Hardware-basierte Sicherheit für Kommunikationsinfrastrukturen

Dr. Carsten Rudolph
Abteilungsleitung Trust and Compliance

Vertretung: Norman Göttert, M.Sc.

Fraunhofer
SIT

Schäden durch IT-basierte Angriffe

Beispiele

Ausspionieren von Geschäftsgeheimnissen

Fehler in Produktionsprozessen

Schäden an Maschinen oder Produkten

Herausforderungen

Problem

- Geräte und IT-Netzwerke in der Industrie (Automatisierung, Produktion, …) werden miteinander verbunden
- Vergrößerung der Angriffsfläche
- Momentane Lösungen wie Firewalls, IDS oder VPNs sind nicht ausreichend

Technische Herausforderungen

- Verfügbarkeit, Integrität und Echtzeitbedingungen müssen gewahrt werden
- Standardschutzmethoden hierfür nicht geeignet
- Viele ältere Systeme in den Anlagen (mit potentiellen Schwachstellen)

Herausforderungen

F&E Lösungsansatz

- Hardware-basierte Geräteidentifikation und Integritätsüberprüfung
- Hochverteilter Ansatz: Jedes Gerät überprüft alle Nachbarn
- Trennung zwischen Security und funktionaler Kommunikation

Verfügbare Lösung

- Trusted Core Network Prototyp
  - Nutzt Trusted Platform Modul in Hirschmann Router
- Teil des Industrie 4.0 Demostrators auf der CeBIT und HannoverMesse 2014

Hardware-basierte Sicherheit

Trusted Platform Module - TPM

- Standardisiertes Hardware-Modul (TCG)
- Fest integriert in das Gerät
- TPM ermöglicht u.a.
  - Sicherer Speicher für kryptographische Schlüssel und Gerätezustand
  - Zufallszahlengenerator
  - Signaturberechung direkt im Chip
  - Authentische Attestierung des Zustandes eines Gerätes
- Zertifizierte Sicherheit (Security):
  Common Criteria EAL-5 für Chip Design und EAL-4+ für gesamten TPM.

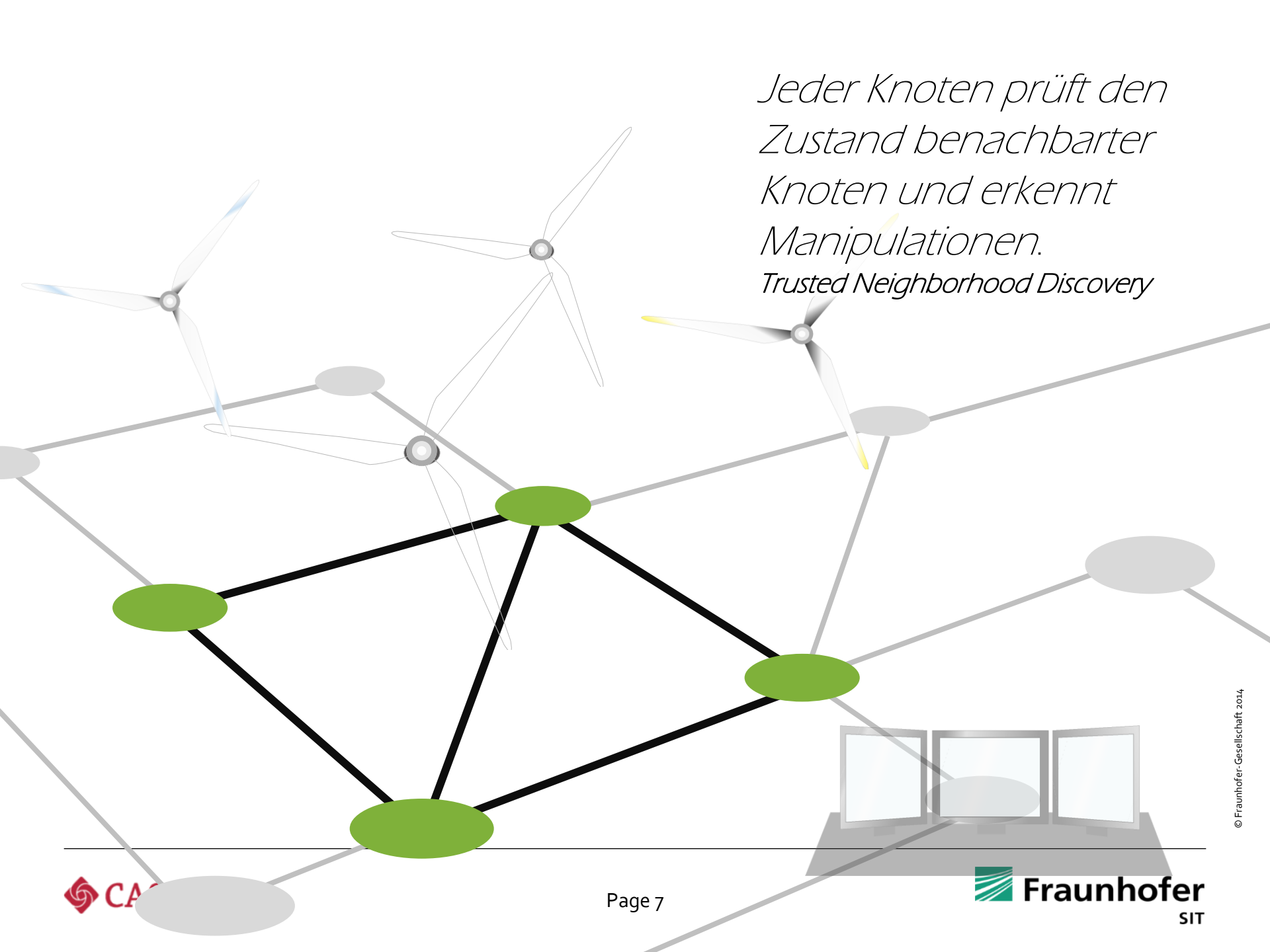
Trusted Core Network

Ziele für verteilte Integritätsprüfung

- Verteilte/redundante Kontrolle (peer-to-peer)
- Ausbreitung von Malware unterbinden
- Monitoring mit schnellen Warnungen
- Schutz vertraulicher Daten
- Sichere und effiziente Managementprozesse

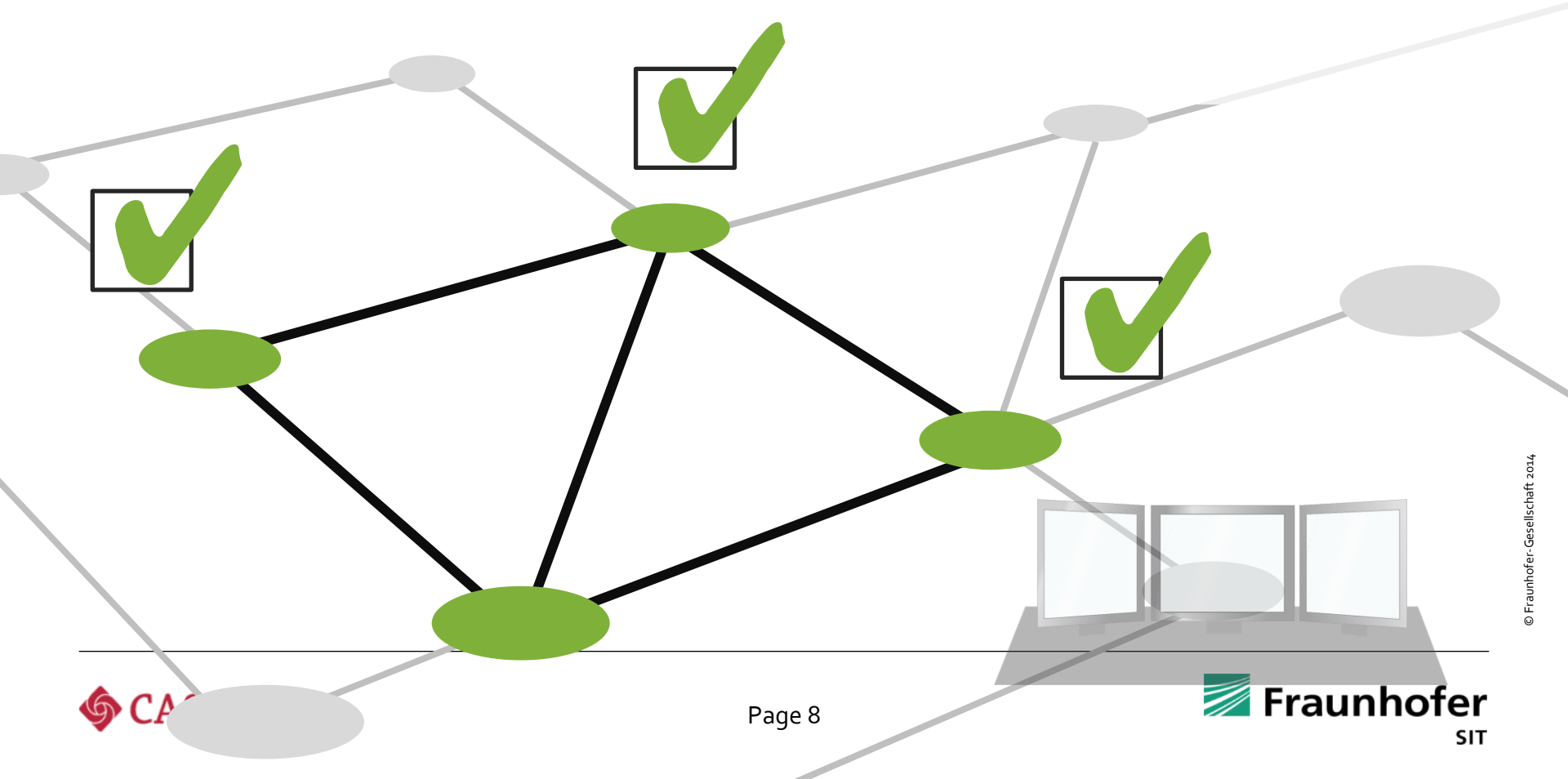
Jeder Knoten prüft den Zustand benachbarter Knoten und erkennt Manipulationen.

Trusted Neighborhood Discovery



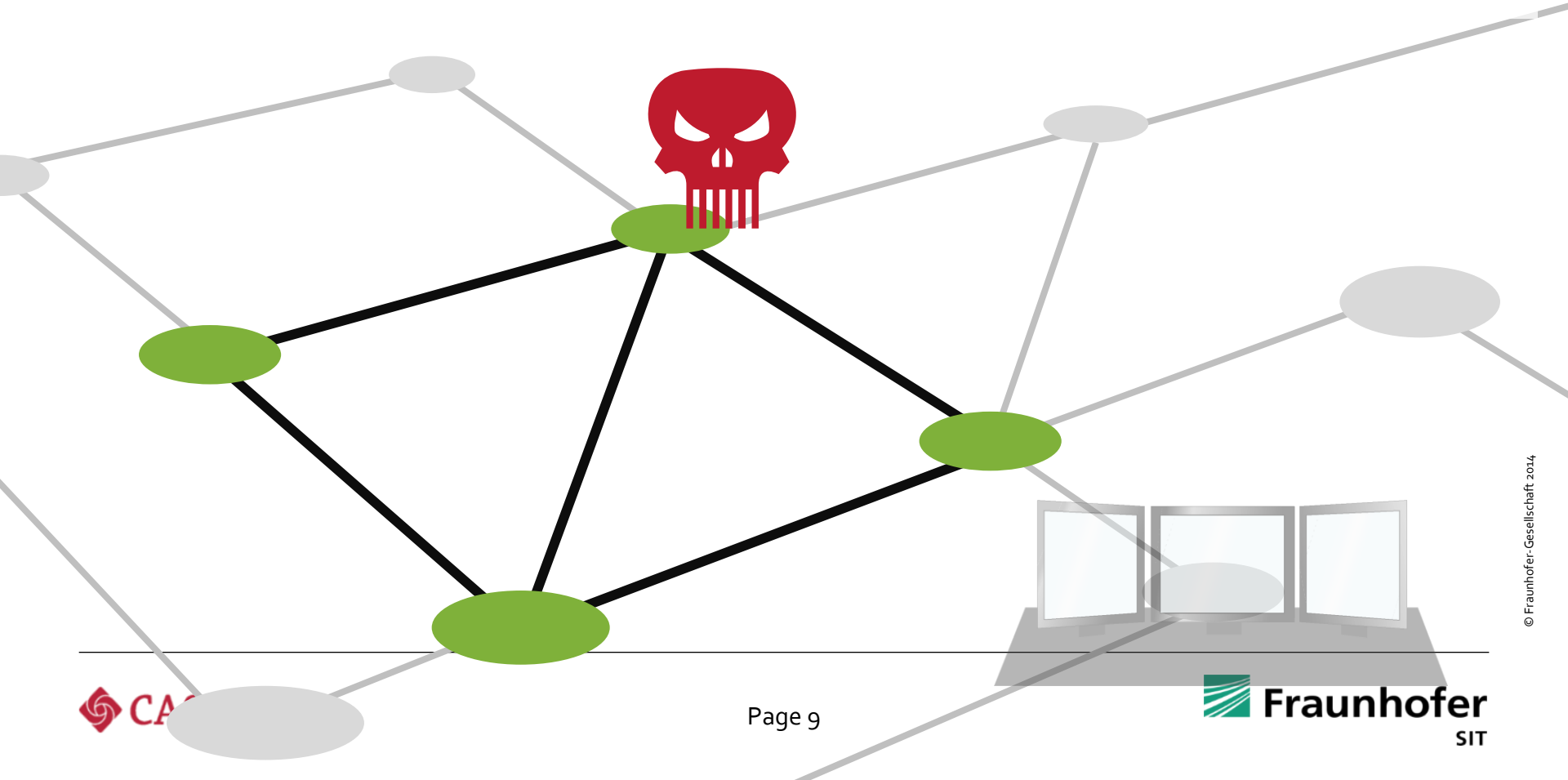
Fraunhofer SIT

Identität und momentaner Zustand werden mit Hilfe des TPMs berichtet.



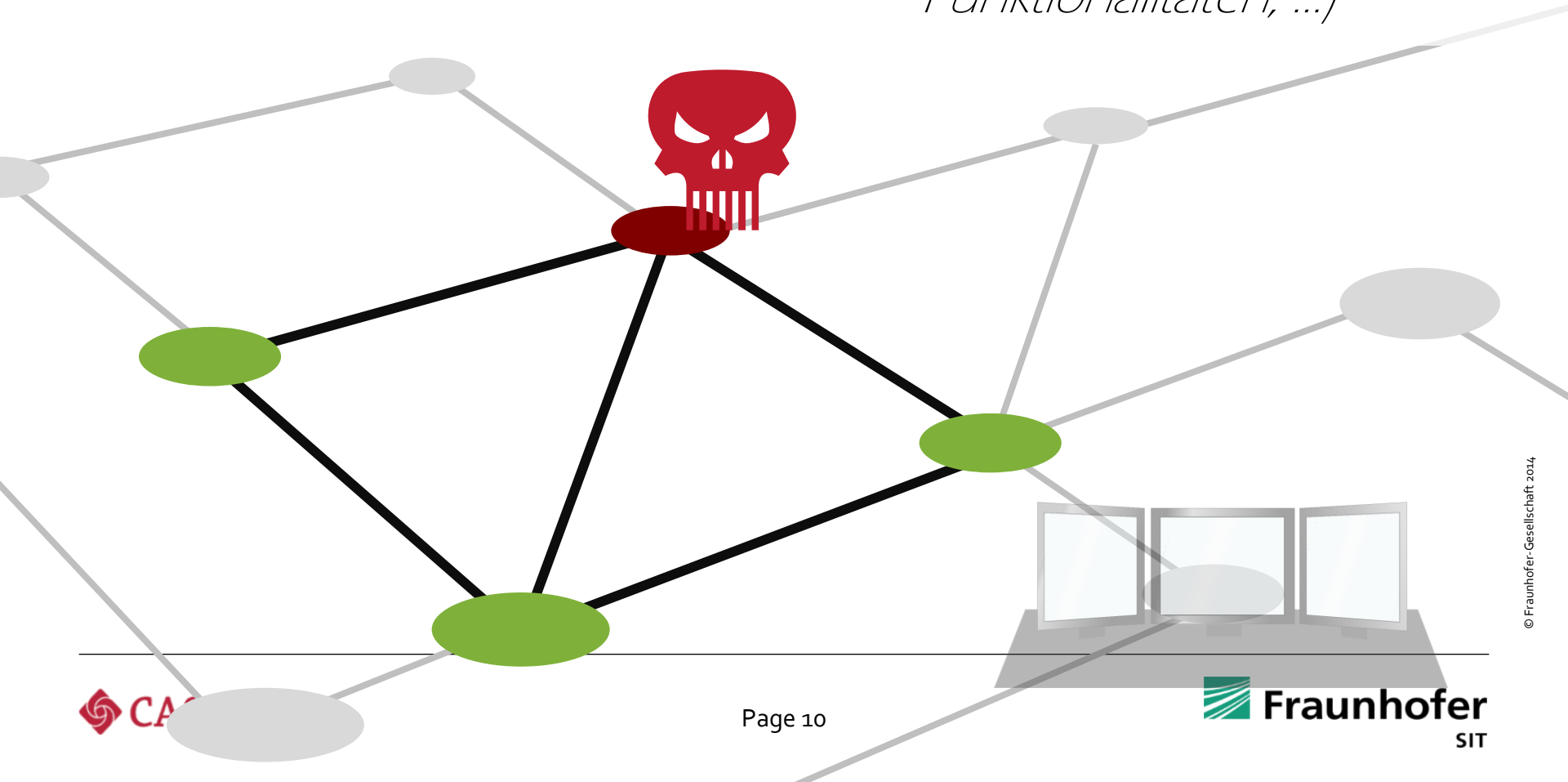
Fraunhofer SIT

Änderungen der Konfiguration oder der Aufruf von irregulärer Software …



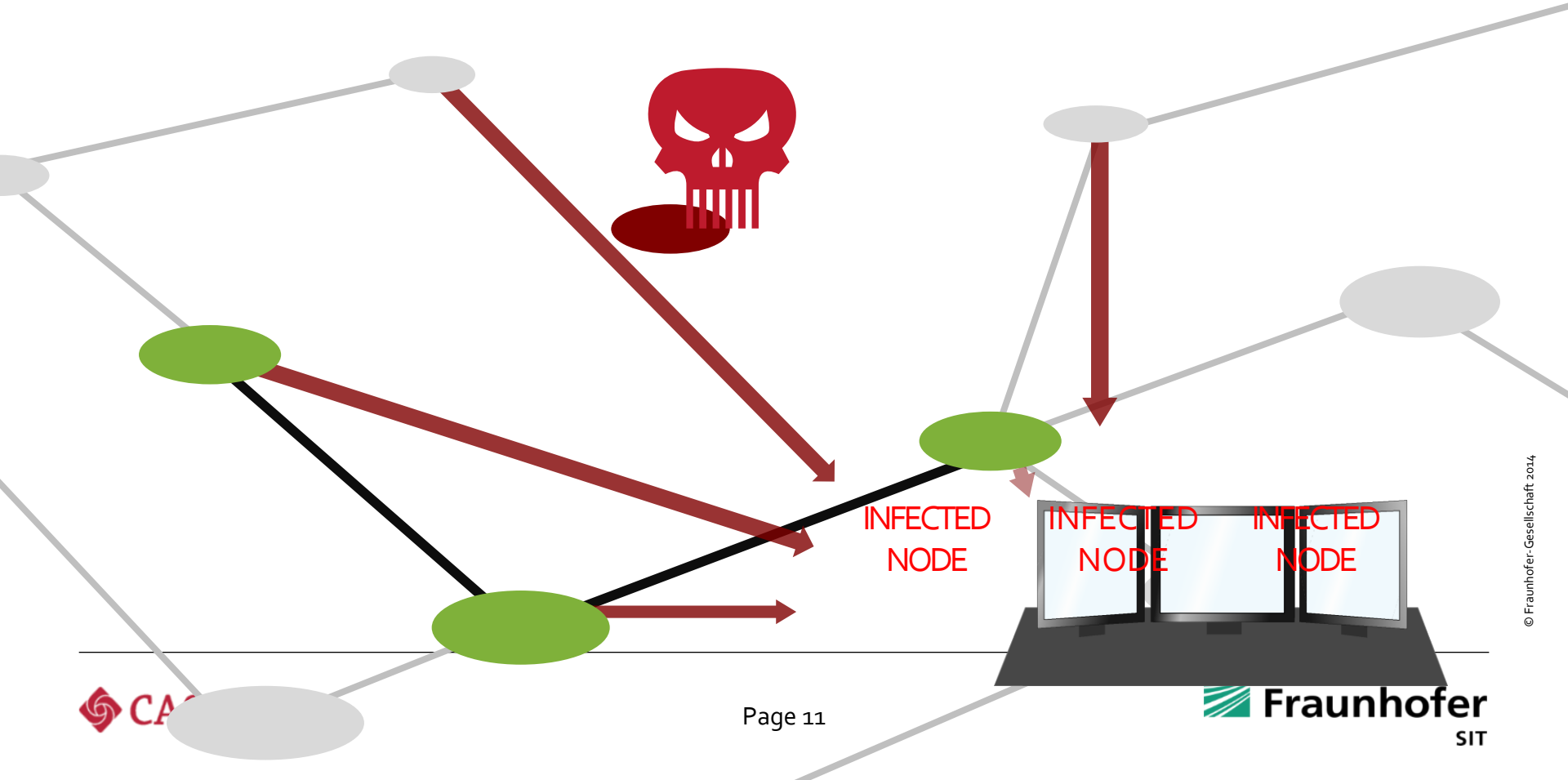
Fraunhofer SIT

... wird erkannt und Gegenmaßnahmen werden eingeleitet (Quarantäne, erhalten essentieller Funktionalitäten, ...)



Fraunhofer SIT

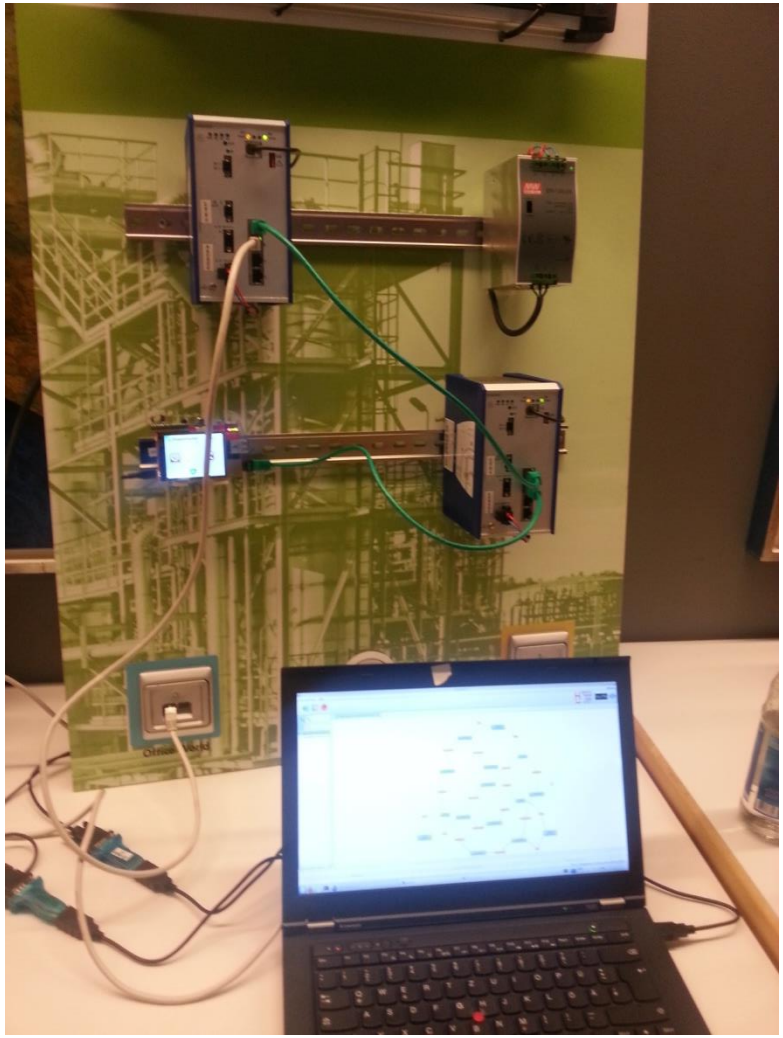
... und der Vorfall wird gemeldet.



Fraunhofer SIT

Trusted Core Network - Prototype

Distributed Health Checks in Industry Networks



Zusammenfassung

- Hardware-basierte Sicherheit ist verfügbar für viele unterschiedliche Plattformen.
- TPMs können für effiziente Prozesse zum Trust Establishment verwendet werden.
- Kombination mit Meta-Daten (IF-MAP Standard) ermöglichen verlässliche Informationen über Infrastrukturen und Prozesse.
- Fraunhofer SIT bietet in diesem Bereich:
  - Entwicklung von neuen Lösungen
  - Unterstützung bei der Implementierung und Integration
  - Sicherheitslösungen über verschiedene Ebenen (Kommunikation, Geschäftsprozesse, Wartungsprozesse, Produktion, etc.)

Kontaktieren Sie uns

Dr. Carsten Rudolph
Tel.: +49 6151 869-344
E-Mail: carsten.rudolph@sit.fraunhofer.de

Norman Göttert, M.Sc.
Tel.: +49 6151 16 75208
E-Mail: norman.goettert@sit.fraunhofer.de

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75
64295 Darmstadt