# IT-Security für Autonomik

Dr. Carsten Rudolph
Abteilungsleitung Trust and Compliance

Fraunhofer
SIT

© Fraunhofer-Gesellschaft 2012

# Autonomik - Herausforderungen

- Autonome Systeme sind in der IT „normal“
- Sicherheitsmechanismen und – protokolle existieren
- Aber: Anforderungen der Autonomik Szenarien
- Benutzer und Geräteidentität unterscheiden
- Prozesse und Topologien dynamisch

# Use Cases: Produktion, Automatisierung, Logistik, Ackerbau, Verkehr, Verteidigung, etc.

**Generelle Eigenschaften**

- **Mobile Geräte ohne direkte Nutzerinteraktion**
- **Nutzung aller möglichen Kommunikationsmedien**
- **Einbindung von Legacy Systemen**
- **Echtzeitanwendungen**
- **Vernetzung von Automatisierung mit Office IT**

**Beispiele für weitere Eigenschaften**

- **Ad-Hoc Vernetzung**
- **Offene Systeme mit Verbindung zu Fremdgeräten**
- **Standardisierte Schnittstellen**

# Risiken und Maßnahmen
# Beispiel: Precise Farming / Landmaschinen

**Basis IT Security**

- Identifikation beteiligter Geräte
- Sicherheit der Kommunikation
- Aufbau der Netze / Mobile Ad-Hoc Netze
- Location / GPS

**Beispiel für weitergehende Themen**

- Gespeicherte Daten als Nachweise für Subventionen
- Subventionsbetrug als Motivation für Angriffe
- Sichere digitale Nachweise / Forensik

# Technologien: ``*Enterprise grade*´´ reicht nicht

**Existierende IT Sicherheitstechnologien stehen zur Verfügung:**

- **Firewalls – Wo ist der Perimeter?**
- **VPNs – Wie definiert man ein ``internes´´ Netz?**
- **Virenschutz – Ist blacklisting der richtige Ansatz?**
- **Intrusion Detection Systeme – Suche nach bekannten Angriffen an bestimmten Stellen im Netz?**

**Zusätzliche Technologien sind nötig:**

- **Hardware-basierte Sicherheit / Trusted Computing**
- **Verteilte Erkennung und Reaktion auf Angriffe Fremdgeräten**
- **Ziel ist der Schutz der Prozesse / der eigentlichen Aufgabe der Systeme**

# Technologien
# Beispiel: Trusted Core Network und TrustMaNet

- **Trusted Core Network:**
  Hirschmann Eagle Router, in die ein TPM integriert ist prüfen sich gegenseitig. Prototyp wurde bei der CeBIT und HannoverMesse 2014 gezeigt.

- **TrustMANET:**
  Vertrauenswürdiges Mobiles Ad-Hoc Netzwerk entwickelt von Fraunhofer SIT.
  Gegenseitige Prüfung in drahtlosen, mobilen Ad-Hoc Netzen.

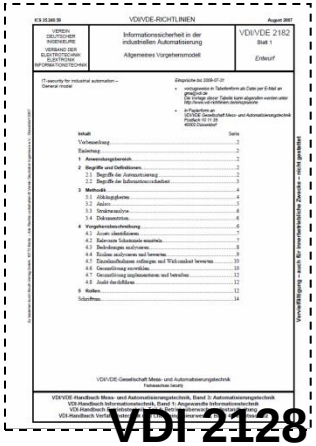
# Effizientes Management: Zero Touch Configuration

- Registrierung der Geräte benötigt lediglich eine eindeutige Gerätekennung (z.B. fingerprint eines krypt. Schlüssels), der das Gerät identifiziert.
- Das Gerät kommt direkt von der Produktion zur Installation. Je nach Protokoll muss keinerlei kundenspezifische Information eingebracht werden.
- Der Techniker schließt das Gerät an (eventuell erst an einen speziellen Konfigurationsport). Die Konfiguration, Registrierung, usw.  ist vollautomatisch.
- Keine USB-Sticks, kein Laptop zur Konfiguration, kein Nutzerinterface am Gerät nötig. Leuchtdioden zeigen die erfolgreiche Konfiguration an. Interaktion nur im Fehlerfall nötig.
- Fraunhofer SIT hat ein Protokoll zur Zero Touch Configuration entwickelt, das auf den Sicherheitsfunktionen des TPM basiert.

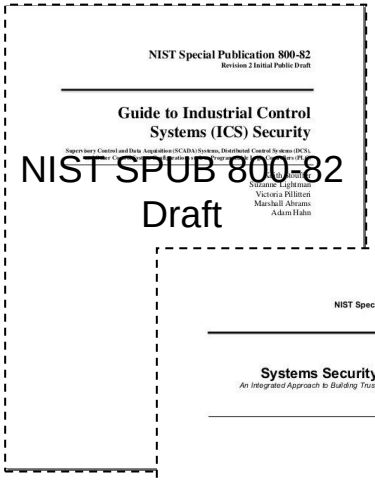
# Recommendations, Standards, Surveys

**VDMA: Survey**

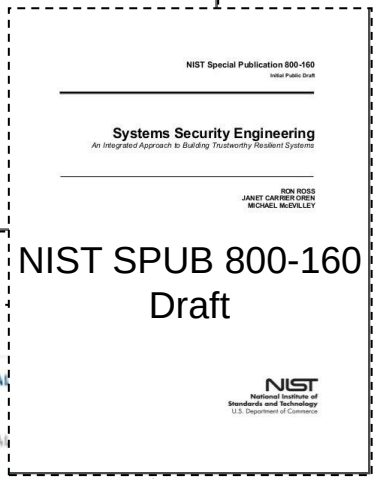
**BSI: ICS Security Kompendium**




**VDI 2128**




NIST SPUB 800-82 Draft




NIST SPUB 800-160 Draft

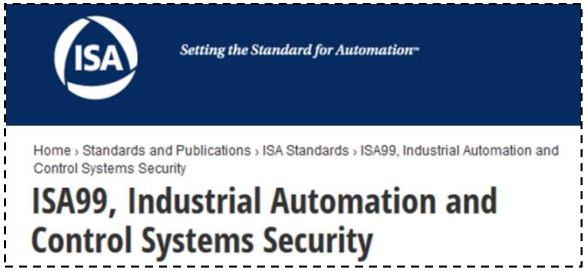
**IEC 62443**

Fraunhofer SIT:

Eberbacher Gespräche

Sicherheit und Industrie 4.0

OPC UA™



# Ausgewählte Offene Fragen

- **Kann man einen (vollständigen) Katalog von Sicherheitsanforderungen in der Autonomik erstellen?**
- **Prozesse zur Cyber Security in der Entwicklung?**
- **Können Referenzplattformen bei der Entwicklung sicherer Systeme in der Autonomik helfen?**
- **Wie weit wird die Integration von Echtzeitanwendungen mit Cloud und ähnlichen Technologien in der Autonomik gehen?**
- **Sind Autonomik Systeme (ähnlich wie andere IKT Systeme) international, also müssen beteiligte Jurisdiktionen berücksichtigt werden?**
- **Sind Unternehmen bereit in der IT Security zusammenzuarbeiten und Daten auszutauschen?**

## Dr. Carsten Rudolph

Carsten.rudolph@sit.fraunhofer.de

**Fraunhofer Institute for**
**Secure Information Technology (SIT)**

Head of Department Trust and Compliance

Rheinstrasse 75
64295 Darmstadt, Germany

Tel: +49 6151 869 344

www.sit.fraunhofer.de