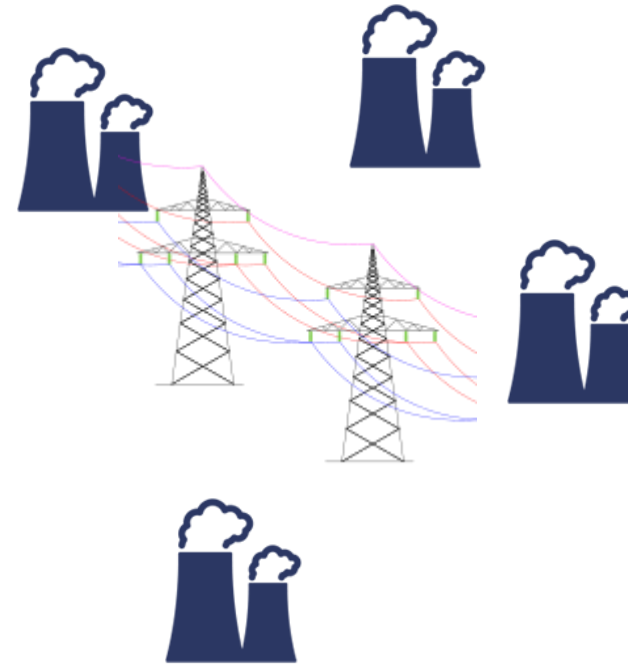
Cyber-Risiken und Defence-in-Depth Strategien

3

!

Vor 20 Jahren ...

- wenige Großkraftwerke sichern fast den gesamten Strombedarf
- Anteil Regenerative: $< 5 \%$
- Anteil Photovoltaik: $< 0,1 \%$



Und heute

...

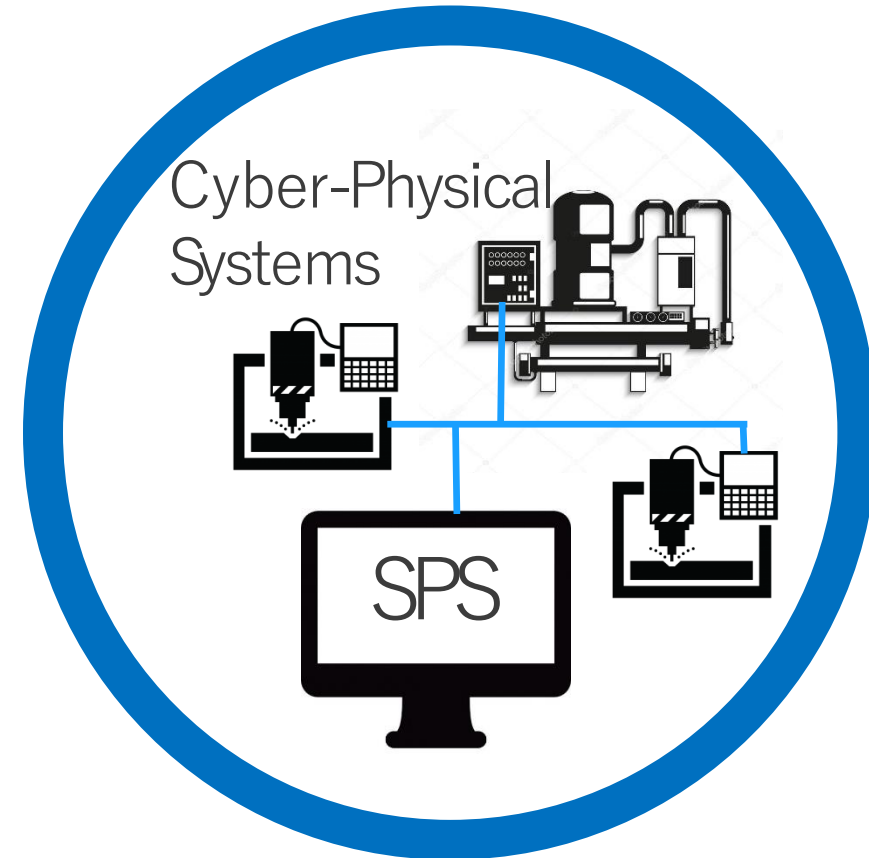
- Viele Millionen kleine und mittlere Anlagen (kW bis MW)
- Anteil Regenerative: > 39 %
- Anteil Photovoltaik: > 7 %

Neue Herausforderungen

- > Kontrollverlust
- > Netzstabilität
- > Dauerhafte Versorgungssicherheit (ausgerichtet am Bedarf / Lastgang)
- > Erneuerbare Energien insgesamt als kritische Infrastruktur

Vor 20 Jahren ...

- Lokale Netzwerke in IT und OT (Operational Technology)
- IT- und OT-Netzwerke getrennt
- Keine Internet-Anbindung: „Air Gap“



Und heute

...

- Viele Millionen lokale Netzwerke
- Direkt oder indirekt verbunden über das Internet
- Aus Cyber-Physical-Systems werden
Industrial Internet-of-Things (IIoT)

Neue Herausforderungen

- > Kontrollverlust
- > Versorgungssicherheit
- > (Neue) Cyber-Angriffsvektoren
- > Digitale Netze als kritische Infrastruktur

BLACKOUT

2-4 GW

Photovoltaik: 40
GWp

1

Industrielle IoT in verteilten Energiesystemen

2

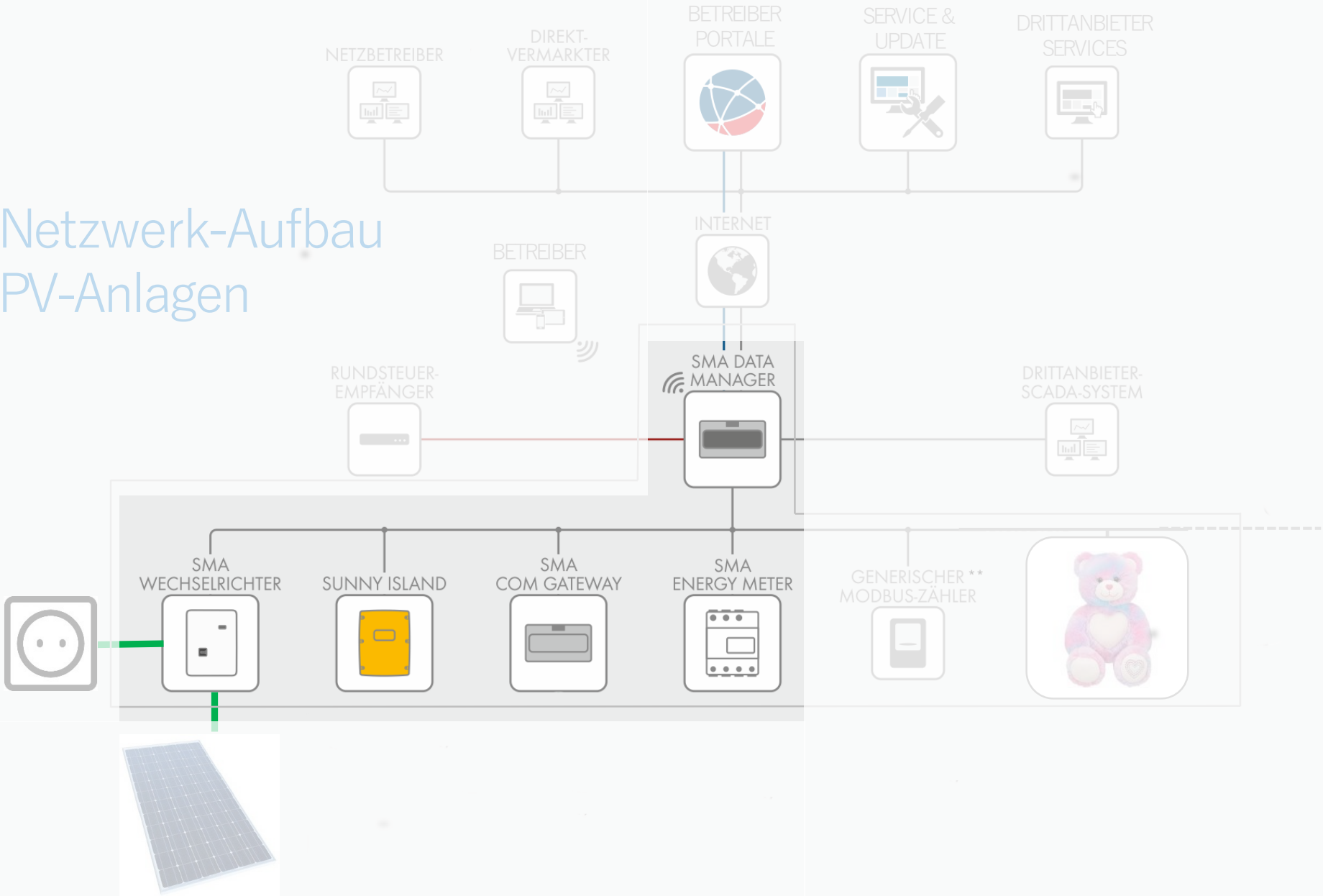
Cyber-Risiken und Defence-in-Depth Strategien

3

!

Wie können wir PV-Anlagen vor Cyber-Attacken schützen?

Netzwerk-Aufbau PV-Anlagen



Randbedingungen für Hersteller von Wechselrichtern und Energiemanagementsystemen

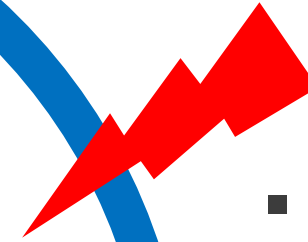
- > Wir sind nicht Betreiber einer Anlage
- > Wir haben keine Kenntnis und keinen direkten Einfluss auf die Architektur eines Anlagen-Netzwerks
- > Heterogene Anlagen- (und damit auch Netzwerk-)struktur:
 - Residential-Anlagen (typ. Hausdach): 3 bis 30kWp
 - Commercial-Anlagen (typ. Industrie): 30 bis 1000kWp
 - Utility-Anlagen (Kraftwerke): > 1 MWp
- > Qualität der Netzwerk-Infrastruktur sehr unterschiedlich (z.B. Überwachung)

Richtlinien & Perimeter

Firewall
Segmentierung



Firewall



- Alte, ungepatchte Standardsysteme
- Falsch konfigurierte Firewalls
- Port-Forwarding


CYBERRISIKEN & DEFENCE IN DEPTH :: SHODAN SCANS

Shodan

Developers

Book

View All...

 SHODAN

Explore

Developer Pricing

Enterprise Access

Contact Us

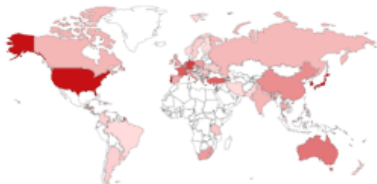
Exploits

Maps

TOTAL RESULTS

3,050

TOP COUNTRIES



Korea, Republic of	602
United States	587
Japan	463
Portugal	437
Germany	253

TOP SERVICES


HTTP	1,578
HTTP (8080)	258
8083	230
HTTP (81)	94
FTP	87


TOP ORGANIZATIONS


Korea Telecom	569
Nos Comunicacoes, S.A.	330
NTT	250
Verizon Wireless	212
Deutsche Telekom AG	162


TOP OPERATING SYSTEMS


Linux 3.x	1
-----------	---

**Korea Telecom**
Added on 2018-11-15 11:30:27 GMT
Korea, Republic of, Gimcheon
[Details](#)


**AT&T Wireless**
Added on 2018-11-15 11:27:58 GMT
United States, Atlanta
[Details](#)

**Verizon Wireless**
Added on 2018-11-15 11:23:47 GMT
United States
[Details](#)

HTTP/1.1 200
Server: 
Cache-Control: max-age=0, s-maxage=0, no-store, no-cache, must-revalidate
Date: Thu, 15 Nov 2018 11:29:47 GMT
Connection: close
Last-Modified: Thu, 15 Nov 2018 11:29:47 GMT
Content-Type: text/xml; charset=utf-8
Content-Length: 2143

HTTP/1.1 200
Server: 
Cache-Control: max-age=604800, s-maxage=604800
Date: Thu, 15 Nov 2018 11:27:41 GMT
Connection: close
ETag: Wednesday, 28 March 2018
Last-Modified: Wed, 28 Mar 2018 12:48:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 449

<!DOCTYPE...

HTTP/1.1 200
Server: 
Cache-Control: max-age=0, s-maxage=0, no-store, no-cache, must-revalidate
Date: Thu, 15 Nov 2018 11:23:35 GMT
Connection: close
Last-Modified: Thu, 15 Nov 2018 11:23:35 GMT
Content-Type: text/xml; charset=utf-8
Content-Length: 2203

Richtlinien &
Perimeter

Firewall

Segmentierung

Verschlüsselung
des Feldbusses



- Heterogene Systeme
- Alte Industrie-Protokolle (Modbus, ...)
- Nicht aktiviert

Richtlinien &
Perimeter

Firewall

Segmentierung

Verschlüsselung
des Feldbusses

Endpoint-Sicherheit

der IoT Devices
(z.B. Wechselrichter)



- > Eliminierung aller Default-Passwörter
- > Passwort-Policy nach Stand der Technik
- > Brute-Force Schutzmechanismen
- > Schließen nicht benötigter Ports
- > Sichere Authentifizierungsverfahren
- > Sichere Update-Mechanismen & Security-Patches

IT ≠ OT , IT ≠ IloT

- Betriebssicherheit! Verfügbarkeit!
- Keine „unkontrolliertes“ Ab-/Anfahren einer Anlage
- Keine automatisierten Änderung der Anlagenparameter
Beispiel: Einführung von FTPS statt FTP
- Aufwändige Validierung, ggf. Neu-Zertifizierung!
- Kompatibilität von Hard- und Software (Anlagenlebensdauer!)

Richtlinien &
Perimeter
Firewall
Segmentierung

Verschlüsselung
des Feldbusses

Endpoint-Sicherheit
der IoT Devices
(z.B. Wechselrichter)



- Schwachstellen in OS oder Standard Applikationen
- Schwachstellen in Individualsoftware (z.B. Web-UI)

Richtlinien &
Perimeter

Firewall
Segmentierung

Verschlüsselung
des Feldbusses

Endpunkt-Sicherheit
der IoT Devices
(z.B. Wechselrichter)

Security Monitoring &
Anomalie-Detektion
in zentralisierten Systemen

!



Ziele: was gewinnen wir durch Security-Monitoring und Anomalie-Detektion?

- > Awareness
- > Identifikation Angriffen auf Einzelanlagen
 - verkürzte Reaktionszeit
- > Identifikation von Massenangriffen („Blackout-Szenario“)
- > Angriffe voraussehen: „Predictive Security“

Herausforderungen

- > Bereits gelöst? Für **IT**: ja! Aber für **OT und IIoT** – nein!
- > Teilweise **embedded systems** ohne Standard-Betriebssystem
- > IIoT-Devices = **UN**trusted computing base
- > Devices sind bzgl. **Performance** und **Speicherbedarf**
kostenoptimiert
- > Dezentrale Anlagen i.d.R. **ohne** kontinuierliche Netzwerk-
Überwachung
- > **Kosten** Security-Equipment **zu hoch** in Relation zu
Anlagenkosten

Anforderungen an Monitoring & Anomalie-Detektion

- > **Auslagerung** nötiger Ressourcen und Prozesse für Monitoring und Analyse „in die **Cloud**“
- > Entwicklung von **preislich adäquaten** Technologien und Geschäftsmodellen (durch die Hersteller solcher Systeme)
- > **Mandantenfähige** Systeme für viele 1000 Anlagen
- > Industrie- bzw. Technologie-**spezifische** Anomalieerkennung (Minimierung der False-Positives!)

DER FEIND IN MEINER ANLAGE :: AGENDA



1

Industrielle IoT in verteilten Energiesystemen

2

Cyber-Risiken und Defence-in-Depth Strategien

3

!

Cyber Security für verteilte Energieerzeugung

**Regulation &
Standards**

**EVUs &
Netzbetreiber**

**Installateure
& Betreiber**

**Integratoren
& Hersteller**

**Security
Crowd**

Networking - z.B. German OWASP Day