GÜDEL

Produktgestaltung für Industrie 4.0 – Umgang mit Cyber Security am Beispiel Condition Monitoring

Agenda

Einführung Güdel Condition Monitoring

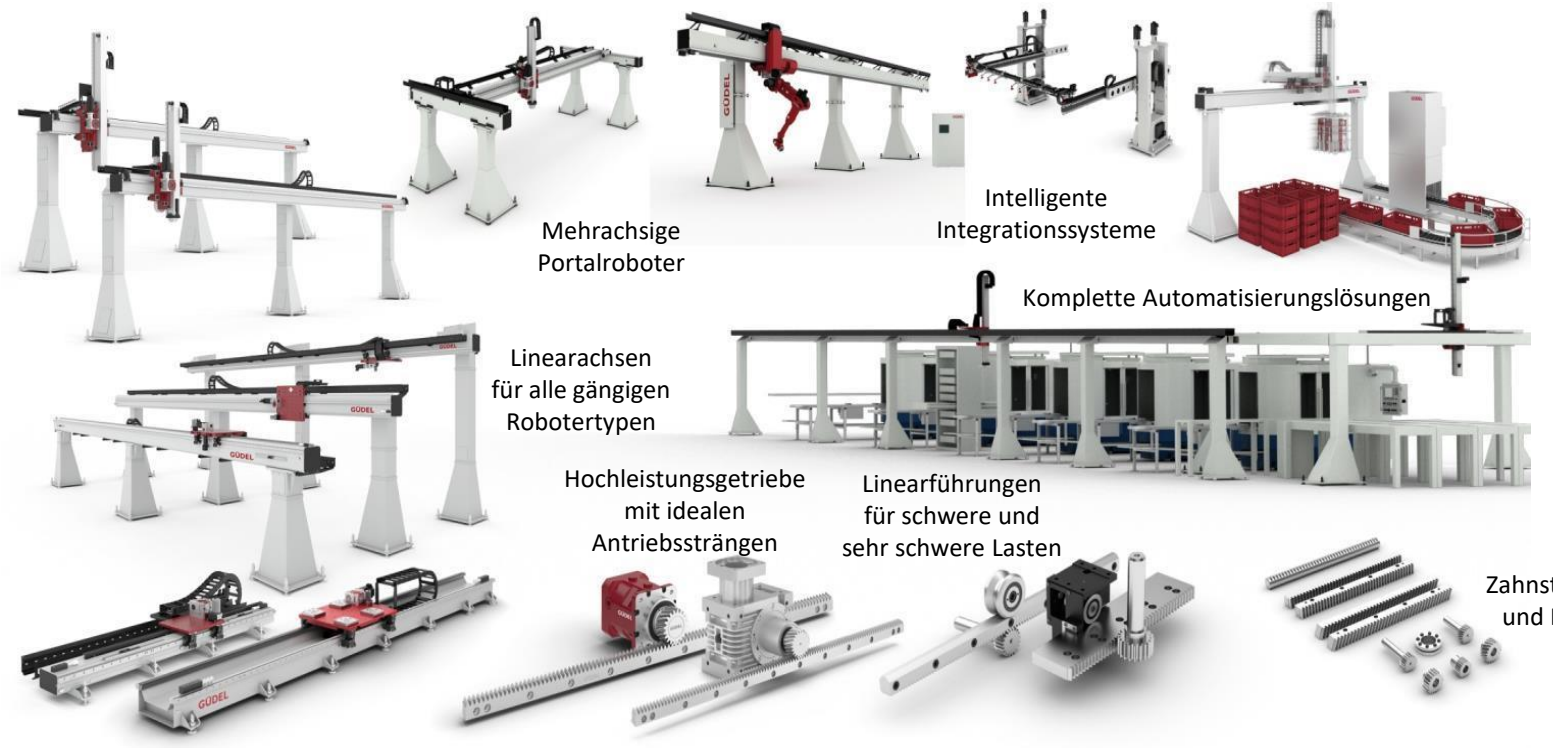
Security über den gesamten Produktlebenszyklus

- In der Entwicklung
- Beim Verkauf
- Im Betrieb
- Ausserbetriebnahme

Abgrenzung der Verantwortlichkeiten

Güdel AG

Von Komponenten zu Automationslösungen



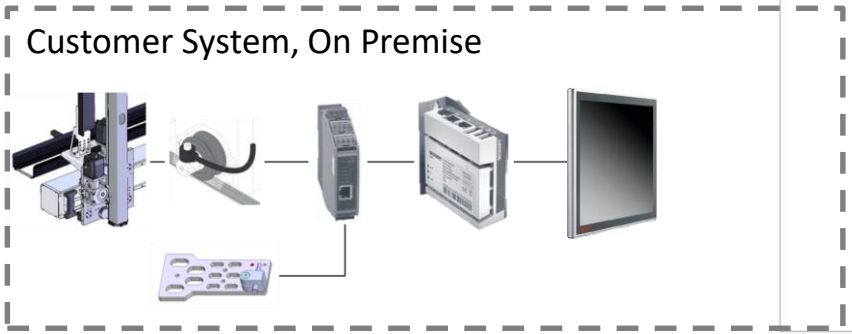
Güdel Condition Monitoring
Überwachung des Führungssystems

Kundenversprechen

Produktumfang

Überwachung des Zustandes anhand von mechanischen Kenngrössen

M



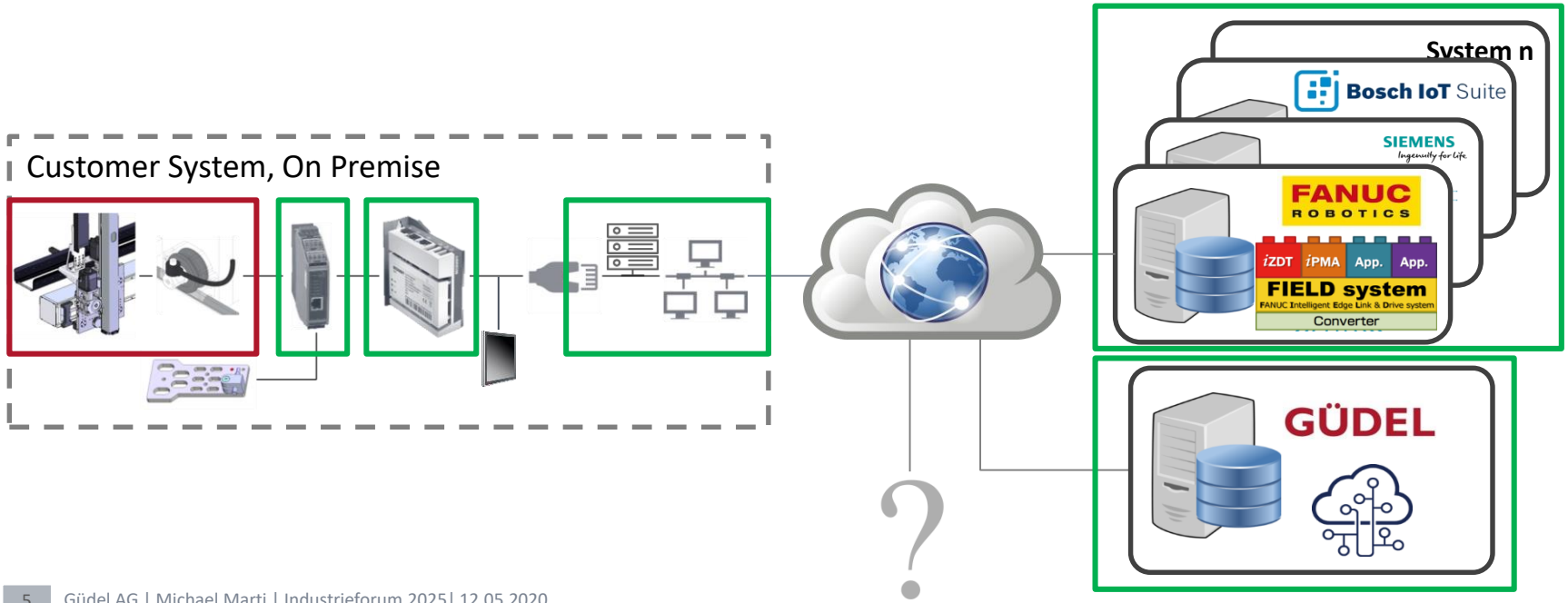
Güdel Condition Monitoring
Überwachung des Führungssystems

Kundenversprechen

Produktumfang

Überwachung des Zustandes anhand von mechanischen Kenngrössen

Mechanische Anbindung, Sensor, Auswertungseinheit, IPC, HMI



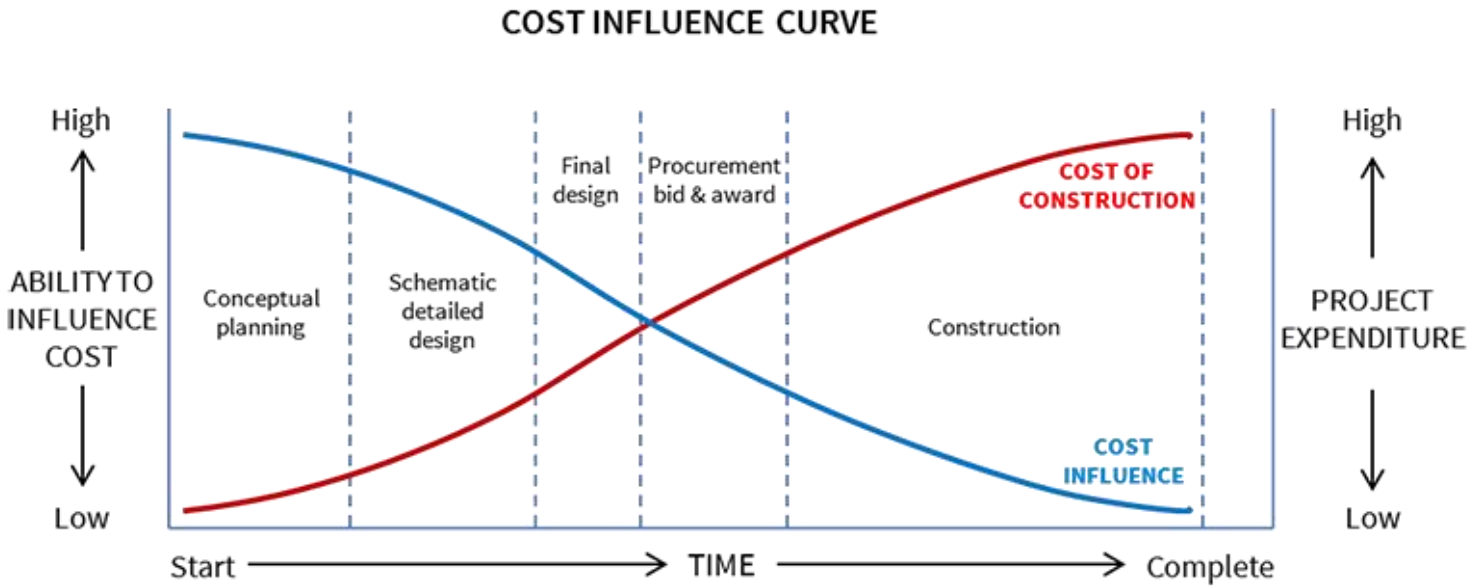
Security über den gesamten Produktlebenszyklus

In der Entwicklung

Durchführen einer Bedrohungsanalyse (Threat modeling)

- Definition der zu schützenden Ressourcen und Abschätzung möglicher Auswirkungen
  - Datenverlust — Reputationsschäden, Knowhow Verlust, …
  - Störung Produktion/Betrieb — Produktivitätsverluste, Lieferverzögerungen, …
  - Physische Schäden an Anlagen — Sachschaden, Personenschäden, …
- Analyse von Schwachstellen
  - Schnittstellen/Kommunikation — Industrial Ethernet, WLAN, …
  - Eingabemedien — Laptop, USB-Stick, Smartphone, …
  - Benutzer — Einfaches Passwort, …
- Bedrohungsszenarien
  - Potentielle Angreifer — Virus, Spam, DoS, Spyware, Sabotage, Ransomware, Social Engineering…
  - Administratoren, normale Benutzer — Vorsätzlich, unabsichtlich, …
  - Andere Systeme

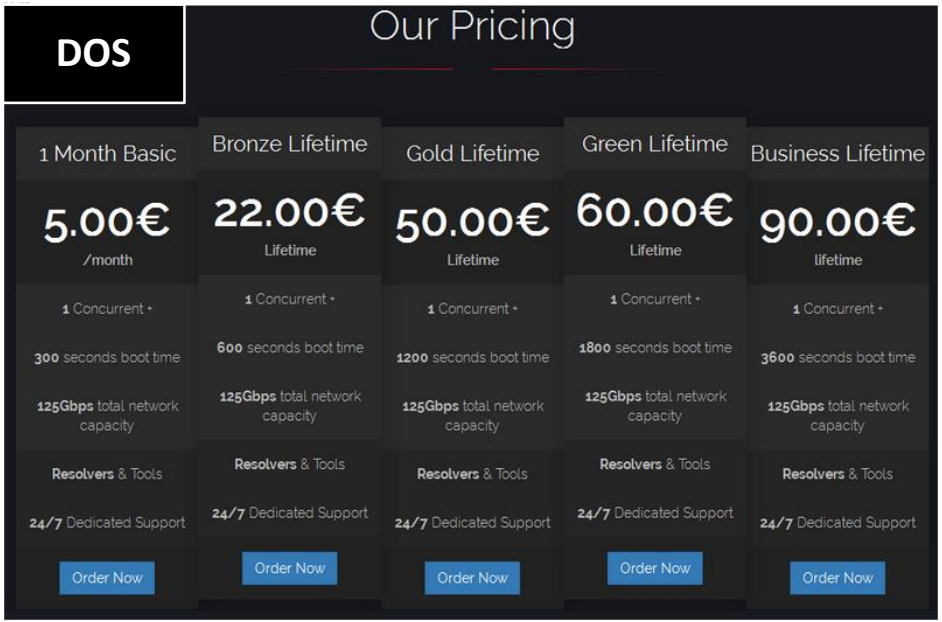
Security über den gesamten Produktlebenszyklus
In der Entwicklung



Security über den gesamten Produktlebenszyklus
In der Entwicklung

Durchführen einer Bedrohungsanalyse (Threat modeling)

- Definition der zu schützenden Ressourcen und Abschätzung möglicher Auswirkungen
  - Datenverlust
  - Störung Produktion/Betrieb
  - Physische Schäden an Anlagen
- Analyse von Schwachstellen
  - Schnittstellen/Kommunikation
  - Eingabemedien
  - Benutzer
- Bedrohungsszenarien
  - Potentielle Angreifer
  - Administratoren, normale Benutzer
  - Andere Systeme

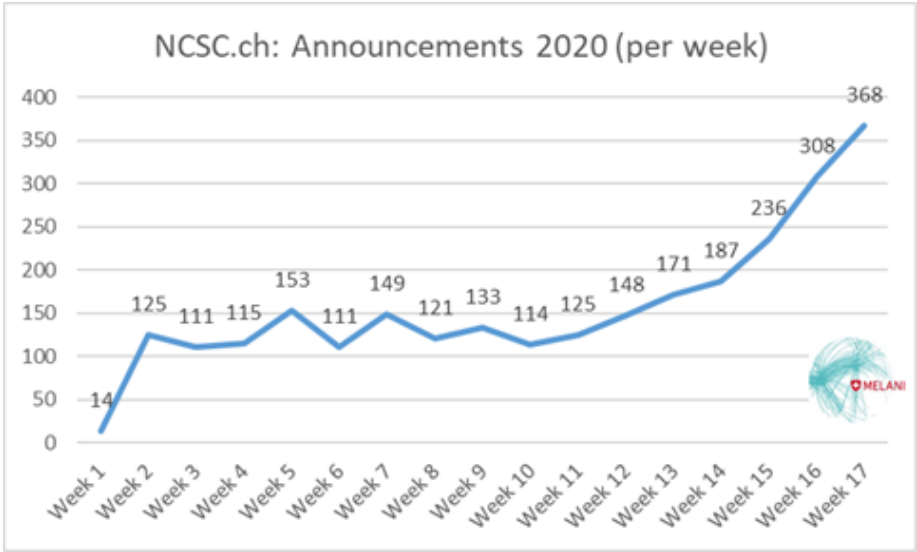


Security über den gesamten Produktlebenszyklus

In der Entwicklung

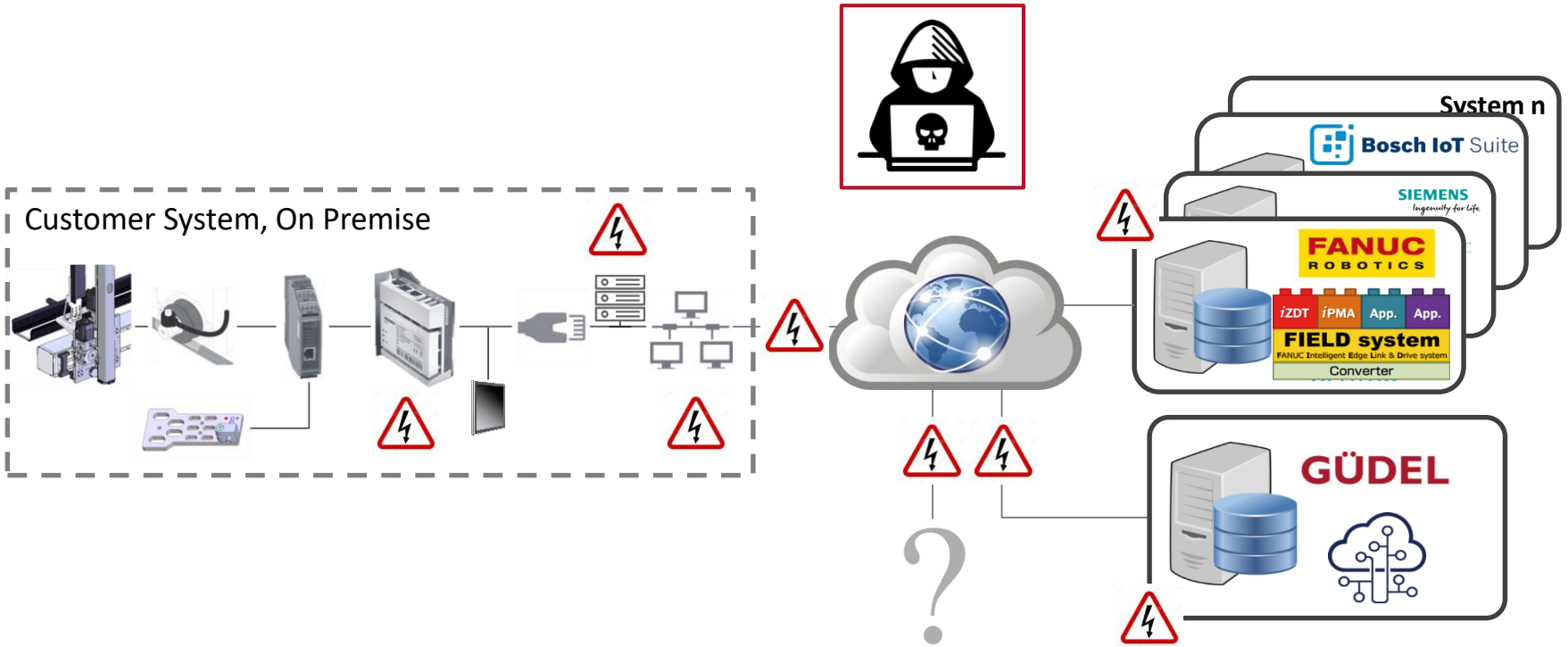
Durchführen einer Bedrohungsanalyse (Threat modeling)

- Definition der zu schützenden Ressourcen und Abschätzung möglicher Auswirkungen
  - Datenverlust
  - Störung Produktion/Betrieb
  - Physische Schäden an Anlagen
- Analyse von Schwachstellen
  - Schnittstellen/Kommunikation
  - Eingabemedien
  - Benutzer
- Bedrohungsszenarien
  - Potentielle Angreifer
  - Administratoren, normale Benutzer
  - Andere Systeme



Security über den gesamten Produktlebenszyklus

In der Entwicklung



Security über den gesamten Produktlebenszyklus
In der Entwicklung

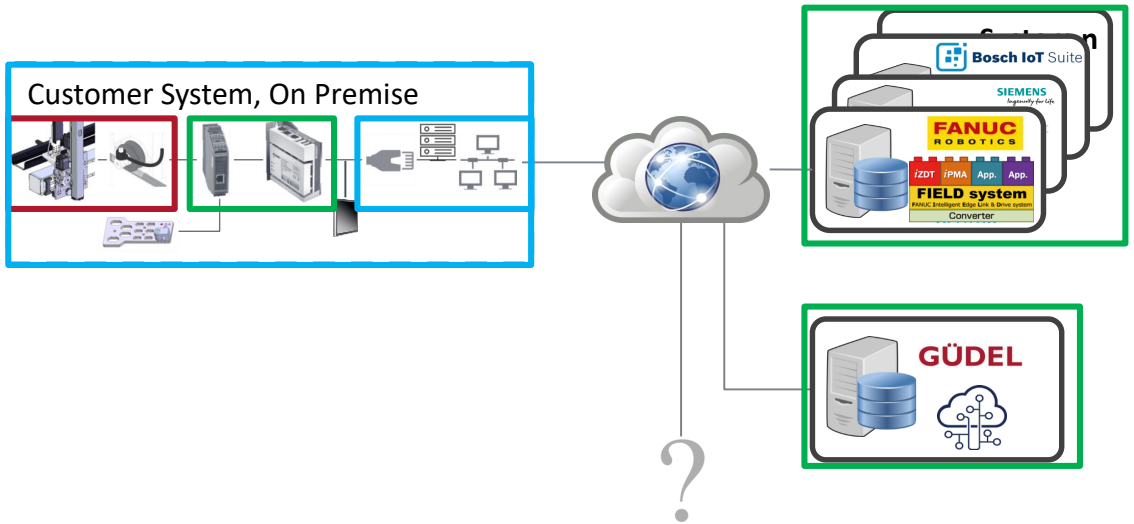
Durchführen einer Bedrohungsanalyse (Threat modeling) (Frontloading analog best practice Ansatz Entwicklung)

- Definition der zu schützenden Ressourcen und Abschätzung möglicher Auswirkungen
  - Datenverlust — Reputationsschäden, Knowhow Verlust, …
  - Störung Produktion/Betrieb — Produktivitätsverluste, Lieferverzögerungen, …
  - Physische Schäden an Anlagen — Sachschaden, Personenschäden, …
- Analyse von Schwachstellen
  - Schnittstellen/Kommunikation — Industrial Ethernet, WLAN, …
  - Eingabemedien — Laptop, USB-Stick, Smartphone, …
  - Benutzer — Einfaches Passwort, …
- Bedrohungsszenarien
  - Potentielle Angreifer — Virus, Spam, DoS, Spyware, Sabotage, Ransomware, Social Engineering…
  - Administratoren, normale Benutzer — Vorsätzlich, unabsichtlich, …
  - Andere Systeme

Security über den gesamten Produktlebenszyklus
In der Entwicklung

Festlegung der Systemgrenzen

- Was können wir als **Lieferant/Hersteller** beeinflussen?
- Was muss über **Drittparteien** umgesetzt werden?
- Was kann nur der **Endkunde** umsetzen?



Security über den gesamten Produktlebenszyklus
In der Entwicklung

Festlegung der Systemgrenzen

- Was können wir als **Lieferant/Hersteller** beeinflussen?
- Was muss über **Drittparteien** umgesetzt werden?
- Was kann nur der **Endkunde** umsetzen?

Massnahmen zur Risikominderung

- Sichere Verbindungen	VPN, Firewall, …
- Sichere Datenablage	Authentifizierung, ….
- Security durch Isolation	Netzwerksegmentierung, ...
- Lifecycle traceability	Updates, Versionierung, …

Security über den gesamten Produktlebenszyklus

In der Entwicklung

Das IT System des Anbieters wird neu Teil eines Produktangebots

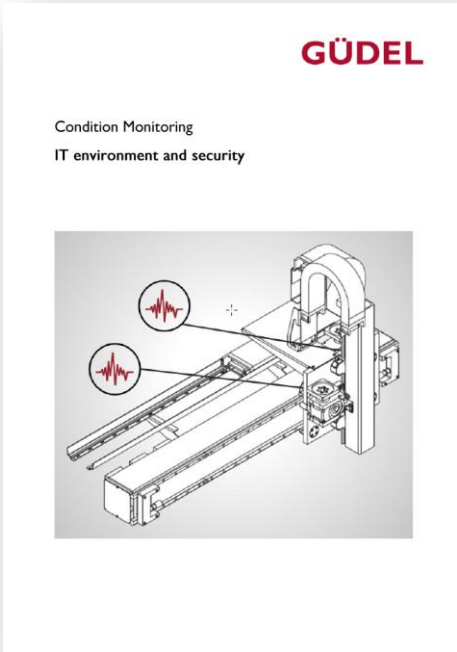
- Einbezug IT und Klärung der Verantwortlichkeiten
  - Kampf der Kulturen: Engineering vs. IT

  ⇒ Es braucht einen Vermittler zur Übersetzung der Anforderungen
- Definition der Rolle in der Entwicklung und im Betrieb
  - Applikationsverantwortung — Produkt-/Servicemanager (Kennt und definiert Nutzerbedürfnisse)
  - Serviceverantwortung — Entscheidung über die Bereitstellung des Services (P&L)
  - Betriebsverantwortung — Unterhalt und Betreuung der Infrastruktur

Security über den gesamten Produktlebenszyklus
Beim Verkauf

Diskussionen mit Kunden

- Security ist kein Mehrwert sondern ein Kostenfaktor
  - ⇒ Kundensicht: Keine Begeisterungs- sondern eine Muss-Anforderung
  - ⇒ Immer eine Risikoabwägung
  - ⇒ Es gibt keine absolute Sicherheit, es ist nur eine Frage des Aufwands
- Umfang, Schnittstellen und Verantwortlichkeiten sind zu klären
  - Was fordert der Markt, was ist der Kunde bereit einzugehen?
  - Wie weit gehen Mitbewerber?
  - Kampf der Kulturen: OT (Shopfloor) vs. IT (Office)
  - ⇒ Es braucht einen Vermittler
  - ⇒ Bereitstellung eines Merkblattes für Kunden zur Überzeugung der internen Stakeholdern.



Security über den gesamten Produktlebenszyklus
Im Betrieb

- Security ist kein Produkt sondern ein Prozess
- Wenn mehrere Systeme von unterschiedlichen Anbieter eingesetzt werden, dann …
  … hat keiner die Übersicht und ein Verständnis der Abhängigkeiten und gegenseitiger Beeinflussung
  … gibt es verschiedene Lebenszyklen der Komponenten/Teilsystemen
  … gibt es unterschiedliche Security Ansätze
- No full safety without security

Security über den gesamten Produktlebenszyklus
Ausserbetriebnahme (noch in Arbeit)

Variante 1: On Premise

- Lokale IT ist für den Betrieb und die Ausserbetriebnahme verantwortlich

Variante 2: Cloud Lösung

- Globale zentrale Nutzerverwaltung durch Güdel
- Rollen und Rechte sind durch Güdel definiert, werden aber vom Kunde vergeben
- Seitens Kunde ist ein Administrator notwendig, der die Rollen und Rechte innerhalb seiner Organisation verwaltet
- Erfasste Instanzen/Assets
  - Kunde kann neue Assets erfassen und alte abmelden
  - Kunde kann seine Daten löschen
  - Kunde macht das Mapping der Accounts zu den Assets
- Assets und Accounts müssen vom Kunden regelmässig geprüft und aktualisiert werden. Die Motivation erfolgt durch eine kostenpflichtige Subscription

Abgrenzung der Verantwortlichkeiten

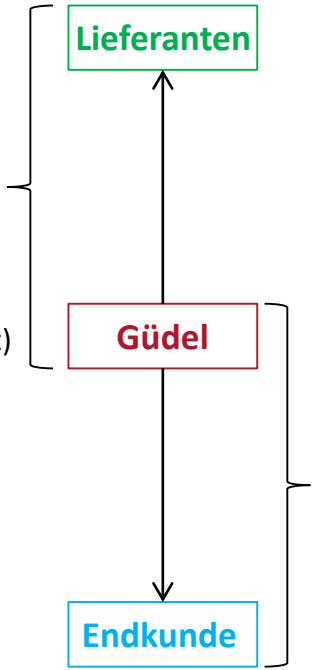
Wo hört die Verantwortung des Lieferanten auf und wo fängt die Verantwortung des Kunden an?

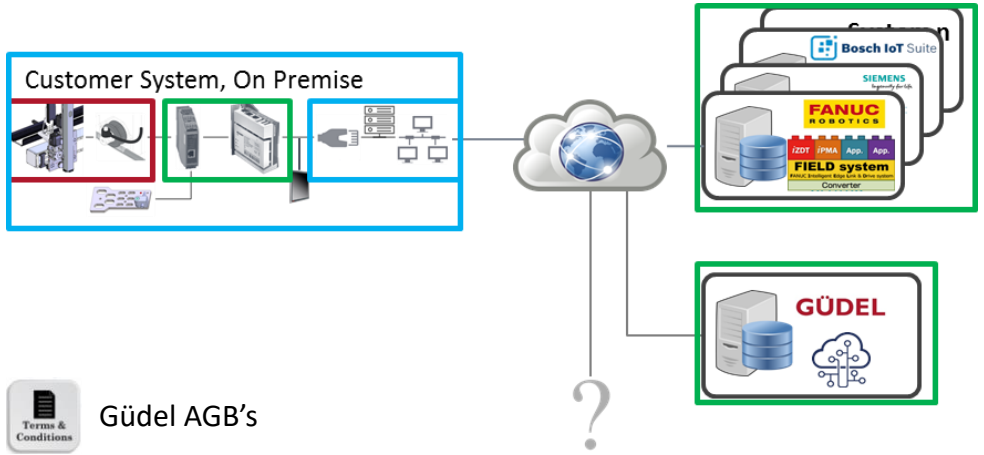
Welche Verantwortlichkeiten und Vereinbarungen bestehen zwischen den Parteien

Standard Lieferantenvertrag
(Updates Firmware)

Standard Enterprise
Subscription (Security Cloud)

Partnerschaftsagreement
(Security, Device Management)





Terms & Conditions

Güdel AGB's

Produktabgrenzung

Security 2025
Eine Arbeitsgruppe der Initiative **Industrie 2025**

SECURITY 2025

Beta-Version

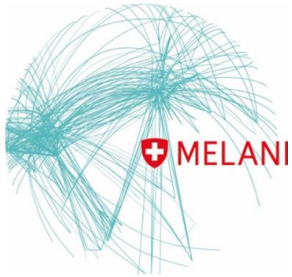
www.security2025.ch

Security 2025

Eine Arbeitsgruppe der Initiative **Industrie 2025**

Security 2025

Eine Arbeitsgruppe der Initiative **Industrie 2025**



NTT Security

GÜDEL

SWISSMEM

ELCA

RUZ

AMMANN

seitzvalve

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BWL

FH
Berner
Fachhochschule

PHOENIX CONTACT

ABB

Lassen Sie uns die nächsten Schritte gemeinsam angehen.

GÜDEL