



## Industrial IT Security

Sicherheitssoftware für die fertigende Industrie

ondeso  und 

für **sicheres** Management der  
Industrial IT

Juni 2013

## ICS-CERT berichtet von Viren-Infektionen bei US-Stromversorgern

Das US-amerikanische Computer Emergency Response Team berichtet in seinem aktuellen **ICS-CERT Monitor[2]** von gleich zwei Viren-Infektionen bei US-amerikanischen Stromversorgern im letzten Quartal 2012!

**Im ersten Fall** stellte ein Mitarbeiter, der routinemäßig Kontrollsysteme wartete, fest, dass sein hierfür **genutzter USB-Stick** nicht mehr richtig zu funktionieren schien.....

Einer der Funde soll stark an eine bereits "bekannte hochentwickelte Schadsoftware" erinnern haben. – Die Beschreibung passt zu dem Wurm **Stuxnet[3]**, der Industriebetriebe im Iran.....

**Im zweiten Fall** waren Maschinen in einem Elektrizitätswerk durch den **USB-Stick** eines **externen Mitarbeiters** infiziert worden..... Das ICS-CERT spricht in diesem Fall von "Crimeware", die die Geräte störte. Bis das Elektrizitätswerk wieder ans Netz gehen konnte, dauerte es mehr **als drei Wochen**.

Quelle: Heise.de

- Entstehendes Anwendungsfeld „Industrial-IT Security“ gestützt durch Viren wie Stuxnet / Duqu.
- gezielte Spionageangriffe auf Fertigungs- & Infrastrukturanlagen
- Zufällige Infektionen
- Unsichere Verwendung von USB-Datenspeicher in sensiblen Produktionsbereichen



Virenangriffe auf Industrie- & Infrastrukturanlagen rücken seit dem Auftauchen von Stuxnet und Duqu sowie dem vom BSI als Cyber-War beschriebenen Netzattacken in das Blickfeld der Sicherheitsverantwortlichen.

Zunehmende Risiken für Industrie- & Infrastrukturunternehmen durch Viren-, Spionage- und Sabotage-software erfordern neue, prozessorientierte Software Lösungen zur zentralen, inneren Absicherung ihrer Anlagen.

**ondeso bietet als Erster Softwareprodukte für dieses neu entstehende Marktsegment „Industrial IT Security“**

- Unwissenheit über Sicherheitslücken
- Fortfahren der Produktion - wissend um Sicherheitslücken
- Senkung des Risikos - hoher Aufwand durch proprietäre Eigenentwicklungen
- Infrastruktur muss zusammenwachsen, die Organisation kann nicht so einfach zusammengeschoben werden (fehlende Kompetenzen und benötigtes Knowhow)
- Lange Nutzungsdauer der Anlagen und Steuersysteme
- Heterogen wachsende Infrastruktur
  - Steuerungsrechner
  - Netzwerktopologie
- Produktionsorientierte Wartungszyklen
- Herstellergetriebene Systemauswahl
- Kein IT-Fachpersonal in den Fertigungen

## Kernprodukte



Sicheres Release & Patchmanagement für kritische Produktionssysteme



Kontrollierte, revisions-sichere Übertragung von Daten via USB zwischen Büro- und Prozessnetz



## Informationstool



Systeminformationen für den erleichterten Support durch den IT-Helpdesk

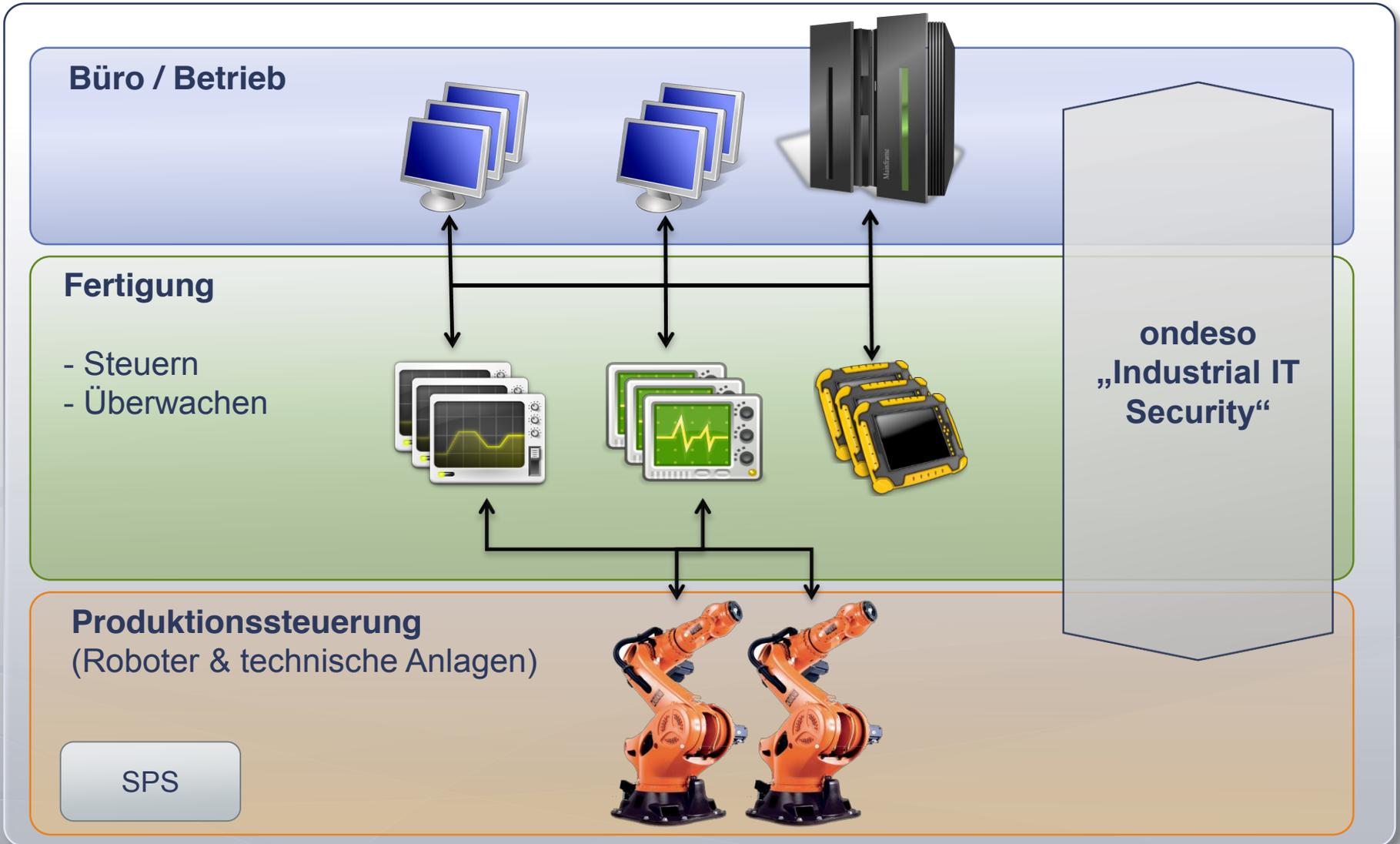


## Einsatzmöglichkeiten

- PatchManagement
- Imaging
- USB-Lock/Control
- Virus Pattern Update / Execute Scan
- Softwareinstallation
- Dashboarding
- Inventory
  
- ondeso Device Control



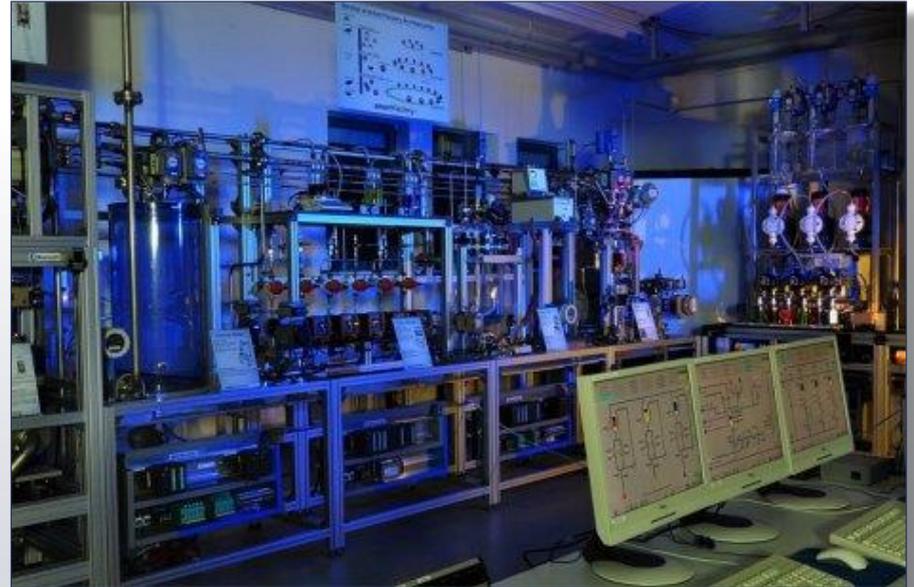
# Wo ordnet es sich ein / grenzt sich ab



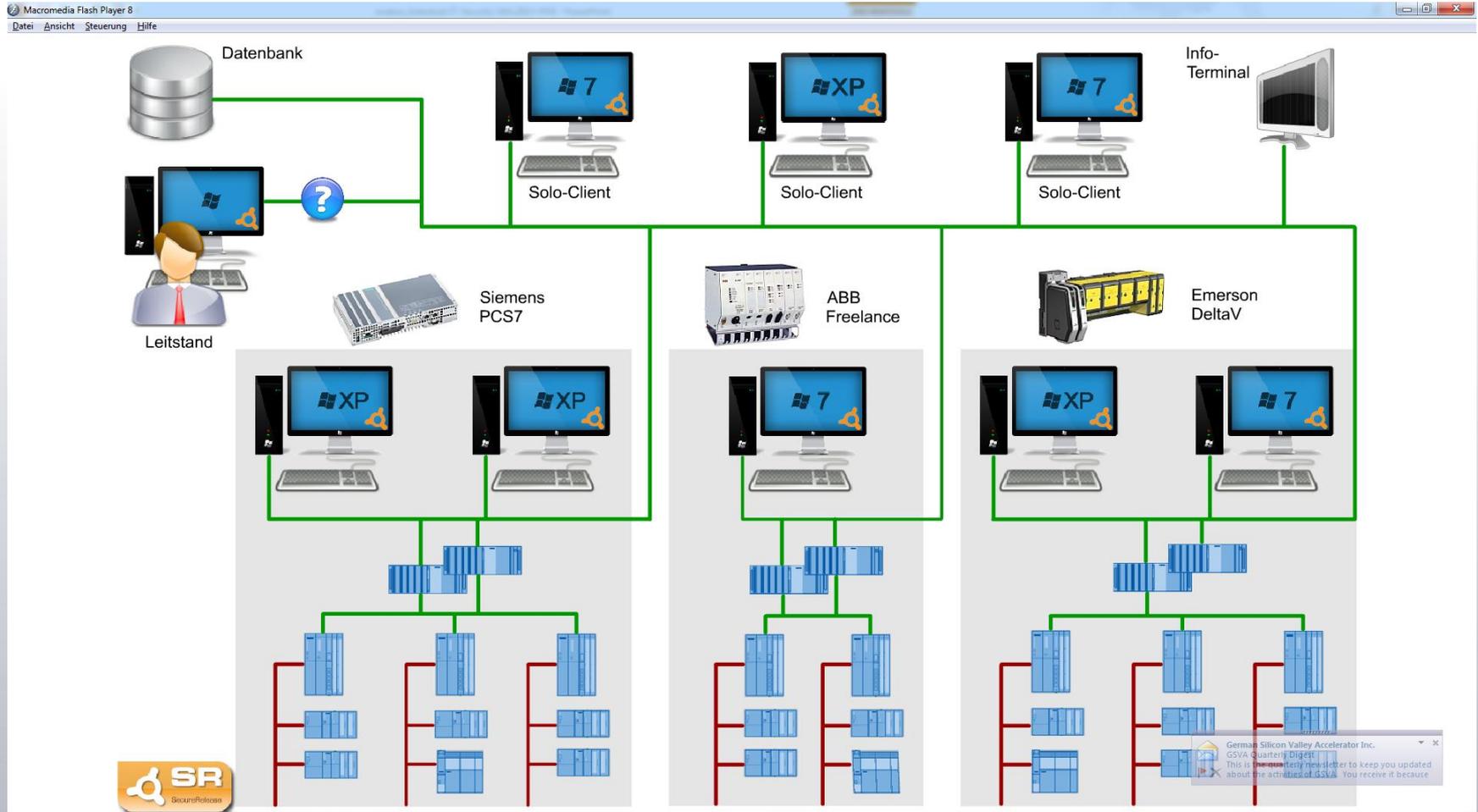
Softwareleitstand:

- Prozessplanung & Analyse
- Sicherheitsupdates
- Dokumentiert Änderungen  
revisionsicher & vorbereitet  
für Audits

Kontrollierter Umgang mit  
USB-Massenspeicher



**von „reaktiv manuell“ zu  
„planerisch prozessorientiert“**



- Senkt den Administrationsaufwand um bis zu 50%
- Verkürzt Rüstzeiten um 20%
- Erhöht Sicherheit
- Minimiert Ausfallzeiten
- Optimiert Prozesse – orientiert am Fertigungsprozess
- Dokumentiert Änderungen revisionssicher & bereitet Audits vor
- Ist ohne IT-Fachpersonal einsetzbar
- Niedrige TCO
- Herstellerübergreifende systemneutrale Lösung



# ondeso SecureRelease



Dashboard - ondeso SR Suite

Common Offline Patch Management Device Control Software Deployment Basic Installation / Configuration Management System Defaults System Administration

Responsibles Operators Groups Clients Job Adverts. Assigned Single Run Jobs Remote Tasks Assigned Remote Tasks Images Quick info Dashboard Client Dashboard Tracing Refresh

View

---

Security levels

Patch install overview Pilot based Active client based

Category	Count
missing	535
installed	319

Patch pilot result details

Pilotpatch installation Patch pilot results Banded pilot results Pilot results

Category	Count	Percentage
missing	8	53%
installed	6	40%
obsolete	1	7%

---

New reported

Clients Patches Responsibilities Operators

State	Client	Description	Reportdate
●	BR-PANEL01		6/11/2012 17:09:44 17:09:44

Patch results

Installation duration Copy duration

State by install	Title	Installation duration
●	Sicherheitsupdate für Windows 7 für x64-basierte Systeme (KB2491683)	00:00:58
●	Security Update for Windows XP (KB2707511)	00:00:43
●	Sicherheitsupdate für Windows 7 für x64-basierte Systeme (KB2479943)	00:00:32
●	Sicherheitsupdate für Windows 7 für x64-basierte Systeme (KB2509553)	00:00:28
●	Sicherheitsupdate für Windows 7 für x64-basierte Systeme (KB2079403)	00:00:19
●	Kumulatives Sicherheitsupdate für ActiveX Killbits unter Windows 7 für x64-basierte Systeme (KB2618451)	00:00:16
●	Security Update for Windows XP (KB2719985)	00:00:16
●	Security Update for Windows XP (KB2718523)	00:00:13

---

2.5.3.21129 (Client: AD) DB Server: 192.168.254.128 | DB-Schema ondeso\_srs\_sr (12120306)

Start [Taskbar icons] 7:22 PM 12/3/2012

- Wissen Sie, **welche** Releasestände sich in Ihrer **Produktion** befinden?
- Sind die Releasestände auch in der Produktion **chronologisch** und **revisionssicher dokumentiert**?
- Haben Sie einen **Rollout-Prozess** speziell für die Produktion?
- Ist geregelt, **wer, wann, was** und **wie** an Releasestände ändern darf?
- Können Sie **vor** einem Rollout feststellen, ob dieser **erfolgreich** an bestimmten Maschinentypen laufen **wird**?
- **Was passiert**, wenn ein Rollout **nicht erfolgreich** durchgeführt wird?

Die **ondeso SR-Suite** hilft Ihnen all diese Fragen **positiv** beantworten zu können!

# Voraussetzung



Database



Share



## Minimaler Eingriff in das Betriebssystem des Zielsystems:

Dateien ausschließlich unter  
**%programfiles%\ondeso**

Registrywerte ausschließlich unter  
**HKLM\ondeso**

Keine Registrierung von DLLs



Workflows **steuern** die **visuelle Oberfläche** und somit die Prozesse der Client GUI.

Über das „Workflow Tailoring Modul“ können bedarfsorientierte Kundenworkflows konzipiert werden.



Jobs und Policies **steuern** den **Service** der ondeso SR.

Über die SR Administrationsoberfläche können bedarfsorientierte Jobs und Policies konzipiert und an Zielgruppen bzw. –clients zugewiesen werden.

# UseCases – ondeso default Workflows

## Security Scan

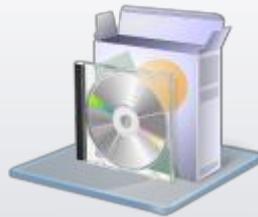
Prozessrechner



Database

## Patch Management

Software



Zielsystem

## USB Control

Prozessrechner

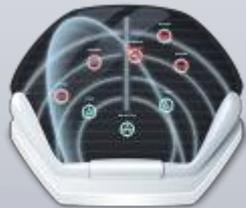


USB Control

# UseCases – ondeso default Workflows

## Inventory

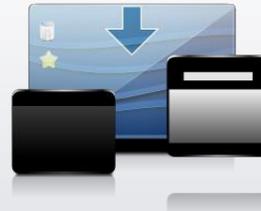
Prozessrechner



Inventory

## Client Dashboard

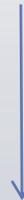
Software



Zielsystem

## Client Backup

Prozessrechner



File Share

# UseCases – ondeso default Workflows

## Job Execution

(non Service Installation)

Jobs

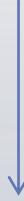


Zielsystem

## WUA Information

(offline No DB)

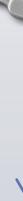
Windows Update



Zielsystem

## Framework

Workflow Items



Zielsystem

# UseCases – ondeso default Workflows

## Security Scan

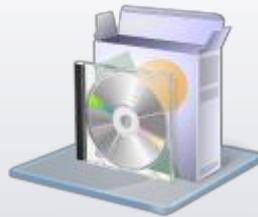
Prozessrechner



Database

## Patch Management

Software



Zielsystem

## USB Control

Prozessrechner



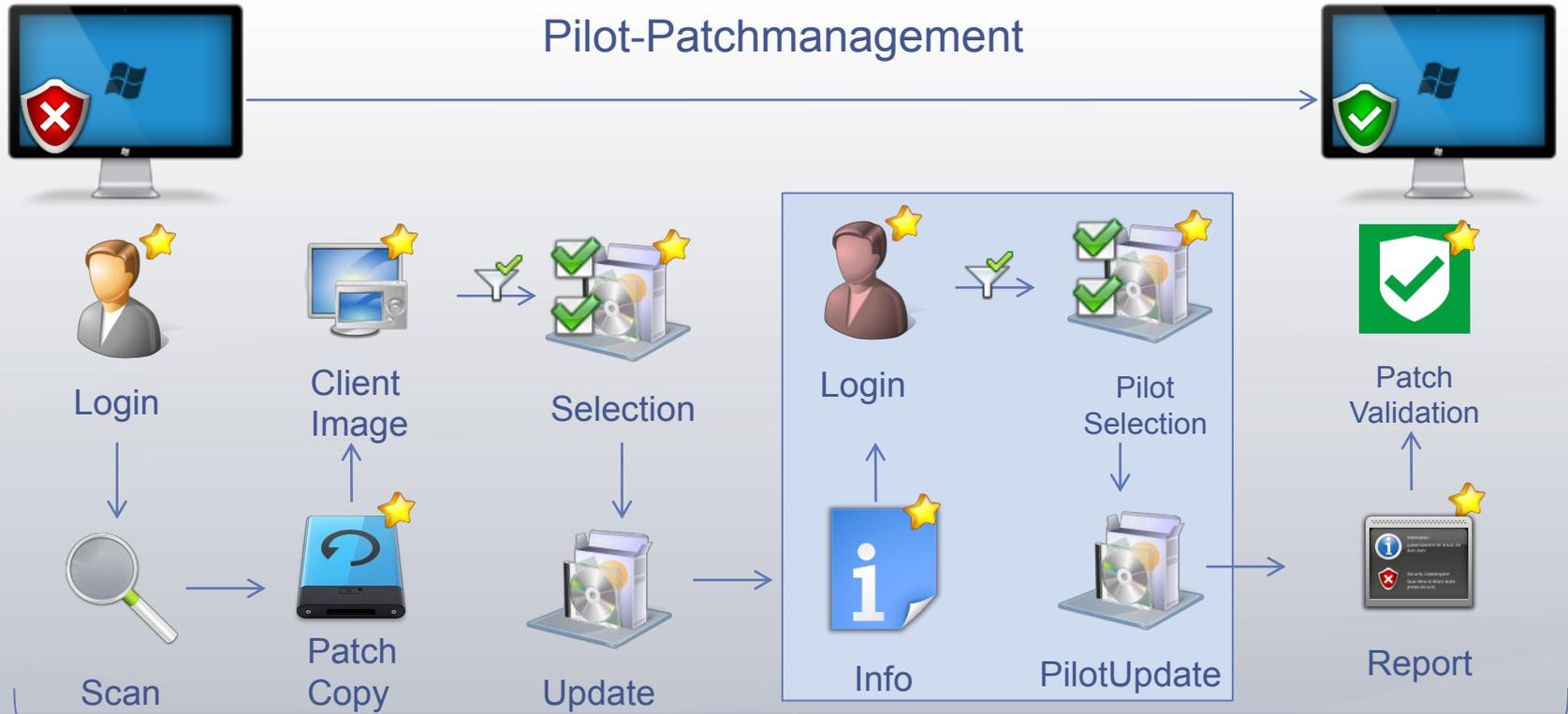
USB Control

## Operating System Pilot-Patchmanagement

Prozessrechner

Prozessrechner

### Pilot-Patchmanagement



Client Security Level

- Zielsystem entspricht Compliance
- Zielsystem entspricht NICHT Compliance

# UseCases – ondeso default Workflows

## Inventory

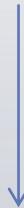
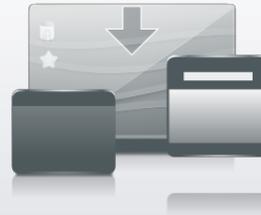
Prozessrechner



Inventory

## Client Dashboard

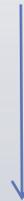
Software



Zielsystem

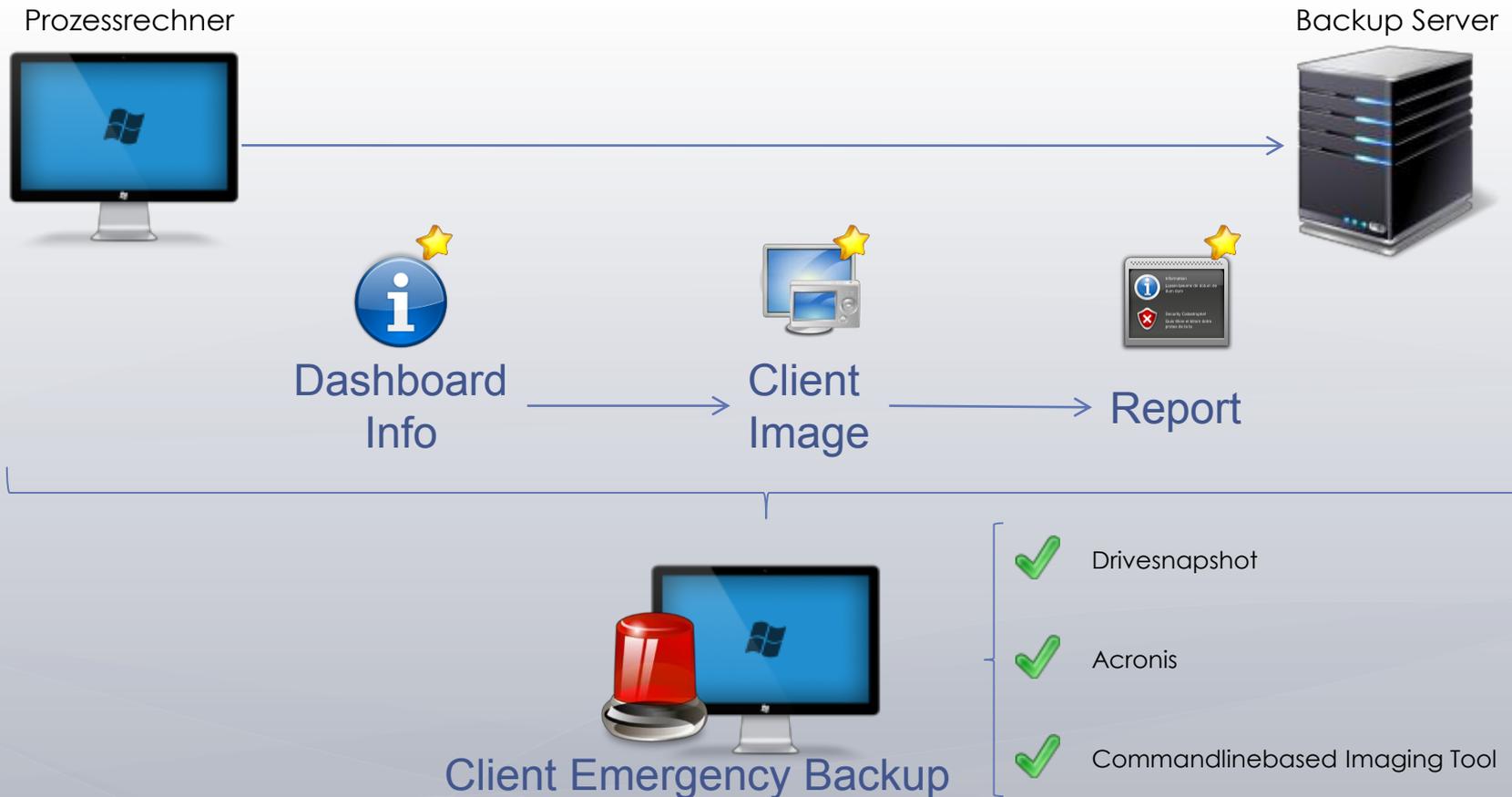
## Client Backup

Prozessrechner



File Share

# Client Backup



# UseCases – ondeso default Workflows

## Job Execution

(non Service Installation)

Jobs



Zielsystem

## WUA Information

(offline No DB)

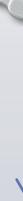
Windows Update



Zielsystem

## Framework

Workflow Items



Zielsystem

# Job Execution (No Service Installation)

Assigned Jobs



Zielsystem



Dashboard  
Info



Client  
Jobs



Report



Job Operations



Registry



Folder



Execution



Backup



Power



Archive

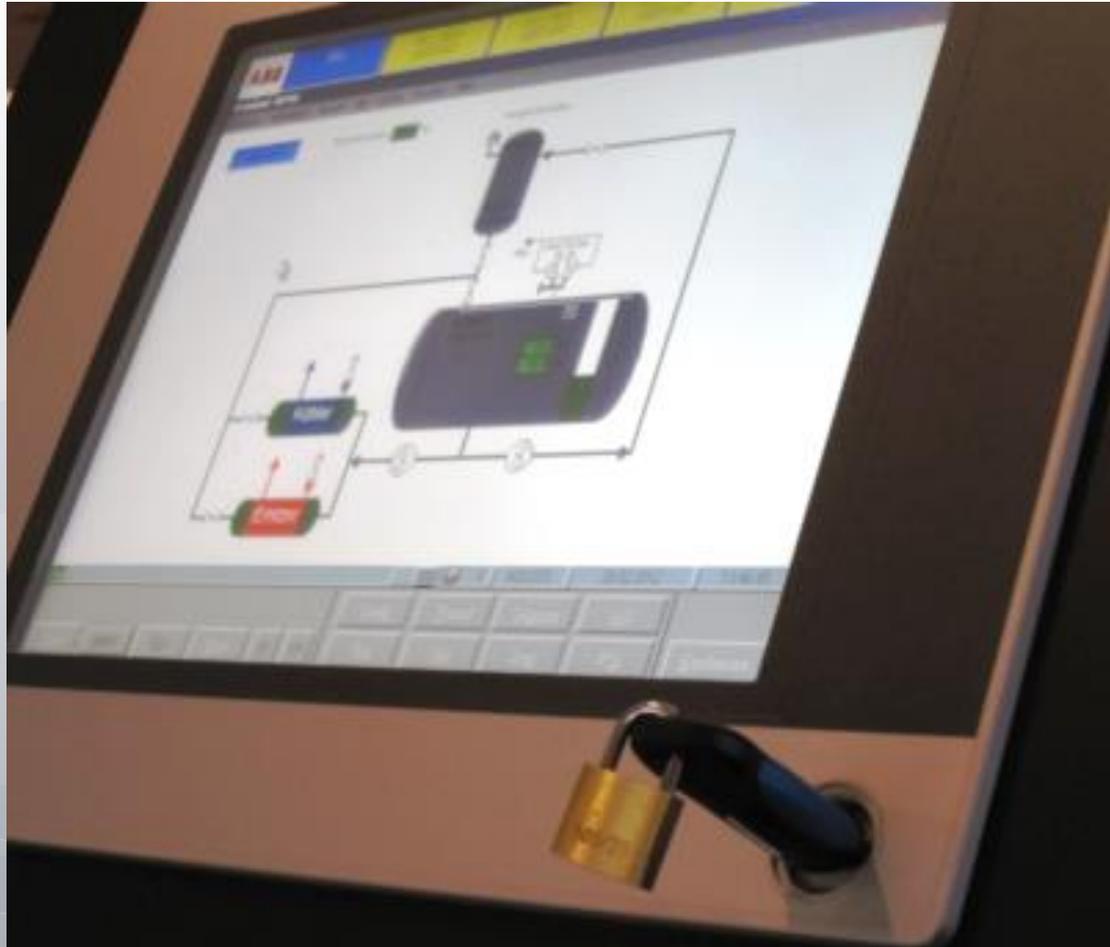


User



Network

# Indeso DeviceControl



## Fragestellungen im Kontext von USB-Speicher-Verwendung in der Produktion

- Wissen Sie, **welche** USB-Speicherdevices in der **Produktion** verwendet werden?
- Wird die Verwendung in der Produktion **chronologisch** und **revisionssicher dokumentiert**?
- Haben Sie einen **Verwendungs- und Freigabeprozess** speziell für die Produktion?
- Ist geregelt, **wer, wann, was** und **wie** USB-Speicher verwenden darf?
- Wissen Sie welche Daten über USB in die Produktion gebracht und welche wieder **mitgenommen** werden?

**ondeso DeviceControl** hilft Ihnen all diese Fragen **positiv** beantworten zu können!

# Voraussetzung



Database



Share



## Minimaler Eingriff in das Betriebssystem des Zielsystems:

Dateien ausschließlich unter  
**%programfiles%\ondeso**

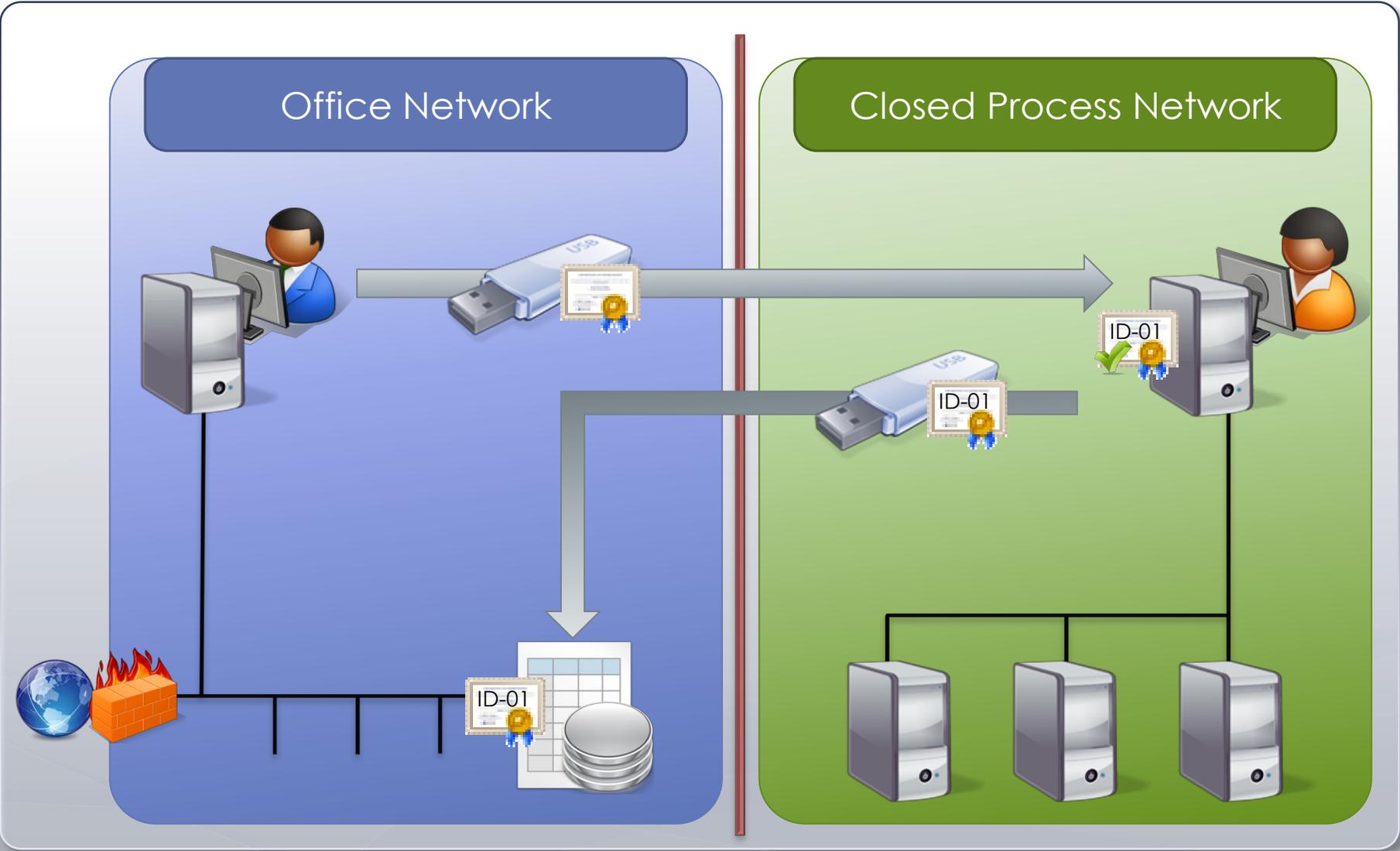
Registrywerte ausschließlich unter  
**HKLM\ondeso**

Keine Registrierung von DLLs

### Einsatzmöglichkeit für getrennte Prozessnetze

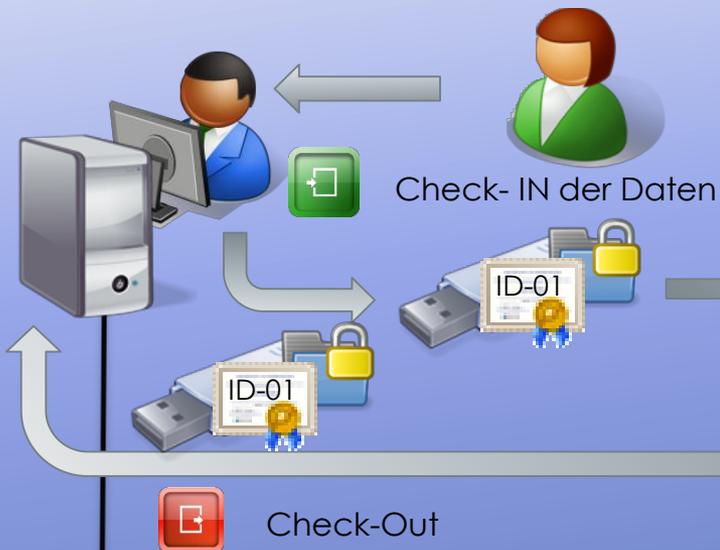
- Set-Up Prozess (Preparation)
- Check-In Prozess
  - Vorprüfung (Virusscan) von USB-Datenträgerinhalten im Office-Netz
  - Dokumentation & Verschlüsselung der Inhalte
- Operate-Prozess
  - Dedizierte Freigabe in den Prozessnetzen für einzelne Rechner oder durch dedizierten Filerclient
- Check-Out Prozess
  - Entschlüsselung der Feedbackdaten erfolgt erst bei erneutem Scan im Office-Netz

# Preparation (Certificate Exchange)

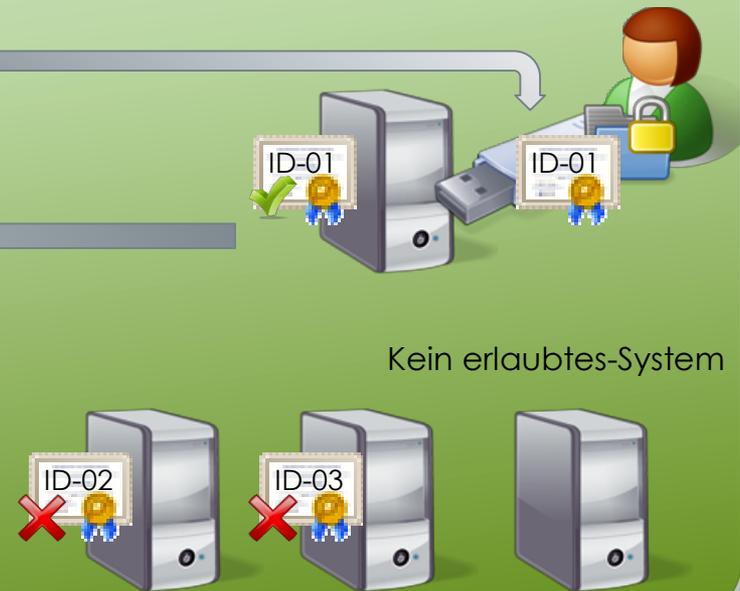


# Process for one dedicated target client

## Office Network



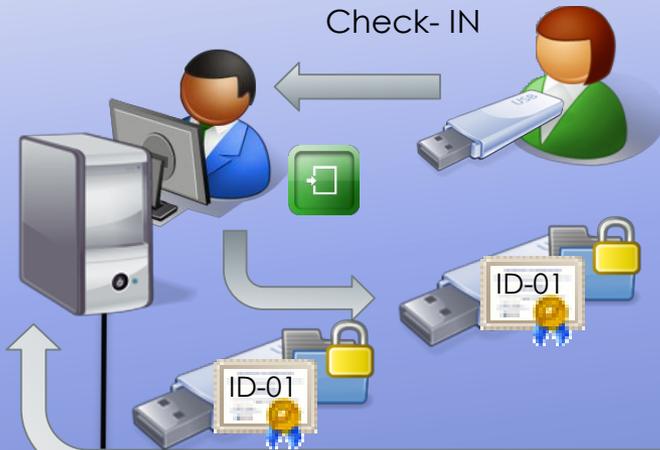
## Process Network



# Process for closed process network

## Office Network

Check-IN



Check-Out



## Closed Process Network



Share



# DC Prozess-Schritte

**DB Netz**



Check- IN

**Prozessnetz**



Operate

**DB Netz**



Check-Out



**Kompletter Ablauf**

# Pilot/Vorprojekt - Projektplan

## Installation Testumgebung

- Virtuell (VMWare ESXi)
- Eigene Hardware
- In bestehende Infrastruktur
- Dauer 1 Tag

## Schulung

- 2 Tage Vorort Schulung
- Installation in Testumgebung
- ondeso default Workflows
- Übergabe Dokumentation

## Testphase für Kunde

- 2 – 3 Wochen Testphase
- Evaluieren von zusätzl. Lösungsanforderungen

## 2. Schulung

- Integration von Kundenanforderungen
- Rolloutvorbereitung (Software)
- Projektabstimmung für Rollout
- Dauer 2 Tage

Optionales Rolloutkonzept zusammen mit ondeso oder einem Partner anfertigen.

## Rollout

- Software - Rollout

Vielen Dank für Ihre Aufmerksamkeit



SECURITY | TRACEABILITY | AVAILABILITY | REPORTING | STANDARDIZATION