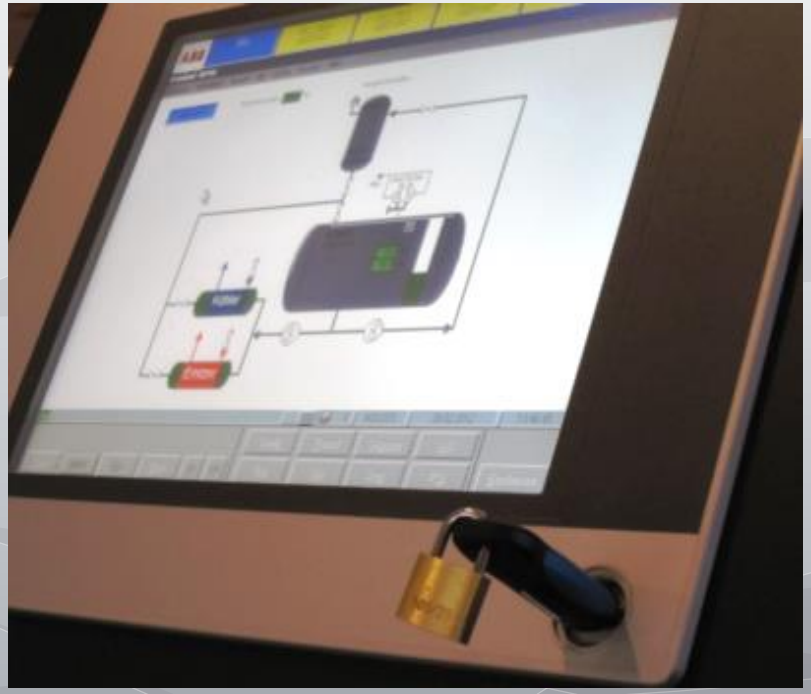
ondeso
certified . efficient . protection



Industrial IT Security

Sicherheitssoftware für die fertigende Industrie

ondeso SR SecureRelease und DC DeviceControl

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" erinnert haben. – Die Beschreibung passt zu dem Wurm **Stuxnet[3]**, der Industriebbetriebe 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

Einführung

- 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 Produktions-bereichen

Einführung

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“

Herausforderungen in der Industrie

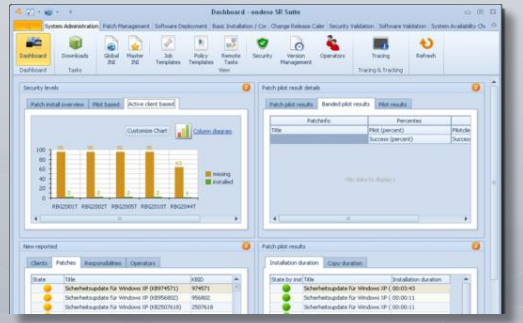
- Unwissenheit über Sicherheitslücken
- Fortfahren der Produktion - wissend um Sicherheitslücken
- Senkung des Risikos - hoher Aufwand durch proprietäre Eigenentwicklungen
- Infrastruktur muss zusammenwachsen, die Organisation kann nicht so einfach zusammengeschoben werden (fehlende Kompetenzen und benötigtes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

ondeso Software-Produkte

Kernprodukte

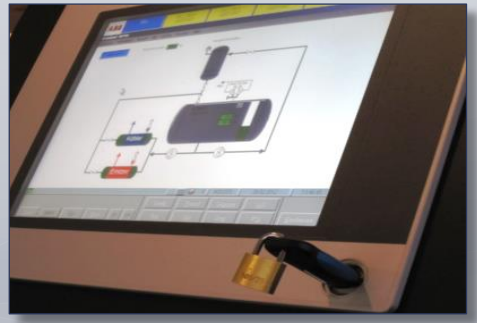
SR SecureRelease

Sicheres Release & Patchmanagement für kritische Produktions-systeme



DC DeviceControl

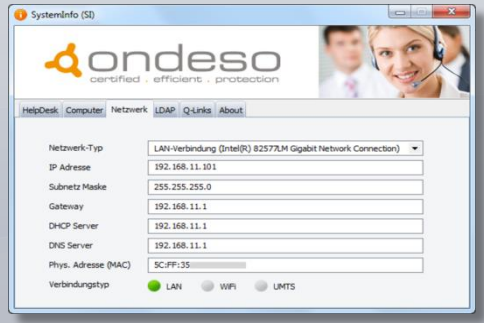
Kontrollierte, revisions-sichere Übertragung von Daten via USB zwischen Büro- und Prozessnetz



Informationstool

SI SystemInfo

Systeminformationen für den erleichterten Support durch den IT-Helpdesk



Customizing Client GUI – Workflows

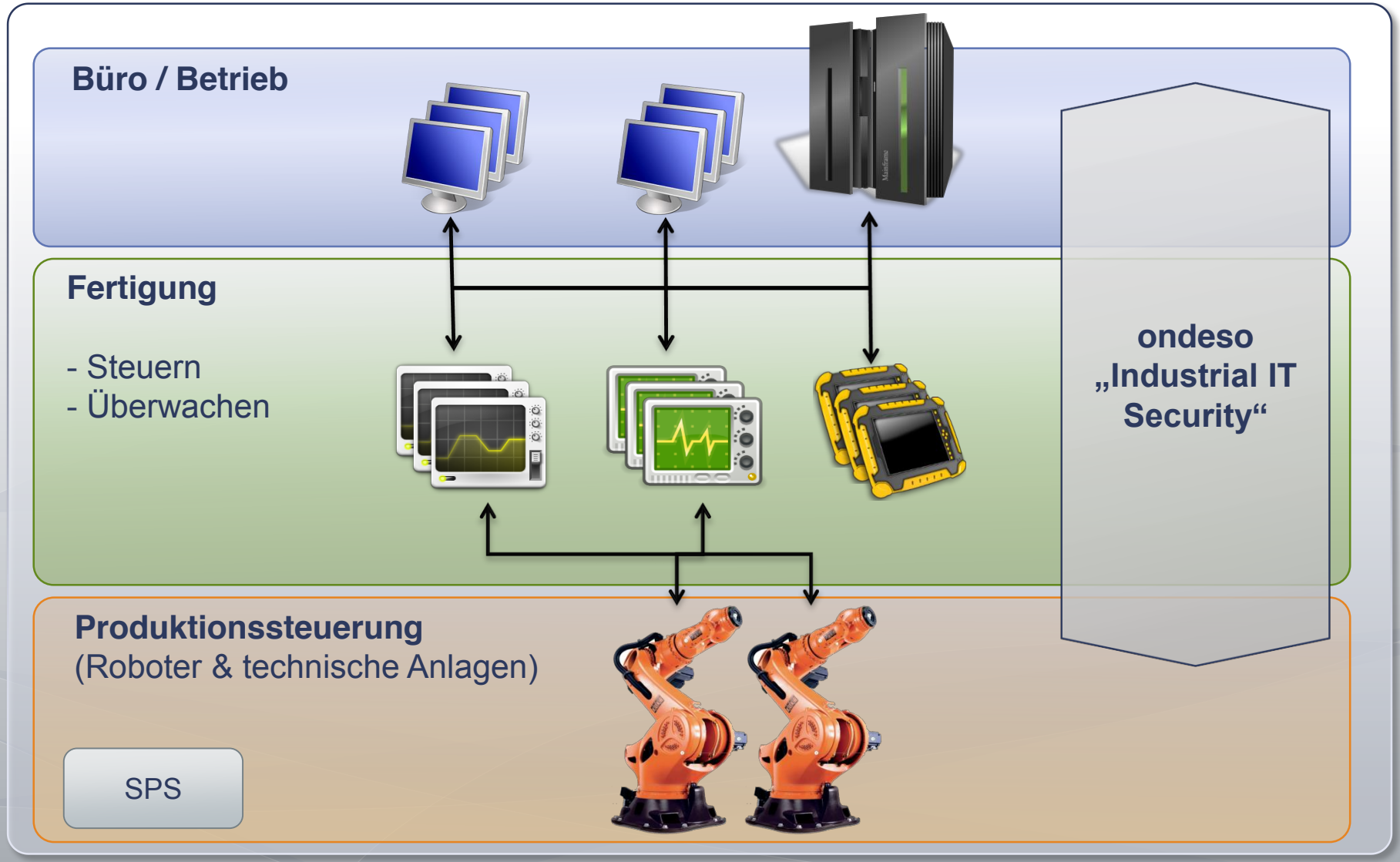
Einsatzmöglichkeiten

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

- ondeso Device Control

Wo ordnet es sich ein / grenzt sich ab

ondeso
certified . efficient . protection



Secure Release Management Software

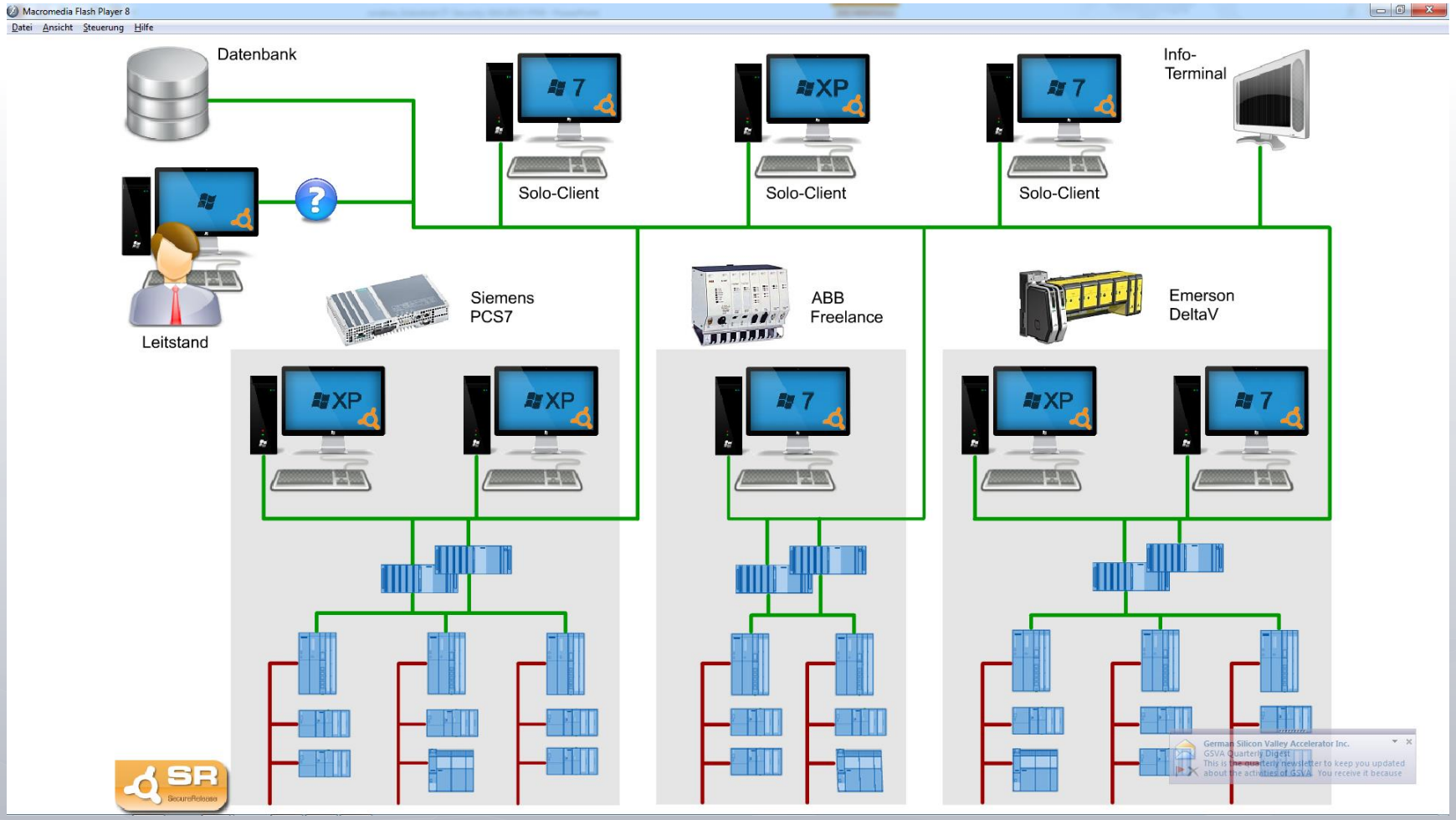
Softwareleitstand:

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

Kontrollierter Umgang mit USB-Massenspeicher

von „reaktiv manuell“ zu „planerisch prozessorientiert“

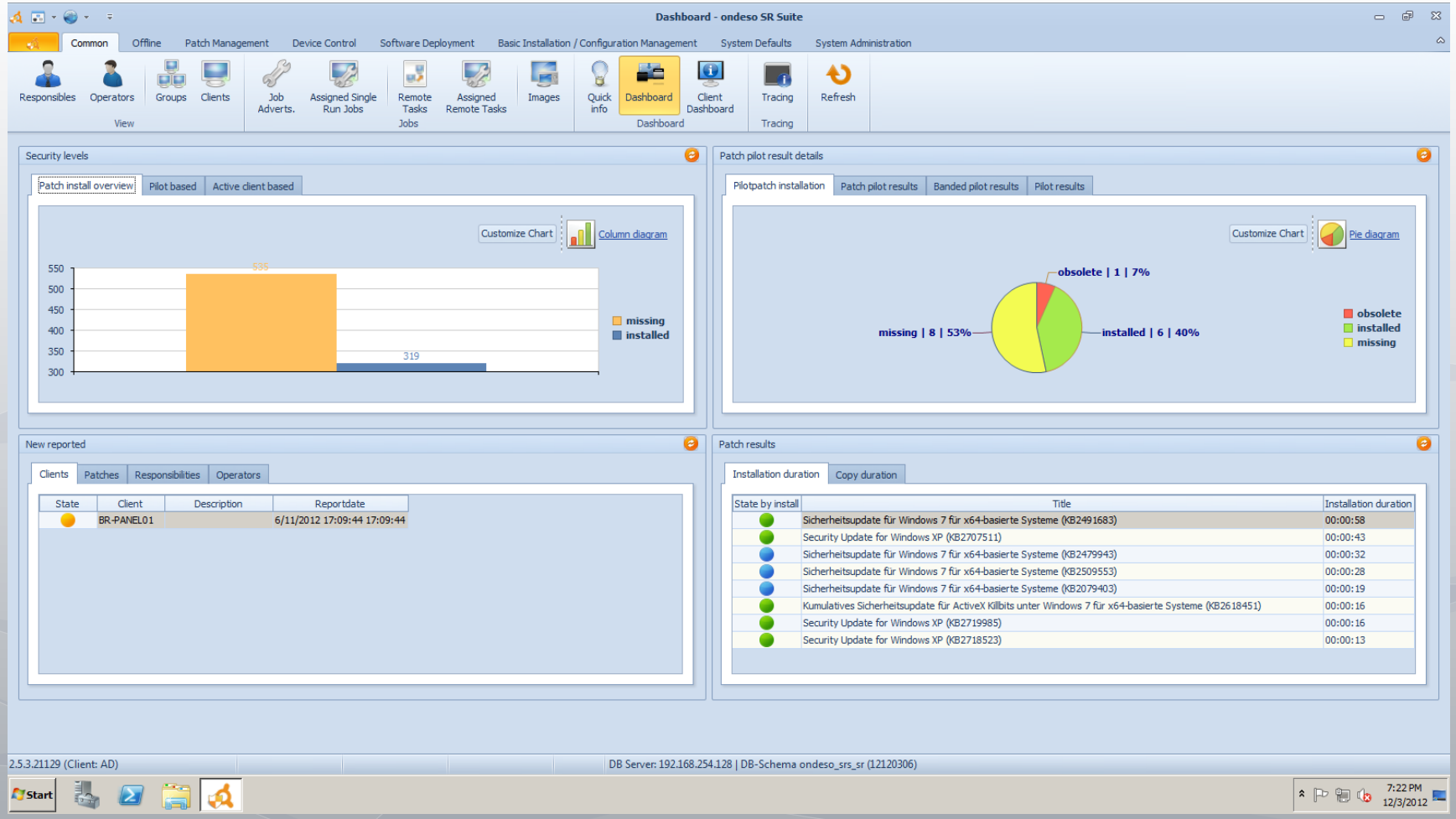
ondeso Industrial-IT Leitstand



Softwarelösung von ondeso

- 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



Fragestellungen im Kontext von Release Management

ondeso
certified . efficient . protection

- 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

Minimaler Eingriff in das Betriebssystem des Zielsystems:

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

Registrywerte ausschließlich unter **HKLM\ondeso**

Keine Registrierung von DLLs

Systemsteuerung

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

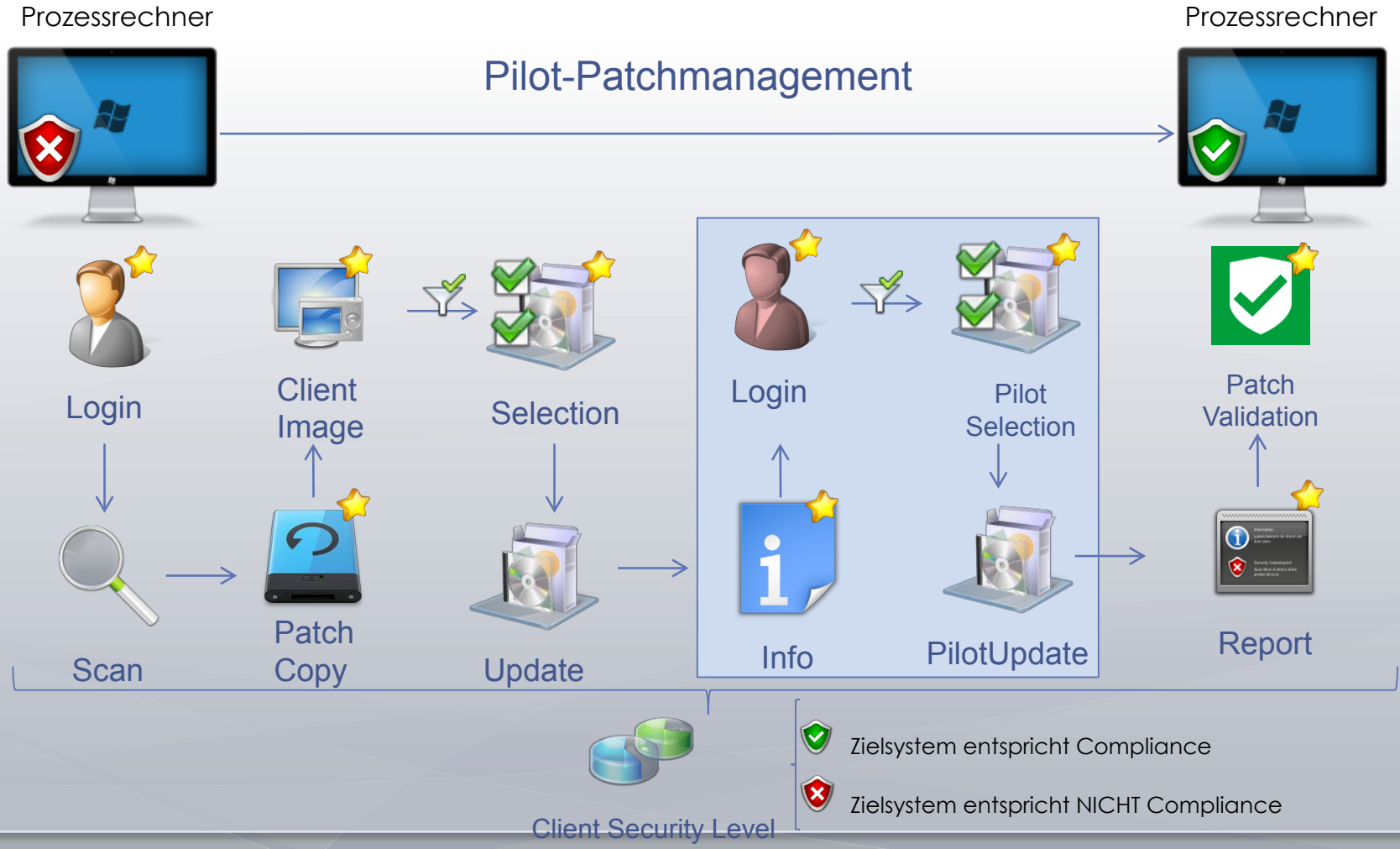
USB Control

Prozessrechner

USB Control

Pilot-Patchmanagement

Operating System Pilot-Patchmanagement



UseCases – ondeso default Workflows

Inventory

Prozessrechner

Inventory

Client Dashboard

Software

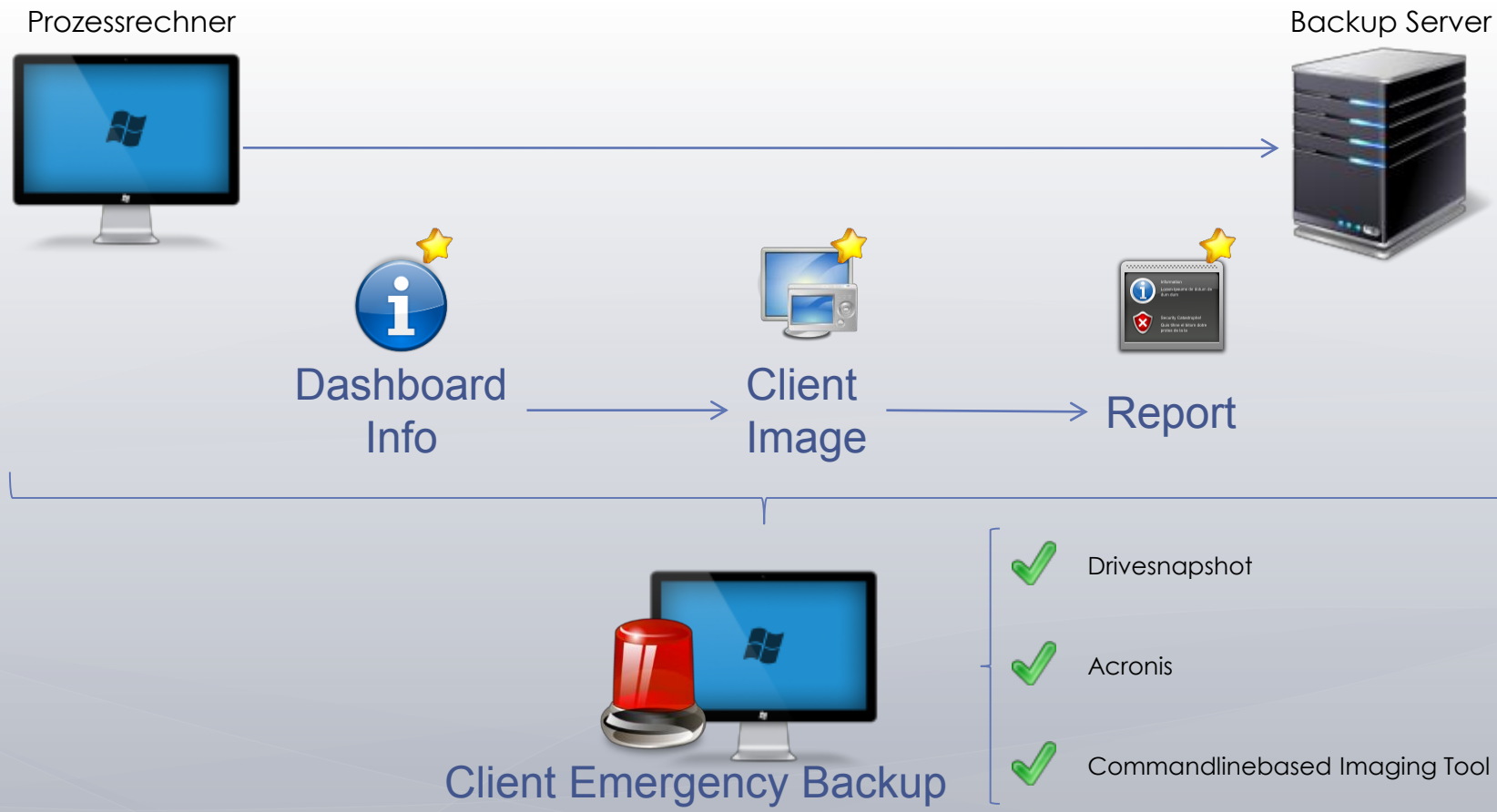
Zielsystem

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

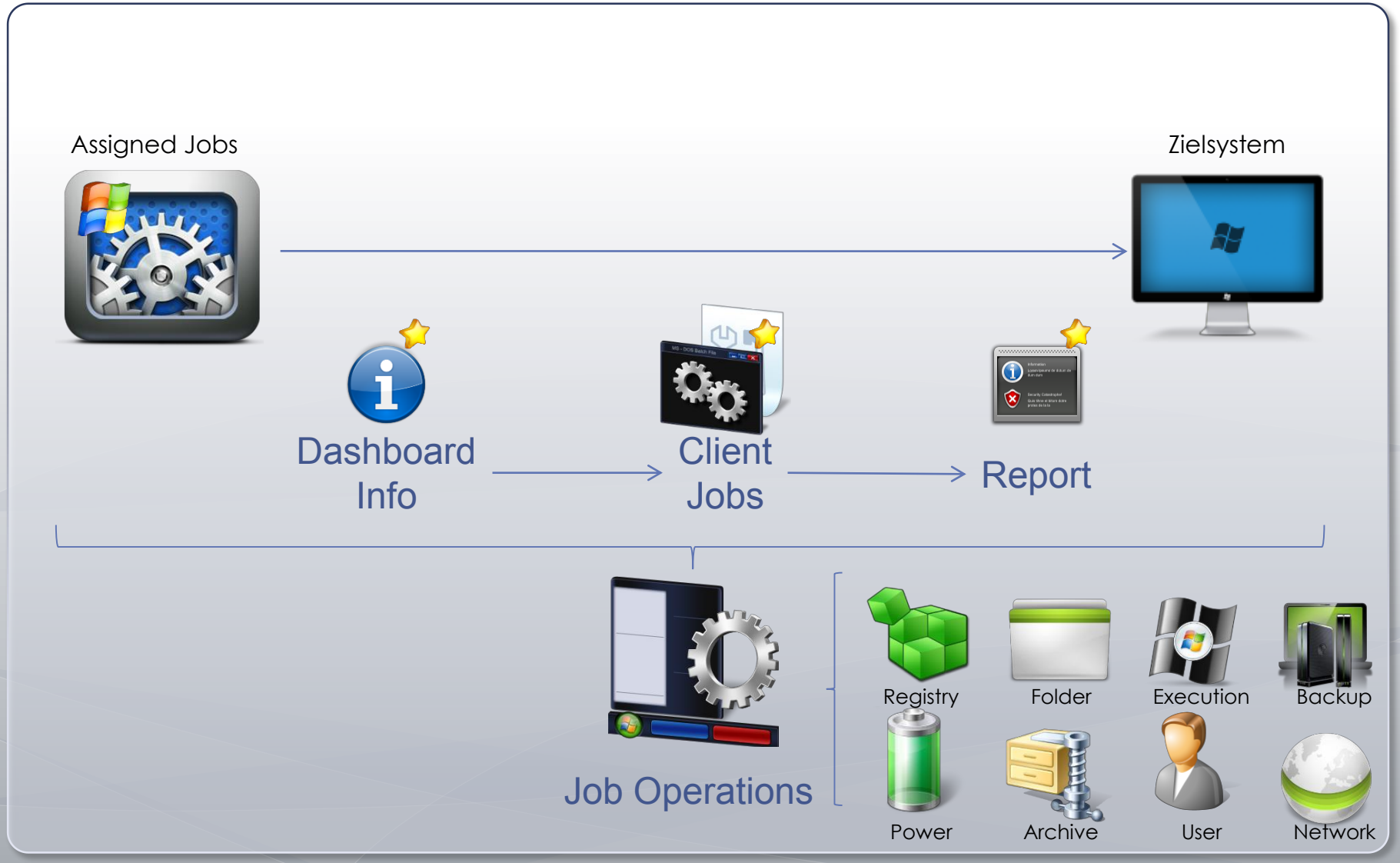
Zielsystem

Framework

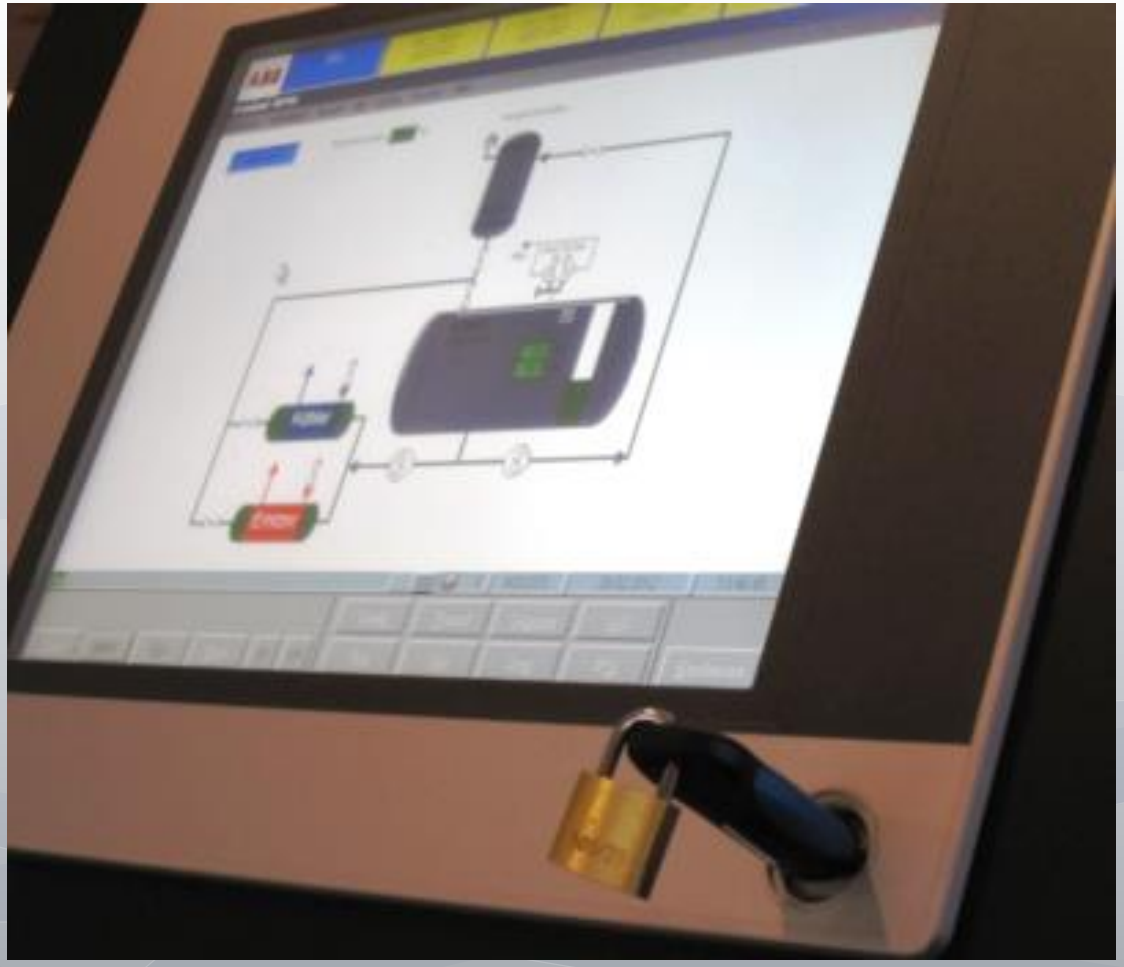
Workflow Items

Zielsystem

Job Execution (No Service Installation)



ondeso 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

Minimaler Eingriff in das Betriebssystem des Zielsystems:

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

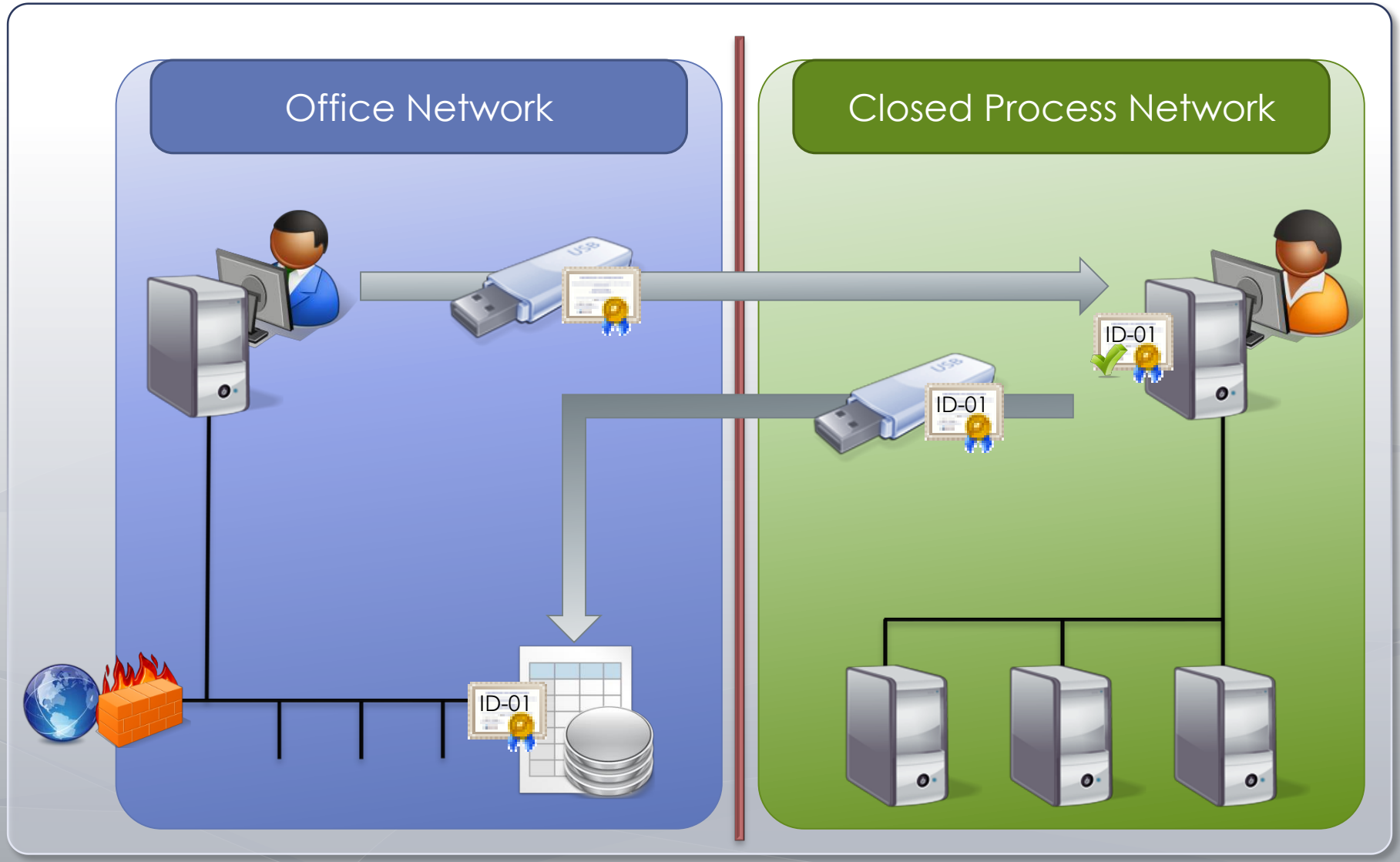
Registrywerte ausschließlich unter **HKLM\ondeso**

Keine Registrierung von DLLs

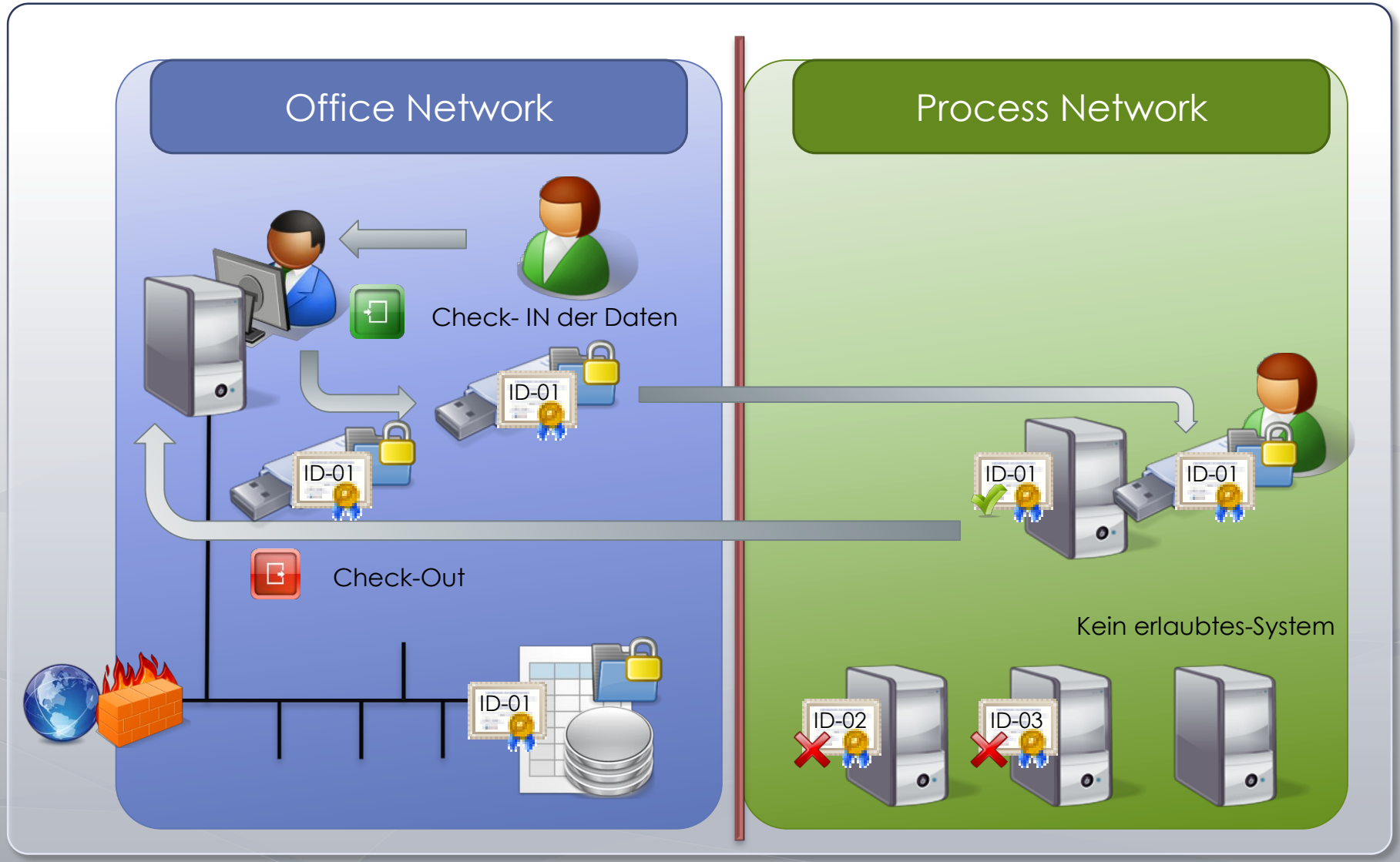
Einsatzmöglichkeit für getrennte Prozessnetze

- 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

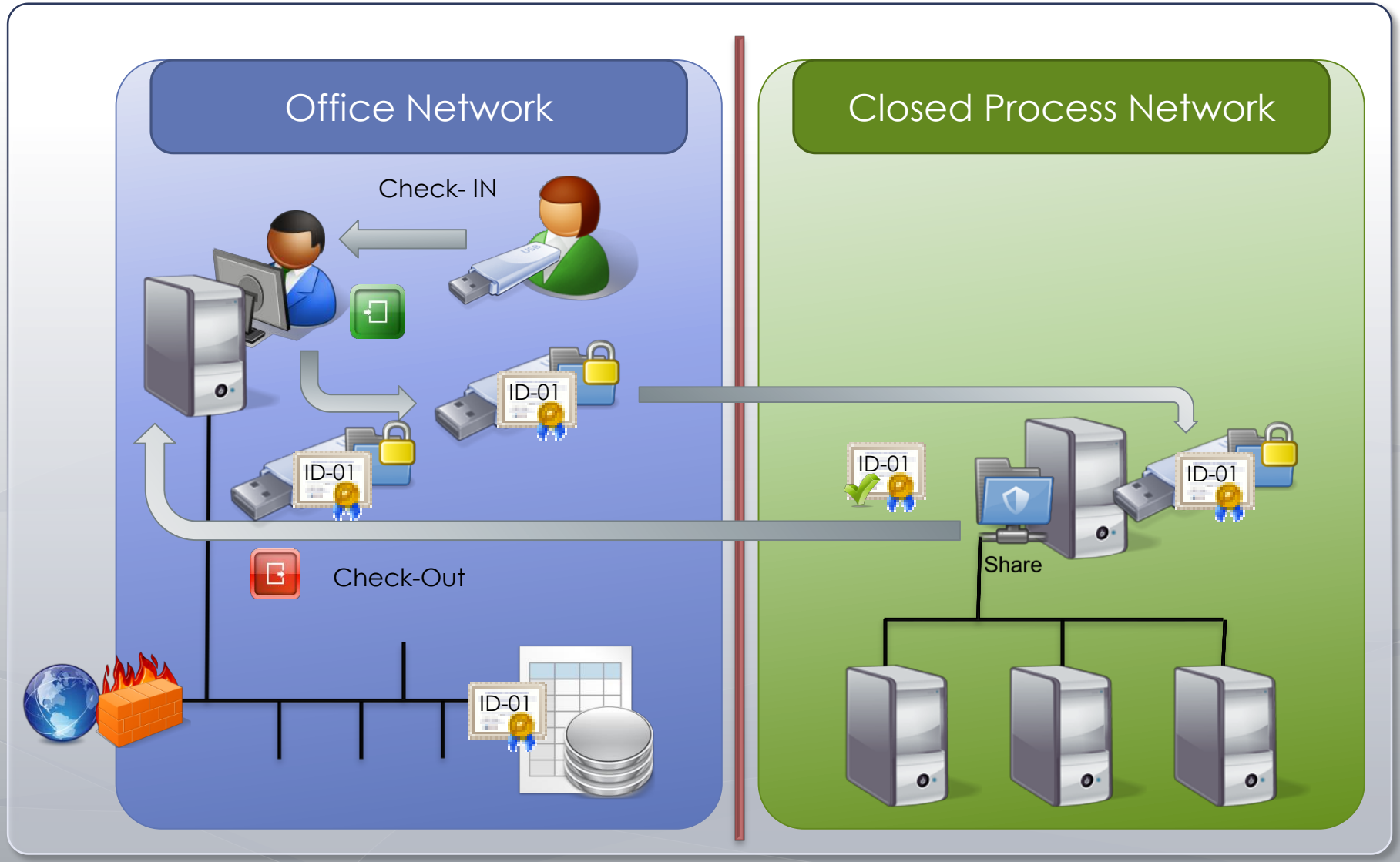
Preparation (Certificate Exchange)



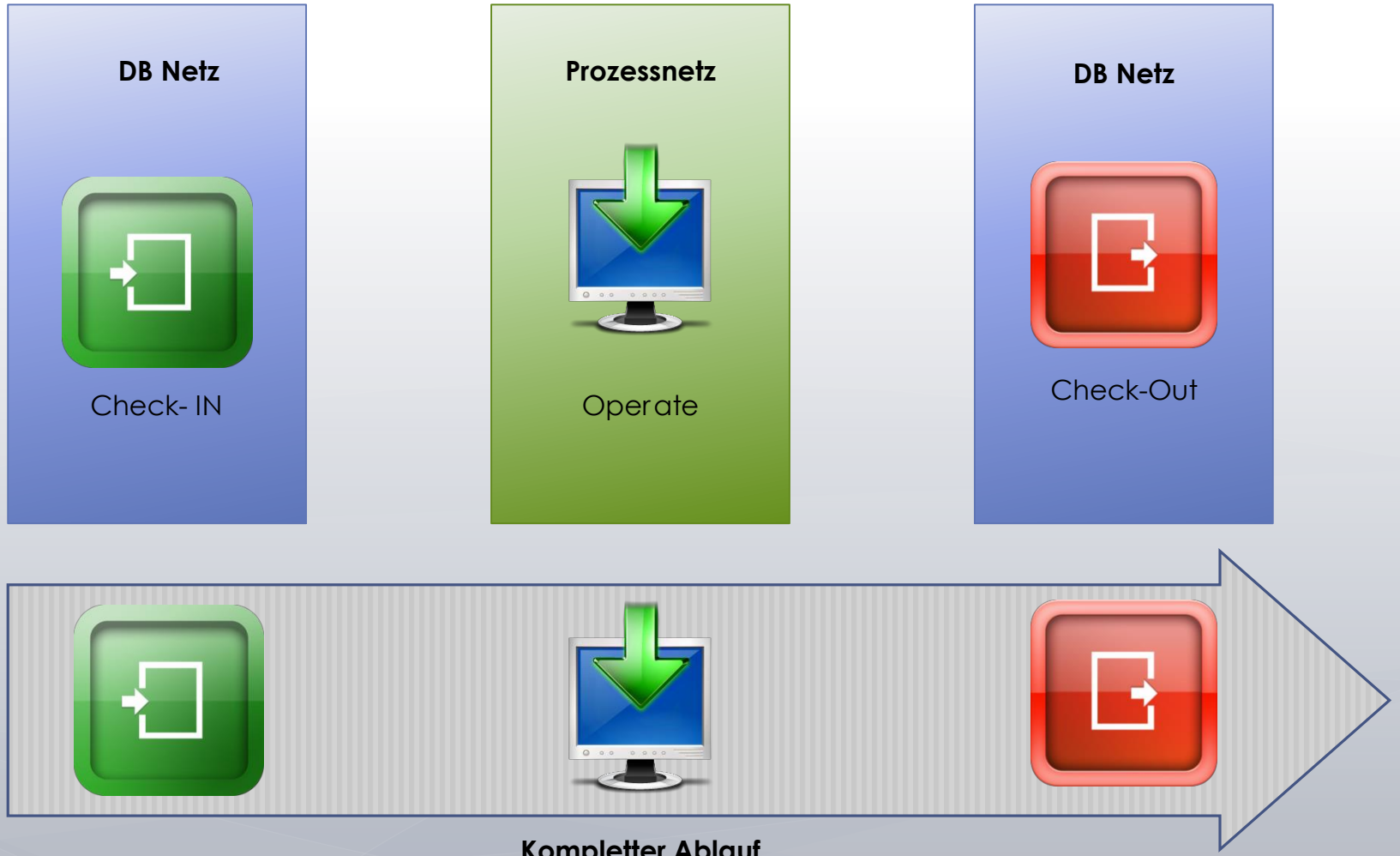
Process for one dedicated target client



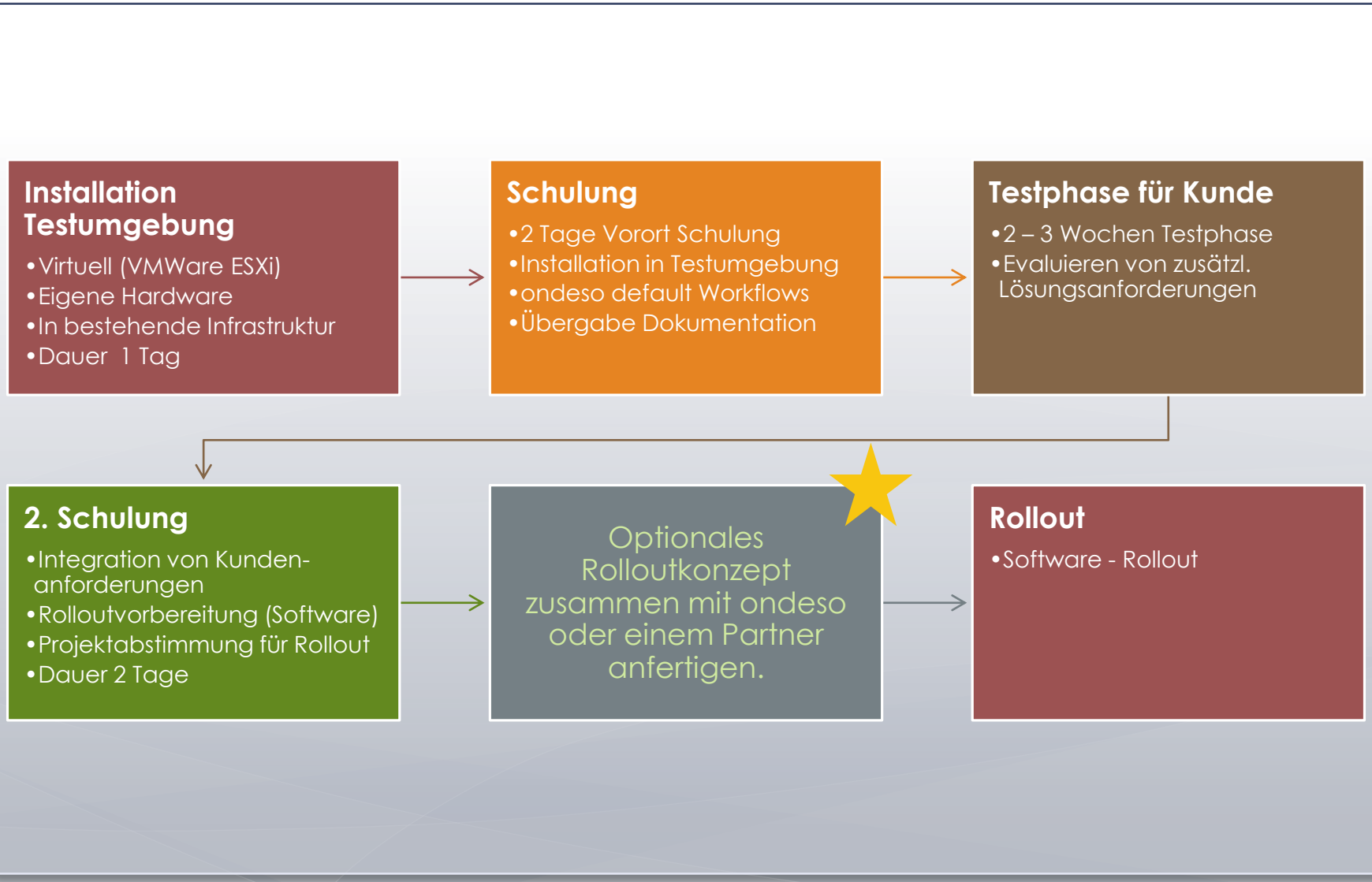
Process for closed process network



DC Prozess-Steps



Pilot/Vorprojekt - Projektplan



Vielen Dank für Ihre Aufmerksamkeit

ondeso
certified . efficient . protection

SECURITY | TRACEABILITY | AVAILABILITY | REPORTING | STANDARDIZATION