

2020-10-27



PROMOTIONS-
KOLLEG



DIGITALISIERUNG
DER PRODUKTION

Entwicklung eines ganzheitlichen Security- Management-Konzeptes für die digitale Produktion

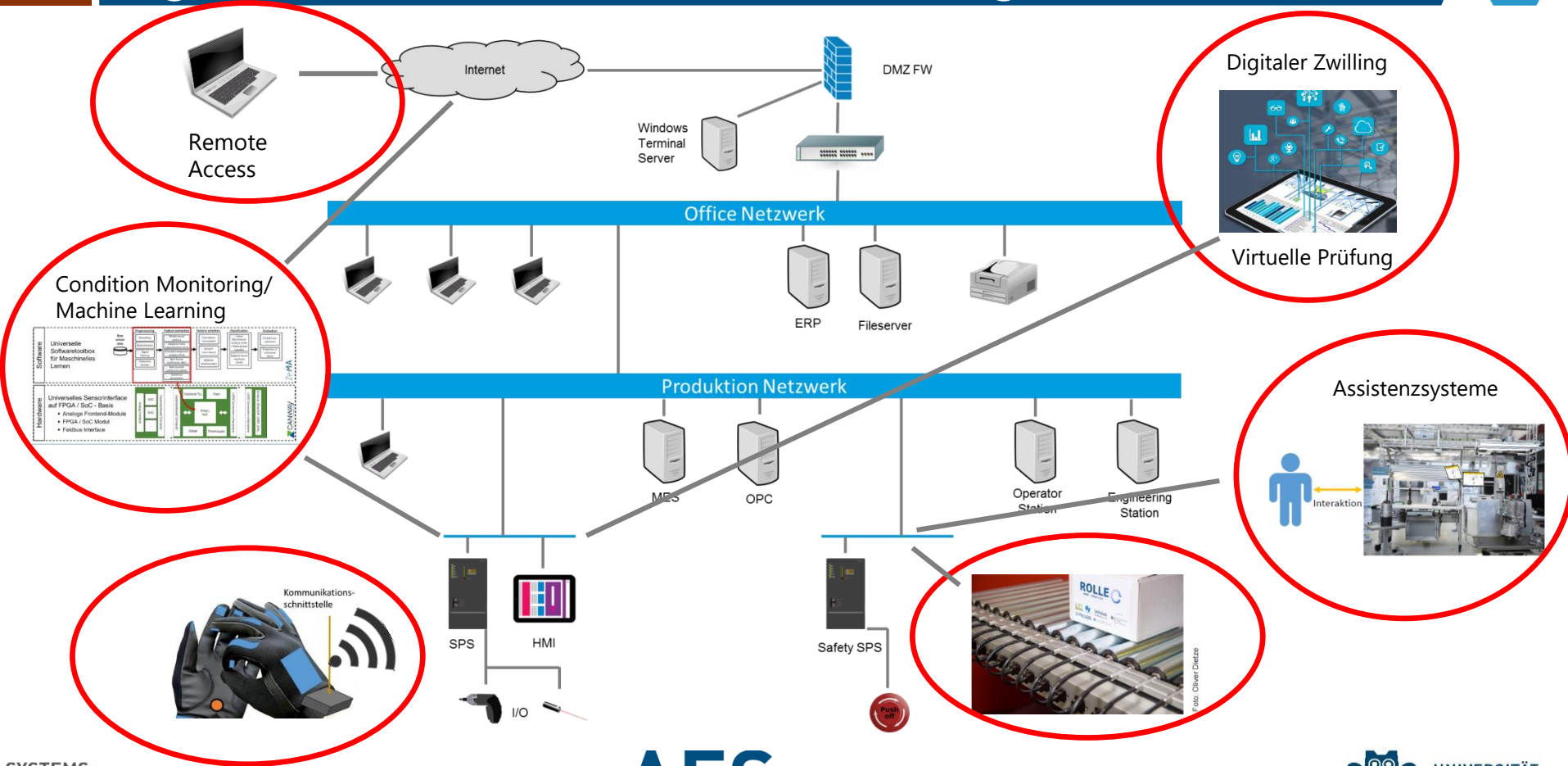
Ontologiebasiertes IT-Security Management

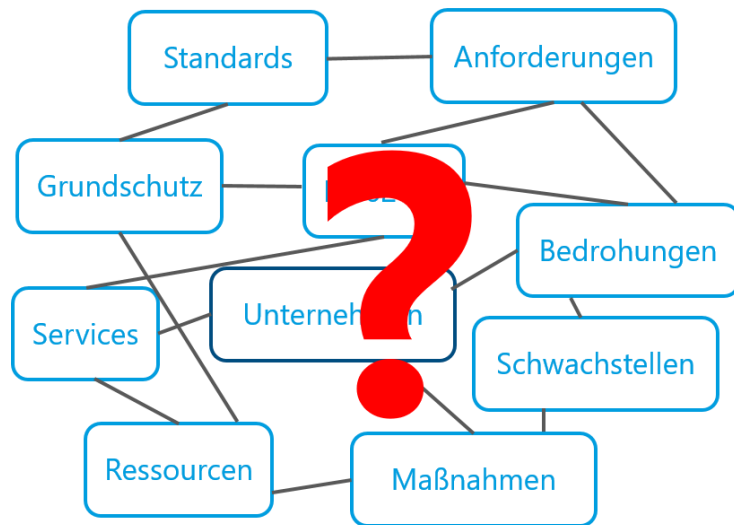
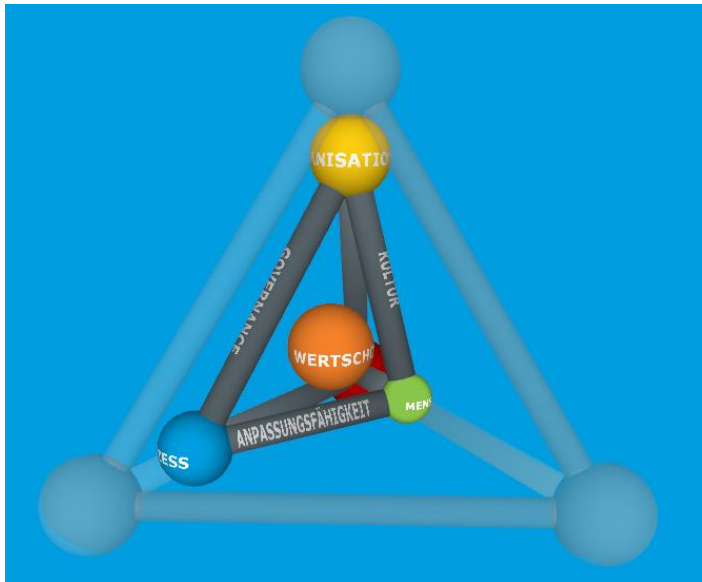


Christian Siegwart, M.Sc.



1. Motivation/Rückblick
2. Ontologie - Basics
3. Ontologie-Engineering
4. Ausblick



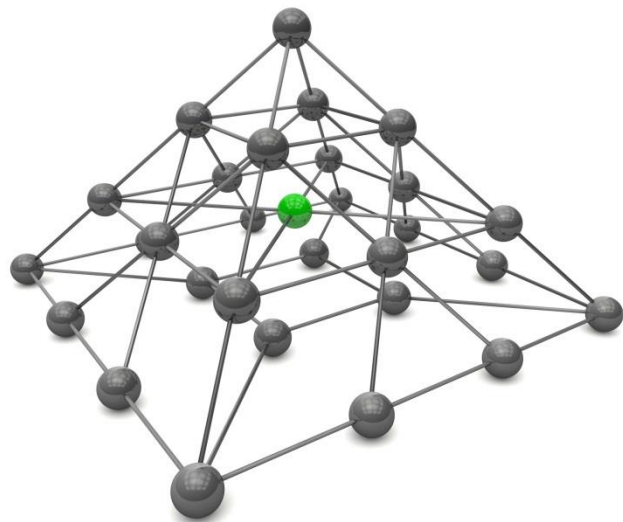


Wie können Inhalte für Unternehmen einfach nutzbar gemacht werden?

Sieglwart, C.; Scherhag, F.; Krammel, M.; Frey, G.: Ganzheitliche IT-Security Reifegradbestimmung. Proceedings of the Kongress Automation 2020, VDI-Berichte Nr. 2375, VDI-Verlag GmbH, Baden-Baden, Germany, July 2020.



- Informationen aus unterschiedlichen Quellen (Standards, Schwachstellen, ...) => Missverständnisse vermeiden
- Umwandlung der vorhandenen Informationen in nutzbare Daten für Unternehmen (besonders relevant für KMU)
- Schematische Abbildung eines Wissensbereichs benötigt, inklusive der Beziehung zwischen den Informationen
- Ziel: Maschinenlesbares Wissensmodell im Bereich IT-Security Management (für KMU)
- Forschungsprojekt GrundschutzPlus-Aktivator gestartet (<https://www.security4kmu.de>)



Grundschutz^{PLUS}
Aktivator



- Nutzung Ontologien zur Wissensrepräsentation in der Informatik seit 90er Jahren
- Definition:
- (Maschinenlesbare) Repräsentation der Begriffe eines realen Themenbereichs entwickeln und die Beziehungen zwischen den Objekten beschreiben
- Anwendungen:

*An ontology is
an explicit specification
of a conceptualization*

Tom Gruber, 1993

Wissensrepräsentation

Semantic Annotation

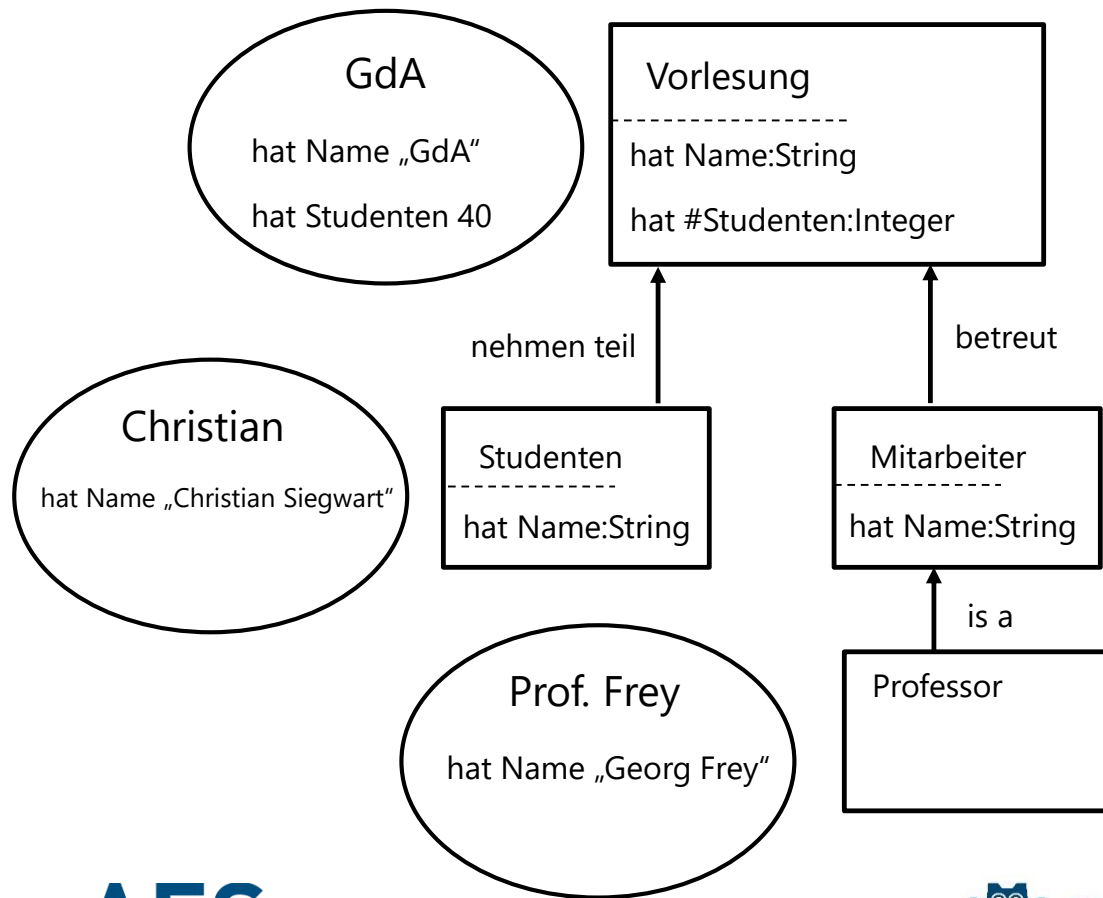
Semantic Search



- Domain Ontology
- Einfaches Beispiel
Lightweight Ontology
- Typische Bestandteile:
Konzepte/Klassen

Eigenschaften/
Relationen

Instanzen





■ Vorgehen:

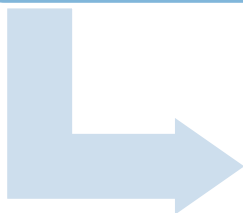


Lightweight
Ontology



- Motivation
- Analyse des entsprechenden Themenbereichs und Beschreibung des Scope.

Was ist der Betrachtungsgegenstand?



- Definition von Konzepten (Klassen), und Beschreibung der Relationen
- Darstellung in UML Diagramm

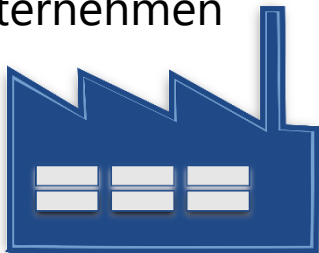
**Welche Begriffe sind relevant?
Wie sind sie miteinander verbunden?**



- Implementierung der informalen Lightweight Ontologie mit Hilfe formaler Ontologiesprachen

- Scope: IT-Security Management (Fokus KMU)

Unternehmen

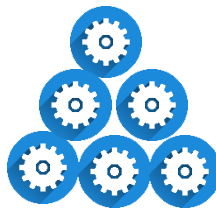


Ressourcen



Umsetzung

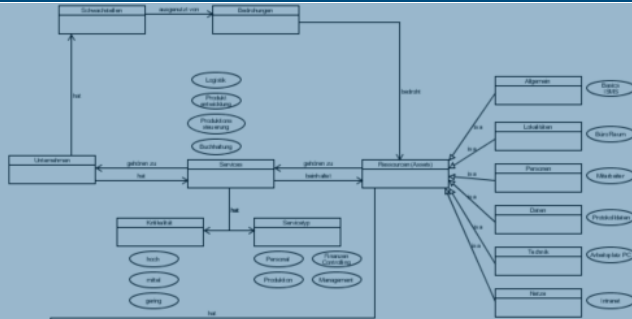
- Quellen:
BSI IT-Grundschutz
IEC 62443



Prozesse

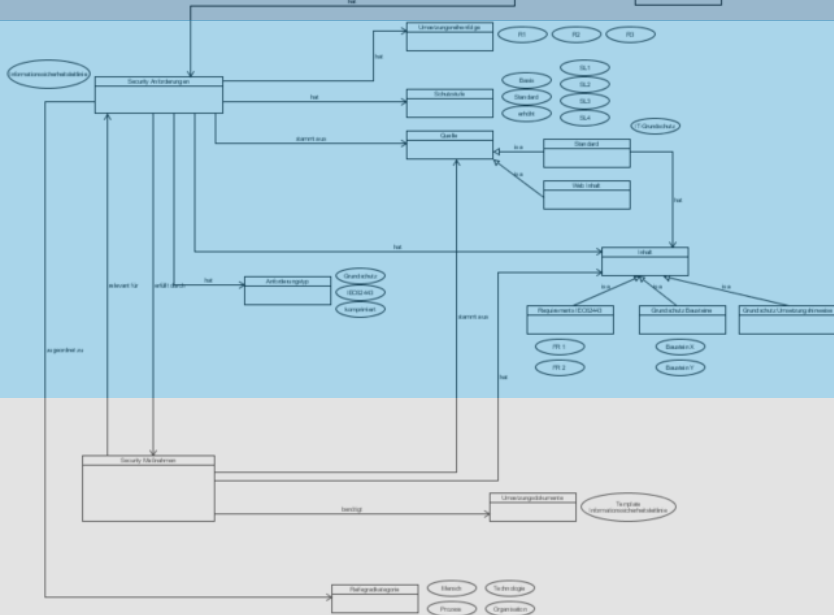


Anforderungen



Unternehmen

- Services (Logistik, Produktionssteuerung, Buchhaltung, Recruiting, ...)
- Ressourcen
Übergeordnete, Personen, Technik, ...
Arbeitsplatz PC, Mitarbeiter, Server, ..



Security Anforderungen

- Umsetzungsreihenfolge (R1,R2,R3)
- Schutzstufe (Grundschatz oder 62443)
- Bedrohungen
- Quelle

Abbilden der Grundschatz Baustein
Informationen + IEC 62443 FR's

Security Maßnahmen

- Passende Maßnahmen zu den Anforderungen
z.B. Umsetzungshinweise BSI IT-Grundschatz



unterstützt durch:



Ontologie



Implementierung



Analyse





ME SAAR
DIE METALL + ELEKTROINDUSTRIE

