DATENMANAGEMENT FÜR IHRE AUTOMATISIERTE PRODUKTION

Willkommen zum Webinar

versiondog im Einsatz bei KRITIS Betrieben

AUVESY.

WILLKOMMEN ZUM WEBINAR

- Bitte schreiben Sie Ihre Fragen als Chat mit Angabe der E-Mail Adresse
- Unser Ziel ist es, keine Fragen offen zu lassen
  - Komplexere Fragen, werden wir im Nachgang beantworten
- Bitte schalten Sie Ihr Mikrofon stumm

Vorankündigung

Webinar-Reihe:

AUVESY Conference 2020 switch to digital

SWITCH TO DIGITAL

AUVESY Conference 2020

14./15. Mai mit virtuellen und kostenlosen Webinar-Vorträgen

Moderation

Iwona Glauser

Sales Managerin

Iwona.glauser@auvesy.de

AUVESY GmbH

Referenten

Dirk Thielker

Sales Manager

Dirk.thielker@auvesy.de

AUVESY GmbH

Georg Seiß

Business Development Manager

Georg.seiss@auvesy.de

AUVESY GmbH

AUVESY.

AUVESY.
Conference 2020
switch to digital

TREFFEN SIE UNSERE REDNER VIRTUELL

AUVESY Conference 2020

14./15. Mai mit virtuellen und kostenlosen Webinar-Vorträgen

AGENDA 2020
Jetzt Webinare buchen!

Buchen Sie unsere Webinar-Vorträge:

z.B.

- Neues aus der AUVESY Entwicklung (14. Mai)
- Qualifizierung 4.0 auf dem Shopfloor (14. Mai)
- IEC 62443 – Cyber-Security in der Industrieautomatisierung (14. Mai)
- AUVESY Image Service – In vier Schritten zum Image (15. Mai)
- versiondog eOS Client – Die Lösung für Windows NT, XP & LINUX (15. Mai)

uvm.

Die gesamte Agenda finden Sie auf unserer Website
www.auvesy.de/auvesy-conference.html

AUVESY.

UNSERE THEMEN

Einsatz von versiondog in KRITIS Unternehmen

- IT-Sicherheit in der Industrial IT
- Funktionalitäten von versiondog
  - (Detektion/Prävention & Reaktion)
- IT-Grundschutz & IT-Grundschutz-Kompendium
- Bausteine des IT-Grundschutz
  - Prozess- und Systembausteine

AUVESY.

IT-SICHERHEIT IN DER INDUSTRIAL IT

- ERFAHRUNG
- EINORDNUNG

AUVESY.

KRITIS - REFERENZEN AUS DER WASSERWIRTSCHAFT

Abwasserverband Main-Taunus

Berliner Wasserbetriebe

Emscher Genossenschaften Lippeverband

Aquafin NV, Aartselaar Belgien

Bonita Springs Utilities, Florida USA

Hansewasser, Bremen

Rand Water Johannisburg, Südafrika

City of Columbus Utilities Columbus, USA

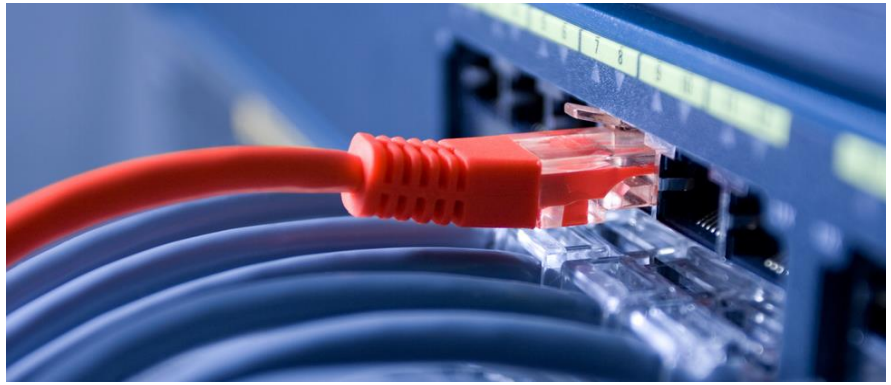
SA Water, Adelaide Australien

„KRITIS-Unternehmen müssen die Nachhaltigkeit ihrer Schutzmaßnahmen nachweisen und entsprechende Standards umsetzen. Dazu gehört beispielsweise, nach einem Störfall sehr schnell wieder „betriebsfähig“ zu sein.“

Jörg Saathoff, Abteilungsleiter Instandhaltung EGLV

AUVESY.

UNTERSCHIEDLICHE KONZEPTION DER IT-SYSTEME



Office IT – Priorität: **Vertraulichkeit**

- **Hohe Verfügbarkeit** von Schutzsystemen
- Möglichkeit der **Systemverlangsamung**
- Rechner können häufig **heruntergefahren** werden
- **Selten eine physische** Gefahr für Mensch, Natur und Umwelt

Industrial IT – Priorität: **Verfügbarkeit**

- **Antivirus nicht möglich** (verlangsamt das System)
- Systeme waren **isoliert konzipiert**
- Neustart des Systems bedingt **Ausfallzeiten**
- **Kaum** Verfügbarkeit von **Schutzsystemen**
- **Physikalische Gefahr** für Mensch, Natur und Umwelt

AUVESY.

STUXNET

- Ungewollte Manipulation, die versiondog erkannt hätte

Zero Days

IMDb 7,8/10

Filmstarts.de 60 %

In der Dokumentation berichten Insider von der Entwicklung des Geheimprogramms "Olympic Games" - einer Software, die die Infrastruktur ganzer Staaten lahmlegen kann, ohne Spuren zu den Verursachern zu hinterlassen. Die packende Story eines Quellcodes, der außerhalb des Cyberspace schweren Schaden anrichtete, ... +

IMDb Wikipedia Offizielle Website

Erscheinungsdatum: 8. Jul 2016 (Vereinigte Staaten)

Regisseur: Alex Gibney

Zusammenfassung: FSK: 16 · 2016 · 1 Std. 56 Min. · Dokumentarfilm

AUVESY.

ICS VULNERABILITIES

Siemens Security Advisory by Siemens ProductCERT

SSA-731239: Vulnerabilities in SIMATIC S7-300 and S7-400 CPUs

Publication Date: 2016-12-09
Last Update: 2020-03-10
Current Version: V1.6
CVSS v3.1 Base Score: 7.5

SUMMARY

Two vulnerabilities have been identified in SIMATIC S7-300 and S7-400 CPU families. One vulnera could lead to a Denial-of-Service, the other vulnerability could result in credential disclosure.

Siemens recommends specific mitigations. Siemens will update this advisory when new infor becomes available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	Update to V3.X.14 to mitigate the first (CVE-2016-9158), and follow recom from section Workaround and Mitig second vulnerability (CVE-2016-91 https://support.industry.siemens.c ps/13752/dl
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	Update to V6.0.6 to mitigate the (CVE-2016-9158), and follow re from section Workaround and M second vulnerability (CVE-201 https://support.industry.sieme view/109474874

DE

CODESYS

CODESYS SECURITY-INFORMATIONEN

Mit zunehmender Vernetzung von Maschinen und Anlagen via Internet spielt der Schutz vor Cyberattacken eine immer größere Rolle. Das Th Group hohe Priorität und ist integraler Bestandteil des Entwicklungsprozesses.

Die in den CODESYS-Produkten integrierten Security-Funktionen werden permanent gepflegt und erweitert. Alle CODESYS Softwarekompo Sicherheitslücken überprüft. Zudem verpflichtet sich die CODESYS Group, verifizierte Sicherheitslücken in einem angemessenen Zeitraum z (PDF) finden Sie alle wichtigen Informationen rund um das Thema CODESYS Security.

Melden Sie Sicherheitslücken!

CODESYS Security Advisories

Letzte Änderung	Advisory-Nummer	Advisory (PDF)
01.04.2020	2020-03	Security update for CODESYS V3 web server
01.04.2020	2020-02	Security update for various CODESYS V3 products using the CODESYS communicatio
23.01.2020	2020-01	Security update for several CODESYS V3 products containing a CODESYS communica
18.12.2019	2019-11	Security update for CODESYS Control V2
18.12.2019	2019-10	Security update for CODESYS V3 web server
23.10.2019	2019-09	Security update for CODESYS V2.3 ENI server
24.04.2020	2019-08	CODESYS V3 various products password handling vulnerabilities
18.12.2019	2019-07	Security update for CODESYS Control V3 OPC UA Server
18.12.2019	2019-06	Security update for several CODESYS V3 products containing a CODESYS communica
24.04.2020	2019-05	CODESYS V3 Library Manager cross-site scripting vulnerability

AUVESY.

47 ELEMENTARE GEFÄHRDUNGEN IT-GRUNDSCHUTZ-KOMPENDIUM 2020

• G01 Feuer • G02 Ungünstige klimatische Bedingungen • G03 Wasser • G04 Verschmutzung, Staub, Korrosion • G05 Naturkatastrophen • G06 Katastrophen im Umfeld • G07 Großereignisse im Umfeld • G08 Ausfall oder Störung der Stromversorgung • G09 Ausfall oder Störung von Kommunikationsnetzen • G010 Ausfall oder Störung von Versorgungsnetzen • G011 Ausfall oder Störung von Dienstleistern • G012 Elektromagnetische Störstrahlung • G013 Abfangen kompromittierender Strahlung • G014 Ausspähen von Informationen (Spionage) • G015 Abhören • G016 Diebstahl von Geräten, Datenträgern oder Dokumenten • G017 Verlust von Geräten, Datenträgern oder Dokumenten • G018 Fehlplanung oder fehlende Anpassung • G019 Offenlegung schützenswerter Informationen • G020 Informationen oder Produkte aus unzuverlässiger Quelle • G021 Manipulation von Hard- oder Software • G022 Manipulation von Informationen • G023 Unbefugtes Eindringen in IT-Systeme • G024 Zerstörung von Geräten oder Datenträgern • G025 Ausfall von Geräten oder Systemen • G026 Fehlfunktion von Geräten oder Systemen • G027 Ressourcenmangel • G028 Software-Schwachstellen oder -Fehler • G029 Verstoß gegen Gesetze oder Regelungen • G030 Unberechtigte Nutzung oder Administration von Geräten und Systemen • G031 Fehlerhafte Nutzung oder Administration von Geräten und Systemen • G032 Missbrauch von Berechtigungen • G033 Personalausfall • G034 Anschlag • G035 Nötigung, Erpressung oder Korruption • G036 Identitätsdiebstahl • G037 Abstreiten von Handlungen • G038 Missbrauch personenbezogener Daten• G039 Schadprogramme • G040 Verhinderung von Diensten (Denial of Service) • G041 Sabotage • G042 Social Engineering • G043 Einspielen von Nachrichten • G044 Unbefugtes Eindringen in Räumlichkeiten • G045 Datenverlust • G046 Integritätsverlust schützenswerter Informationen • G047 Schädliche Seiteneffekte IT-gestützter Angriffe

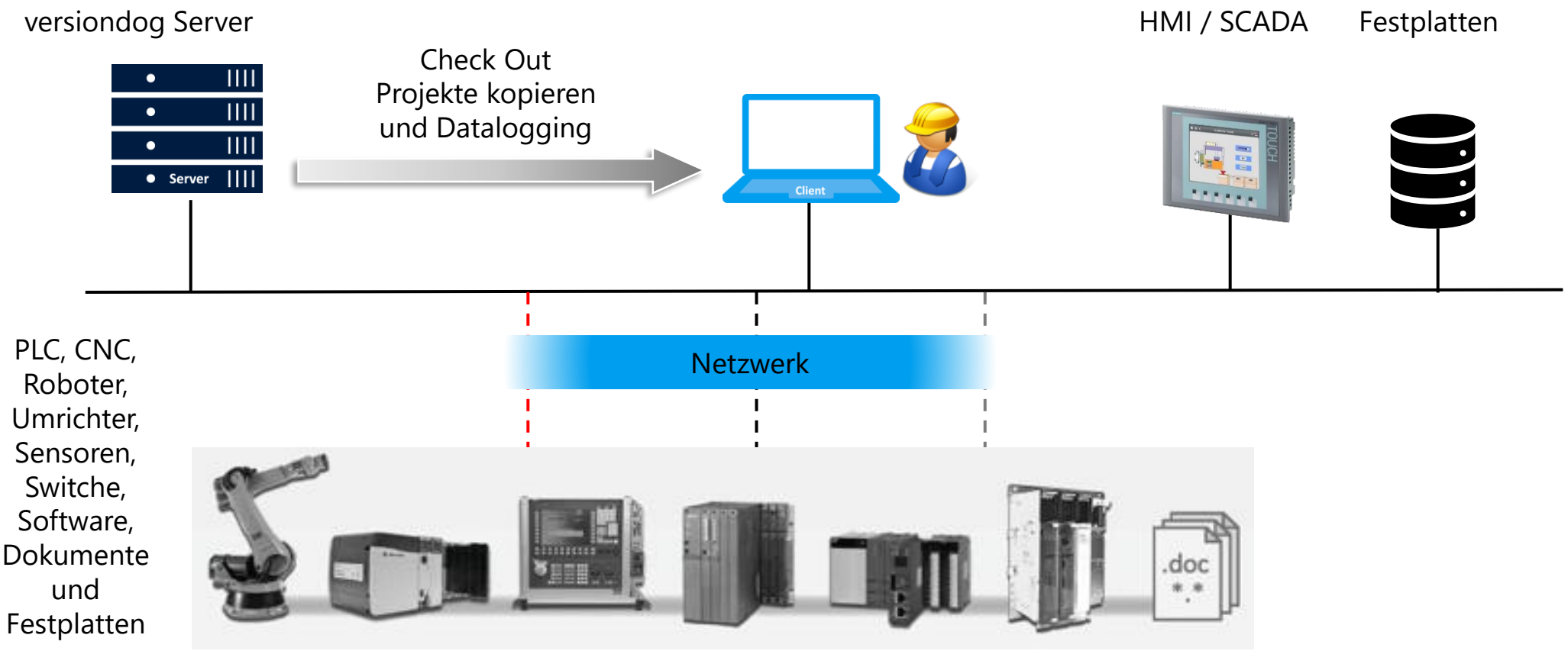
AUVESY.

FUNKTIONALITÄT VON VERSIONDOG

- VERSIONIERUNG / VERGLEICH
- BACKUP / VERGLEICH
- DISASTER RECOVERY / DOKUMENTATION
- E-MAIL BENACHRICHTIGUNG

AUVESY.

VERSIONDOG VERSIONIERUNG



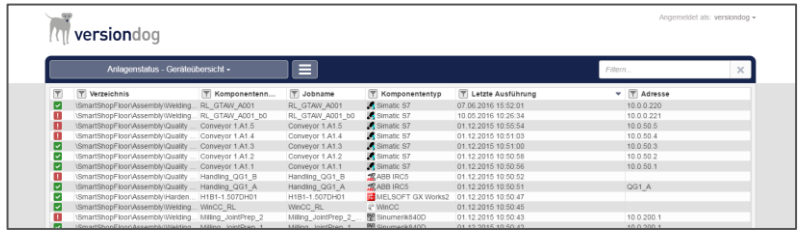
VERSIONDOG VERSIONIERUNG UND REPORT

VERSIONIERUNG/VERGLEICH

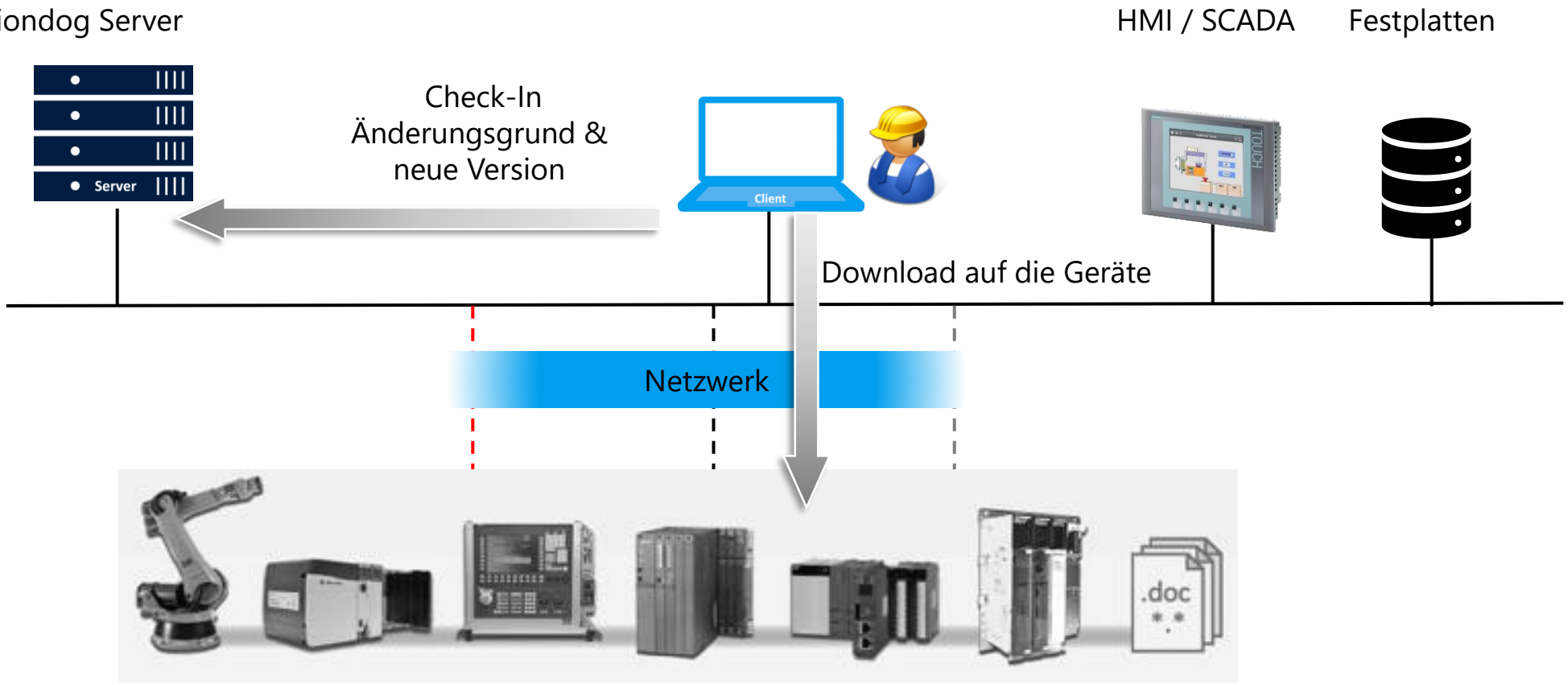
BACKUP

DOKUMENTATION / DISASTER RECOVERY

BENACHRICHTIGUNG

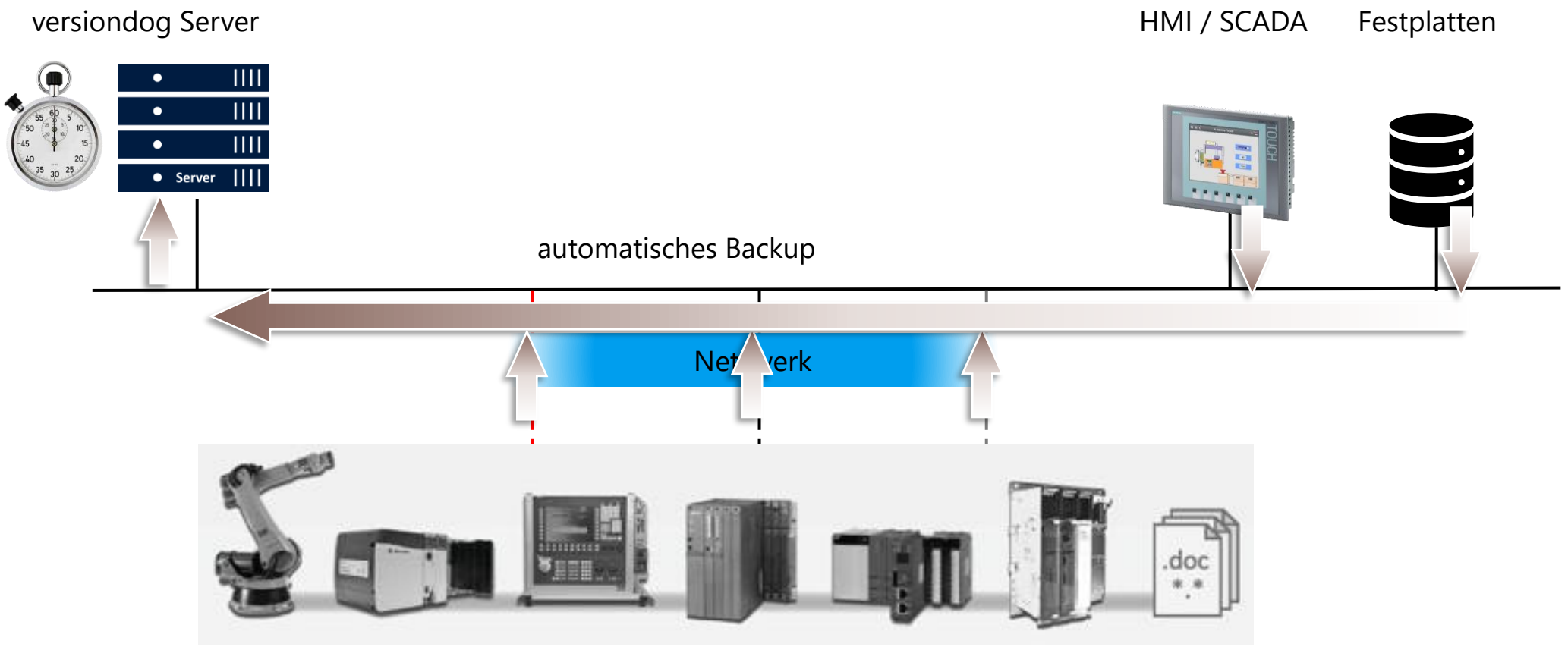


Report & Änderungshistorie



AUVESY.

VERSIONDOG BACKUP



AUVESY.

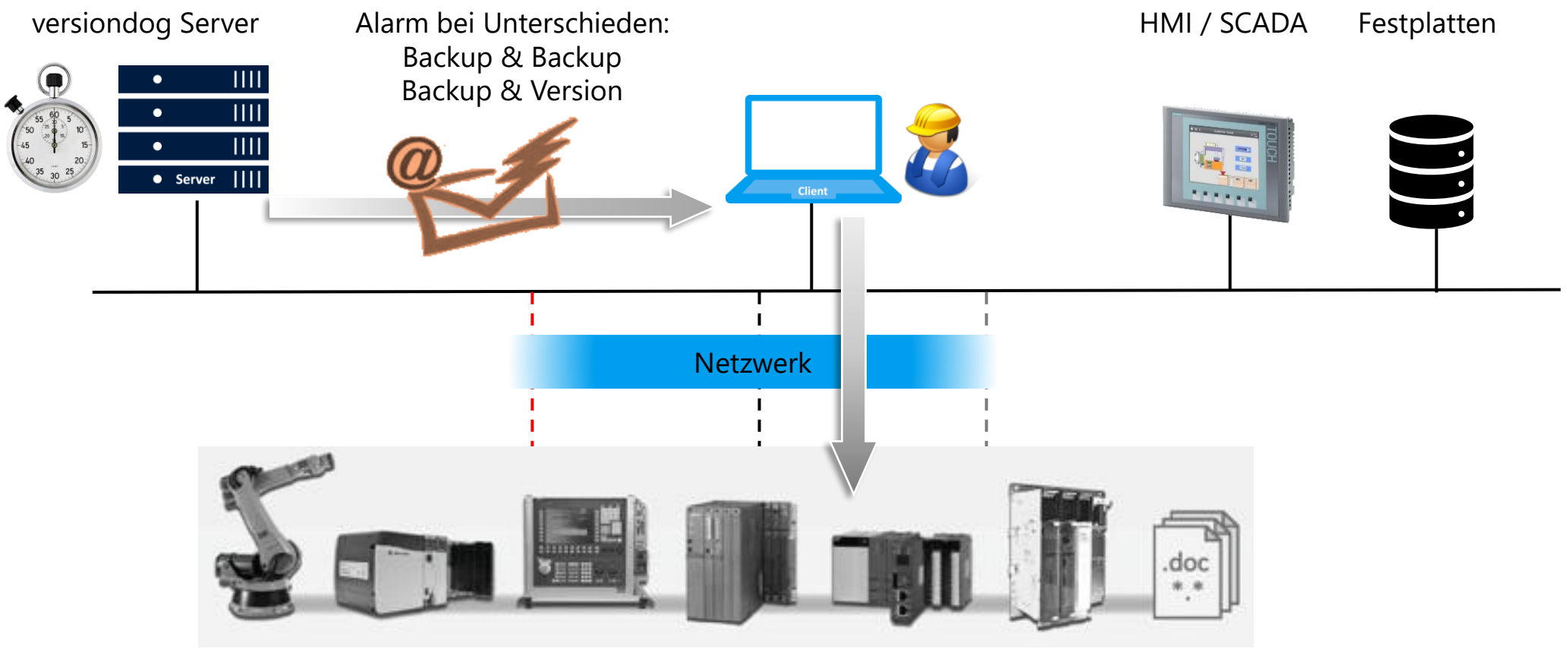
VERSIONDOG E-MAIL UND DISASTER RECOVERY

VERSIONIERUNG/VERGLEICH

BACKUP

DOKUMENTATION / DISASTER RECOVERY

BENACHRICHTIGUNG



AUVESY.

IT-GRUNDSCHUTZ-KOMPENDIUM

- Methodik des IT-Grundschutzes
- Ersetzt die IT-Grundschutz-Kataloge
- Konkretisierung des IT-Grundschutz
  - Einführung in Grundschutz Standards
  - Konkrete Anforderungen
  - Gefährdungen

AUVESY.

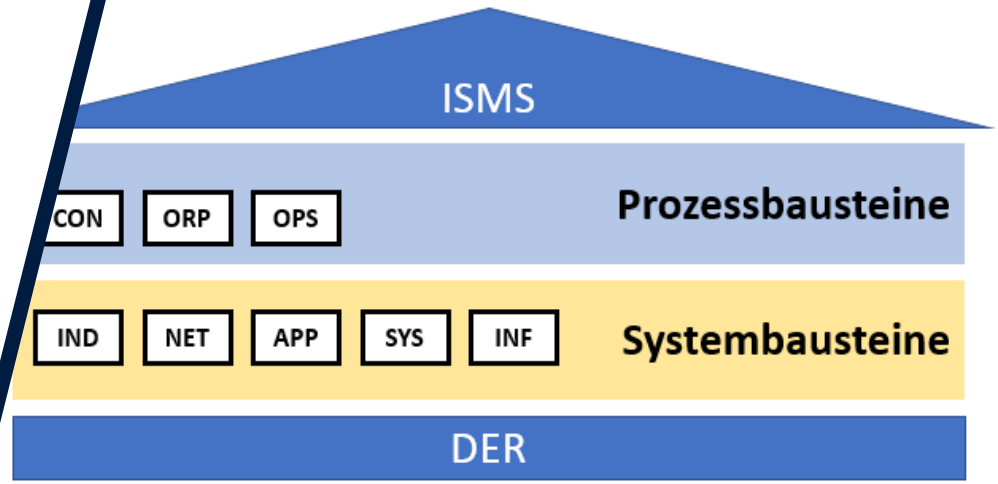
BAUSTEINE DES IT-GRUNDSCHUTZ

- ANFORDERUNGEN
- UMSETZUNG
- FUNKTIONALITÄTEN

AUVESY.

BAUSTEINE DES IT-GRUNDSCHUTZ

- Bausteine:
  - Prozessbausteine
  - Systembausteine
- Anforderungen:
  - MUSS (Basis Absicherung)
  - SOLL (Standard Absicherung)



IT-Grundschutz-Schichtenmodell

Für jeden Baustein und Zielobjekt gilt:
1. Die Gefährdungslage zu erkennen
2. MUSS und SOLL Anforderungen zu identifizieren
3. die Anforderungen an das Zielobjekt umzusetzen.

AUVESY.

PROZESSBAUSTEINE UMSETZUNG

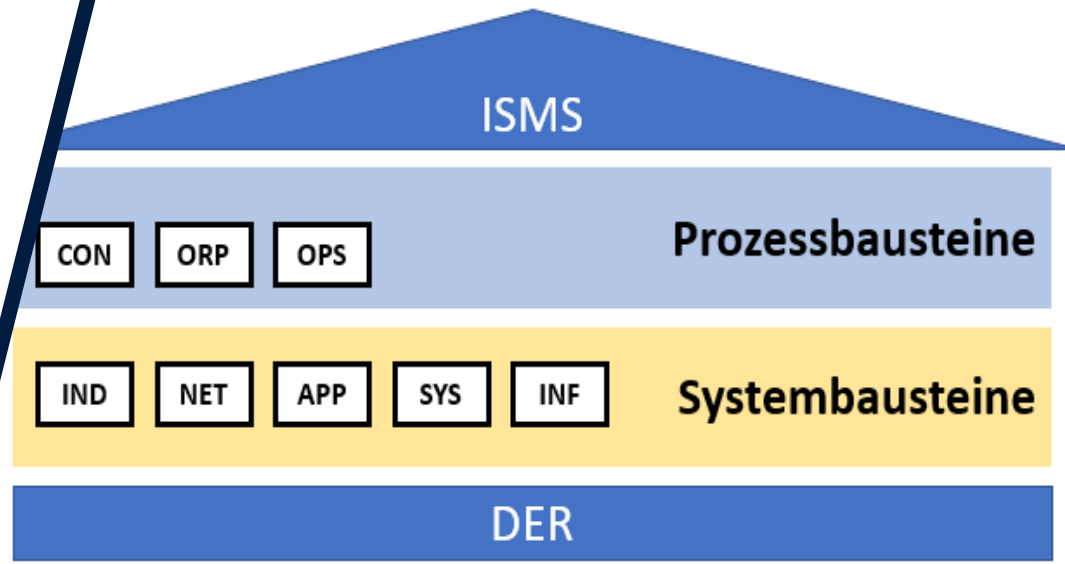
- Prozess-Bausteine:
  - CON.3: Datensicherungskonzept
  - DER.1: Detektion von sicherheitsrelevanten Ereignissen
- Versiondog Funktionalitäten zur Umsetzung

VERSIONIERUNG/VERGLEICH

BACKUP/VERGLEICH

DOKUMENTATION / DISASTER RECOVERY

BENACHRICHTIGUNG



IT-Grundschutz-Schichtenmodell

AUVESY.

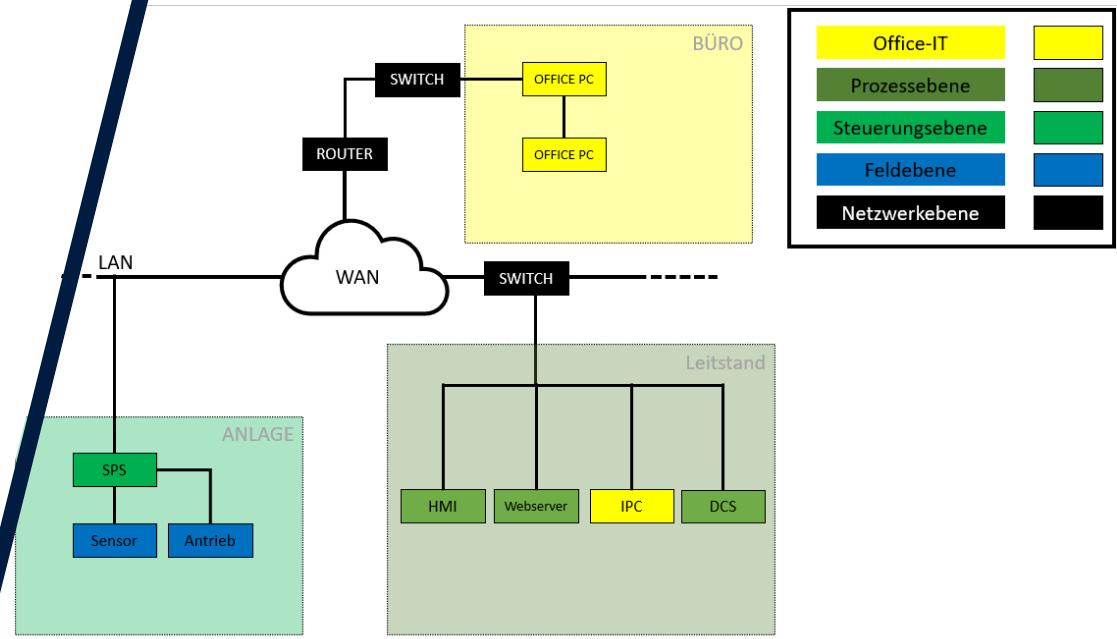
SYSTEMBAUSTEINE UMSETZUNG

- System-Bausteine:
  - IND
    - IND.1 Betriebs- und Steuerungstechnik
    - IND.2.1 Allgemeine ICS-Komponente
    - IND.2.2 Speicherprogrammierbare Steuerung (SPS)
    - IND.2.3: Sensoren und Aktoren

IND
IND
IND

  - NET
    - NET.3.1: Router und Switches

NET



AUVESY.

SYSTEMBAUSTEINE UMSETZUNG

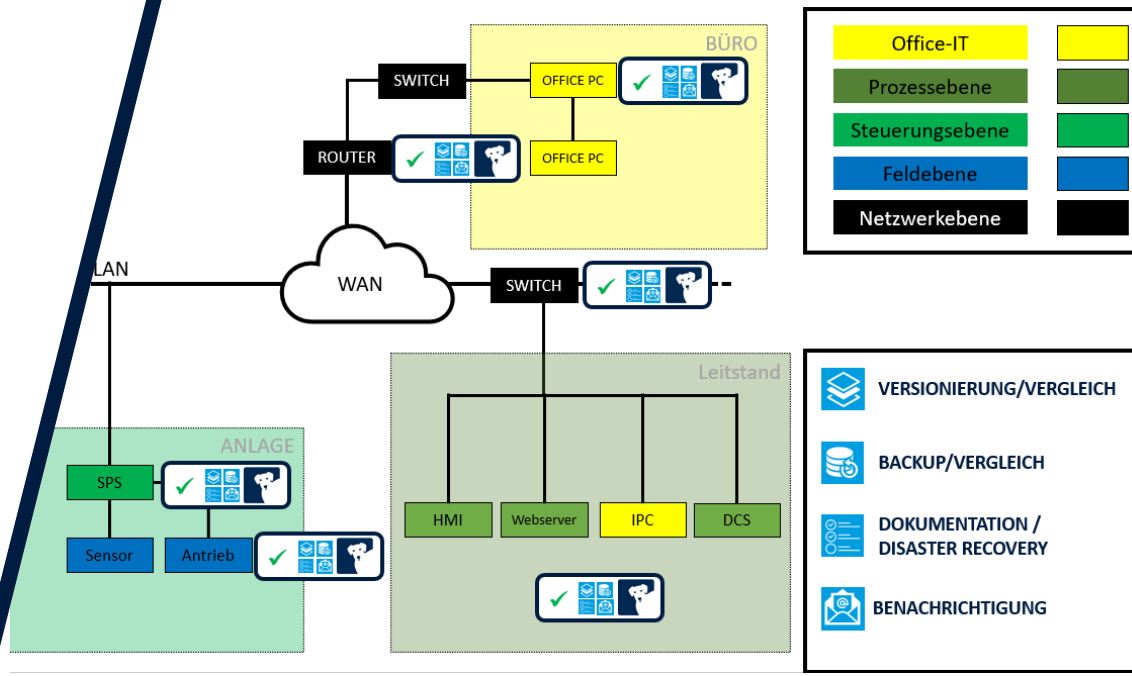
- Umsetzung der Anforderungen für System-Bausteine:

VERSIONIERUNG/VERGLEICH

BACKUP/VERGLEICH

DOKUMENTATION / DISASTER RECOVERY

BENACHRICHTIGUNG



AUVESY.

KONKRETE BEISPIELE

Baustein	Anforderung	MUSS Anforderung	SOLL Anforderung
IND Bausteine			
IND.1: Betriebs- und Steuerungstechnik Gefährdungslage (2.4 / 2.5 / 2.7 /2.8)			
IND.1.A3	Schutz vor Schadprogrammen	X	
IND.1.A6	Änderungsmanagement im OT-Betrieb		X
IND.1.A9	Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten		X
IND.1.A10	Monitoring, Protokollierung und Detektion [Bereichssicherheitsbeauftragter]		X

IND.1.A3 Schutz vor Schadprogrammen

ANFORDERUNG

- [...] Es MÜSSEN geeignete technische und organisatorische Schutzmaßnahmen festgelegt sein. [...]

UMSETZUNG

- ✓ Erstellung von Datensicherung in Form von Versionen
- ✓ Erstellung von Datensicherung in Form von Backups
- ✓ DETEKTION von Änderungen durch Vergleich der Datensätze
- ✓ Bereitstellung von Disaster Recovery

AUVESY.

KONKRETE BEISPIELE

Baustein	Anforderung	MUSS Anforderung	SOLL Anforderung
IND Bausteine			
IND.1: Betriebs- und Steuerungstechnik Gefährdungslage (2.4 / 2.5 / 2.7 /2.8)			
IND.1.A3	Schutz vor Schadprogrammen	X	
IND.1.A6	Änderungsmanagement im OT-Betrieb		X
IND.1.A9	Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten		X
IND.1.A10	Monitoring, Protokollierung und Detektion [Bereichssicherheitsbeauftragter]		X

IND.1.A6 Änderungsmanagement im OT-Betrieb

ANFORDERUNG

- [...]Für Änderungen an der OT SOLLTE ein Änderungsprozess (Change-Management) definiert, dokumentiert und gelebt werden. Der Änderungsprozess SOLLTE gewährleisten, dass Änderungen geplant, dokumentiert, und angemessen auf unerwünschte Nebeneffekte und Funktionalität getestet werden. [...]

UMSETZUNG

- ✓ Versionierung
- ✓ Backup
- ✓ Vergleich
- ✓ Dokumentation

AUVESY.

KONKRETE BEISPIELE

- Weitere Informationen?
  - Anwenderbericht „Alles klar beim Wasser“
  - AUVESY Leitfaden für KRITIS Betreiber
    - Ab Juni 2020 verfügbar
  - Vortrag „IEC 62443 – Cyber-Security in der Industrieautomatisierung (14. Mai)” auf der AUVESY Conference 2020
  - Weitere Informationen erhalten Sie von Ihrem Ansprechpartner/-in bei AUVESY

Alles klar beim Wasser

IT-Sicherheit kritischer Infrastrukturen (KRITIS) mit dem Datenmanagementsystem versiondog

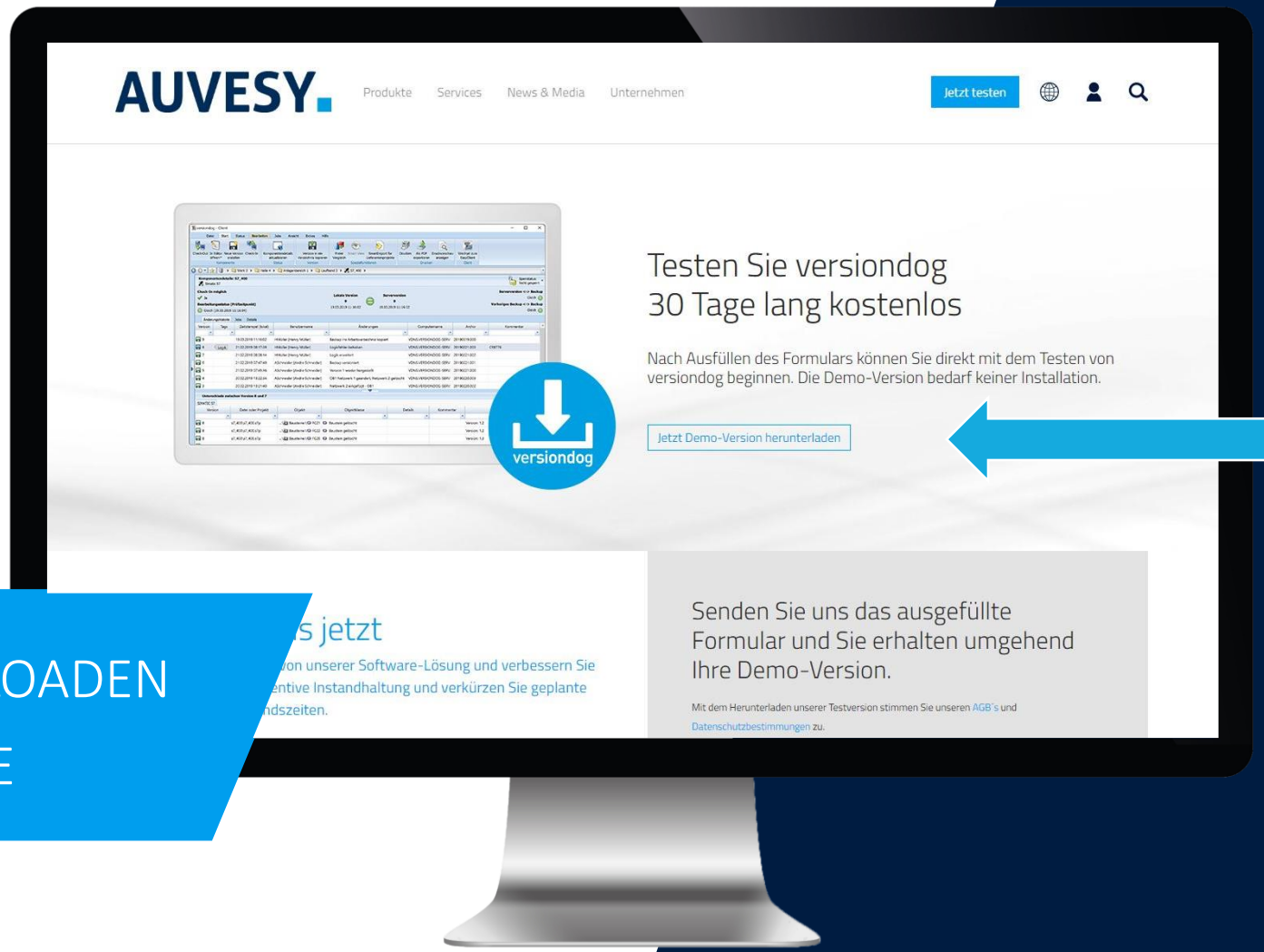
Hochwasserschutz und die Entsorgung von Abwasser sind hochtechnisierte Aufgaben. Ohne leistungsstarke Steuerungen und IT-Netzwerke läuft da – im wahrsten Sinn des Wortes – nichts. Mit dem Datenmanagement-System versiondog erleichtert AUVESY

inzwischen rund 5.000 angelegte Komponenten verwaltet.

Gegründet wurde die Emschergenossenschaft schon 1899 als erster deutscher Wasserwirtschaftsverband. Dieses Modell stand

AUVESY.

VERSIONDOG DEMO-VERSION



EINFACH DOWNLOADEN

WWW.AUVESY.DE

AUVESY.

Vielen Dank für Ihre Aufmerksamkeit!

Sie haben weitere Fragen?

Feedback ?

Wir sind für Sie da!

Ihr Ansprechpartner

Dirk Thielker

Sales Manager

Dirk.thielker@auvesy.de

Ihre Ansprechpartnerin

Iwona Glauser

Sales Managerin

Iwona.glauser@auvesy.de

AUVESY.