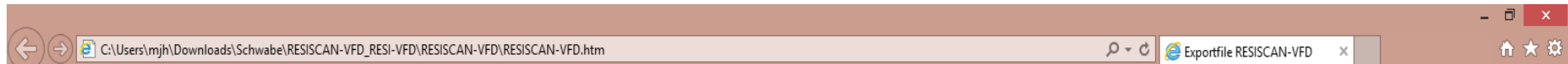
























So geht "Ersetzendes Scannen" TR-03138 (RESISCAN) heute mit CDE



RESISCAN Verfahrensdokumentation								
Anwendung	Alias	Projekt-ID	Owner	Abteilung	Autoren	Version	Stand	Status
RESISCAN-VFD	RESI-VFD	TR 3138-VFD	h&p	GL	mjh/sm	1.0	2014-10-24	offen

Inhaltsverzeichnis							
Index	Topic	Angaben	Datei	Status	Hilfe	Owner	
0	Hinweise						
0.1	Arbeiten mit RESISCAN-VFD			offen			
1	Einleitung						
1.1	Aufgabenstellung und Rechtsrahmen			offen			
1.2	Organisatorisches Umfeld			offen			
1.3	IT-Umfeld und Einbettung Scansystem			offen			
2	Grundlegende Angaben						
2.1	Dokumentarten*			offen			
2.3	Scanprozess*			offen			
2.4	Mitarbeiter - Qualifikation - Verantwortlichkeit*			offen			
2.5	<i>Systemüberblick</i>						
2.5.1	Komponenten Scansystem (S1-S6)			offen			
2.5.1.1	Scanner (S1)*			offen			
2.5.1.2	Scan-Workstation (S2)*			offen			
2.5.1.2.1	Client (S2/A1)*			offen			
2.5.1.2.2	Scan-Software (S2/A2)*			offen			
2.5.1.2.3	Index-Software (S2/A3)*			offen			
2.5.1.2.4	Integritätssicherungs-Software (S2/A4)*			offen			
2.5.1.3	Scan-Cache (S3)			offen			
2.5.1.4	Integritätssicherungs-Hardware (S4)						
2.5.1.5	Server (S5)*			offen			
2.5.1.6	IT-Infrastruktur (S6)						
2.5.1.7	Kommunikationsverbindungen (K1-K9)			offen			
2.5.2	Datenstrukturen (D3 - D6)*			offen			
2.5.3	Screenshots Human Interface						

So geht "Ersetzendes Scannen" TR-03138 (RESISCAN) heute mit CDE

Arbeiten mit RESISCAN-VFD

Einleitende Anmerkungen

A) Die Kürzel Ax, Dx, Sx und Kx entsprechen in Bedeutung und Nutzung der Definition in der BSI TR-03138 (RESISCAN).

B) Der Begriff "Maßnahme" wird in der TR-03138 (RESISCAN) sowohl für eine "durchzuführende Aktion" (gem. Duden) als auch für die entsprechende "implementierte Maßnahme" verwendet; hierbei handelt es sich um zwei ontologisch und semantisch verschiedene Objekte. Nachfolgend wird die Manifestation der Maßnahme benannt: Änderung HW/SW, Technische Einrichtung, Anweisung, Vorkehrung usw. sowie Veränderung in der Umgebung, Änderung in der Organisation etc. und Maßnahme nur als durchzuführende Aktion verstanden.

C) Zum Kick-off des Projektes wird eine RESISCAN-VFD Anwendung erzeugt; anschließend werden die Autoren der Verfahrensdokumentation namentlich erfasst und eingetragen. Der Projektleiter erhält das Rechte „project“, die Bearbeiter einzelner Topics (Themen gem. Index) das Recht „index“ zugeordnet; hierbei werden auch die Benutzernamen und Passwörter vergeben. Personen, die nur Einsicht in die VFD haben möchten, erhalten das Recht „view“, der Administrator das Recht „admin“. Der Administrator kann keine Dokumente einsehen oder Veränderungen vornehmen. Falls der Projektleiter auch als Fachadministrator fungiert, kann er sich das Recht „all“ zuweisen, die Vereinigung von „project“ und „admin“. Die Verarbeitung kann verteilt erfolgen. Hierfür ist die Installation auf einem Server erforderlich bzw. die Cloud-Variante zu nutzen.

D) Falls der Text in der Spalte Topic mit einem* abschließt, ist in der Hilfe-Seite, - erreichbar unter der Spalte "Hilfe" -, der Link auf ein Template im .docx-Format angegeben. Dieses Template kann heruntergeladen (rechte Maustaste und "Ziel speichern (IE/FF), Link speichern unter (Chrome)")

So geht "Ersetzendes Scannen" TR-03138 (RESISCAN) heute mit CDE

und als Vorlage zur Bearbeitung verwendet werden. Nach dem lokalen Speichern und Ausfüllen des Templates wird der erstellten Datei ein passender Name zugewiesen und diese unter dem entsprechenden Index hochgeladen.

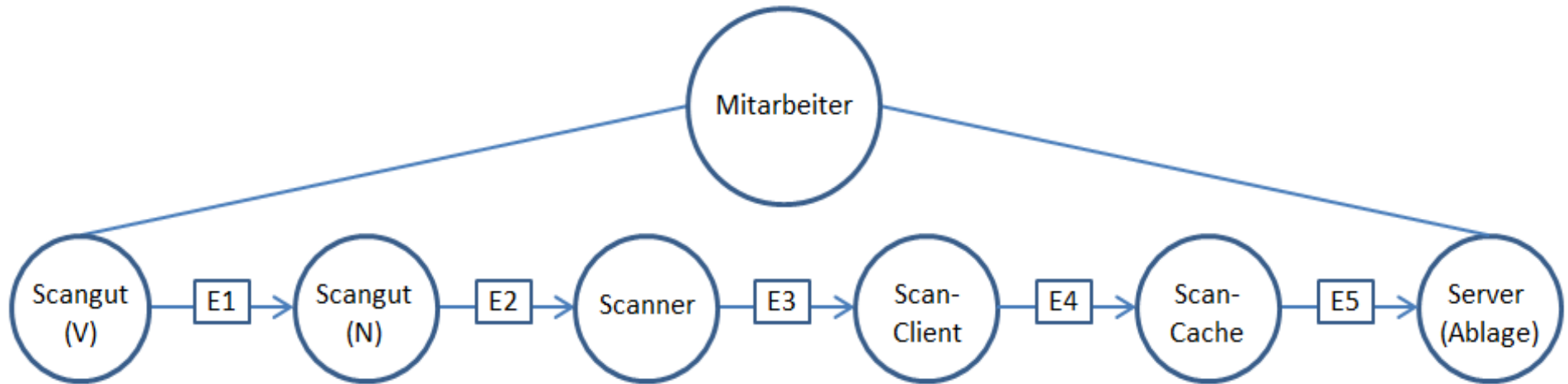
E) In der Spalte Anlagen können Hinweise, Links (<http://...>), Verweise und auch der Kommunikation zwischen den Autoren dienende temporäre Kommentare eingetragen werden. Diese Kommentare müssen nach Beendigung der Arbeiten gelöscht bzw. durch passende Angaben ersetzt werden.

Darstellung des Scan-Prozesses

Der Scan-Prozess wird durch einen Graphen mit einfach benannten Kanten (E_i) und Knoten (S_1 - S_6) als Systemteilnehmer visualisiert. Die Systemteilnehmer repräsentieren physische Objekte. Die Knoten enthalten die Beschreibung der Systemteilnehmer mit nativen Attributen und Prädikaten gem. der TR-03138 (RESISCAN) Schutzbedarfs- und Risikoanalyse. Unter dem Namen der Kante (E_i)[S_i, S_{i+1}] werden die zwischen S_i und S_{i+1} stattfindenden Ereignisse, Verbindungen und implementierten Maßnahmen dargestellt. Die Bedienperson bzw. -personen werden als Herrscher des Prozesses angesehen. Jeder Systemteilnehmer kann als Datenquelle und/oder Datensinke dienen. Daten und Dokumente werden von links nach rechts verfolgt gem. dem Pfeil unter $E(i)$. Unter $E(i)$ werden tabellarisch alle am Übergang vom Teilnehmer links von $E(i)$ zum Teilnehmer rechts von $E(i)$ beteiligten Elemente aufgeführt. Zu den Elementen zählen: Sachverhalte, Ereignisse, Daten, Verbindungen, Sicherheit, Umgebungsaspekte, Anweisungen und technische sowie organisatorischen Einrichtungen und Vorkehrungen.

Systemteilnehmer : Mitarbeiter, Scangut(V), Scangut(N), Scanner, Scan-Client, Scan-Cache, Server

So geht "Ersetzendes Scannen" TR-03138 (RESISCAN) heute
mit CDE



Legende:

V: = vor Vorbereitung

N: = nach Vorbereitung

Ex: = Kante von Teilnehmer(i) zu Teilnehmer(i+1)

REx: = Rolle zu Ex (sofern Bedienpersonal involviert)

So geht "Ersetzendes Scannen" TR-03138 (RESISCAN) heute mit CDE

Erläuterung

Die obige Darstellung dient dazu, Beschreibungselemente kompakt zusammenzufassen und visuell unterstützt zu lokalisieren. Der Scanprozess wird lediglich als verfolgbarer Daten- bzw. Objektfluss zwischen den Teilnehmern vereinfacht. Das Scangut erfährt in E1, der Dokumentvorbereitung, eine „Metamorphose“. Es wird „scanfähig“ gemacht, geordnet, geprüft und evtl. werden Fahnenträgerblätter (Stapelführungsblätter/Deckblätter) mit Barcodes, Metadaten etc. versehen. Danach wird das Scangut in den Scanner eingelegt (E2); unter E1 und E2 werden alle Anweisungen und Aktionen des Bedienpersonals sowie getroffene Sicherheitsvorkehrungen beschrieben. Mit dem Scannen erzeugt der Scanner, der nun als Datenquelle auftritt, das Scanprodukt und sendet es via Interface zum Scan-Client; das Scanobjekt tritt nun in Form von Daten und nicht mehr als physischer Teilnehmer auf. Unter E3 wird neben der die Kommunikationsverbindung K1 dargestellt, wie der Bediener mit dem Scan-Client interagiert (relevant Screenshots), wie die Datenobjekte D3-D6 erzeugt und an welche Datensenke sie übertragen werden; E4 erfolgt auch die Beschreibung der Nachbearbeitung. Die Integritätssicherung kann zum Teil auch unter E4 erklärt werden, falls es zu Interaktionen mit dem Scan-Client kommt; sonst erfolgt die Darstellung deren wesentlicher Funktionen unter E5. Die Richtung der Pfeile zwischen den Kanten Ei soll hauptsächlich den Weg der zu verfolgenden Daten visualisieren und auch erlauben, Kommunikationsverbindungen darzustellen.

Bearbeitung

A) Die Bearbeitung beginnt mit dem Index 1, der Einleitung. Die jeweiligen Hilfedateien in der Spalte „Hilfe“ liefern Vorgaben und Beispiele. Hier und in den folgenden Abschnitten kann die Bearbeitung eines Themas einem oder mehreren Ownern zugeordnet und der Bearbeitungszustand eingetragen werden.

B) Unter "Grundlegende Angaben" werden zu Beginn die Systemteilnehmer mit Namen und elementaren Eigenschaften gem. status quo aufgeführt. Das entspricht einer Ist-Aufnahme der Scan-Hardware und -Software (s.a. Strukturanalyse), der Benennung der zu verarbeitenden

So geht "Ersetzendes Scannen" TR-03138 (RESISCAN) heute mit CDE

Dokumentarten, des Bedienpersonals und seiner Rollenprofile gefolgt von Angaben zur Administration und Wartung der Scan-Hard- und Software. Zur Information, wenn auch hier nicht unbedingt benötigt, sind in den Hilfedateien die Hinweise zu Gefahren und Maßnahmen eingeblendet. Auf der Kante zwischen zwei Teilnehmern können, sofern Personal an den Ereignissen mitwirkt, die unter dem Kantennamen spezifiziert werden, Rollen für einzelne Schritte definiert werden. Die Einzelrolle wird mit ER(x,i) bezeichnet. Das Rollenprofil eines Mitarbeiters wird als Menge von Rollen dargestellt.

C) Als nächstes werden die Abschnitte unter den Indizes 4-7, Dokumentenvorbereitung (RA), Scannen (RA), Nachbearbeitung des Scanprodukts (RA) und Integritätssicherung (RA) bearbeitet, da einige Elemente der Übergreifenden Regelungen und Einrichtungen (Index 3) von den Ergebnissen der Risikoanalyse abhängen können. Hier werden die Ergebnisse zur Risikoanalyse und die entsprechenden umgesetzten Maßnahmen erfasst. Systemteilnehmer und Ereignisse werden bzgl. potentieller benutzerdefinierter Bedrohungen und allgemeiner Gefährdungen gem. Grundschatz durchleuchtet; hierbei werden die unter Index 2, Grundlegende Angaben eingetragenen Beschreibungen der Eigenschaften der Scan-Systemkomponenten in der Analyse berücksichtigt. Die in den Templates der Hilfedateien bereit gestellten Tabellen können hierzu verwendet und erweitert werden. Zur Orientierung wird bei der Diskussion jedes Teilnehmers in den Vorlagen jeweils der Graph des Scan-Prozesses eingeblendet und die relevanten Teilnehmer und Kanten werden darin rot markiert.

D) Abschließend werden die Übergreifenden Regelungen und Einrichtungen bearbeitet.

E) Die Verfahrensdokumentation kann nun als HTML exportiert und Dritten zur Prüfung überlassen werden.