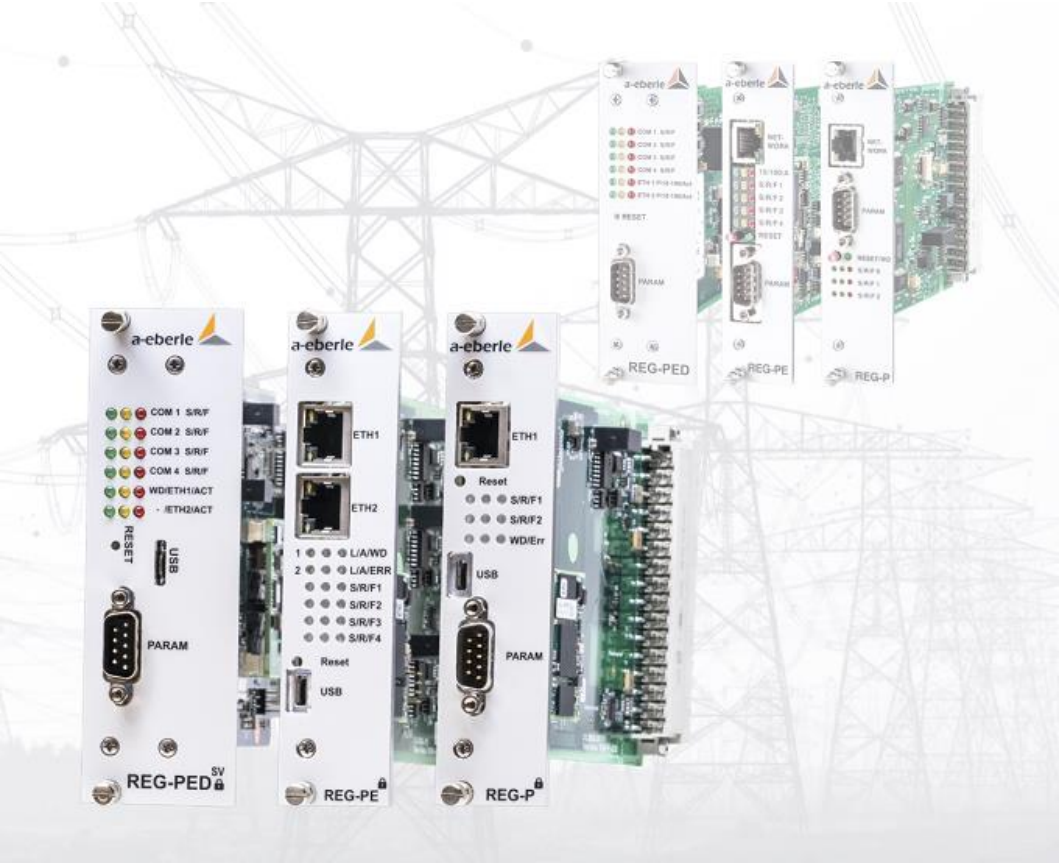
a-eberle

Leittechnik

Administrator-Handbuch



d

WICHTIG

VOR DER ANWENDUNG SORGFÄLTIG LESEN

ALS ZUKÜNFTIGE REFERENZ AUFBEWAHREN

Die Vorlage wurde auf Basis der DIN EN 82079-1: 2013-06 erstellt.

Autor	Abteilung	Änderungen	Version	Datum
Wolfgang Borchers	REGCOMMS	Erste Version	0.1	16.10.2016
Wolfgang Borchers	REGCOMMS	Großrevision	1.0	18.10.2017
Wolfgang Borchers	REGCOMMS	Überprüfung aller Kapitel	1.1	15.05.2018
Wolfgang Borchers	REGCOMMS	Überprüfung von skriptgesteuerten Upgrades	1.2	28.05.2018
Wolfgang Borchers	REGCOMMS	Überprüfung aller Kapitel	1.3	08.05.2019
Fabian Seidel	REGCOMMS	Überprüfung aller Kapitel nach 200210_REGCOMMS_Administrator DE.docx	1.4	27.09.2019
Wolfgang Borchers	REGCOMMS	Überprüfung aller Kapitel	1.5	05.11.2019
Wolfgang Borchers	REGCOMMS	Erweiterung des Usermanagements für REG-PE Typ TK860	1.6	10.02.2020

Inhaltsverzeichnis

1. Benutzerführung

Dieses Administratorhandbuch enthält Informationen über die WinConfig-Software, die für Administratorzwecke bestimmt ist und sich insbesondere auf den sicheren Zugriff auf Fernwirkkarten und sicherheitsrelevante Aktionen in WinConfig konzentriert. Detaillierte Informationen zur Konfiguration der Fernwirkkarten REG-P / REG-PE / REG-PED / REG-PEDSV / PQI-DA finden Sie im WinConfig Benutzerhandbuch.

Lesen Sie das Administratorhandbuch in seiner Gesamtheit und verwenden Sie das Produkt nur, wenn Sie das Administratorhandbuch verstanden haben.

1.1 Zielgruppe

Das Administrator-Handbuch richtet sich an ausgebildetes Fachpersonal.

Der Inhalt dieses Administratorhandbuchs muss für Personen zugänglich sein, die mit der Installation und dem Betrieb des Systems beauftragt sind.

1.2 Warnhinweise

Aufbau der Warnhinweise

Warnhinweise sind wie folgt aufgebaut:

⚠ SIGNALWORT	**Art und Quelle der Gefahr!** Folgen bei Nichtbeachtung. Maßnahme, um die Gefahr zu vermeiden.

Abstufung der Warnhinweise

Warnhinweise unterscheiden sich nach Art der Gefahr wie folgt:

⚠ GEFAHR!	Warnt vor einer unmittelbar drohenden Gefahr, die zum Tod oder zu schweren Verletzungen führt, wenn sie nicht gemieden wird.

⚠ WARNUNG!	Warnt vor einer möglicherweise gefährlichen Situation, die zum Tod oder schweren Verletzungen führt, wenn sie nicht gemieden wird.

⚠ VORSICHT!	Warnt vor einer möglicherweise gefährlichen Situation, die zu mittelschweren oder leichten Verletzungen führt, wenn sie nicht gemieden wird.

HINWEIS!	Warnt vor einer möglicherweise gefährlichen Situation, die zu Sach- oder Umweltschäden führt, wenn sie nicht gemieden wird.

1.3 Tipps

Tipps zum sachgerechten Umgang mit dem Gerät und Empfehlungen.

1.4 Weitere Symbole

Handlungsanweisungen

Aufbau der Handlungsanweisungen:

➲ Anleitung zu einer Handlung.

↳ Handlungsresultat falls erforderlich.

Listen

Aufbau nicht nummerierter Listen:

0 Listenebene 1

– Listenebene 2

Aufbau nummerierter Listen:

1) Listenebene 1

2) Listenebene 1

1. Listenebene 2
2. Listenebene 2

1.5 Mitgeltende Dokumente

Beachten Sie für die sichere und korrekte Verwendung der Anlage auch die zusätzlich mitgelieferten Dokumente sowie einschlägige Normen und Gesetze.

1.6 Aufbewahrung

Bewahren Sie die Bedienungsanleitung, inklusive der mitgeltenden Dokumente griffbereit in der Nähe des Systems auf.

1.7 Aktualisierte Dokumentation

Die aktuellsten Versionen der Dokumente können unter https://www.a-eberle.de/de/downloads bezogen werden.

2. Lieferumfang

3. Sicherheitshinweise

- Bedienungsanleitung beachten.
- Bedienungsanleitung immer beim Gerät aufbewahren.
- Sicherstellen, dass das Gerät ausschließlich in einwandfreiem Zustand betrieben wird.
- Sicherstellen, dass ausschließlich Fachpersonal das Gerät bedient.
- Gerät ausschließlich nach Vorschrift anschließen.
- Sicherstellen, dass das Gerät nicht über den Bemessungsdaten betrieben wird
- Gerät nicht in Umgebungen betreiben, in denen explosive Gase, Staub oder Dämpfe vorkommen.
- Sicherstellen, dass Schutzabdeckungen vorhanden und funktionstüchtig sind.
- Sicherstellen das Fünf Sicherheitsregeln nach DIN VDE 0105 immer eingehalten werden.
- Gerät ausschließlich mit handelsüblichen Reinigungsmitteln reinigen.

4. Sicherheit bei den Kartenmodellen REG-P, PE, PED, REG-PED^{SV} TK28-x und TK102

- Bitte beachten Sie, dass die Cyber Security-Funktionen nur in Fernwirkkarten ab Herstellungsdatum 2018 ("TK28-4, TK28-6 und TK102") verfügbar sind, nicht in den Vorgängerkarten ("TK517, TK509, TK400, TK860 und TK885").
- Die Sicherheitsbedürfnisse in den oben genannten Kartenmodellen werden durch eine rollenbasierte Zugriffskontrolle mit der Verwendung von Active Directory-Objekten und RADIUS-Funktionalität abgedeckt. Für die Kommunikation mit der Karte werden nur gesicherte Protokolle mit Verschlüsselung verwendet. Der Benutzer wird authentifiziert und dann wird seine Berechtigung für jede Aktion ausgewertet. Dieses Konzept umfasst Zugriffsmethoden mit zugeordneten Protokollen, Rollen von Benutzern und Aktionen, für die die Berechtigung nach der Benutzerrolle ausgewertet wird.

4.1 Zusammenfassung der Zugriffsmethoden und Protokolle für Benutzer

- WinConfig online (Web-Zugang)
  - Der Internetbrowser-Client (vergleichbar zum Internet Explorer) verbindet den im Linux-Betriebssystem integrierten Webserver auf der Karte.
  - Es wird das Protokoll HTTPS mit direkter Berechtigung verwendet.
- WinConfig Konsolen-/Shell-Menü (Terminalzugriff)
  - Der Terminal-Client (vergleichbar zu PUTTY) verbindet den im Linux-Betriebssystem integrierten SSH-Server auf der Karte.
  - Das Protokoll SSH mit direkter Autorisierung wird verwendet.
- WinConfig offline (Webzugriff und Transferzugriff)
  - Der Internetbrowser-Client (vergleichbar zum Internet Explorer) verbindet den Remote-Client-seitigen proprietären Webserver (Teil der WinConfig offline). Ein spezieller Serverteil kommuniziert mit der Karte.
  - Die Datenübertragung erfolgt über das Protokoll HTTPS mit direkter Berechtigung.
  - Netzwerk-Scan (Broadcast-Funktionen) und Systemparametrierung verwenden UDP verschlüsselt mit AES256 mit HTTPS-Vorautorisierung.
- Remote-Skript-Upgrade-Zugriff (Terminalzugriff)
  - Der Command line-SSH-Client (vergleichbar zu PLINK) verbindet den im Linux-Betriebssystem integrierten SSH-Server auf der Karte.
  - Es wird das Protokoll SSH mit direkter Autorisierung verwendet.

4.2 Rechtevergabe - Rollen Zugriffskonzept

Die Vergabe der Rechte für bestimmte im System definierte Aktionen erfolgt über die rollenbasierte Zugriffskontrolle (RBAC).

- Rollen-zu-Benutzer
  - Die dynamische Zuweisung erfolgt durch Active Directory. Jede im System definierte Rolle wird auf eine Benutzergruppe abgebildet.
- Aktionen-zu-Rollen
  - Die statische Zuordnung ist in der Definitionsdatei innerhalb der Kartenfirmware fest kodiert (auf Wunsch für bestimmte Methoden bereitgestellt). Diese Datei kann von den Systemadministratoren geändert werden.

4.3 Login-Modi

Es sind 2 Login-Modi implementiert.

- Der RADIUS-Modus verwendet den RADIUS-Server zur Authentifizierung von Benutzer und Karte und stellt die Informationen für die Autorisierung von Aktionen über VSA-Strings zur Verfügung. Dieser Modus hat Vorrang.
- Der zweite Notfallmodus ist der Passwortmodus. Dieser verwendet die lokal zwischengespeicherten Anmeldeinformationen für die Authentifizierung, und dann fungiert der Benutzer als eingebetteter Admin-Benutzer des Systems. Der Active Directory-Server ist die Quelle für die im Cache gespeicherten Anmeldeinformationen.

4.3.1 Login und Logout

Die Anmeldung kann über ein Dialogfenster erfolgen, das erscheint, wenn ein Benutzer versucht, über einen Internetbrowser und HTTPS-Zugang auf die Fernwirkkarte zuzugreifen. Das Dialogfeld zeigt auch den aktuell eingestellten Login-Modus an.

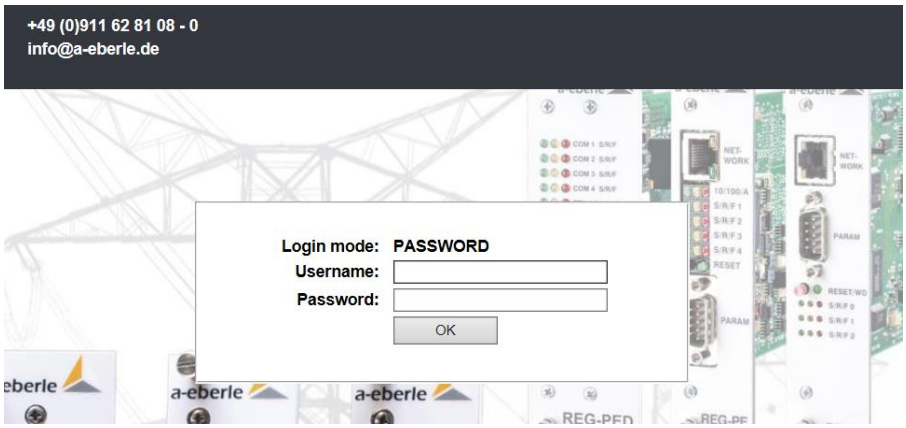
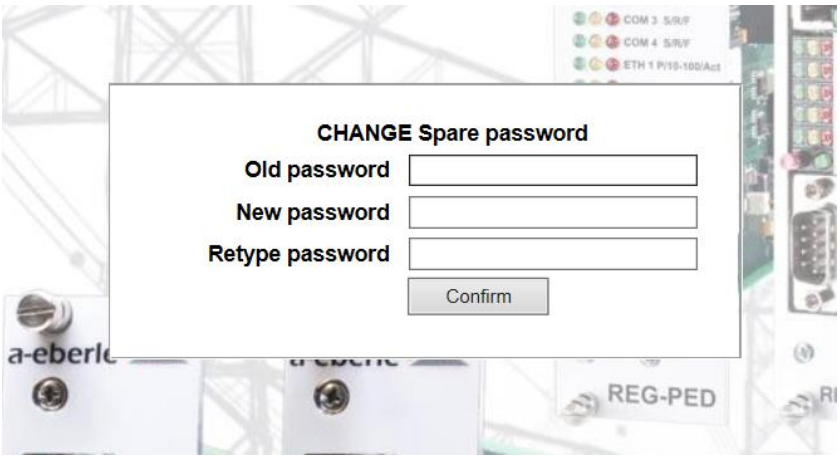
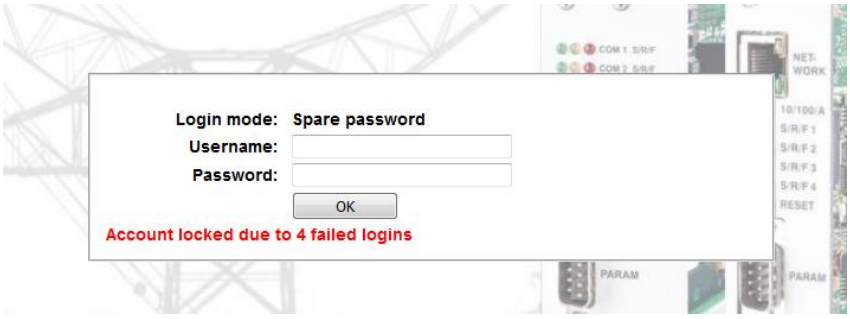


Figure 1: Anmeldedialog

Falls Sie sich zum ersten Mal einloggen, wird eine Änderung des Standard-Passworts verlangt:



Nach 4 fehlgeschlagenen Versuchen wird der Zugang für 60 Sekunden lang gesperrt. Dies wird durch folgende Meldung signalisiert:



Die Benutzer können sich über einen speziellen Button auf der linken Seite des Fensters in der Online-WinConfig abmelden.

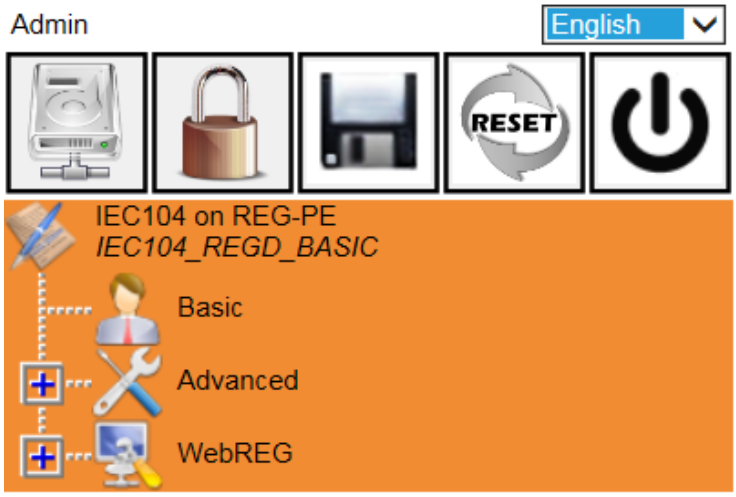
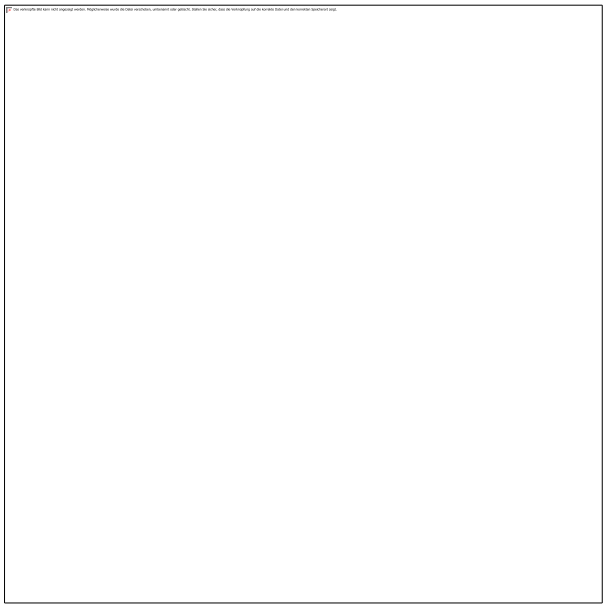


Figure 2: Abmelde-Taste

4.3.2 Sonderfunktion für Leittechnikkarten des Typs TK28 und TK102

Die Betriebsart Notfallpasswortmodus („Spare Password“) wird im Hochlauf für eine kurze Zeit im Display des Spannungsreglers angezeigt.



4.3.3 RADIUS-Modus

4.3.3.1 Definition von Rollen und Rechten

Gemäß dem Rollenkonzept-Dokument sollten die Active Directory-Objekte und RADIUS-Serverparameter implementiert werden, um die gewünschte WinConfig RADIUS-Funktionalität zu erreichen.

Für jede definierte Rolle muss es eine eigene AD-Gruppe geben und jede dieser Gruppen muss über den entsprechenden VSA-Stringsatz verfügen. Dies ist notwendig, da die gleichen VSA-Strings im RADIUS-Client auf der TK-Karte fest programmiert und ausgewertet werden. Das bedeutet, dass die Anzahl der VSA-Zeichenketten und Werte obligatorisch sind; die zugrunde liegenden Namen der Sicherheitsgruppen sind benutzerdefinierbar.

Die Zugriffsregeln sind in der Datei *rbac.def* im Dateisystem der Fernwirkkarten definiert. Die Elementarregeln bestehen aus drei Objekten im Format:

Zugriffsmethode_ActionType_Rolle_ActionType_Rolle

worauf:

- **AccesMethod** ist ein Name, der aus dem Satz der Methoden (Anwendungen) ausgewählt wird, die für den Datenzugriff verwendet werden. Mögliche Werte sind:
  - OfflineWinConfig, OnlineWinConfig, ShellMenu, WebReg, ScriptBasedUpgrade
- **ActionType** ist ein Name, der aus dem Satz von Aktionen ausgewählt wird, die für eine bestimmte *AccessMethod* definiert sind. Mögliche Werte sind:
  - Für OfflineWinConfig: transfer_to, transfer_from, set_net, set_services, set_ emergency_pwd, set_ certificates

- Für OnlineWinConfig: change_settings, save_settings, set_net, set_services, security_management, set_emergency_pwd, set_certificates
- Für ShellMenu: shell_access, get_logs, set_net, set_services, security_management
- Für WebReg: parameters_read, parameters_update, panel_watch, panel_setKey, terminal_read, terminal_update, RGL_read, RGL_update, log_read, UTC_read, UTC_update, DST_read, DST_update, Communication_read, Communication_update, Statistics_read, simulation_read, simulation_start, Simulation_tapPos, simulation_values, simulation_monitor, IOmap_read, IOmap_update, basVal_read, basVal_update, autoMan_read, autoMan_update, time_update, timeGroup_update, features_read, features_update, ram_read, ram_backup, ram_restore, firmware_update, UDM_update
- Für ScriptBasedUpgrade: Es ist keine Aktion definiert, die AccessMethod repräsentiert den ActionType, so dass die Regeln aus zwei Objekten im Format bestehen:
- Zugriffsmethode_Rolle

0 ***Rolle*** ist der Name der Benutzerrolle, wie sie im RADIUS und AD gemäß dem Rollenkonzept-Dokument definiert ist. Mögliche Werte sind:

- Administrator, Kontrolloperator, Schutzbediener, Übertragungsgeräteoperator, UPSOperator, PDVOperator, BMSOperator, Extern, Beobachter, Manipulator, RemoteOperator

Jede positive Elementarregel (Berechtigung erteilt) ist als eine Zeile der Datei *rbac.def* definiert. Alle anderen elementaren Regeln werden abgelehnt. Der Benutzer mit den entsprechenden Rechten kann neue Definitionen in das System hochladen oder die Definitionen auf den Standard-Werkzustand zurücksetzen, die in den folgenden Tabellen definiert sind.

Table 1: Definition von Rollen

Definition von Rollen	AD Security Group - Beispiel	VSA-String - mandatory
Administrator	AE-Administrators	Administrator
Leittechnik-Operator	AE-ControlOperators	ControlOperator
Schutztechnik-Operator	AE-ProtectionOperators	ProtectionOperator
Übertragungstechnik-Operator	AE-TransmissionEquipmentOperators	TransmissionEquipmentOperator
USV-Operator	AE-UPSOperators	UPSOperator
PDV-Operator	AE-PDVOperators	PDVOperator
ZLT-Operator	AE-BMSOperators	BMSOperator
Dienstleister (extern)	AE-Externs	Extern
Beobachter	AE-Observers	Observer
Schaltpersonal (lokal)	AE-Manipulators	Manipulator
Netzleitstellen-Operator (Remote)	AE-RemoteOperators	RemoteOperator

Table 2: Offline-WinConfig-Zugriffsmethode Aktionen - zur Rolle von Standardrechten

VSA-String - obligatorisch	Online WinConfig Aktionen Rechte - Standard					
	Übertra-gung_an	*Trans-fer_von*	*set_net*	*set_ser-vices*	*set_notfall_pwd*	*set_zertifi-kate*
Administrator	ja	ja	ja	ja	ja	ja
ControlOperator	ja	ja	nein	ja	ja	nein
ProtectionOpera-tor	ja	ja	nein	ja	ja	nein
Übertragungs-technikBetreiber	ja	ja	nein	ja	ja	nein
UPSOperator	ja	ja	nein	ja	ja	nein
PDVOperator	ja	ja	nein	ja	ja	nein
BMSOperator	ja	ja	nein	ja	ja	nein
Extern	nein	nein	nein	nein	nein	nein
Beobachter	nein	ja	nein	nein	nein	nein
Manipulator	nein	ja	nein	nein	nein	nein
RemoteOperator	nein	nein	ja	nein	nein	nein

Table 3: Online-Zugriffsmethode WinConfig Aktionen - um Standardrechte zu definieren, Teil 1.

VSA-String - obligato-risch	Online WinConfig Aktionen Rechte - Standard				
	Einstellungen ändern	*Spei-chern_der_Einstellungen*	*set_net*	*set_services*	*Sicherheitsmanagement*
Administrator	ja	ja	ja	ja	ja
ControlOperator	ja	ja	nein	ja	nein
ProtectionOperator	ja	ja	nein	ja	nein
TransmissionEquipment-Operator	ja	ja	nein	ja	nein
UPSOperator	ja	ja	nein	ja	nein
PDVOperator	ja	ja	nein	ja	nein
BMSOperator	ja	ja	nein	ja	nein
Extern	nein	nein	nein	nein	nein
Beobachter	nein	ja	nein	nein	nein
Manipulator	nein	ja	nein	nein	nein
RemoteOperator	nein	nein	ja	nein	nein

Table 4: Online-Zugriffsmethode WinConfig Aktionen - um Standardrechte zu definieren, Teil 2.

VSA-String - obligatorisch	Online WinConfig Aktionen Rechte - Standard	
	set_notfall _pwd	*set_zertifikate*
Administrator	ja	ja
ControlOperator	ja	nein
ProtectionOperator	ja	nein
TransmissionEquipment-Operator	ja	nein
UPSOperator	ja	nein
PDVOperator	ja	nein
BMSOperator	ja	nein
Extern	nein	nein
Beobachter	nein	nein
Manipulator	nein	nein
RemoteOperator	nein	nein

Table 5: Zugriffsmethode für das Shell-Menü - Aktionen zur Vergabe von Standardrechten für Rollen

VSA-String - obligatorisch	Shell-Menü WinConfig Aktionen Rechte - Standard				
	Shell_Zugang	*Protokolle abrufen*	*set_net*	*set_services*	*Sicherheitsmanagement*
Administrator	ja	ja	ja	ja	ja
ControlOperator	nein	ja	nein	ja	nein
ProtectionOperator	nein	ja	nein	ja	nein
TransmissionEquipment-Operator	nein	ja	nein	ja	nein
UPSOperator	nein	ja	nein	ja	nein
PDVOperator	nein	ja	nein	ja	nein
BMSOperator	nein	ja	nein	ja	nein
Extern	nein	nein	nein	nein	nein
Beobachter	nein	ja	nein	nein	nein
Manipulator	nein	ja	nein	nein	nein
RemoteOperator	nein	nein	ja	nein	nein

Table 6: Remote-Skript-basierte Upgrade-Zugriffsmethode Aktionen - um Standardrechte für Rollen zu definieren.

VSA-String - obligatorisch	Remote-Skript-basiertes Upgrade - Standard
Administrator	ja
ControlOperator	nein
ProtectionOperator	nein
TransmissionEquipment-Operator	nein
UPSOperator	nein
PDVOperator	nein

VSA-String - obligatorisch	Remote-Skript-basiertes Upgrade - Standard
BMSOperator	nein
Extern	nein
Beobachter	nein
Manipulator	nein
RemoteOperator	ja

Table 7: WebReg-Aktionen - zur Vergabe von Standardrechten, Teil 1.

VSA-String - obligatorisch	WebReg-Aktionen - zur Vergabe von Standardrechten an Rollen									
	Gelesene Parameter	**Update der Parameter**	**Panel - beobachten**	**Panel - Set-Taste**	**Terminal lesen**	**Terminal-Update**	**RGL lesen**	**RGL-Update**	**LOG gelesen**	**UTC lesen**
Administrator	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
ControlOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Schutz-Operator	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Getriebe-Equipment-Betreiber	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
UPSOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
PDVOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
BMSOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
Extern	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein
Beobachter	ja	nein	ja	nein	ja	nein	ja	nein	ja	ja
Manipulator	ja	nein	ja	nein	ja	nein	ja	nein	ja	ja
RemoteOperator	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein

Table 8: WebReg-Aktionen - zur Vergabe von Standardrechten, Teil 2.

VSA-String - obligatorisch	WebReg-Aktionen - zur Vergabe von Standardrechten an Rollen								
	UTC-Update	**Kommunikation gelesen**	**Kommunikationsupdate**	**Statistik gelesen**	**Simulation gelesen**	**Simulationsstart**	**Simulation TapPos**	**Simulationswerte**	**Simulationsmonitor**
Administrator	ja	ja	ja	ja	ja	ja	ja	ja	ja
ControlOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
ProtectionOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
Getriebe-Equipment-Betreiber	ja	ja	ja	ja	ja	ja	ja	ja	ja
UPSOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
PDVOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
BMSOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
Extern	nein	nein	nein	nein	nein	nein	nein	nein	nein
Beobachter	nein	ja	nein	ja	ja	nein	nein	nein	ja
Manipulator	nein	ja	nein	ja	ja	nein	nein	nein	ja
RemoteOperator	nein	nein	nein	nein	nein	nein	nein	nein	nein

Table 9: WebReg-Aktionen zur Vergabe von Standardrechten, Teil 3.

VSA-String - obligatorisch	WebReg-Aktionen - zur Vergabe von Standardrechten an Rollen								
	I/O-Map lesen	**Update der I/O-Karte**	**Gelesene Grund-werte**	**Fort-schreibung der Grund-werte**	**Automa-tisch/manuell lesen**	**Automati-sches/manuelles Up-date**	**Zeitup-date**	**Gelesene Funktio-nen**	**Funkti-ons-Update**
Administrator	ja	ja	ja	ja	ja	ja	ja	ja	ja
ControlOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
ProtectionOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
Getriebe-Equipment-Betrei-ber	ja	ja	ja	ja	ja	ja	ja	ja	ja
UPSOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
PDVOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
BMSOperator	ja	ja	ja	ja	ja	ja	ja	ja	ja
Extern	nein	nein	nein	nein	nein	nein	nein	nein	nein
Beobachter	ja	nein	ja	nein	ja	nein	nein	ja	nein
Manipulator	ja	nein	ja	nein	ja	nein	nein	ja	nein
RemoteOperator	nein	nein	nein	nein	nein	nein	nein	nein	nein

Table 10: WebReg-Aktionen zur Vergabe von Standardrechten, Teil 4.

VSA-String - obligatorisch	WebReg-Aktionen - zur Vergabe von Standard-rechten an Rollen				
	RAM le-sen	**RAM-Ba-ckup**	**RAM-Wieder-herstellung**	**Firmware-Update**	**UDM-Update**
Administrator	ja	ja	ja	ja	ja
ControlOperator	ja	ja	ja	ja	ja
ProtectionOperator	ja	ja	ja	ja	ja
Getriebe-Equipment-Betrei-ber	ja	ja	ja	ja	ja
UPSOperator	ja	ja	ja	ja	ja
PDVOperator	ja	ja	ja	ja	ja
BMSOperator	ja	ja	ja	ja	ja
Extern	nein	nein	nein	nein	nein
Beobachter	ja	nein	nein	nein	nein
Manipulator	ja	nein	nein	nein	nein
RemoteOperator	nein	nein	nein	nein	nein

4.3.3.2 Aktionen zum Steuern von fest codierten Rechten in A-Eberle-Geräten

Online WinConfig überträgt die für den aktuellen Benutzer und die Verbindungssitzung gültigen Actions-to-Role-Rechte auch in das angeschlossene A-Eberle-Gerät (RegSys). WinConfig übersetzt die RADIUS-Rollen in die definierten Regsys-Rollen in der externen *Rollenmatrix …..* XLSM-Datei. Die externe Datei erstellt eine Bitmaske namens CLIUM, die den Rollen auf dem Regsys-Gerät entspricht. Die Hashtabelle mit Zuordnung der RBAC-Rollen im A-Eberle-Gerät zu denen von WinConfig ist unten zu sehen. Es ist zwingend erforderlich, die Namen der Regsys-Rollen genauso zu halten, wie sie in der Hashtabelle definiert sind. Weitere Informationen finden Sie im A-Eberle Gerätehandbuch.

Regsys Rollen des A-Eberle-Geräts beinhalten auch ein spezielles Konto des Panel-Benutzers, das für den lokalen Zugriff über das Geräte-Panel vorgesehen ist. Das Konto von Panel-User hat keinen Bezug zu den RADIUS-Rollen.

Die Benutzerrechte des A-Eberle-Geräts werden nach Ablauf des vordefinierten Inaktivitäts-Timeout automatisch in den Grundzustand versetzt.

Table 11: Definition von Rollen

Definition von Rollen	AD Security Group - Beispiel	Regsys Rollen
Administrator	AE-Administrators	Administrator
Leittechnik-Operator	AE-ControlOperators	Leittechnik-Operatoren
Schutztechnik-Operator	AE-ProtectionOperators	Schutztechnik-Operator
Übertragungstechnik-Operator	AE-TransmissionEquipmentOperators	Übertragungstechnik-Operatoren
USV-Operator	AE-UPSOperators	USV-Operator
PDV-Operator	AE-PDVOperators	PDVOperator
ZLT-Operator	AE-BMSOperators	ZLT-Operator
Dienstleister (extern)	AE-Externs	Dienstleister
Beobachter	AE-Observers	Beobachter
Schaltpersonal (lokal)	AE-Manipulators	Schaltpersonal
Netzleitstellen-Operator (Remote)	AE-RemoteOperators	Netzleitstellen-Operator
Panel-User 1		REGSys Rolle nur für den Lokalen Benutzer 1
Panel-User 2-5		REGSys Rolle nur für den Lokalen Benutzer 2-5

4.3.3.3 Windows Server R2 2008 und 2016 Konfiguration Schritt für Schritt

Als Implementierungsbeispiel wird die Konfiguration von Windows Server R2 2008 für die Arbeit als RADIUS-Server verwendet. Die Konfiguration von Windows Server 2016 ist ähnlich; es werden die gleichen Dialogfelder verwendet. Der RADIUS-Server wird unter Windows als *Netzwerkrichtlinienserver* bezeichnet. Die Konfiguration kann im Server-Manager vorgenommen werden:

- Rollen->Netzwerkrichtlinie und Zugriffsdienste -> NPS im Windows Server 2008,
- Werkzeuge-> Netzwerkrichtlinienserver im Windows Server 2016.

➲ Hinzufügen von Gruppen zum Active Directory gemäß der Definition von Rollen und Rechten.

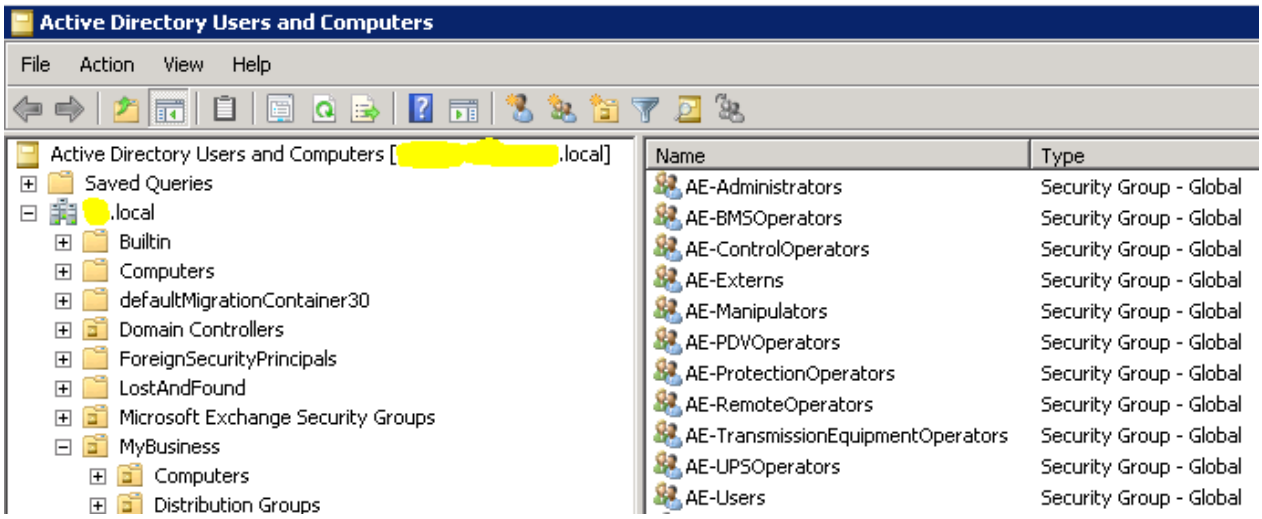
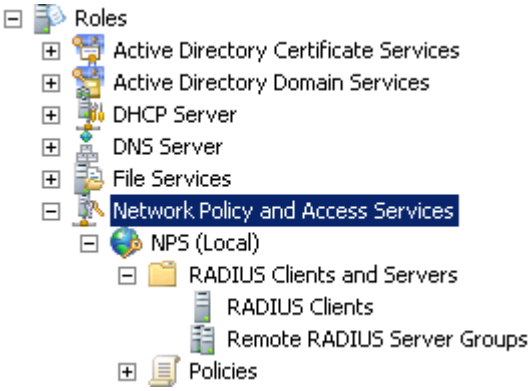


Figure 3: Hinzufügen von Gruppen

- Fügen Sie Domänenbenutzer zu einer oder mehreren erstellten Gruppen hinzu.
  - In diesem Dokument finden Sie eine Anleitung, wie Sie mit AD-Gruppen und -Benutzern arbeiten:

    http://pc-addicts.com/create-ad-users-groups-server-2016/
- Installieren Sie RADIUS auf dem Windows Domain Controller (fügen Sie NPS über den Server Manager zu den Serverrollen hinzu).



  - Fügen Sie alle TK-Karten (IP-Adressen) der RADIUS-Client-Gruppe hinzu:

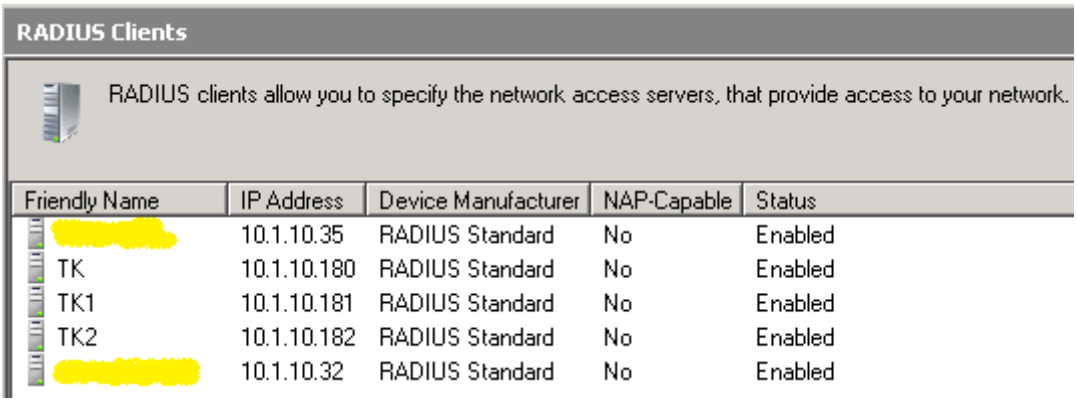


Figure 4: Hinzufügen von TK-Karten

- Es ist notwendig, das Passwort "Shared Secret" für jeden Client zu definieren. Es könnte für alle Clients gleich sein. Dieses gemeinsame Geheimnis muss mit Win-Config auf der Karte eingestellt werden:

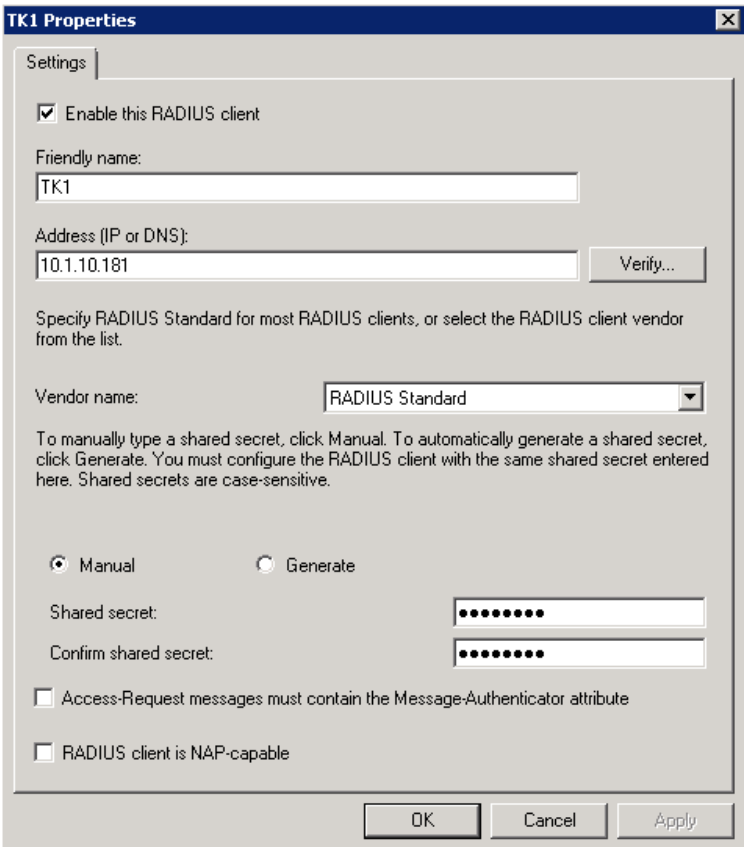


Figure 5: Gemeinsames Geheimnis

➲ Konfigurieren Sie Netzwerkrichtlinien und VSAs.

- Die Netzwerkrichtlinie muss für jede Active Directory-Benutzergruppe festgelegt werden, die im ersten Schritt hinzugefügt wird. Der Server-Manager wird für die Netzwerkrichtlinie verwendet:

Network Policies

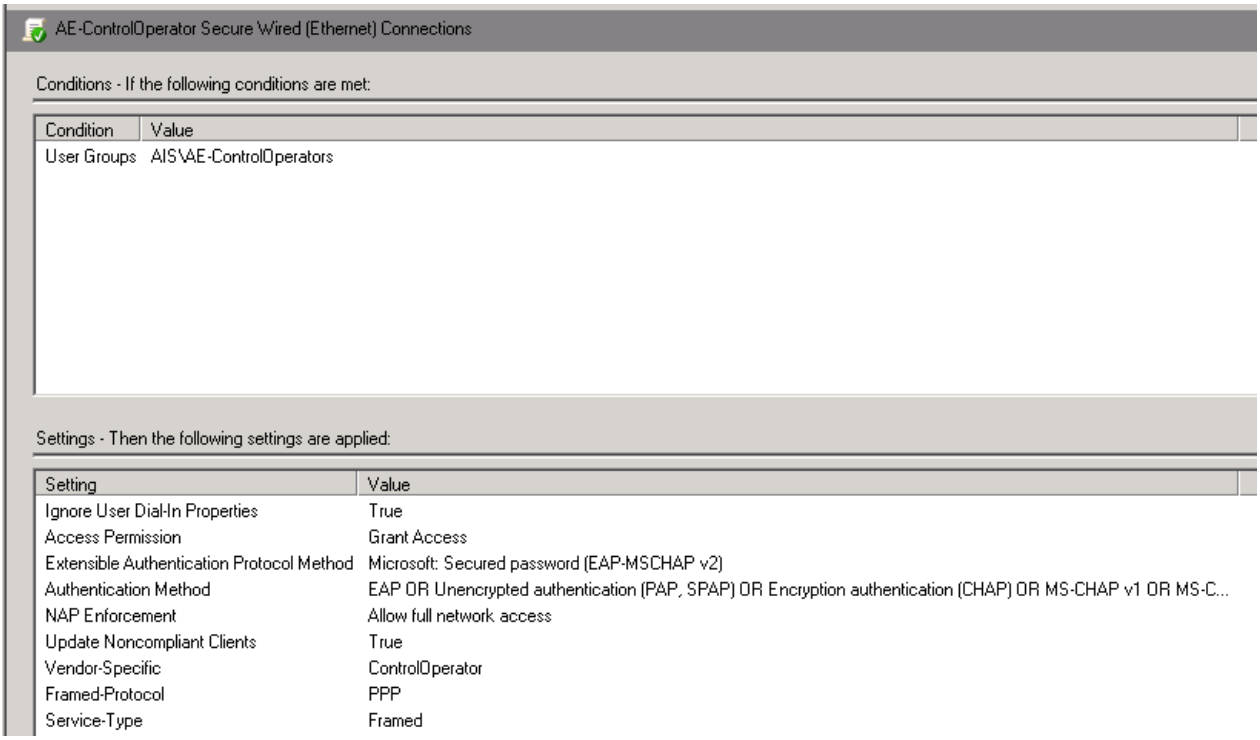
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can

Policy Name	Status	Processing Order	Access Type	Source
AE-Administrator Secure Wired (Ethernet) Connections	Enabled	1	Grant Access	Unspecified
AE-ControlOperator Secure Wired (Ethernet) Connections	Enabled	2	Grant Access	Unspecified
AE-ProtectionOperator Secure Wired (Ethernet) Connections	Enabled	3	Grant Access	Unspecified
AE-TransmissionEquipmentOperator Secure Wired (Ethernet) Connecti...	Enabled	4	Grant Access	Unspecified
AE-UPSOperator Secure Wired (Ethernet) Connections	Enabled	5	Grant Access	Unspecified
AE-PDVOperator Secure Wired (Ethernet) Connections	Enabled	6	Grant Access	Unspecified
AE-BMSOperator Secure Wired (Ethernet) Connections	Enabled	7	Grant Access	Unspecified
AE-Manipulator Secure Wired (Ethernet) Connections	Enabled	8	Grant Access	Unspecified
AE-User Secure Wired (Ethernet) Connections	Enabled	9	Grant Access	Unspecified
AE-Extern Secure Wired (Ethernet) Connections	Enabled	10	Grant Access	Unspecified
AE-RemoteOperator Secure Wired (Ethernet) Connections	Enabled	11	Grant Access	Unspecified

Figure 6: Netzwerkrichtlinien

HINWEIS!	Beachten Sie, dass die Richtlinien in der Verarbeitungsreihenfolge aufgelöst werden, wenn NPS die erste Richtlinie mit gewährtem Zugriff findet, verwendet sie es. Die Zuordnung der Benutzergruppe wird also innerhalb der ersten Richtlinie aufgelöst und nur dieser entsprechende VSA-String wird an den Antragsteller (TK-Karte) zurückgegeben.

↳ Jede Netzwerkrichtlinie muss auf diese Weise konfiguriert werden (Standard):



AE-ControlOperator Secure Wired (Ethernet) Connections

Conditions - If the following conditions are met:

Condition	Value
User Groups	AIS\AE-ControlOperators

Settings - Then the following settings are applied:

Setting	Value
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Secured password (EAP-MSCHAP v2)
Authentication Method	EAP OR Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 OR MS-C...
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	ControlOperator
Framed-Protocol	PPP
Service-Type	Framed

Figure 7: Konfiguration der Netzwerkrichtlinien

- Die Methoden für die Bedingungen - Authentifizierung sollten für alle Richtlinien wie diese festgelegt werden:

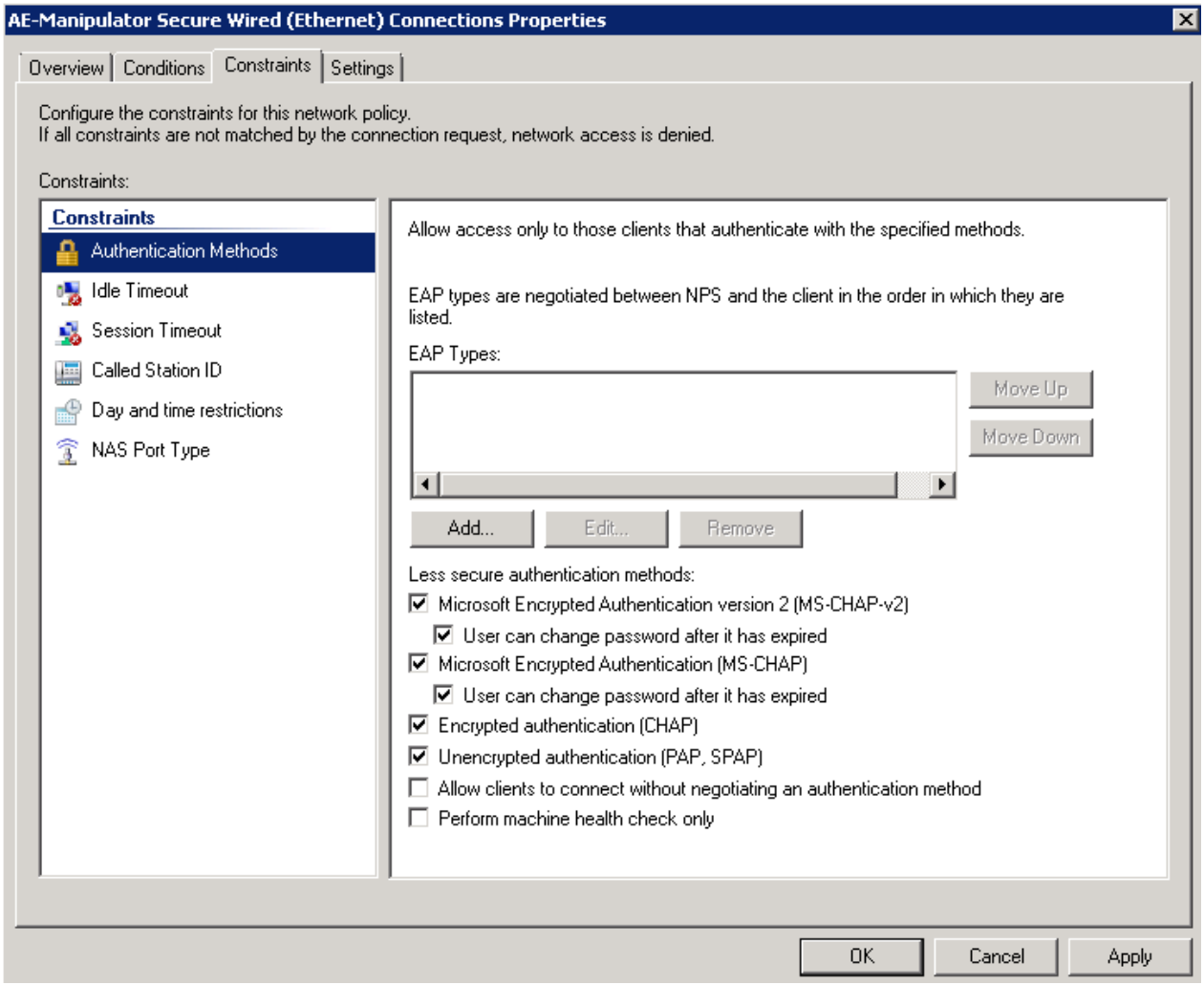


Figure 8: Authentifizierungsmethoden

- Das Attribut Vendor-Specific wurde entsprechend der Benutzergruppe Active Directory auf den gewünschten Pflichtwert gesetzt:

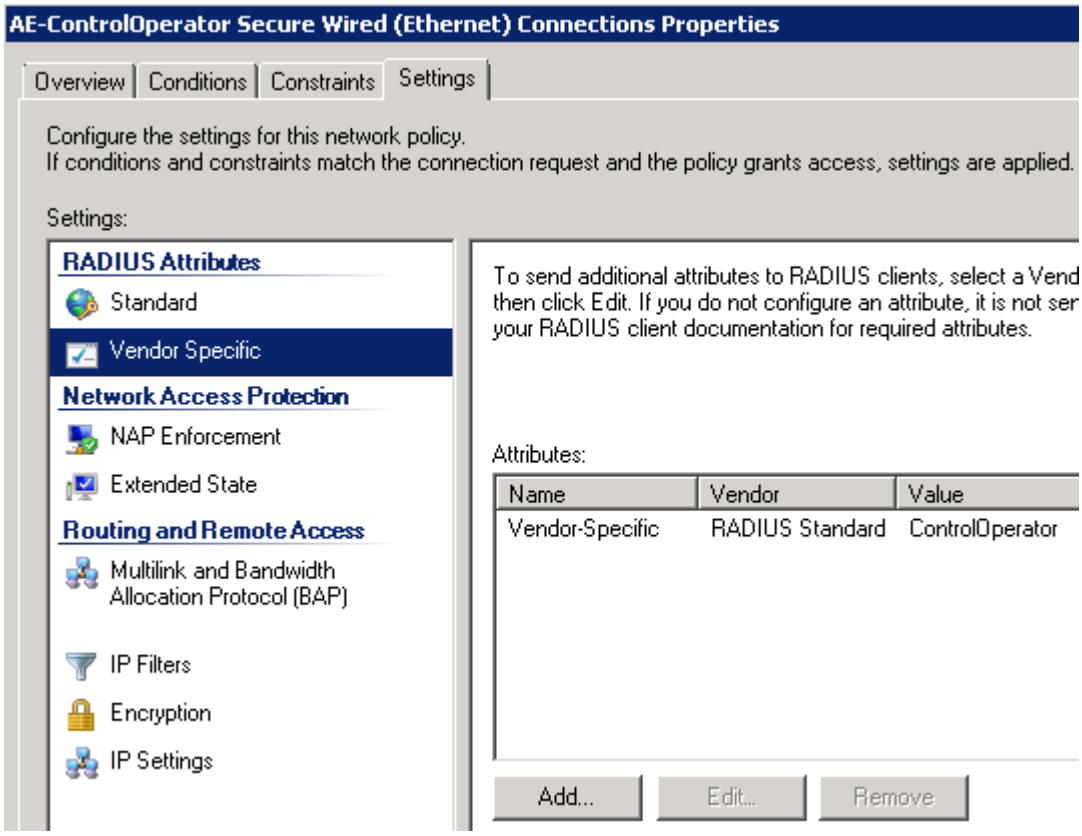


Figure 9: Lieferantenspezifische Attribute

- Dieses Vendor-Specific-Attribut sollte wie folgt gesetzt werden (Vendor Code Wert spielt keine Rolle):

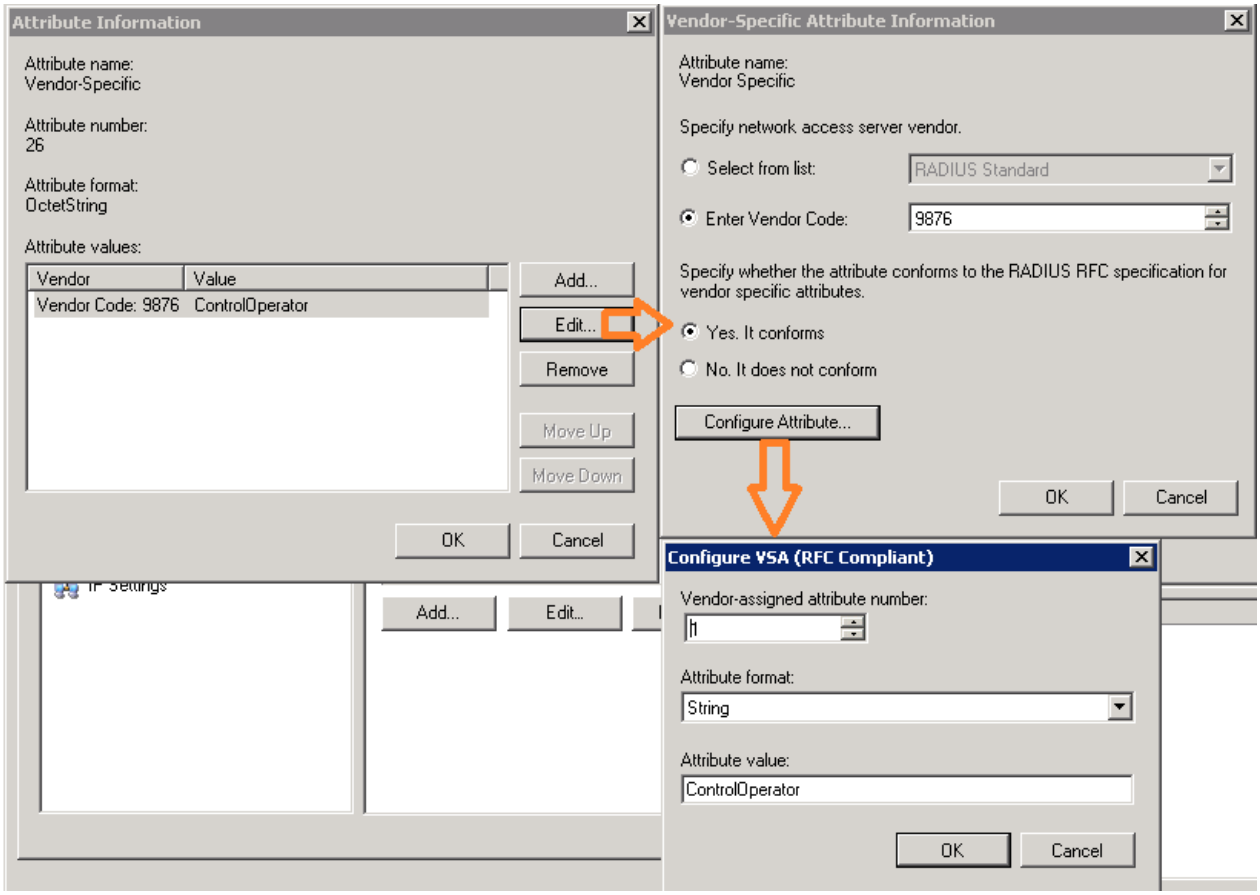


Figure 10: Herstellerspezifische Attribut-Einstellung

4.3.3.4 RADIUS-Modus-Einstellungen in WinConfig

Die Eigenschaften des RADIUS-Modus können auf der Sicherheitsseite von online WinConfig eingestellt werden:

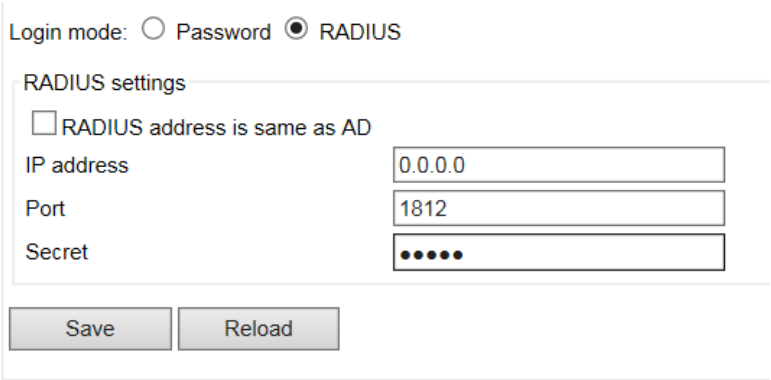


Table 12: Einstellungen des Radiusmodus

Einstellung	Wert
RADIUS-Adresse ist identisch mit AD	Der RADIUS-Server kann auf dem gleichen PC wie der Active Directory-Server implementiert werden.
RADIUS IP-Adresse	IP-Adresse des RADIUS-Servers (TK-Karten haben keinen DNS-Client implementiert, daher ist die IP-Adresse obligatorisch).
Port	TCP-Port des RADIUS-Serverdienstes
Geheimnis	Freigabe des für diese TK-Karte konfigurierten Geheimnisses auf dem Server

4.3.4 Passwortmodus

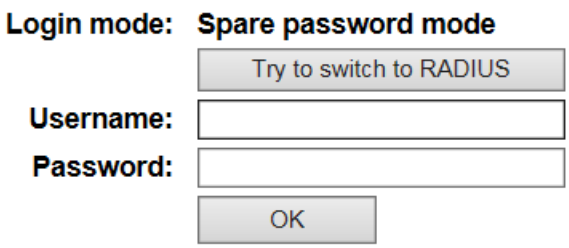
Das eingebettete Admin-Konto dient zur Autorisierung von Aktionen im Passwortmodus. Das Passwort dieses Kontos (sog. Notfallpasswort) wird lokal im Betriebssystem der Karte gespeichert, aber periodisch aus dem Active Directory zwischengespeichert (Caching wird vom Systemdämon durchgeführt). Die Version dieses Passworts mit der gleichen Methode wird ebenfalls zwischengespeichert. Dieser Mechanismus ermöglicht die Anmeldung an der Karte für den Fall, dass kein RADIUS-Server angeschlossen werden kann. Diese Passwortversion wird dem Benutzer nach dem Zurücksetzen der TK-Karte für kurze Zeit auf dem Display des angeschlossenen REGSYS-Gerätes angezeigt und der Systemadministrator konnte das richtige Passwort für diese Version bereitstellen.

Das Admin-Konto im Passwortmodus verwendet die gleichen Rechte wie die Administratorrolle im Radius-Modus.

Es ist notwendig, den AD zu ändern, um die richtigen Informationen für diesen Login-Modus bereitzustellen.

Wenn die Fernwirkkarte in den RADIUS-Modus geschaltet wird und der RADIUS-Server nicht verfügbar ist, wechselt die Karte nach erfolglosem Anmeldeversuch im RADIUS-Modus automatisch in den Passwort-Modus. Die Fernwirkkarte unternimmt jedoch regelmäßig Versuche, den RADIUS-Server zu verbinden. Wenn der RADIUS-Server verfügbar ist, schaltet sich die Fernwirkkarte im Hintergrund wieder in den RADIUS-Modus. Wenn also der Passwortmodus aus Betriebsgründen wünschenswert ist, ist es notwendig, die Karte in den Passwortmodus zu schalten, indem man die Sicherheitseinstellungen verwendet.

Der Benutzer hat die Möglichkeit, *bei Bedarf* in den RADIUS-Modus zu wechseln, *indem er* im Anmeldedialog die Schaltfläche *Try to switch to Radius* verwendet. Wenn der RADIUS immer noch nicht verfügbar ist, hat der Versuch keine Wirkung und der Benutzer kann im *Passwortmodus* fortfahren.



HINWEIS!	Der Name des Passwortmodus ist benutzerdefinierbar, wobei der *Spare-Passwortmodus* standardmäßig eingestellt ist. Sowohl der Modusname als auch das Passwort können in den Sicherheitseinstellungen geändert werden.

4.3.4.1 AD-Server und Schema Vorbereitung Schritt für Schritt

Neue obligatorische AD-Attribute:

Es ist zwingend erforderlich, dem AD-Schema zwei neue Attribute mit den folgenden gemeinsamen Namen / Anzeigenamen hinzuzufügen:

- ae-WinConfig-AdminEmergencyPasswort / aeWinConfigAdminEmergencyPasswort
- ae-WinConfig-AdminEmergencyPasswordVersion / aeWinConfigAdminEmergencyPasswordVersion

Die empfohlene Methode, wie man ein erweitertes AD-Schema durch den Editor für eingebettete AD-Attribute von Windows Server hinzufügt, ist hier beschrieben:

https://social.technet.microsoft.com/wiki/contents/articles/20319.how-to-create-a-custom-attribute-in-active-directory.aspx

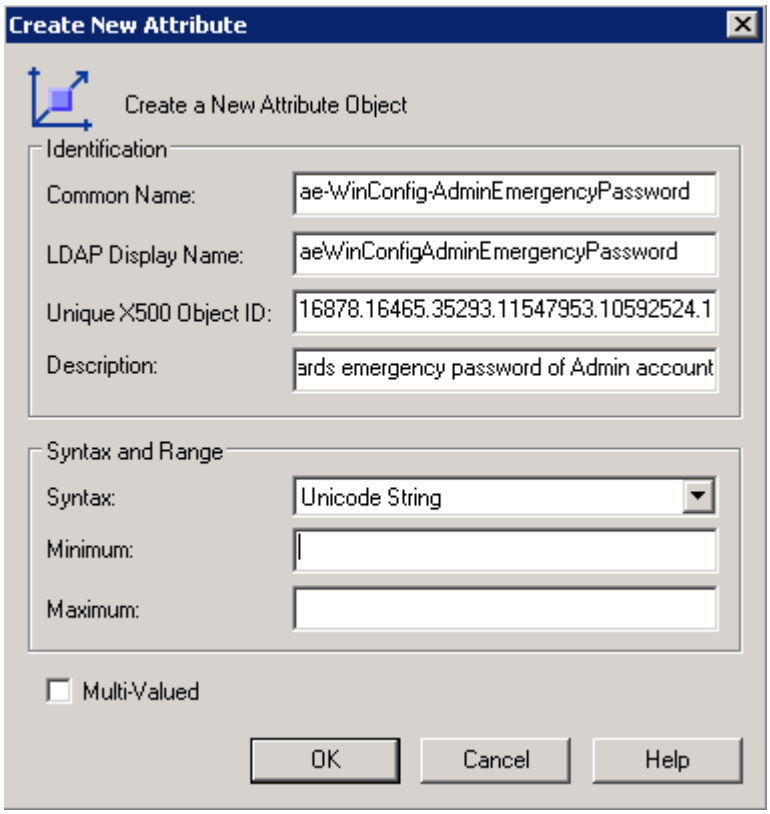


Figure 11: Beispiel, wie der Administrator die eindeutige OID-Eigenschaft jedes neuen Attributs füllen muss.

Die Effizienz und Schnelligkeit der Erzeugung des richtigen IOD wird hier beschrieben:

https://gallery.technet.microsoft.com/scriptcenter/56b78004-40d0-41cf-b95e-6e795b2e8a06

Diese beiden neuen Parameter müssen der Benutzerklasse zugeordnet werden, wie im oben genannten Dokument beschrieben.

Um die Weitergabe der neuen Parameter an alle gewünschten AD-Objekte zu gewährleisten, wird empfohlen, den Active Directory-Dienst oder Windows neu zu starten.

AD-Benutzer mit obligatorischem Anzeigenamen:

Der folgende Benutzer muss in der Gruppe Benutzer des AD mit diesem Anzeigenamen existieren (es wird empfohlen, einen neuen Benutzer mit dieser Eigenschaft anzulegen. Es ist ratsam, Nach- und Vorname leer zu lassen und den gewünschten Anzeigenamen in den vollen Namen einzugeben):

Admin für A-Eberle Karten

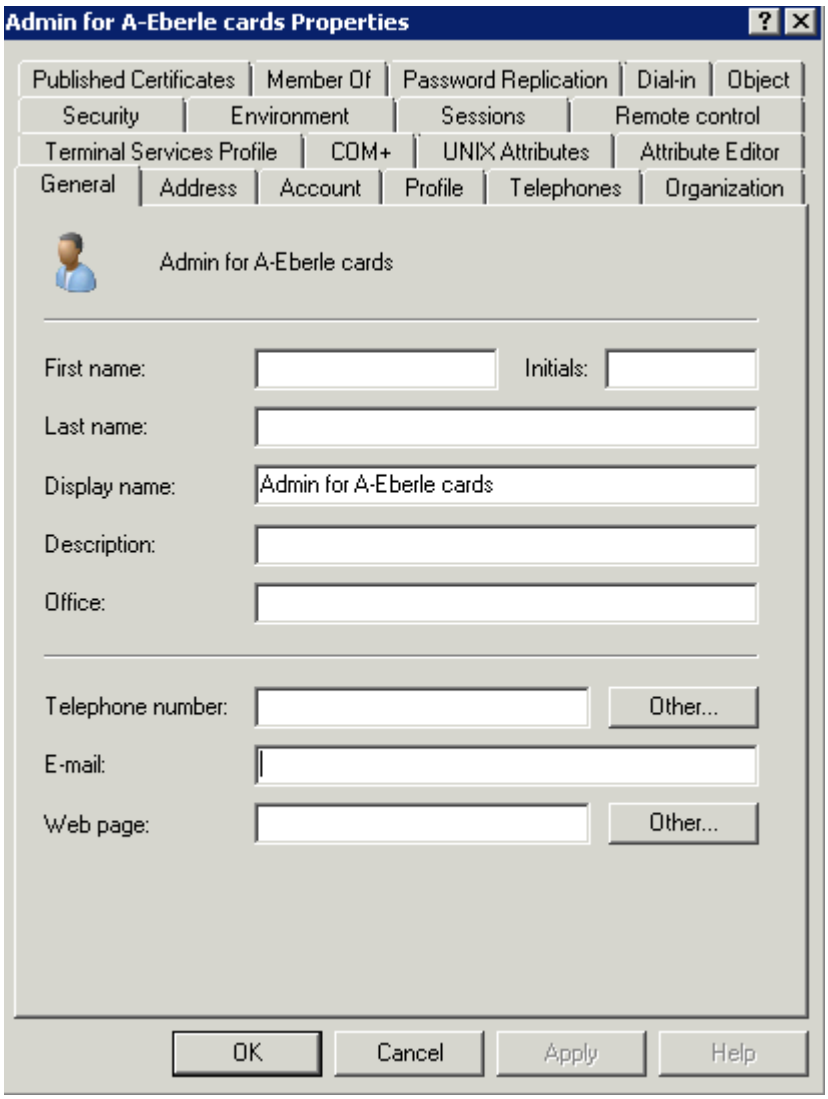


Figure 12: Admin für A-Eberle Karten

Das Benutzerobjekt *Admin for A-Eberle cards Properties* dient als Container für entsprechende Attribute. Der LDPAS-Client aus den TK-Karten zwischenspeichert Login-Attribute aus diesem Objekt. Dies ist auch der Ort, an dem Sie die folgenden Attribute festlegen können (dieser Vorgang sollte vom AD-Administrator automatisiert werden):

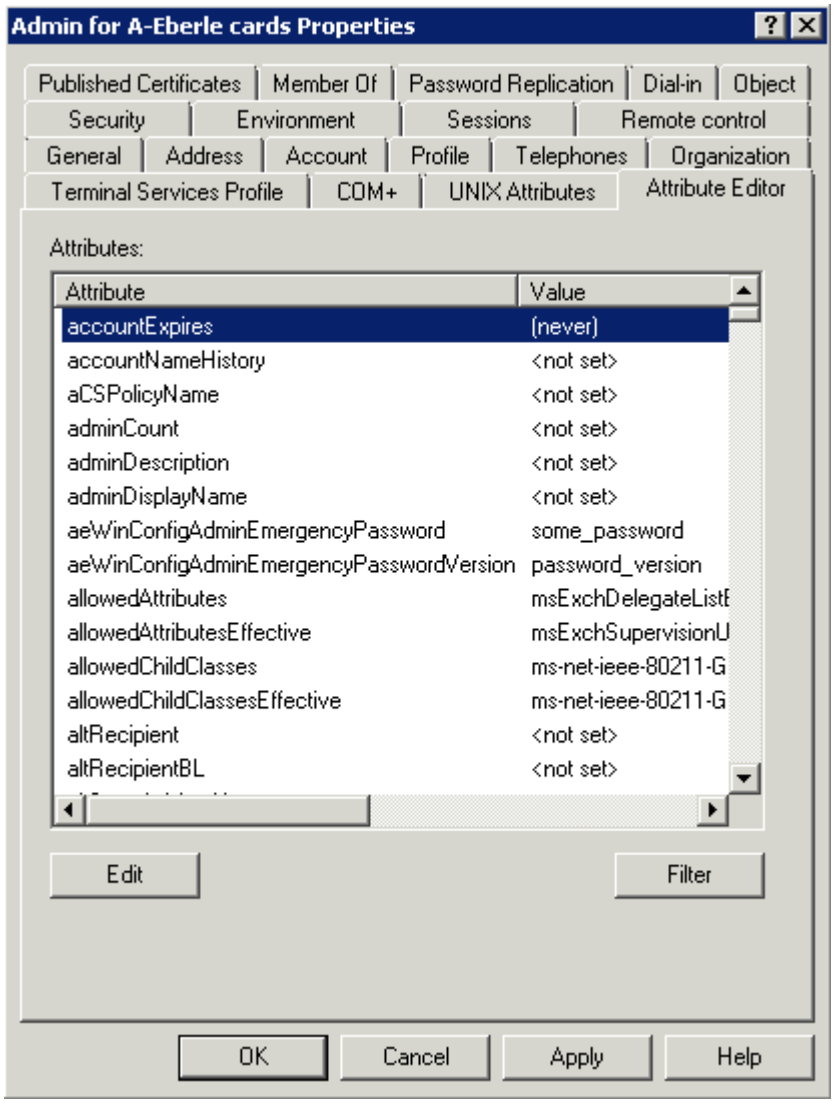


Figure 13: Konfiguration der Attribute

Es ist zwingend erforderlich, ein entsprechendes Serverzertifikat auf dem AD-Server zu installieren, das genauso heißt wie der FQDN des Servers, um die richtige Autorisierung über LDAPS zu gewährleisten.

Gute Praxis ist es, lokal installierte Zertifizierungsdienste zu verwenden, Zertifikatsanforderungen zu erstellen, das Zertifikat auszustellen und lokal zu installieren.

Weitere Informationen finden Sie in der Microsoft-Dokumentation, z.B. https://gallery.technet.microsoft.com/Windows-Server-2016-Active-165e88d1

4.3.4.2 Einschränkung der Benutzernamen

Verwenden Sie Buchstaben (A ....Z, a...z) und/oder Zahlen (0...9) in Benutzernamen.

Vermeiden Sie die Verwendung von Sonderzeichen (Nicht-Buchstaben). Die einzigen zulässigen Sonderzeichen sind unten aufgeführt.

Erlaubte Sonderzeichen: - _

4.3.4.3 Einstellungen des Passwortmodus in WinConfig

Figure 14: Einstellung des Passwortmodus, RBAC und andere Sicherheitseinstellungen

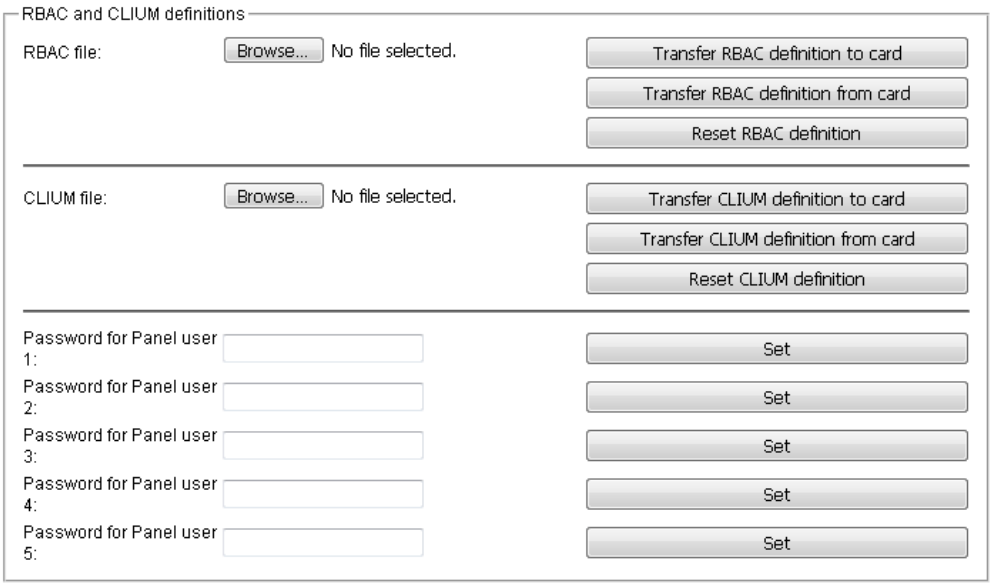


Figure 15: Einstellung des Passwortmodus, RBAC und andere Sicherheitseinstellungen

Table 13: AD-Servereinstellungen

Einstellung	Wert
IP-Adresse des AD-Servers	IP-Adresse des AD-Servers (TK-Karten haben keinen DNS-Client implementiert, daher ist die IP-Adresse obligatorisch).
LDAPS-Port	TCP-Port des LDAPS-Serverdienstes, der auf dem AD-Server läuft - normalerweise 636
AD-Server FQDN	TK-Karte verwendet LDAPS-Protokoll, um mit AD zu kommunizieren, in diesem Fall ist es zwingend erforderlich, den FQDN-Namen AD-Server zu kennen. Dieser Name muss mit dem Namen des für LDAPS verwendeten Zertifikats übereinstimmen.
AD Benutzername FQDN	Name des AD-Benutzers, der die Rechte zum Lesen der im Cache gespeicherten ae.... Attribute hat (er wird lokal mit den üblichen PAM-Sicherheitsverfahren verschlüsselt gespeichert). Es ist zwingend erforderlich, den FQDN-Benutzernamen zu verwenden. Es ist empfehlenswert, den nach dem in Kapitel 0 beschriebenen Verfahren erstellten Benutzer zu verwenden, da dieser Benutzer Eigentümer der gewünschten Attribute ist und einen sicheren Zugriff hat.
AD-Benutzerpasswort	Passwort dieses Benutzers (es wird lokal mit den üblichen PAM-Sicherheitsverfahren verschlüsselt gespeichert)
CA-Zertifikat	Das Zertifikat der Behörde, die das Zertifikat für den LDAPS-Server ausgestellt hat.

Der Login-Modus kann als Passwort oder Radius gewählt werden, aber auch der Name des Passwortmodus kann benutzerdefiniert werden. Der Standardmodusname ist *Spare password*. Auch das Passwort für diesen Modus kann später über die Schaltfläche *Passwort ändern* geändert werden.

4.4 Verwaltung der RBAC-Definitionsdateien

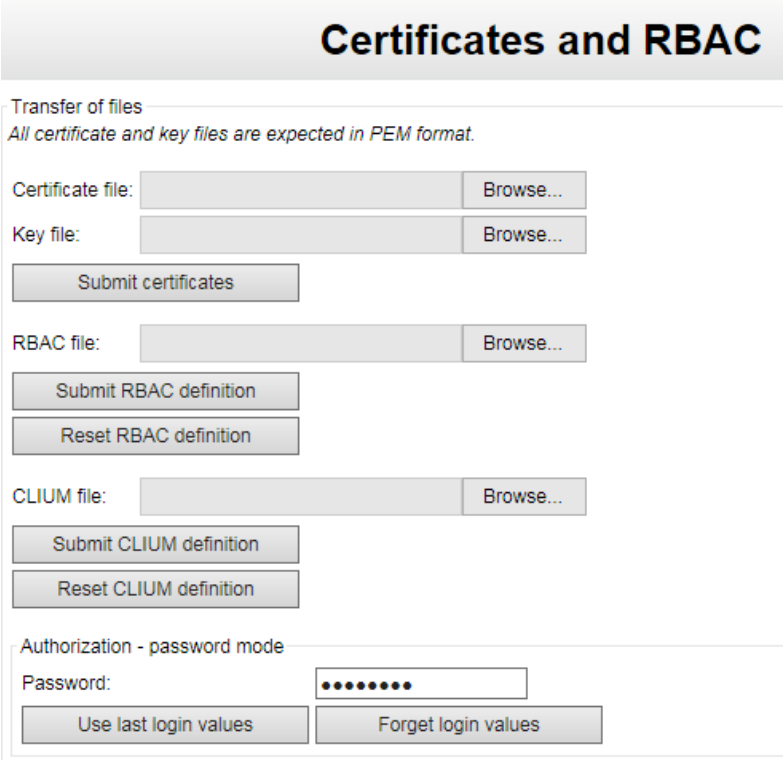
Es gibt 2 Dateien mit Definitionen von Actions-to-Role-Rechten - WinConfig RBAC und CLIUM Definitionsdateien. Die CLIUM-Definitionsdatei enthält Regeln für A-Eberle-Geräte (RegSys), siehe Kapitel 4.3.3.2.

Das grundlegende Sicherheitsverhalten der CLIUM-Definitionsdatei:

- Die in der CLIUM-Datei definierten Sicherheitsrichtlinien sind nur aktiv, wenn sich ein Benutzer in der Online-WinConfig angemeldet hat.
- Die Rolle des angemeldeten Benutzers wird verwendet, um die entsprechende Matrix von Sicherheitsrichtlinien festzulegen (siehe Dokumentation des Regulators).
- Wenn sich ein Benutzer aus der Online-WinConfig abgemeldet hat, werden die RegSys-Sicherheitsrichtlinien nach einem definierten Timeout innerhalb der RegSys wieder in den Grundzustand zurückgesetzt. Das Vorhängeschloss-Symbol erscheint in der Regleranzeige und der Betrieb des Reglers ist nicht zulässig.
- Im Falle des Hochladens einer neuen CLIUM-Definitionsdatei an die Regulierungsbehörde ist es notwendig, sich in der Online-WinConfig abzumelden und erneut anzumelden, um die neu definierte Matrix effektiver Sicherheitsrichtlinien zu verwenden.

Die WinConfig RBAC-Definitionsdatei ist im Kapitel 4.3.3.1 beschrieben. Diese Datei kann im Online- und Offline-WinConfig-Modus auf die Karte übertragen werden. Die Aktion *set_certificates* wird für die Autorisierung der Übertragung verwendet.

Die RBAC-Definitionsdatei kann in den in dieser Dokumentation beschriebenen Auslieferungszustand zurückgesetzt werden. Dieser Vorgang ist nur für die Rolle des Administrators reserviert und nicht in den RBAC-Definitionen enthalten, um ein Deadlock im Falle einer beschädigten RBAC-Datei auf der Karte zu vermeiden.



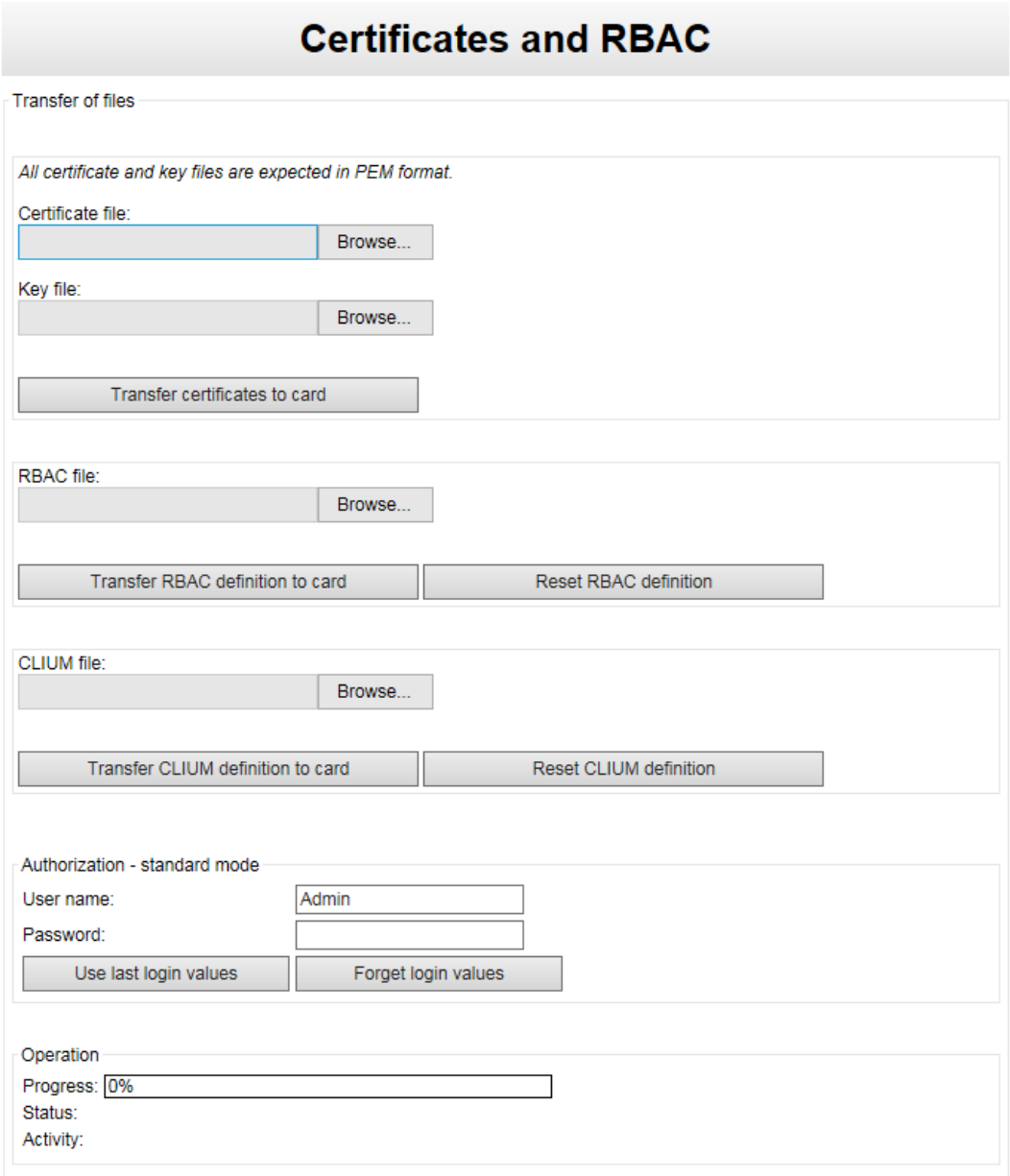


Figure 16: Offline WinConfig Verwaltung von RBAC-Definitionsdateien

4.5 Verwaltung von Sicherheitszertifikaten

Die Arbeit mit Zertifikaten unterliegt der Public Key Infrastructure (PKI). Das Zertifikat wird von der *Zertifizierungsstelle* nach Erhalt der *Zertifikatsanforderung* ausgestellt. Dieses Zertifikat kann z.B. für die Verschlüsselung von HTTPS verwendet werden, wie in der folgenden Spalte 1) beschrieben.

Nach den PKI-Regeln ist ein neues Zertifikat erforderlich, wenn:

0 Die Gültigkeit des ursprünglichen Zertifikats abgelaufen ist.

0 Das Zertifikat wurde entweder von der *Zertifizierungsstelle* (Verdacht auf unbefugte Nutzung etc.) oder auf Antrag des Zertifikatinhabers (Offenlegung des privaten Schlüssels etc.) widerrufen.

4.5.1 Sicherheitszertifikate in den Fernwirkkarten TK28-4, TK28-6 und TK102

1) Das Zertifikat, das für die Verschlüsselung der HTTPS-Kommunikation in Online- und Offline-WinConfig verwendet wird:

Dieses Zertifikat mit Schlüssel ist vorinstalliert und wird mit dem WinConfig-System auf Karten geliefert. Das Zertifikat wird für die Zwecke von WinConfig für regped.teledata.de mit der Gültigkeit bis 2050 ausgestellt. Ein Benutzer kann das Zertifikat mit Hilfe des Offline-WinConfig nach der Erkennung und Boardauswahl über die Option *Zertifikate einreichen* durch ein eigenes *Zertifikat/Privatschlüsselpaar* ersetzen.

2) Das CA-Zertifikat zur Überprüfung der verschlüsselten Kommunikation mit dem LDAPS-Protokoll:

Dieses Zertifikat ist notwendig für die automatische Änderung des Notfallpasswords aus dem Active Directory-Speicher. Alle Zertifikate, die von Zertifizierungsstellen Ende 2017 vom Windows[tm]-System erhalten wurden, werden mit dem WinConfig-System auf den Boards geliefert. Diese Zertifikate können über die Option *Benutzerverwaltung* in WinConfig online durch andere CA-Zertifikate ersetzt werden.

4.6 Funktionalitätskonzepte

Der Passwort-Login-Modus gilt, wenn der RADIUS-Server nicht verfügbar ist.
Dies tritt in der folgenden Situation auf:

0 Im RADIUS-Modus gab es eine erfolglose Anmeldung, da der RADIUS-Server nicht erreichbar ist. Die Fernwirkkarte wechselt automatisch in den Passwortmodus.

Um in diesem Fall die richtigen Informationen über den Login-Modus zu erhalten, muss ein Benutzer wie folgt vorgehen:

- Online-Modus: Machen Sie einen neuen Anmeldeversuch.
  - Der PASSWORD-Modus erscheint nach der Aktualisierung des Browsers.
- Offline-Modus: Nach erfolgloser Anmeldung muss eine neue Erkennung durchgeführt werden, um die Informationen zum Karten-Login-Modus zu aktualisieren.
  - Der Passwortmodus erscheint nach der Erkennung.
- Serielle Konsole
  - Der Passwortmodus erscheint nach erfolgloser Anmeldung bei RADIUS.
- SSH-Konsole

↳ Das gleiche Verhalten wie bei der seriellen Konsole, aber die Informationen zum Login-Modus sind für den Benutzer nicht sichtbar.

Eine erfolglose Anmeldung im RADIUS-Modus kann auch dann auftreten, wenn ein Benutzer sein Passwort vergessen hat oder die RADIUS-Einstellungen versehentlich in der Fernwirkkarte beschädigt wurden. Die folgenden Schritte können in dieser Situation durchgeführt werden:

➲ Trennen Sie die Karte vom Netzwerk.

↳ RADIUS wird unzugänglich.

➲ Schließen Sie das Board lokal mit dem Notebook an.

➲ Folgen Sie einem der oben genannten Szenarien.

HINWEIS!	Hinweis: In diesem Fall wird die Karte nur vorübergehend in den PASSWORD-Modus geschaltet und die Boardsoftware versucht regelmäßig mit einer Dauer von 1 Stunde, sich wieder mit dem RADIUS-Server zu verbinden. So wird die Karte automatisch in den RADIUS-Modus geschaltet, wenn sich ein Benutzer abmeldet und der RADIUS-Server verfügbar wird.

Die werkseitige Auslieferung beinhaltet ein Standardpasswort, das dringend empfohlen wird, es am Ende des SAT zu ändern.

Das Notfallpasswort wird vom Online-Webserver WinConfig oder vom zentralen Active Directory festgelegt.

Das Notfallpasswort kann auch von der Offline-WinConfig festgelegt werden, wenn der RADIUS nicht verfügbar ist und das Passwort zuvor nicht von der Online-WinConfig geändert wurde, so dass der Benutzer nicht gezwungen ist, die Online-WinConfig zum ersten Mal zu verwenden. Der HTTPS-Zugang wird für die Übertragung des neuen Passworts auf die Karte verwendet, um eine sichere Übertragung der wichtigen Daten zu gewährleisten.

Grundannahmen:

1) Funktionsweise des WinConfig offline:

- Das WinConfig offline kann nach den üblichen Windows-Regeln gestartet werden.
- Die Arbeit mit den Einstellungen und der Kartenerkennung kann von jedem durchgeführt werden, der die entsprechenden Rechte für den angeschlossenen PC hat.
- Diese Aktionen werden nach der Kartenauswahl vorab authentifiziert: Daten von/zu Karte übertragen, Diensteinstellungen und IP-Einstellungen.
- Die Vorauthentifizierung erfolgt durch den angeschlossenen Online-WinConfig-Webserver entsprechend den Karteneinstellungen - über das RADIUS- oder Notfall-Online-WinConfig-Konto. Der Benutzer des Offline-WinConfig wird darüber informiert, welche Anmeldeinformationen er verwenden soll (Offline-WinConfig erhält diese Informationen während des Erkennungsprozesses, genau wie andere Dienstinformationen).

- Der Benutzer muss das Notfallpasswort setzen, wenn es noch nicht gesetzt ist und der RADIUS nicht verwendet wird.

2) Die Karte enthält zunächst nur den RADIUS-Client ohne die Verbindungsinformationen des RADIUS-Servers (IP-Adresse etc.). Es gibt ein erstes Online-WinConfig-Webzugangskonto auf der Karte (Admin/teledata) und der Benutzer darf nur das Initialpasswort dieses Logins auf das Notpasswort ändern (das Programm wendet dafür Regeln an). Der Begriff "Notfallpasswort" bezeichnet das Passwort des Standard-Admin-Kontos des Online-Webservers WinConfig. Dieses Admin-Konto mit dem Notfall-Login funktioniert erst, wenn das werkseitig voreingestellte Online-Passwort für den WinConfig-Webzugriff in Notfall eins geändert wurde.
3) Das Notfallpasswort kann mit Hilfe des Online- oder Offline-WinConfig innerhalb der ersten Anmeldung festgelegt werden. Bei diesem Vorgang wird das Admin-Konto auf dem Online-Webserver von WinConfig mit Notfallpasswort wiederhergestellt. Der Benutzer wird die RADIUS-Verbindungsinformationen in der Online-WinConfig einstellen.
4) Das Notfallpasswort wird aus dem AD zwischengespeichert, falls der AD-Server im LAN sichtbar ist. Diese Methode hat Vorrang vor der lokalen Zuordnungsmethode.
5) Erfolglose Anmeldeversuche werden auf MicroSD und auf dem entfernten SYSLOG-Server protokolliert.

Basisszenarien auf den Fernwirkkarten *REG-P (TK28-4)*, *REG-PE (TK28-6)* und *REG-PED^{SV} (TK102)*:

1) Der Endverbraucher greift erstmals vor Ort auf A-Eberle-Geräte zu, die mit den oben genannten Fernwirkkarten ausgestattet sind (Online-Verfahren WinConfig) und RADIUS ist nicht verfügbar.
2) Der Endverbraucher wird auf das A-Eberle-Gerät, das mit den oben genannten Fernwirkkarten ausgestattet ist (Online-Verfahren WinConfig), für die nächsten Male zugreifen und RADIUS ist verfügbar.
3) Der Endverbraucher wird auf das A-Eberle-Gerät, das mit den oben genannten Fernwirkkarten ausgestattet ist (Online-Verfahren WinConfig), für die nächste Zeit zugreifen und RADIUS ist nicht verfügbar.
4) Der Endbenutzer greift aus der Ferne auf das A-Eberle-Gerät zu, das mit den oben genannten Fernwirkkarten ausgestattet ist (WinConfig Offline-Verfahren), für die Karte, welche die RADIUS-Authentifizierung verwendet.
5) Der Endverbraucher wird das mit den oben genannten Fernwirkkarten ausgestattete A-Eberle-Gerät (WinConfig Offline-Verfahren) erstmals für die Karte ohne RADIUS-Authentifizierung benützen.
6) Der Endverbraucher wird das mit den oben genannten Fernwirkkarten ausgestattete A-Eberle-Gerät für die Karte ohne RADIUS-Authentifizierung das nächste Mal benützen (WinConfig Offline-Verfahren).

Die Szenarien 2,3,4,6 könnten nach 1 oder 5 verwendet werden (der Endbenutzer muss die Authentifizierung auf den Karten einleiten).

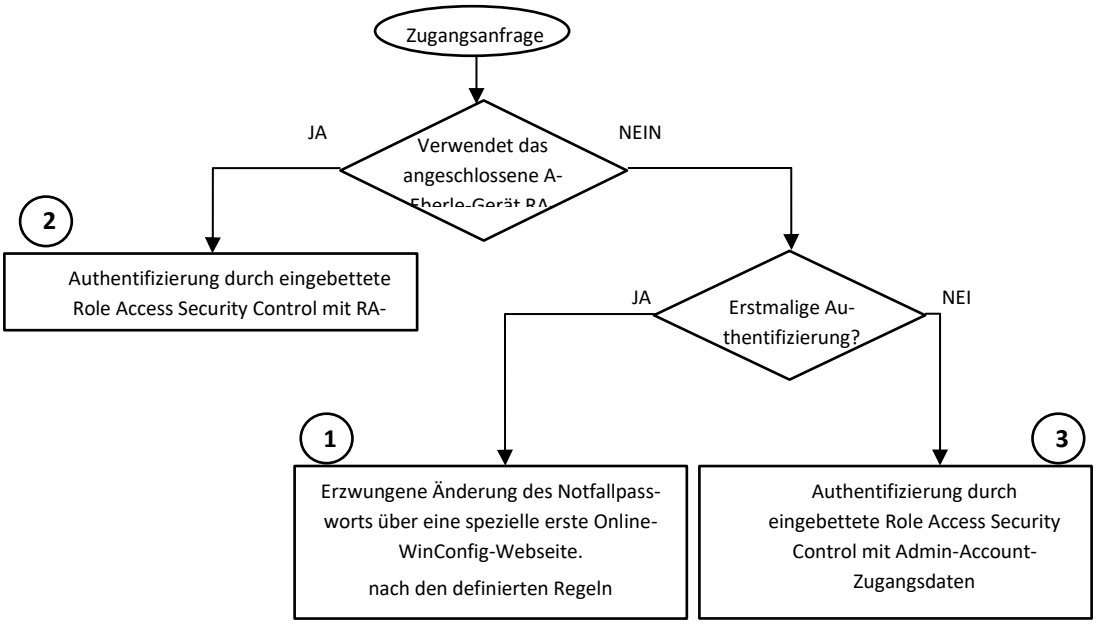


Figure 17: Online-Zugriffsmethode WinConfig - erste/nächste Authentifizierung

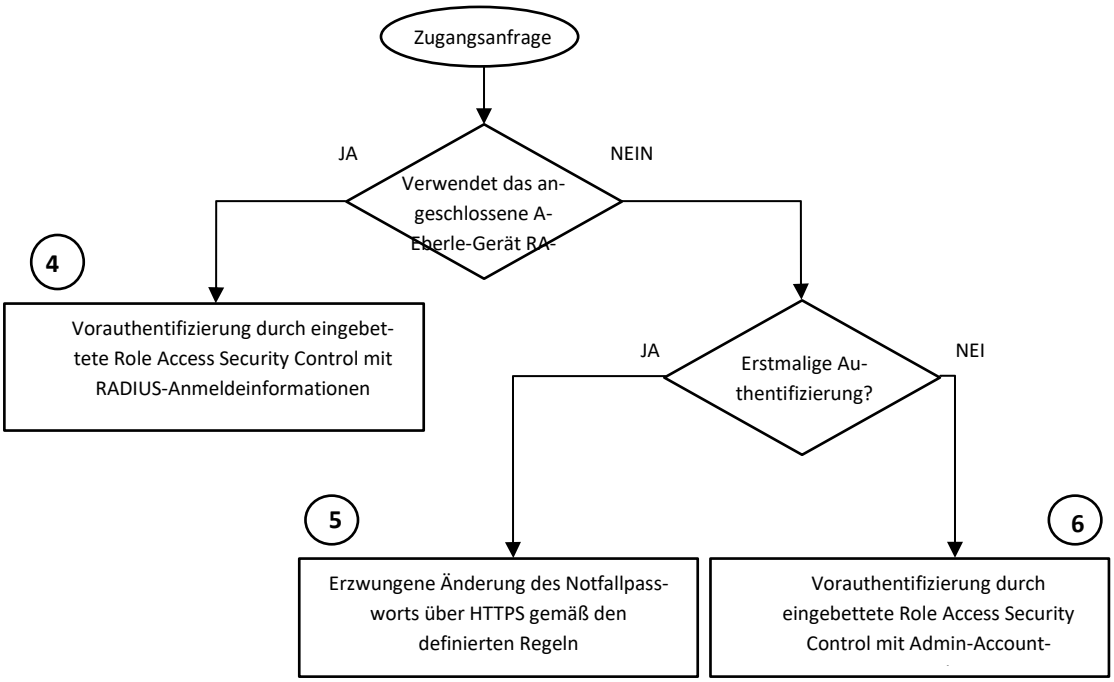


Figure 18: Offline WinConfig Zugriffsmethode - Erst-/Nachträgliche Zeitauthentifizierung

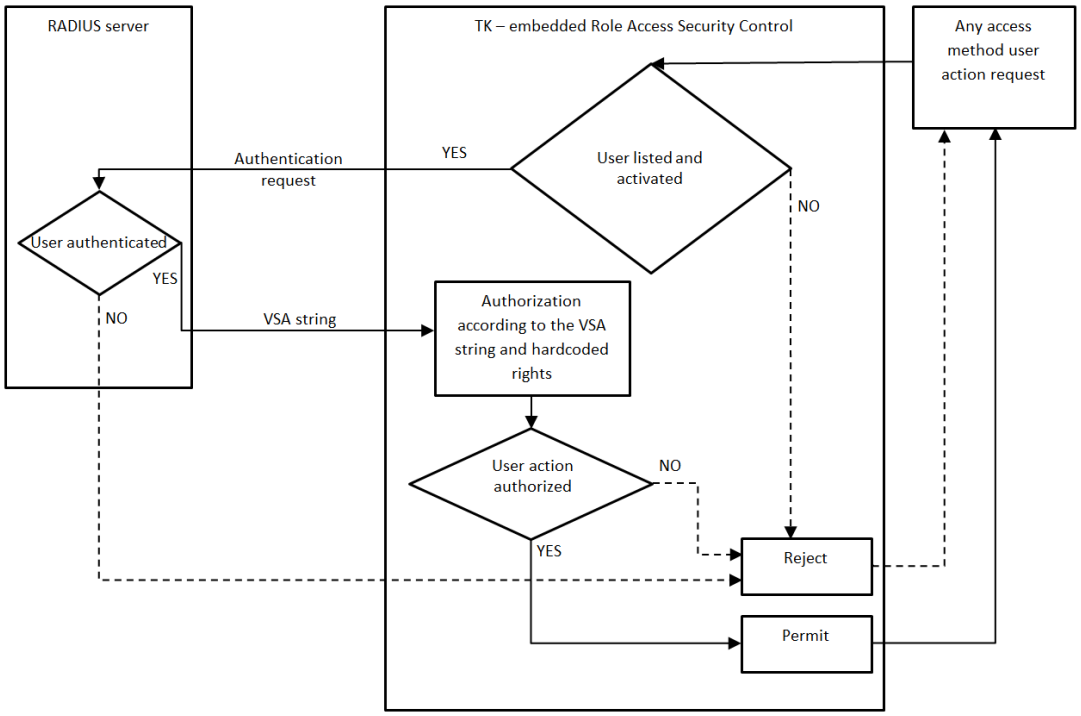


Figure 19: Berechtigungsszenario für Benutzeraktionen - RADIUS-Anmeldemodus

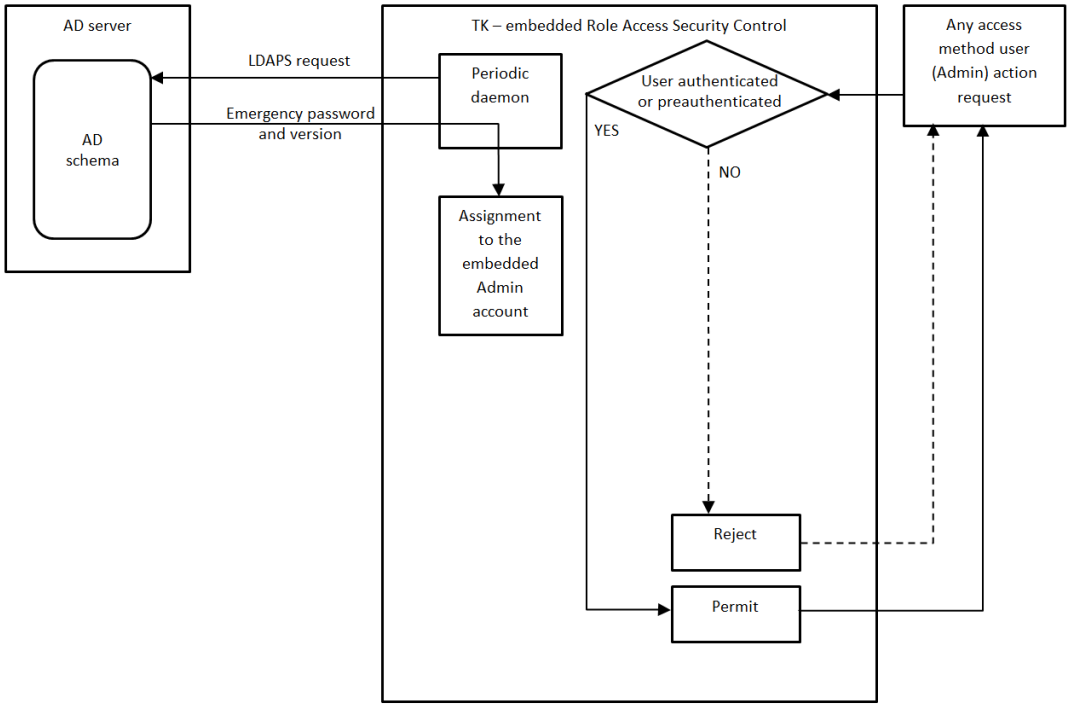


Figure 20: Benutzeraktion Autorisierungsszenario - Passwort-Login-Modus

5. Sicherheit in den Fernwirkkarten REG-PE und REG-PED Modelle TK8xx

5.1 Zusammenfassung der Zugriffsmethoden und Protokolle für Benutzer

- WinConfig online (Web-Zugang)
  - Der Internetbrowser-Client (vergleichbar zum Internet Explorer) verbindet den im Linux-Betriebssystem integrierten Webserver auf der Karte.
  - Es wird das Protokoll HTTPS mit direkter Berechtigung verwendet.
- WinConfig Konsolen-/Shell-Menü (Terminalzugriff)
  - Der Terminal-Client (wie PUTTY) verbindet den im Linux-Betriebssystem integrierten SSH-Server auf der Karte.
  - Das Protokoll SSH mit direkter Autorisierung wird verwendet.
- WinConfig offline (Webzugriff und Transferzugriff)
  - Der Internetbrowser-Client verbindet den Remote-Client-seitigen proprietären Webserver (Teil des WinConfig offline). Ein spezieller Serverteil kommuniziert mit der Karte. Es wird empfohlen, den Internet Explorer zu verwenden, da andere Browser Probleme bei der Anzeige der Webserver-Seiten haben können.
  - Die Datenübertragung erfolgt über das Protokoll HTTPS mit direkter Berechtigung.
  - Netzwerk-Scan (Broadcast-Funktionen) und Systemparametrierung erfolgen über UDP mit HTTPS-Vorautorisierung.

5.2 Rollenkonzept für Fernwirkkarten REG-PE der Baureihe TK8XX

Das Sicherheitssystem in Fernwirkkarten TK8xx verwendet zwei Rollen - Administrator und Benutzer. Administratoren- und Benutzerrollen verwenden Rechte, wie sie für Administrator und Beobachter in RBAC-Definitionen definiert sind. Der Standardbenutzer ist Admin/teledata und gehört zur Rolle Administrator.

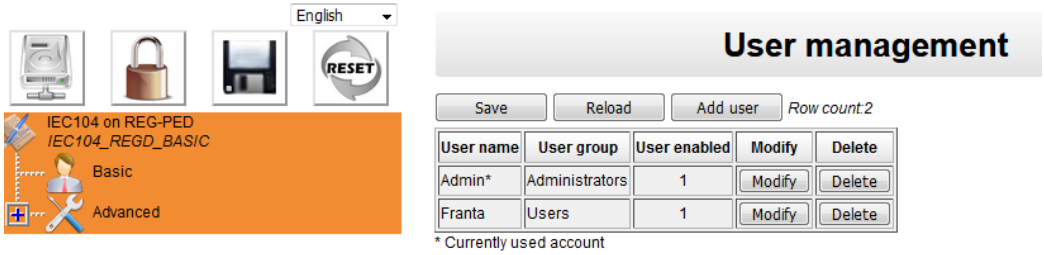


Figure 21: Verfügbare Rollen für Karten des Typs TK8XX

Die Verwaltung der Benutzer kann über die Online-Winconfig, Seite Benutzerverwaltung (Security) erfolgen, die durch eine Schaltfläche mit Vorhängeschloss-Symbol aufgerufen wird.

Für die Anwendung „DaKo“ (Datenkonzentrator) gibt es zusätzlich die Möglichkeit, bestimmte Funktionen bestimmten Rollen zuzuweisen. Möchten Sie hier eine Änderung der Standardrollen, melden Sie sich bitte bei Ihrem zuständigen Ansprechpartner bei A. Eberle GmbH & Co. KG. Standardmässig darf der User nur alles betrachten, nicht jedoch Parameter verändern und schreiben. Der Administrator verfügt dagegen über die vollen Rechte.

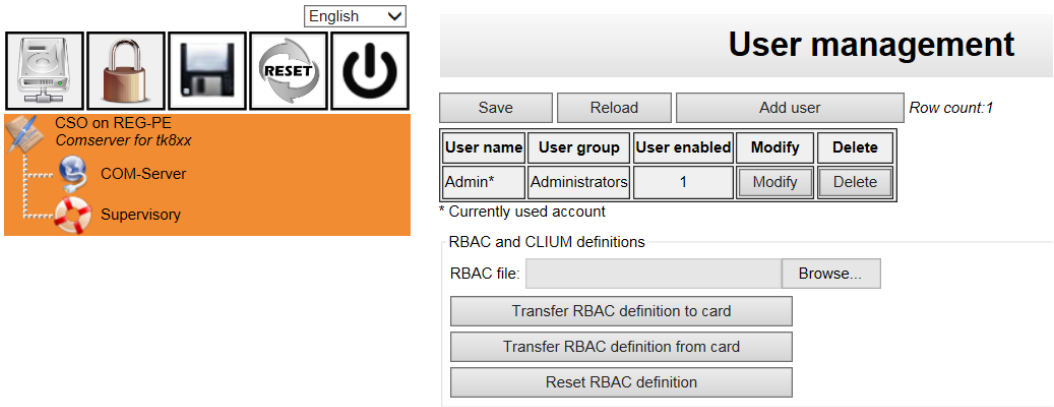


Figure 1: User management für REG-PE (TK860)

5.3 Login-Modi

Die TK8xx-Karten unterstützen *den RADIUS-Modus* nicht, es ist nur der *Passwortmodus* implementiert. Der angemeldete Benutzer hat Rechte gemäß der Rolle, in der er eingeloggt ist.

Figure 2: Beispiel für den Anmeldedialog im http-Modus.

6. WinConfig REG-P / REG-PE / REG-PED / REG-PED^{SV}

6.1 WinConfig Software Einführung

WinConfig ist eine Software zur Verwaltung von Firmware- und Kommunikationsprotokolleinstellungen von Fernwirkkarten und Modulen, die in A-Eberle-Geräteracks platziert werden. WinConfig besteht aus Offline- und Online-Teilen.

6.1.1 Offline und online WinConfig

Offline WinConfig ist ein webbasiertes Programm zur Erstellung und Verwaltung von Dateien mit Protokolleinstellungen, zur wechselseitigen Übertragung von Einstellungen und Firmware von einem Benutzer-PC zu REG-P / REG-PE / REG-PED / REG-PEDSV-Karten und -Modulen sowie zur Identifizierung von REG-P / REG-PE / REG-PED / REG-PEDSV-Geräten, die mit dem Netzwerk verbunden sind. Darüber hinaus kann Offline WinConfig auch zur Konfiguration von Netzwerk- und Sicherheitsparametern der angeschlossenen Fernwirkkarte verwendet werden.

Offline WinConfig gliedert sich in zwei Hauptteile: den lokalen Webserver und die lokale Website mit Anwendungsbibliotheken. WinConfig startet einen lokalen Webserver und einen Standard-Webbrowser auf Ihrem PC.

Für verschiedene Konfigurationen können Einstellungen ohne direkte Verbindung zur Fernwirkkarte vorbereitet, gespeichert und abgerufen werden. Die Einstellungen werden in .xml-Dateitypen gespeichert.

Die Online-Winconfig wird ebenfalls zusammen mit den Einstellungen und der Kommunikationsfirmware an die Fernwirkkarte übertragen. Diese Software ermöglicht die Verwaltung von Kommunikationsprotokolleinstellungen und Systemfunktionen, die sich auf die Verwaltung von Fernwirksystem-Software, Benutzerverwaltung usw. mit hohem Sicherheitsniveau konzentrieren.

Die Fernwirkkarten REG-P Typ TK400 sind nicht mit Online WinConfig ausgestattet. Diese Karten müssen mit einem COM-Server ausgestattet sein, um sich im Netzwerk zu identifizieren. Der COM-Server ist Teil aller IEC101, IEC103 Protokolle, die als Firmware installiert sind und über die Offline WinConfig zugänglich sind. Der COM-Server kann bei den Typen TK519 und TK509 REG-P ohne Ethernet-Verbindung nicht funktionieren.

Sollte Ihnen einer der in diesem Dokument verwendeten Begriffe unklar sein, können Sie sich an das Glossar am Ende dieses Dokuments halten, um eine Erklärung zu erhalten. Andernfalls können Sie uns gerne mit Ihren technischen Fragen unter dieser E-Mail-Adresse kontaktieren: info@a-eberle.de

6.1.2 Offline WinConfig Softwarelösung

Offline WinConfig Programmausstattung besteht aus einem Webserver Mohican, der mit aktiven Seiten für GUI und Bibliotheken ausgestattet ist, die in C# entwickelt wurden. NET Software-Entwicklungsumgebung zur Kommunikation mit Fernwirkkarten, Dateidiensten und zusätzlichen Hilfsfunktionen.

Offline WinConfig bereitet die Einstellungen für REG-P / REG-PE / REG-PED mit den Protokollen IEC101, IEC103, IEC104, DNP3 und Modbus sowie dem COM-Server auf einem lokalen Host (lokaler Webserver) vor und speichert sie in einem Standard-Dateiformat -.XML-Datei. Die Einstellungsdatei kann dann bei den Modellen TK8xx, TK28x und TK102 des Kartentyps REG-P / REG-PE / REG-PED / REG-PEDSV per HTTPS auf den Flash-Speicher der Karte übertragen werden. WinConfig erstellt Binärdateien im Intel HEX-Format und überträgt sie bei REG-P-Karten der Typen TK400, TK509, TK519 in den Kartenspeicher. Die serielle Übertragung

über A-Eberle-Gerät oder Ethernet-Übertragung kann je nach REG-P-Typ verwendet werden. Die Firmware wird immer zusammen mit den Einstellungen übertragen, WinConfig verwendet die neueste Firmware, die zum Lieferumfang gehört.

6.1.2.1 Offline WinConfig Prozesse, Ressourcen und Sicherheit

Es gibt nur einen Windows-Prozess namens *WinConfig.exe,* der die gesamte Funktionalität abdeckt und intern als In-Prozess-Komponenten realisiert ist. Das Sicherheitsverhalten dieses Prozesses (Zugriffsrecht, Integrität, etc.) muss je nach Host-Umgebung über Standardmethoden von Microsoft Windows eingestellt werden. Die Ressourcenverwaltung (freier Speicherplatz auf der Festplatte, Verwendung von RAM, TCP/UDP-Verbindungen) basiert auf Standardmethoden von Windows und .NET.

6.1.2.2 Offline WinConfig - Mohican Server TCP Portverwaltung und Protokollierung

Der vom Mohican Webserver verwendete Standard-TCP-Port ist Port 8080. Um Konflikte im Falle der Belegung dieses Ports zu vermeiden, prüft WinConfig immer, ob der TCP-Port 8080 frei ist. Wenn nicht, dann versucht WinConfig, die Portnummer zu erhöhen und findet den ersten freien Port. Diese Portnummer wird in die WinConfig-Konfigurationsdatei geschrieben und somit für den WinConfig-Betrieb verwendet. Der beschriebene Test wird immer beim Start von WinConfig durchgeführt.

Die WinConfig-Software erstellt zwei Protokolldateien:

- Die Protokolldateien, die von C#-Bibliotheken erstellt wurden.

Diese Dateien werden im WinConfig-Installationsordner erstellt und nach dem Format *YYYY.MM.DD* benannt. *WinConfig. log,* wobei *YYYY.MM.DD* das Datum der Erstellung der Protokolldatei ist. Die maximale Tiefe der Protokolldateien beträgt 10 Tage; ältere Dateien werden beim Start von WinConfig gelöscht.

- Die Protokolldateien, die vom Mohican Webserver erstellt wurden.

Die vom Mohican Webserver erstellte Protokollierung ist standardmäßig deaktiviert. Die Protokollierung kann durch Bearbeiten der folgenden Zeile in der Konfigurationsdatei *Mohican.conf im* WinConfig-Installationsordner eingeschaltet werden:

<Logging state="off">../log/httpserver.log</Logging>

Um die Anmeldung einzuschalten, ändern Sie die Option *Logging state* auf *"on".* Die Option ermöglicht auch die Einstellung des Namens und des Ordners der Protokolldatei. Im oben genannten Beispiel lautet der Name der Protokolldatei *httpserver.log* und wird im Unterordner */log des* Installationsordners von WinConfig erstellt.

Anmerkung:

Aus Sicherheitsgründen beschränkt der eingebettete WEBserver immer mehrere Anmeldungen auf online WinConfig und auch Anmeldekonflikte zwischen online und offline WinConfig (Datentransfer). Es ist daher ratsam, sicherzustellen, dass niemand in der Online-WinConfig angemeldet ist, wenn das Board von OfflineWinConfig verwaltet wird, da in diesen Fällen ein Zugriffskonflikt auftreten kann.

6.1.3 Online WinConfig Softwarelösung

Die Software der Fernwirkkarten vom Typ TK28x und TK102 basiert auf einem Embedded-Linux-Betriebssystem, das für die entsprechende Hardware zusammengestellt wurde. Die Funktionalität von online WinConfig wird durch die Konfiguration von Linux-Systemteilen - Diensten und Komponenten (Daemons) - gewährleistet, die durch Prozesse ergänzt werden, die die WinConfig-Funktionen sicherstellen.

Das Sicherheitsverhalten von online WinConfig bezüglich Zugriffsrechten, Integrität usw. wird über Linux-Einstellungen und -Parameter sowie durch die Implementierung von Role Based Access Control (RBAC) festgelegt.

Die Ressourcenverwaltung (freier Speicherplatz auf dem Flash, Verwendung von RAM, TCP/UDP-Verbindungen) basiert auf Standard-Linux-Konfigurationen, die bei Bedarf optimiert werden (z.B. Verhalten von TCP-Verbindungen).

Die RBAC-Zugriffsregeln stellen sicher, dass nur autorisierte Zugriffe auf das Fernwirksystem in Offline- und Online-WinConfig erfolgen. Nur autorisiertes Personal kann sich anmelden, Parameter und Eigenschaften des Systems ändern. Unbefugter Zugriff ist ausgeschlossen und ein hohes Maß an Sicherheit ist gewährleistet.

WinConfig prüft auch Benutzereingaben auf Richtigkeit, Vollständigkeit und schließt somit die Möglichkeit ungültiger Benutzereingaben aus. Bei der Änderung wichtiger Systemparameter ist jedoch besondere Vorsicht geboten und fundierte Kenntnisse erforderlich, da unvorsichtige Änderungen zu unerwarteten Fehlfunktionen führen können.

6.1.3.1 Online-WinConfig-Prozesse und -Dämonen

Systemprozesse, die das Linux-Betriebssystem durch die WinConfig-Funktionalität vervollständigen:

- *goahead* - online WinConfig Webserver mit Änderungen für WebREG,
- *prp_pcap_tap_userspace* - Verwaltung des PRP-Redundanzwerks,
- *txrx_ledd* - Daemon zur Verwaltung von LED-Dioden zur Anzeige der Aktivität der seriellen Schnittstellen,
- *udpsrv* - UDP-Daemon zur Verwaltung der Kommunikation mit Offline WinConfig und Reg-P-Loader,
- *dropbear* - SSH-Server (Version 2015.71),
- *regploader* - nur für TK28-8 Kartentyp, Kommunikation mit REG-P-Loader (Windows-basiertes Programm),
- *regsysupgrader* - Software zur Kommunikation mit dem Regler für die Übertragung von Firmware und UDM-Dateien,
- *viaregsysloader* - nur für den Kartentyp TK28-4, Übertragung der Kommunikationsprotokolleinstellungen mit RegSys-Gerät und Bootloader-Software,
- */bin/sh* - verschiedene Skripte zur Unterstützung der WinConfig-Funktionalität.
- *TLS* Version 1.2

Table 14: Protokollbasierte Daemons und deren Verwendung

	CSO	DNP3	IEC101	IEC104	IEC61850
ser2net	ja	ja	ja	ja	ja
dnp3xreg	-	ja	-	-	-
regx101	-	-	ja	-	-
iec104	-	-	-	ja	-
regx850		-	-	-	ja
regxsv	-	-	-	-	ja

6.1.4 Anmeldung der Fernwirkkarten TK28x und TK102

Es gibt mehrere verschiedene Teile der Fernwirksoftware, welche die Protokollierung unabhängig voneinander durchführen - Systemteile der Software, WebReg und Anwendungsfirmware. Die Einstellung für die Anwendungsprotokollierung finden Sie im Aufsichtsteil der Protokolleinstellungen.

Table 15: Anmeldung im TK28x und TK102 - System

Anmeldung im TK28x und TK102 - System				
Ziel - Format	*Logger (Logread) zum RAM - Linux-ähnliche Textdatei*	*UDP SYSLOG Server - syslog*	*MicroSD - Linux-ähnliche Log-Textdatei*	*Linux-Konsole - Text*
WinConfig Teil / Wo soll eingestellt werden?	*fest programmiert*	*im Online-Web eingestellt (Aufsichtsrat)*	*im Online-Web eingestellt (Aufsichtsrat)*	*fest programmiert*
WinConfig Systemskripte	ja	nein	nein	ja
An- und Abmeldung des Systems (ssh, Konsole, Online-WinConfig-Webserver)	ja	ja	ja	nein
REG-P-LADER (TK28-8 CSO-Anwendung Fernlader)	ja	ja	ja	nein
PTP-Operationen	nein	ja	ja	nein
Aktualisierung der Firmware/Einstellungen	ja	ja	ja	ja
REGSYS-Upgrade (A-Eberle Geräte-Firmware oder UDM-Upgrade)	ja	ja	ja	ja
Sicherheitsmaßnahmen (RBAC, CLIUM, CERTIFICATE, RADIUS)	nein	ja	ja	nein
Änderung der Einstellungen	nein	ja	ja	nein
Änderung der Netzwerkparameter	nein	ja	ja	nein
CPU- und Speicherschwellenwerte	nein	ja	ja	nein
Viaregsysloader (TK28-4 Fernwirkkarteneinstellungen Upload über A-Eberle Gerät)	nein	nein	nein	ja
WebREG	nein	ja	ja	nein

Table 16: Anmeldung in TK28x und TK102 - Protokollanwendungen, WebREG

Anmeldung in TK28x und TK102 - Protokollanwendung, WebREG				
Ziel - Format	*Logger (Logread) zum RAM - Linux-ähnliche Log-Textdatei*	*UDP SYSLOG Server - syslog*	*Roh-TCP - Text*	*Linux-Konsole - Text*
WinConfig Teil / Wo soll eingestellt werden?	*fest programmiert*	*gesetzt im Online-Web (Security GUI)*	*Hardcode - wenn MicroSD mit FAT32-Partition vorhanden ist*	*fest programmiert*
Protokollanwendungen	nein	Einige*	nein	alle (außer CSO)

* alle Anwendungen außer IEC104 und DNP3

Hinweise zur Protokollierung:

1) Der Logger (lokale Protokollierung) stellt die Standard-Linux-Protokollierung in eine Textdatei dar. Die Fernwirkkarten verwenden ramdisk für den Anwendungsbetrieb, so dass lokale Protokolle nach dem Neustart verschwinden. Die lokale Protokolldatei kann über das Shell-Benutzermenü oder den Befehl logread gelesen werden.
2) Das System und der WebReg-Syslog funktionieren in dem Fall, wenn die IP-Einstellung des Syslog-Servers nicht 0.0.0.0 ist oder in der Online-WinConfig leer ist.
3) Der erfolglose Anmeldeversuch wird in jedem Fall lokal protokolliert und im Syslog gemeldet, wenn die IP-Einstellung des Syslog Servers nicht 0.0.0.0 oder leer ist in der Online-WinConfig.
4) Der erfolglose Anmeldeversuch wird auf der microSD protokolliert, falls diese vorhanden ist. Das Protokoll hat die Form einer permanenten Protokolldatei, die über das Shell-Benutzermenü, über cat oder andere Befehle gelesen werden kann. Es kann auch extern in Windows gelesen werden.
5) Alle Protokolldateien sind als runder Puffer organisiert und werden als FIFO gelesen (die Auflistung zeigt die älteste als oberste Zeile auf dem Bildschirm).

6.1.4.1 Speicherung von Protokolldateien in MicroSD

Die Fernwirkkarten TK28x und TK102 können mit einer microSD-Speicherkarte zur lokalen Speicherung von Protokolldateien ausgestattet werden.

Das Boardsystem ermöglicht auch eine erste Systeminitialisierung mittels MicroSD. Die MicroSD kann zu diesem Zweck mit einer Bootpartition und einer Linux-Partition ausgestattet werden. Die Protokollierungssoftware von online WinConfig prüft die MicroSD zunächst auf das Vorhandensein von Partitionen. Die folgenden Situationen können auftreten:

- Wenn keine Partition in der MicroSD vorhanden ist, versucht die Protokollierungssoftware, die Protokollierungspartition zu erstellen.
- Wenn eine Partition vorhanden ist, versucht die Protokollierungssoftware, sie für die Protokollierung zu verwenden.
- Wenn zwei Partitionen vorhanden sind, versucht die Protokollierungssoftware, eine dritte Partition für die Protokollierung zu erstellen.
- Wenn drei oder mehr Partitionen vorhanden sind, versucht die Protokollierungssoftware, die dritte Partition für die Protokollierung zu verwenden.

Alle erfolgreichen oder erfolglosen Versuche werden auf dem syslog-Server protokolliert.

Die Protokolle werden in Protokolldateien mit fester Kapazität und automatischer Erstellungsart gespeichert.

Wenn die Protokolldatei voll ist, speichert die Protokollierungssoftware sie mit dem aktuellen Datum und startet die Protokollierung in eine neue Datei.

Wenn die Protokollierungspartition fast voll ist, wird eine Warnmeldung an den Syslog-Server gesendet. Der Schwellenwert kann in den *Überwachungseinstellungen* in WinConfig online über das Symbol eingestellt werden.

Wenn die gesamte Protokollierungspartition voll ist, wird die älteste Protokolldatei gelöscht.

6.1.4.2 Protokollierungseinstellungen in der Online-WinConfig

Die Protokollierungseinstellungen sind in den Überwachungseinstellungen in WinConfig online über das Symbol verfügbar. Die Protokollierungseinstellungen sind für die Protokollierung von Syslog- und CD-Karten verfügbar. Die Standardwerte der Protokollierungsoptionen werden auf die gängigsten Werte gesetzt.

Table 17: Überwachungseinstellungen in der Online-WinConfig

Einstellung	Format	Bereich	Standard	Beschreibung
Syslog IP	IP-Adresse	4x 0 bis 255	0.0.0.0	IP-Adresse des syslog Servers
Syslog-Anschluss		0 bis 65535	514	Port des syslog Servers
An-/Abmeldung		Kontrollbox	überprüft	Protokollierung der An- und Abmeldung
PTP		Kontrollbox	überprüft	Protokollierung von PTP-Vorgängen

Einstellung	Format	Bereich	Standard	Beschreibung
Firmware/ Einstellungen aktualisieren		Kontrollbox	überprüft	Protokollierung der Upgrade-Firmware/Einstellungen
Aktualisieren der REGSYS-Firmware		Kontrollbox	überprüft	Protokollierung der Aktualisierung der REGSYS-Firmware
Sicherheit (RBAC, CLIUM, CERTIFICATE, RADIUS)		Kontrollbox	überprüft	Protokollierung von Sicherheitsmaßnahmen (RBAC, CLIUM, CERTIFICATE, RADIUS)
Änderung der Einstellungen		Kontrollbox	überprüft	Protokollierung von Einstellungsänderungen
Änderung der Netzwerkparameter		Kontrollbox	überprüft	Protokollierung der Änderung von Netzwerkparametern
CPU-, Speicher- und Festplattenschwellenwerte		Kontrollbox	überprüft	Protokollierung von CPU-, Speicher- und Festplattenschwellenwerten
Einstellungen für das Inaktivitäts-Timeout: Timeout der Konsole	[s]	30 bis 7200	180	Zeitüberschreitung bei Inaktivität der Konsole
Einstellungen für das Inaktivitäts-Timeout: Web-Timeout	[min]	5 bis 20	1800	Zeitüberschreitung bei Webinaktivität
Einstellungen für das Inaktivitäts-Timeout: RADIUS-Zeitraum	[s]	60 bis 7200	300	Zeitraum, in dem nach dem Vorhandenseins eines RADIUS Servers überprüft wird
Festlegung von Schwellenwerten: Zeitraum	[s]	30 bis 1800	60	Überprüfung des Zeitraums der Schwellenwerte
Festlegung von Schwellenwerten: CPU-Schwellenwert	[%]	50 bis 99	90	CPU-Schwellenwert
Festlegung von Schwellenwerten: Speicherschwelle	[%]	50 bis 99	90	Speicherschwelle
Einstellungen der SD-Karte: Kapazität der Protokolldatei	[MB]	1 bis 3000	90	Kapazität der Protokolldatei
Einstellungen der SD-Karte: Grenzwert für die Protokollspeicherung	[Tage]	1 bis 30	30	Grenzwert für die Protokollspeicherung

Einstellung	Format	Bereich	Standard	Beschreibung
Einstellungen der SD-Karte: Begrenzung des genutzten Platzes	[%]	50 bis 99	90	Begrenzung des genutzten Platzes für die Warnung
SNMP: Als Startup aktivieren		Kontrollbox	überprüft	SNMP-Aktivierung bei der In-betriebnahme
Port		0 bis 65535	161	Port des SNMP-Clients
Benutzer		Textfeld 8-32		Identifizierung des Benutzers
Authentifizie-rungsschlüssel Verschlüsselungs-verfahren		8 bis 32 Zeichen Listbox (MD5, SHA)	SHA	Authentifizierungsschlüssel Verschlüsselungsverfahren
Verschlüsselungs-code Verschlüsselungs-verfahren		8 bis 32 Zeichen Listbox (DES, AES)	DES	Verschlüsselungscode Verschlüsselungsverfahren

HINWEIS!

Notizen:

Die CPU-Last im Linux-System wird als Auslastung des Prozessors durch Prozesse berechnet. Dieser Wert wird in WinConfig auf einen Prozessorkern neu berechnet. Der Wert beinhaltet aktive Prozesse und auch Prozesse, die in einer Warteschlange warten, so dass auch Werte über 100% auftreten können und eine gültige Zahl darstellen.

Weitere Informationen zu den Schwellenwerten im Linux-System finden Sie in den folgenden Referenzen:

https://www.tecmint.com/understand-linux-load-averages-and-monitor-performance/

http://www.brendangregg.com/blog/2017-08-08/linux-load-averages.html

Verwendung von SNMP:

Die Implementierung des Simple Network Management Protocol (SNMP) unterstützt die Version v3: Die verfügbaren Knoten und Daten werden in einer internen Konfigurationsdatei (snmpd.conf) definiert. Die Daten können von der Karte gelesen (geholt) werden, z.B. mit dem MIB Browser Tool.

Das SNMP ist standardmäßig deaktiviert. Verwenden Sie WinConfig online, um SNMP auf dem Board zu aktivieren und Benutzer, Verschlüsselungsmethoden und Schlüssel festzulegen. Die Änderungen werden intern in die Konfigurationsdatei geschrieben. Setzen Sie die Karte zurück, wenn erforderliche Änderungen vorgenommen wurden.

Die verfügbaren Daten können aus den folgenden MIB-Klassen gelesen werden:

- System von SNMPv2-MIB [.1.3.6.1.2.1.1]
- Schnittstellen aus IF-MIB [.1.3.6.1.2.1.2]

Für weitere Informationen siehe z.B.

http://www.net-snmp.org/docs/man/snmpd.conf.html

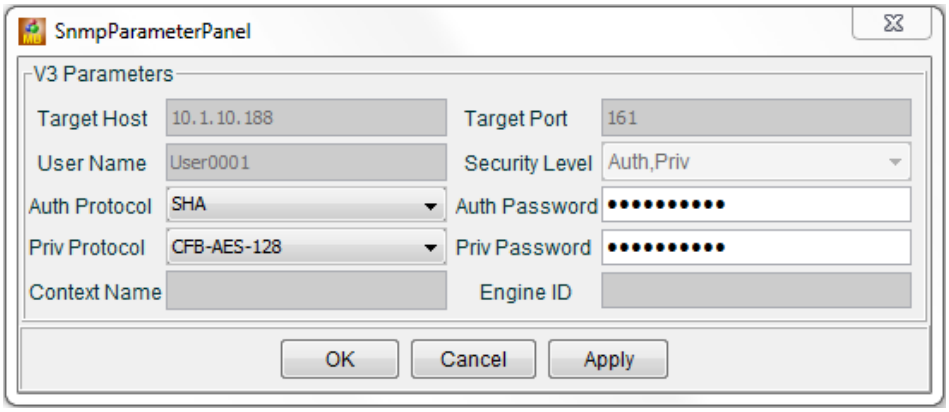


Figure 3: Definition von SNMP-Verbindungsparametern im MIB Browser

N.B.: Eine Liste aller implementierten MIBs ist auf im REGCOMMS Downloadbereich tagesaktuell verfügbar.

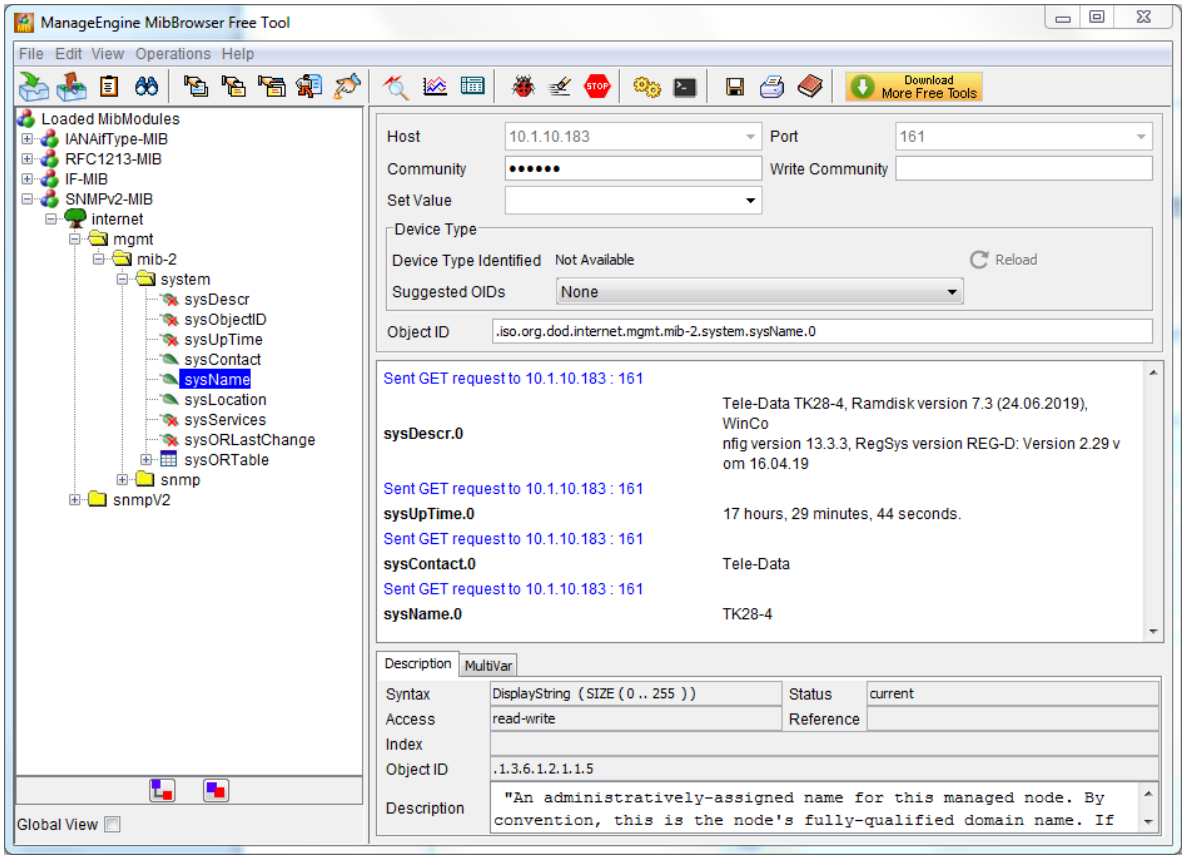


Figure 4: Abrufen der SNMP-Daten im MIB Browser

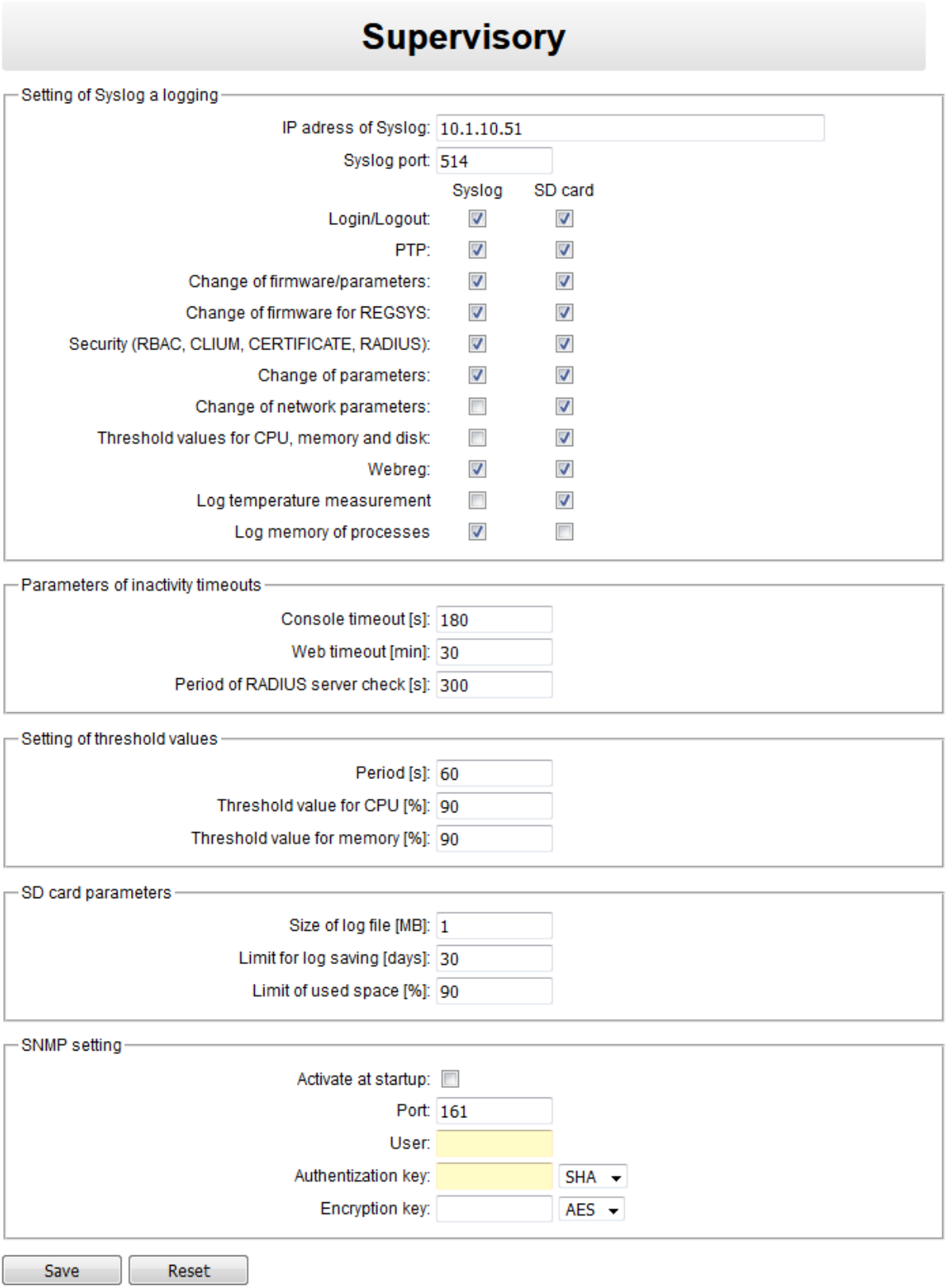


Figure 5: Überwachungseinstellungen in der Online-WinConfig

6.2 REG-PEX Loader Software

Der REG-PEX Loader (RPL) ist ein Softwaretool zur Übertragung von Linux-Kernel und RAM-Disk in die REG-PE(D) (nur TK8xx-Modelle) und PQI-DA Fernwirkkarten, die nur mit der U-Boot-Software ausgestattet sind. Diese Boards können nicht direkt mit WinConfig zusammenarbeiten. Die RPL ermöglicht auch die Änderung der IP-Einstellungen der Karte und die Auswahl des Kernels mit/ohne Verbindungs-Funktion.

Der RPL ist ein Low-Level-Softwaretool und sollte nur von erfahrenen Benutzern verwendet werden.

Die RPL-Software ist im WinConfig-Installationspaket enthalten und kann über die Seite *Transfer from PC über die* Schaltfläche *Run RPL* gestartet werden. Die WinConfig bietet auch den Start von RPL für den Fall, dass keine REG-PE(D) Fernwirkkarte erkannt wird.

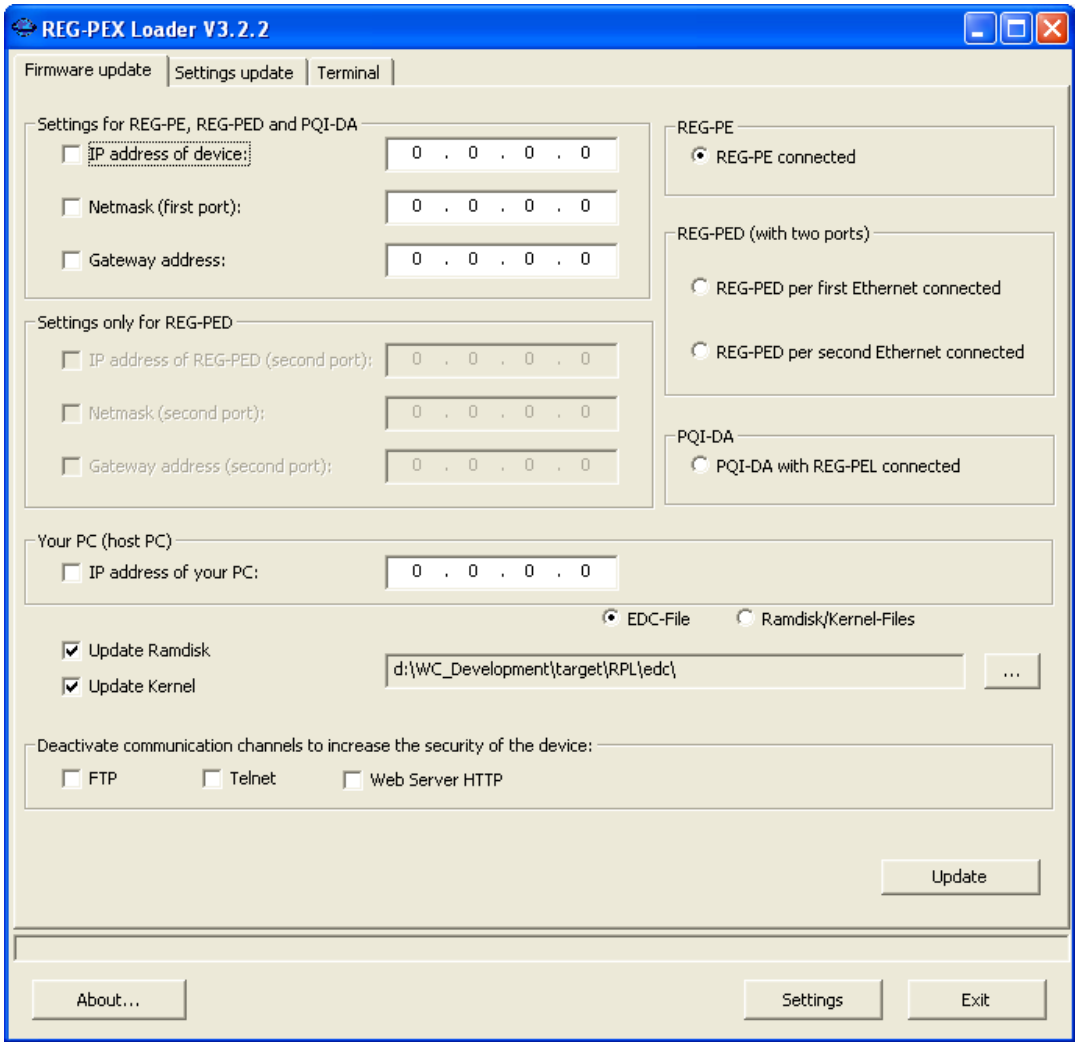


Figure 6: Das RPL-Fenster

Um den Linux-Kernel und die RAM-Disk in den REG-PE(x) zu übertragen, gehen Sie wie folgt vor:

- Verbinden Sie den PARAM-connector der REG-PE(x)-Karte und Ihren Computer mit dem mit dem beim A-Eberle-Gerät mitgelieferten RS232-Kabel oder einem seriellen Nullmodemkabel.
- Verbinden Sie Ihren Computer und die REG-PE(x)-Karte über ein Ethernet-Kabel. Einige Ethernet-Adapter schalten nicht automatisch in den richtigen Modus, daher verwenden Sie bitte vorzugsweise ein Crosslink-Patchkabel.
- Füllen Sie die IP-Adresszeilen im RPL-Fenster aus.
- Verwenden Sie die Schaltfläche (....), um die edc-Datei zu durchsuchen, die sich in den WinConfig-Installationsordnern befindet. Es gibt zwei edc-Dateien, die im WinConfig-Setup verteilt sind, der Unterschied liegt in den Versionen von Kernel - mit/ohne Unterstützung von Verbindungen. Wählen Sie eine beliebige der beiden Dateien als Verbindung aus und verwandte Funktionen können später über die Funktion *Change of IP settings for REG-PE(D) fernwirktechnische Karten* WinConfig eingestellt werden.
- Drücken Sie die Aktualisieren-Taste.

  ↳ Der Updateprozess ist in der Registerkarte RPL Terminal zu sehen.

6.3 Kommunikation mit der Fernwirkkarte REG-P(E)(D)(SV) in WinConfig 11

In WinConfig v.11 wird ein höheres Maß an Sicherheit für die Datenübertragung und Kommunikation mit der Fernwirkkarte REG-PE(D) verwendet. Die Online-WinConfig (www-Seiten im Speicher der Karte) kann in der Seite *Übertragungseinstellungen vom PC* in offline WinConfig oder in der Seite *REG-PE(D) IP-Einstellungen der Karte* in online WinConfig oder im Benutzermenü deaktiviert werden.

Die neue Firmware unterstützt mehrere Funktionen, wie nachfolgend beschrieben.

Die folgenden gesicherten Kommunikationstechnologien werden in WinConfig 11 eingesetzt:

- SSH wird für den Fernzugriff auf die Konsole verwendet. Dieser Zugriff wird typischerweise für die Grundkonfiguration der Karte verwendet. Für diese Art der Verbindung ist ein SSH-Client (z.B. PUTTY) erforderlich.
- HTTPS (HTTP over SSL) wird zusammen mit SSL-Zertifikaten für die Kommunikation zwischen Offline WinConfig und Fernwirkkarte verwendet.

HINWEIS!	Hinweis zur Funktionalität von HTTPS-Konten beim Upgraden/Downgraden von/auf WinConfig 10 Bei einem Benutzer-Upgrade von WinConfig 10 auf 11 mit Offline WinConfig wird eines der HTTPS-Konten (Benutzername und Passwort) aus Version 10 (Passwörter, die von XOR, nicht von SHA2-Hash kodiert werden) verwendet. Die in der von XOR kodierten Version 10 definierten Konten bleiben in der aktualisierten Version 11 erhalten. Das individuelle Konto wird in dem Moment auf die neue SHA2-Codierversion umgestellt, in dem der Benutzer dieses Konto in der WinConfig 11 ändert. Die Datei mit SHA2-kodierten Konten bleibt beim Downgrade von Version 11 auf Version 10 in der Fernwirkkarte. Offline WinConfig 10 mit XOR-Passwortkodierung funktioniert in diesem Fall nicht. Um diese Situation zu lösen, kann der Benutzer die Konten über den FTP- oder seriellen PARAM-Port ändern oder die Kontodatei /mnt/jffs2/config/webs_users.conf löschen. Wenn die Datei gelöscht wird, wird das Standardkonto verwendet.

6.3.1 Regeln für mehr Sicherheit

Es wird dringend empfohlen, mindestens das Online-WinConfig auszuschalten und die werkseitigen Standardpasswörter zu ändern, um höchste Sicherheit für Daten und Software zu gewährleisten, die in der Fernwirktechnik gespeichert sind.

Der Benutzer sollte auch alle Netzwerkdienste deaktivieren, die für den Betrieb und die Verwaltung der Karte nicht erforderlich sind, nämlich SSH und HTTPS (WinConfig).

HINWEIS!	Beachten Sie bei der Erstellung eines neuen Benutzerkennworts auch die Grundregeln für sichere Kennwörter: ➲ Das Passwort sollte mindestens 8 Zeichen lang sein. ➲ Verwenden Sie mindestens einen Groß- und mindestens einen Kleinbuchstaben (A...Z, a...z). ➲ Verwenden Sie mindestens eine Zahl (0....9). ➲ Verwenden Sie mindestens ein Sonderzeichen @%,./!:;=^~-_. Andere Zeichen sind nicht erlaubt.

Für weitere Informationen über sichere und sichere Passwörter empfehlen wir die BSI-Webseiten im Internet (https://www.bsi.bund.de/EN).

6.3.2 Von der Firmware unterstützte Aktionen und deren Verwendung:

Neustart der Karte

- Bereiten Sie eine leere Datei namens *reboot* vor und kopieren Sie diese in den Ordner */xload/new*.
- Warten Sie ca. 20 Sekunden auf den automatischen Neustart der Karte.

Installation neuer XML-Einstellungen und ICD-Datei

- Bereiten Sie eine neue Einstellungsdatei namens *settings.xml* vor und kopieren Sie diese in den Ordner */xload/new*.
- Neue ICD-Datei vorbereiten (falls ein ICD-Wechsel erforderlich ist) und in den Ordner kopieren.
- Bereiten Sie eine leere Datei namens move vor und kopieren Sie diese.
- Warten Sie ca. 20 Sekunden auf das automatische Verschieben und Installieren der Dateien.
- Bereiten Sie eine leere Datei namens *reload* vor und kopieren Sie diese.
- Warten Sie ca. 20 Sekunden, bis die in der vorherigen Reihenfolge übertragenen Dateien automatisch neu geladen wurden. Der Reload kann nur dann verwendet werden, wenn sich die Überwachungsparameter geändert haben. Andernfalls verwenden Sie den *Neustart*, siehe Punkt 1.

Installation neuer Zertifikate

- Gerätezertifikat in der Datei *cert.pem* vorbereiten und in den Ordner */xload/new* kopieren. Das Zertifikat muss im PEM-Format vorliegen.
- Bereiten Sie auch den Schlüssel als *key.*pem-Datei vor und kopieren Sie diese.
- Bei Bedarf erstellen und kopieren Sie auch die Zwischenzertifikate als *intercert.*pem-Datei. Die Zertifikate müssen im PEM-Format vorliegen und vom Zertifikat bis zur obersten Stufe (Root CA) sortiert sein.
- Alternativ kann das CA-Zertifikat auch als *cacert.*pem-Datei kopiert werden.
- Bereiten Sie eine leere Datei namens cert_move vor und kopieren Sie diese in den Ordner */xload/new*.
- Starten Sie die Karte neu, siehe erster Punkt.

6.3.3 SSH-Zugang (REG-PEx, TK102, TK28x)

SSH wird für den Fernzugriff auf die Konsole verwendet. Die Dateiübertragung ist verschlüsselt und durch Benutzerlogin und Passwort geschützt.

Bei den Fernwirkkarten REG-PE(D) kann die *Fernwirkkarte* mit dem Fernwirkkennwort verwendet werden.

Der Zugriff wird durch die Reihenfolge des Benutzermenüs gesteuert, das es dem Benutzer ermöglicht, die Boardeinstellungen anzuzeigen und/oder zu ändern, um Protokolle von Kernel, System und Anwendungen anzuzeigen.

Die Menüführung wird entsprechend der aktuellen Benutzerrolle und den Rechten angepasst.

6.3.4 Menü und Bedeutung der einzelnen Punkte

Hauptmenü

Netzwerk-Menü

➲ *Gehen Sie zum Menü für Netzwerkeinstellung und Diagnose.*

Menü Dienste

➲ *Gehen Sie zum Menü Verwaltung von Netzwerkdiensten (SSH/SFTP, HTTPS).*

Protokoll-Menü

➲ *Zum Menü mit den Protokollen gehen*

Terminalpasswort ändern

➲ *Änderung der SSH- und SFTP-Passwörter. Die Änderung wird auf den aktuell angemeldeten Benutzer angewendet. Das Programm fragt nach der Eingabe des alten und zwei Mal nach dem neuen Passworts. Achtung, eine Änderung wird sofort übernommen.*

Ersatz-Passwort ändern

➲ *Diese Option ermöglicht eine zusätzliche Möglichkeit, das Ersatz-Passwort zu ändern. Der Name* ***Spare password*** *spiegelt auch die mögliche Änderung des Modusnamens wider, d.h. der korrekte Name erscheint in dieser Option, wenn der Name geändert wurde.*

HTTPS-Benutzerverwaltung

➲ *Zur Verwaltung von HTTPS-Benutzern (Offline WinConfig) gehen*

Abmeldung

➲ *Terminal-Abmeldung*

Neustart

➲ *Fernwirkkarte neu starten*

Wiederherstellungsmenü

➲ *Wechseln Sie in den Wiederherstellungsmodus. Dieser Menüpunkt wird nur bei Zugriff über die lokale serielle Schnittstelle angezeigt. Eine weitere Bedingung ist, dass die*

Karte für den Wiederherstellungsmodus vorbereitet sein muss (die Taste R wird gerade gedrückt oder eine Wiederherstellungsanzeige während des Kartenneustarts).

Root Shell starten

➲ *Die Root-Shell ist nur für Administratoren bestimmt und steht für Remoteuser und Localuser nicht zur Verfügung.*

Netzwerk-Menü

Ping ICMP

➲ *Der ICMP-Ping wird für die Diagnose der Netzwerkverbindung bestimmt. Das System fragt nach der IP der Gegenpartei. Es wird das ICMP Echo-Request-Paket verwendet. Die Benutzer-Netzwerk-Schnittstelle wird durch eine Routingtabelle bestimmt.*

Ping ARP

➲ *Der ARP-Ping wird für die Diagnose der Netzwerkverbindung innerhalb eines Subnetzes bestimmt. Das System fragt nach der Gegenpartei-IP und, wenn es mehr Netzwerkschnittstellen (TK885) gibt, nach der Verwendung der Schnittstelle. Dieser Ping geht normalerweise durch die Firewall. Das ARP-Protokoll wird nicht an andere Netzwerke weitergeleitet.*

Routingtabelle anzeigen

➲ *Zeigt die aktuelle Routingtabelle an.*

Schnittstellen anzeigen

➲ *Zeigt die aktuelle Liste der Netzwerkschnittstellen mit Parametern (IP-Adresse, Maske, MAC-Adresse und Statistik der gesendeten und empfangenen Daten).*

Anzeige der gespeicherten Netzwerkparameter (IP-Adressen, Verbindung)

➲ *Zeigt die im Flash-Speicher gespeicherten Netzwerkparameter (IP-Adresse, Maske, Gateway, Zustand der Verbindung) an. Diese Parameter werden nach dem Neustart der Karte verwendet.*

Netzwerkparameter einstellen (IP-Adressen, Verbindung)

➲ *Einstellung der Netzwerkparameter (IP-Adresse, Maske, Gateway, Zustand der* Verbindung*) als eine Reihe von Fragen und Antworten gelöst. Mögliche Optionen der Verbindungsparameter:*

1. *Deaktiviert*
2. *PRP V1*
3. *Broadcast-Modus*
4. *Brücke mit RSTP*

Zurück

➲ *Gehen Sie zum Hauptmenü.*

Menü Dienste

Status der Dienstleistungen

➲ *Zeigt den Status von SSH/SFTP- und HTTPS-Diensten (aktiviert oder deaktiviert) an.*

SSH/SFTP aktivieren

➲ *Aktiviert den SSH/SFTP-Dienst. Die Änderung wird nach dem Neustart der Karte wirksam.*

SSH/SFTP deaktivieren

➲ *Deaktiviert den SSH/SFTP-Dienst. Die Änderung wird nach dem Neustart der Karte wirksam.*

WinConfig aktivieren (https, Netzwerkerkennung)

➲ *Ermöglicht Dienste, die für die Kommunikation mit Offline WinConfig erforderlich sind. Die Änderung wird nach dem Neustart der Karte wirksam.*

WinConfig deaktivieren (https, Netzwerkerkennung)

➲ *Deaktiviert Dienste, die für die Kommunikation mit Offline WinConfig erforderlich sind. Die Änderung wird nach dem Neustart der Karte wirksam.*

WinConfig WWW-Seiten aktivieren

➲ *Aktiviert WinConfig WWW-Seiten.*

WinConfig WWW-Seiten deaktivieren

➲ *Deaktiviert WinConfig WWW-Seiten.*

Zurück

➲ *Gehen Sie zum Hauptmenü.*

HINWEIS!	Achtung: Wenn sowohl SSH/SFTP- als auch HTTPS-Zugriffe deaktiviert sind, ist es nicht möglich, die Karte fernzuschließen. Der lokale Zugriff über den PARAM-Port ist in diesem Fall nur möglich.

Protokoll-Menü

Anwendungs- und Systemprotokollierung

➲ *Zeigt das Protokoll mit Meldungen vom System und von Benutzeranwendungen an.*

Kernel-Protokoll

➲ *Zeigt ein Protokoll mit Meldungen des Systemkerns an.*

Zurück

➲ *Gehen Sie zum Hauptmenü.*

Verwaltungsmenü des HTTPS-Benutzers

Benutzer auflisten

➲ *Zeigt eine Liste der Benutzerkonten für den HTTPS-Dienst (Benutzer von Offline WinConfig) an.*

Benutzerpasswort ändern

➲ *Ändert das Benutzerpasswort. Der Dienst fragt nach dem alten Passwort und zwei Mal nach dem neuen Passwort.*

↳ Die Änderung wird nach dem Neustart der Karte wirksam.

Neuen Benutzer hinzufügen

➲ *Fügt ein neues Benutzerkonto hinzu. Der Dienst fragt nach einem neuen Kontonamen und zwei Mal nach einem Passwort.*

↳ Die Änderung wird nach dem Neustart der Karte wirksam.

Benutzer löschen

➲ *Löscht ein bestehendes Benutzerkonto. Der Dienst fragt nach dem Namen des vorhandenen Benutzerkontos.*

↳ Die Änderung wird nach dem Neustart der Karte wirksam.

Zurück

➲ *Gehen Sie zum Hauptmenü.*

Wiederherstellungsmenü

Neustart und Formatierung von Anwendungen im Rahmen der Firmware

➲ *Setzt das Formatierungskennzeichen und führt einen Kartenreset durch.*

HINWEIS!	Achtung: Dieser Dienst formatiert den jffs2-Bereich ohne die Möglichkeit einer Wiederherstellung. Dieser Service ist nur für Notfallsituationen bestimmt, in denen das Board festsitzt und es keine andere Möglichkeit der Reparatur gibt. Das Offline WinConfig kann somit für die Übertragung neuer Firmware verwendet werden.

Zurück

➲ *Gehen Sie zum Hauptmenü.*

6.3.5 Übertragung von Einstellungen von / zu einem PC

Folgende Möglichkeiten der Datenübernahme stehen zur Verfügung:

- Serielle Übertragung über A-Eberle-Gerät (z.B. REG-D-Regler) mit serieller Booter-Firmware, die im Speicher der Fernwirkkarte gespeichert ist (verfügbar für die Karten TK5xx, TK400 und TK28-4).
- Ethernet-TCP-Übertragung mit Hilfe der im Fernwirkkartenspeicher gespeicherten Ethernet-Booter-Firmware (verfügbar für TK400-Boards). Die Ethernet-Übertragung kann im lokalen Modus mit manuellem Kartenreset oder im Remote-Modus mit automatischem Reset verwendet werden (verfügbar für Fernwirkkarten TK400 mit installierter COM-SERVER- oder CSO-Firmware).
- Ethernet HTTPS-Übertragung (verfügbar für Fernwirkkarten TK8xx, TK28x und TK102) auch im Offline- und Online-Modus.

Übertragen der Einstellungen des Kommunikationsprotokolls vom PC aus

Die Übertragung vom PC zur Fernwirkkarte kann je nach Fernwirkkartentyp und Anwendungsprogramm auf folgende Weise durchgeführt werden:

- Übertragung über eine serielle Verbindung des A-Eberle-Gerätes für Fernwirkkarten der Typen TK28-4, TK517, TK509 und TK400 durch *manuelle Übertragung mit der PC-Taste. Der* Benutzer muss die COM-Port-Nummer des angeschlossenen PCs eingeben und das A-Eberle-Gerät und die Fernwirkkarte manuell in den seriellen Down-/Upload-Zustand versetzen, bevor die Übertragung beginnen kann.
- Übertragung über lokale Ethernet-Verbindung für den Kartentyp TK400 durch *manuelle Übertragung mit der* PC-Taste. Die Fernwirkkarte muss manuell durch einen Reset-Taster auf der TK400-Karte zurückgesetzt werden, um den Ethernet-Booter zu betreiben, so dass diese Art der Datenübertragung nur dann möglich ist, wenn der Benutzer Zugriff auf das A-Eberle-Geräterack hat. WinConfig erkennt automatisch das manuelle Rücksetzen der Fernwirkkarte und wählt automatisch die freie IP-Adresse innerhalb des angegebenen Subnetzes, wenn die aktuelle IP-Adresse der Fernwirkkarte nicht für die Verbindung mit dem Ethernet-Booter verwendet werden kann. IP-Einstellungen für die TCP-Verbindung mit Ethernet-Booter werden nur für die aktuelle TCP-Sitzung verwendet. Bei der manuellen Ethernet-Übertragung muss zuerst die WinConfig-Funktion gestartet und dann die TK400-Karte zurückgesetzt werden, damit das WinConfig-Programm den Start des Ethernet-Booterprogramms erkennen kann.
- Übertragung per Fernzugriff über Ethernet-Verbindung mit COM-Server auf dem Remote-PC und Ethernet-Booter-Anwendungsprogramme für den TK400 durch *Fernzugriff von der* PC-Taste. Wenn die aktuelle IP-Adresse der Fernwirkkarte außerhalb des sichtbaren Subnetzes liegt, wählt das Programm automatisch die freie IP-Adresse innerhalb des angegebenen Subnetzes für die Verbindung mit dem Ethernet-Booter. Der Kartenreset wird in diesem Fall automatisch durchgeführt, so dass diese Art der Datenübertragung für den entfernten Einsatz vorgesehen ist. IP-Einstellungen für die TCP-Verbindung mit Ethernet-Booter werden nur für die aktuelle TCP-Sitzung verwendet. Diese Methode ist für das DNP-Protokoll nicht verfügbar. Die Erkennung der verfügbaren Karten muss durchgeführt werden, bevor die Fernübertragungsfunktion aktiviert werden kann.

- Ferngesteuerte Übertragung vom PC über Ethernet mit dem HTTPS-Protokoll für REG-P (TK28-4), REG-PE (TK28-6) und REG-PED^{SV} (TK102) Fernwirkkarten durch *Ferngesteuerte Übertragung mit der* PC-Taste.

  Die Erkennung der verfügbaren Karten muss durchgeführt werden, bevor die Fernübertragungsfunktion aktiviert werden kann. Die Erkennung der verfügbaren Fernwirkkarten erfolgt durch UDP-Broadcast-Telegramme mit UDP-Port 12000 und einem für die Erkennung entwickelten proprietären Protokoll. Die Datenfernübertragung erfolgt über das HTTPS-Protokoll nach erfolgreicher Benutzer-Vorauthentifizierung entsprechend dem Login-Modus.

  Die UDP-Kommunikation ist durch AES256 für Fernwirkkarten vom Typ TK28x und TK102 verschlüsselt.

  Der Erkennungsalgorithmus ermittelt, ob von einigen der aktiven Network Interface Controllers (NIC) auf dem Benutzer-PC auf die IP-Adresse und Maske der Fernwirkkarte zugegriffen werden kann, ob eine Verbindung der Karte über HTTPS möglich ist und ob es sich um eine erste Verbindung zur Karte nach der Werksinitialisierung handelt (bei den Kartentypen TK28x und TK102).

  Weitere Informationen finden Sie in Kapitel 6.5.4 Einstellungen von der PC-Funktion für Fernwirkkarten Typ REG-PE(D), TK28 und TK102 übernehmen.

In allen Fällen der Datenübertragung werden Fortschrittsanzeige, Bedienschritt und Statusinformationen auf dem Bildschirm angezeigt.

Übertragung von der Fernwirkkarte zum PC

Die Übertragung zum PC (Lesen der Einstellungen von der Fernwirkkarte) kann ähnlich wie die Übertragung vom PC erfolgen:

- Manuelle Übertragung über die serielle Schnittstelle des A-Eberle-Gerätes für die Leiterplattentypen TK28-4, TK517, TK509 und TK400
- Manuelle und lokale Übertragung über Ethernet für den Kartentyp TK400
- Ferngesteuerte Übertragung über Ethernet mit *COM-Server* und Ethernet-Booter-Anwendungsprogrammen für TK400
- Ferngesteuerte Übertragung über Ethernet mit HTTPS-Protokoll für die Kartentypen TK8xx, TK28x und TK102.

Die Benutzeraktionen für die Übertragung auf den PC sind vergleichbar mit denen für die Übertragung vom PC.

HINWEIS!	Wichtiger Hinweis: Bei der Übertragung von Einstellungen vom PC auf die Fernwirkkarte werden diese immer zusammen mit der entsprechenden Anwendung (Protokollkonverter, Firmware), mit online WinConfig (Webseiten etc.) für REG-PE(D)-Karten und auch zusammen mit RAMdisk und Kernel für REG-PE(D)-Karten (optional wählbar) übertragen. So zeigt die von WinConfig nach erfolgreicher Datenübertragung durchgeführte Fernerkennung (Detect on LAN) sowohl die Version der Anwendung (Protokoll, Firmware) als auch die Version von

WinConfig, die ebenfalls auf die Fernwirkkarte übertragen wurde. Die Einstellungsdatei hat die gleiche Versionsnummer wie WinConfig.

Wenn die Verifizierung der digitalen Signatur für die Karten TK28x und TK102 bei der Übertragung von Einstellungen aus dem Offline-WinConfig fehlschlägt, wird der Fehler über die angeschlossene Fernwirkkarte in syslog protokolliert. Für diese Funktionalität ist eine korrekte Einstellung der Protokollierung zu syslog in den Einstellungen der Fernwirkkarte erforderlich.

6.4 Serielle Datenübertragung für REG-P Fernwirkkarten TK5xx, TK400

Für die serielle Datenübertragung muss der Leitungstyp *Serial via A-Eberle Device* und *Serial Port Number* ausgewählt werden. Verwenden Sie ein vollständiges Modemkabel und folgen Sie den Anweisungen auf dem Bildschirm.

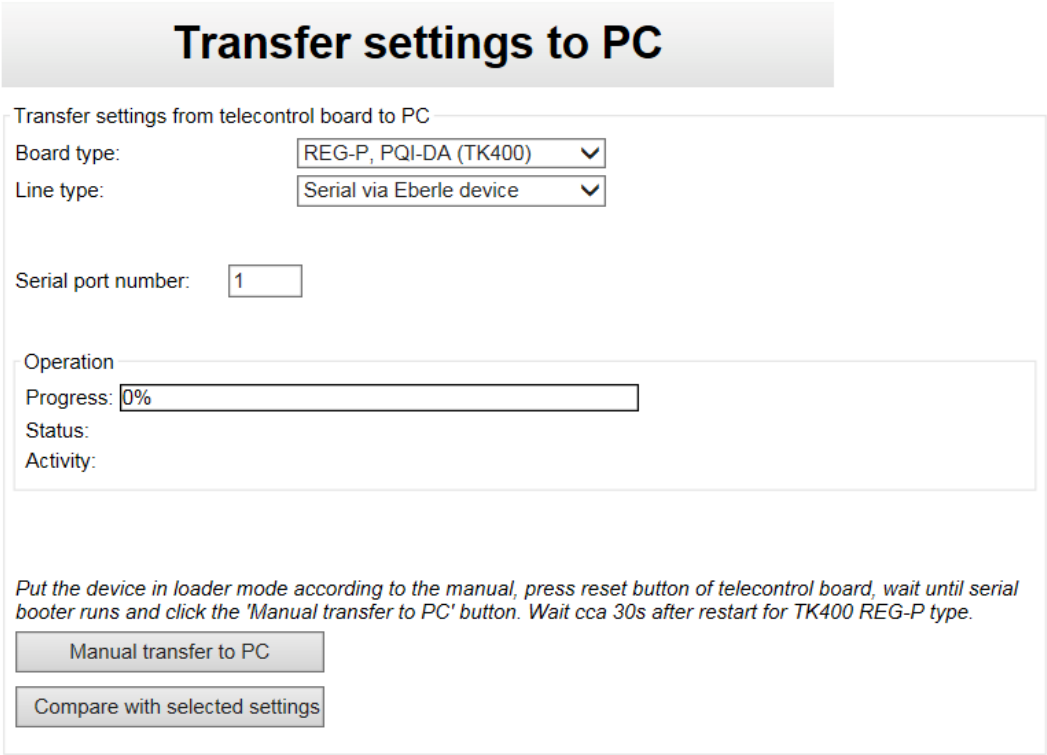


Figure 7: Serielle Datenübertragung, REG-P

Bei Problemen mit der seriellen Übertragung, wenn der USB/Seriell-Konverter in Ihrem PC verwendet wird, können nach Anklicken der Schaltfläche Hinweise zur möglichen Lösung des Problems in einem anderen Browserfenster angezeigt werden.

Das Wichtigste ist, den Parameter Latenztimer auf 1 zu setzen.

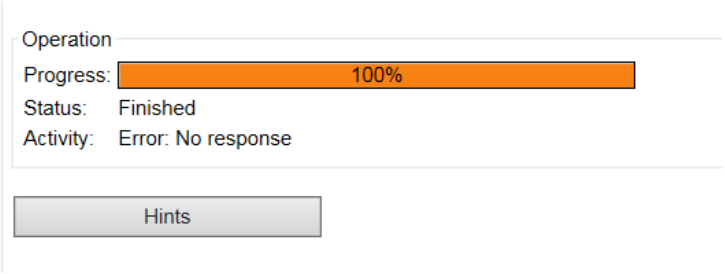
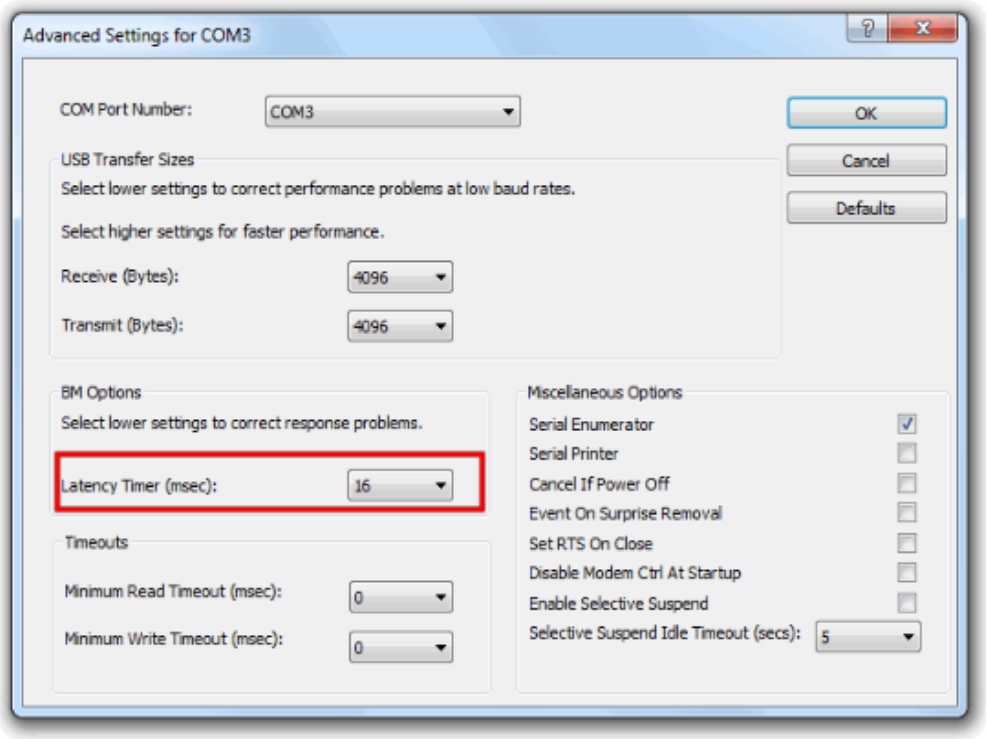
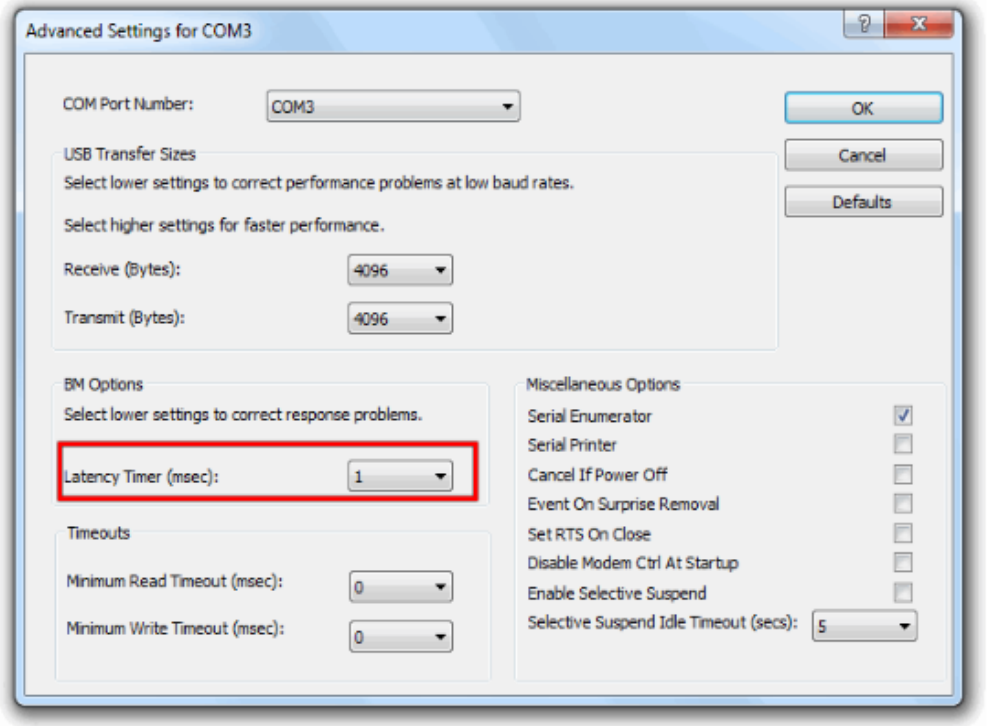


Figure 8: Schaltfläche Hinweise



Select Latency parameter



Change value to 1

Figure 9: Hinweise zur seriellen Übertragung

6.4.1 Serielle Datenübertragung für REG-P Fernwirkkarte TK28-4

Die serielle Datenübertragung für das TK28-4 Board bietet aufgrund des Linux-Betriebssystems mehr Möglichkeiten.

- Die Übertragung von Linux-Systemdateien und Standardanwendungen (CSO) kann je nach Geräteprozessortyp zeitaufwändig sein.
- Die Übertragung von Anwendungen und Einstellungen ist die häufigste Übertragung mit gesicherter Kompatibilität beider Dateien.
- Die Übertragung von Einstellungen sollte nur dann verwendet werden, wenn sichergestellt ist, dass die auf der Karte aufgezeichnete Protokollanwendung mit den neuen Einstellungen kompatibel ist.

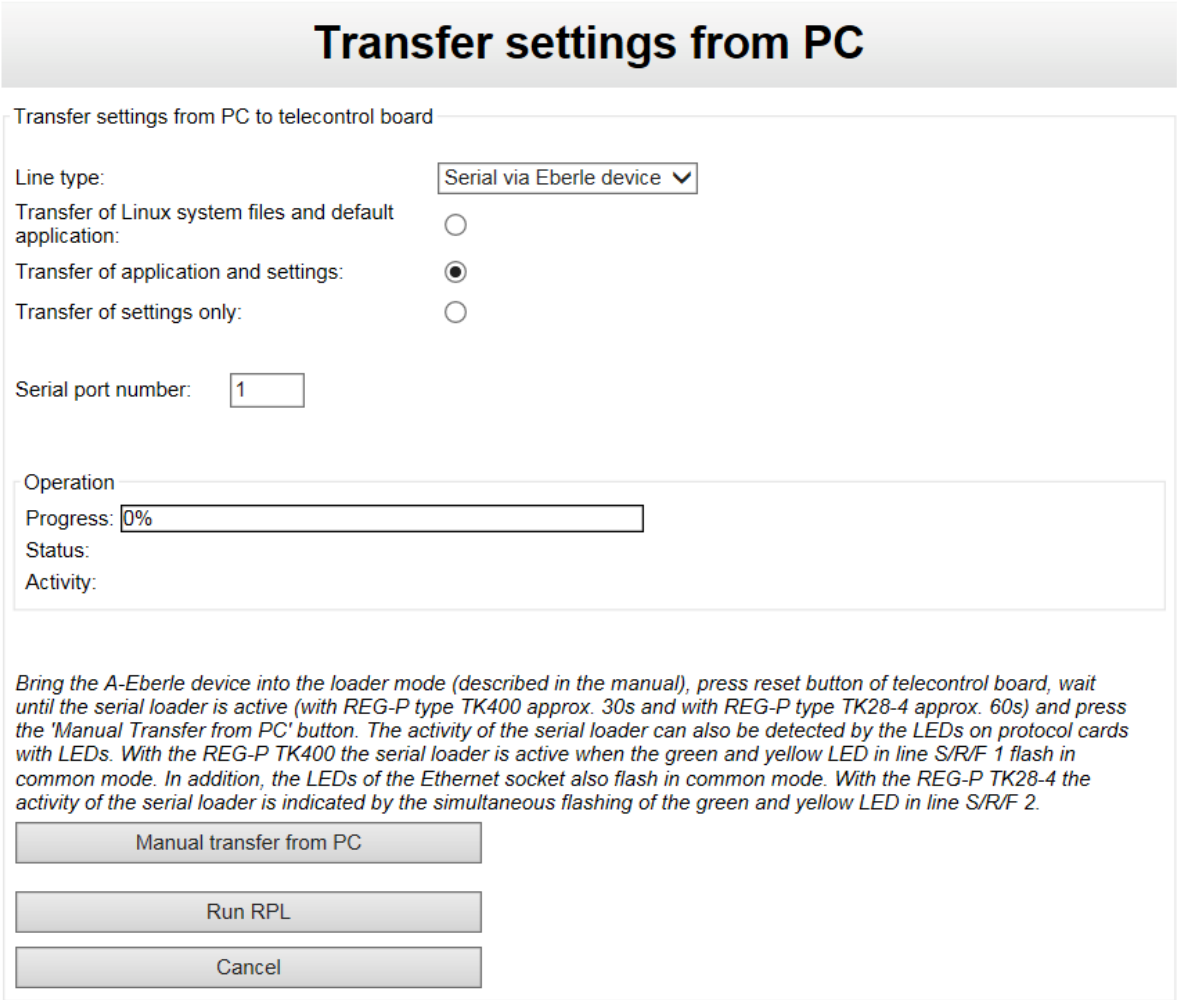


Figure 10: Serielle Datenübertragung, TK28-4

Wenn das Update von Linux-Dateien (Ramdisk) wünschenswert ist, wählen Sie zuerst die erste Option und damit die zweite Option mit der gewünschten Protokollanwendung.

6.5 Ethernet-Datenübertragung

6.5.1 Fernwirkkarte TK400

Die Erkennung der Karte erfolgt durch das COM-Server-Programm (CS oder CSO), das aktiviert werden muss und im Kartenspeicher läuft. Remote-Operationen ohne CS können nicht durchgeführt werden, solange noch eine manuelle Ethernet-Übertragung verfügbar ist.

Ethernet-Operationen sind für das DNP3-Protokoll nicht verfügbar.

Die Datenübertragung von/zu der Karte erfolgt über das Ethernet-Booterprogramm NBOOT, das nach dem Kartenreset läuft. Temporäre Änderung der IP-Einstellungen gilt auch für NBOOT.

6.5.2 Fernwirkkarten REG-P (TK28-4), REG-PE (TK28-6, TK860) und REG-PED^{SV} (TK102, TK885)

Es wird empfohlen, die IP-Adresse des PCs zu ändern, wenn die IP-Adresse der Karte außerhalb des für den PC zugänglichen Adressbereichs liegt.

Für die Fernwirkkarten TK8xx ist es jedoch auch möglich, die WinConfig die Adresse der Fernwirkkarte temporär ändern zu lassen. Die temporäre Änderung der IP-Einstellungen kann für eine oder zwei Kartenschnittstellen gelten, je nach IP-Konfiguration der Karte und des angeschlossenen PCs. Die ursprünglichen IP-Einstellungen der Karte werden nach erfolgreicher Datenübertragung oder nach ca. 5 Minuten Timeout bei einem Verbindungs-abbruch während der Übertragung automatisch erneuert. Beachten Sie, dass diese Option nur für TK8xx-Karten gilt.

Das auf dem Bord laufende Anwendungsprotokoll wird während der Übertragung unterbrochen.

Die Datenübertragung von/zu den Karten TK8xx, TK28x und TK102 erfolgt über ein gesichertes HTTPS-Protokoll.

Übersicht über die Fälle, in denen keine Ethernet-Datenübertragungen durchgeführt werden können:

- Die Fernwirkkarte ist über ein LAN mit einem Router oder einer Firewall verbunden, wodurch verhindert wird, dass von WinConfig verwendete Telegramme durchgelassen werden.
- Der PC, auf dem WinConfig läuft, verfügt über zwei oder mehr Ethernet-Schnittstellen, die an das gleiche Subnetz angeschlossen sind.
- Im angeschlossenen Subnetz gibt es keine freie IP-Adresse, die für die Neuadressierung der Ethernet-Schnittstelle der Fernwirkkarte verwendet werden kann.
- Die Ethernet-Schnittstelle des PCs mit laufendem WinConfig hat die gleiche IP-Adresse wie die angeschlossene Fernwirkkarten Ethernet-Schnittstelle.

6.5.3 Einstellungen von der PC-Funktion übernehmen

Um ausgewählte Einstellungen zu übertragen, klicken Sie bitte auf das Symbol , welches sich im Hauptmenü befindet. Die folgende Datenübertragung erscheint nun auf der rechten Seite des Einstellungsbaums.

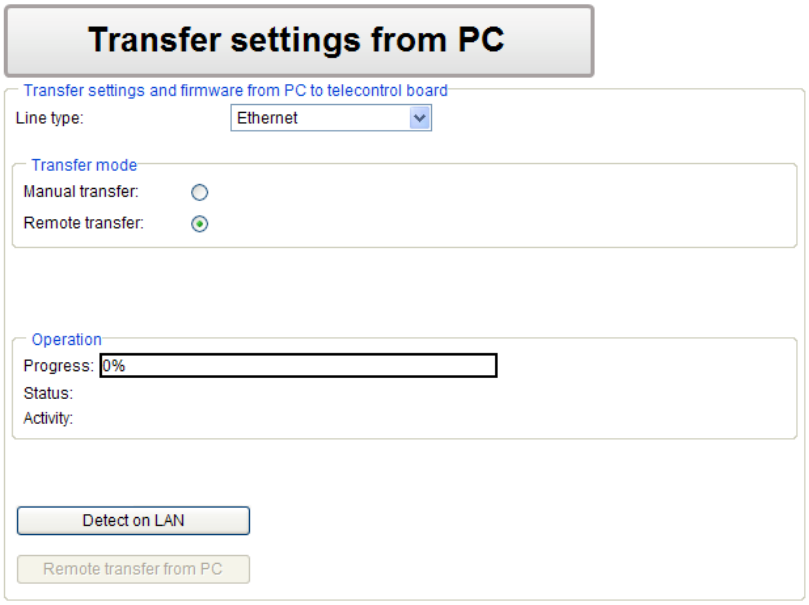


Figure 11: Fernübertragung vom PC, REG-P

Verfügbare Kontrollen:

- *Leitungsart* - Auswahl der Art der Datenübertragung (Ethernet oder seriell über A-Eberle-Gerät)
- *Übertragungsmodus: Manuelle Übertragung oder Fernübertragung* - Wahl der Art der Datenübertragung
- *Detect on LAN* - Funktion der automatischen Erkennung von Fernwirkkarten mit an das LAN angeschlossener CSO- oder COM-SERVER-Firmware. Die Liste der erkannten Boards ist nach erfolgreicher Erkennung in der oben stehenden Tabelle ersichtlich.
- *Fernübertragung vom PC* - Ausführtaste zur Aktivierung der Fernübertragungsfunktion.

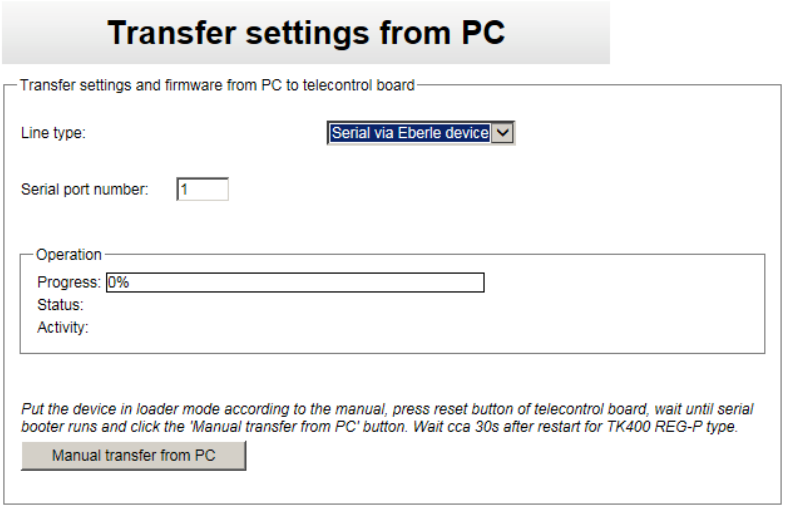


Figure 12: Manuelle Übertragung vom PC aus

Wenn die manuelle Übertragungsfunktion ausgewählt ist, muss der Benutzer das A-Eberle Geräterack für die manuelle Datenübertragung vorbereiten.

Ethernet-Übertragung - klicken Sie **zuerst** auf die Schaltfläche *Manuelle Übertragung vom PC* und setzen Sie **dann** die Fernwirkkarte zurück. WinConfig wartet, bis der Ethernet-Booter läuft, ändert vorübergehend seine aktuellen IP-Einstellungen, baut eine TCP-Verbindung auf und führt den erforderlichen Datentransfer durch. Alle Aktionen werden automatisch ausgeführt.

Serielle Übertragungen - stellen Sie das A-Eberle-Gerät in den Lademodus, setzen Sie die Fernwirkkarte zurück und warten Sie, bis der serielle Booter läuft. Klicken Sie dann auf die Schaltfläche *Manuelle Übertragung vom PC*.

HINWEIS!	Für das Hardware-Handshake während der Datenübertragung muss ein serielles Nullmodemkabel mit Modemsignalen (RTS/CTS) verwendet werden.

6.5.4 Übertragung der Einstellungen vom PC für die Fernwirkkarten TK28-4, TK28-6 und TK102

Der HTTPS-Datentransfer dient zur Übertragung von Einstellungen, wahlweise mit oder ohne Firmware (Linux Kernel und Ramdisk) bei den Fernwirkkartentypen TK8xx, TK28x und TK102. Bei REG-PED (TK885) muss die richtige REG-PED-Version über Auswahlknöpfe ausgewählt werden, wenn auch die Firmware der Fernwirkkarte (Linux Kernel und TK8xx RAM-Disk) übertragen wird. Für eine erfolgreiche Datenübertragung müssen die Login-Daten eingegeben werden.

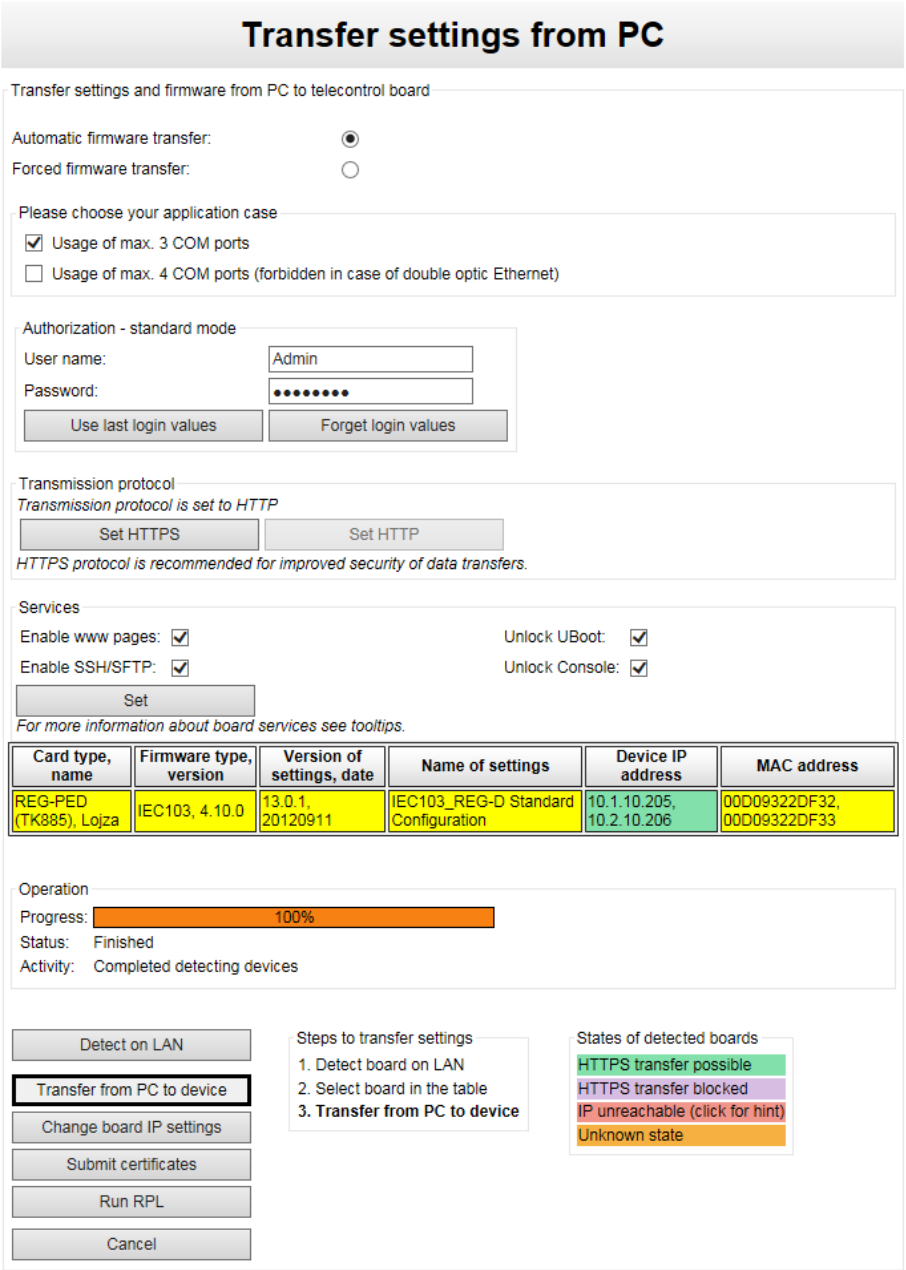


Figure 13: Übertragung vom PC für Fernwirkkarten Typ REG-PE(D)(SV)

Spezielle Kontrollen:

- *Automatischer Firmwaretransfer/Forced Firmwaretransfer* Radio Button - wählen Sie, ob WinConfig über die Notwendigkeit entscheiden soll, auch Kernel, RAM-Disk oder beides zu übertragen (*Automatischer Firmwaretransfer*) oder ob Kernel und RAM-Disk in jedem Fall übertragen werden sollen (*Forced Firmware Transfer*).
- *Auswahl des Anwendungsfalles* - Auswahl der richtigen Version der REG-PED-Karte bezüglich der Verwendung von COM-Ports. Diese Auswahl betrifft die Version der Firmware der Fernwirkkarte.
- *Benutzername* - Benutzeranmeldung für HTTPS-Zugriff Das Admin-Konto im Passwortmodus
- *Passwort* - Benutzerpasswort für den HTTPS-Zugang
- *Letzte Login-Werte verwenden* - zuletzt gespeicherte Login-Werte verwenden
- *Login-Werte vergessen* - sich nicht an die eingegebenen Login-Werte erinnern
- *Übertragungsprotokoll*:
  - HTTPS einstellen - verwenden Sie das HTTPS-Protokoll für den Datentransfer, um die Sicherheit der übertragenen Daten zu gewährleisten,
  - HTTP einstellen - verwenden Sie das standardmäßige ungesicherte HTTP-Protokoll.
- *Verfügbare Board-Services*: *WWW-Seiten aktivieren*, *SSH/SFTP aktivieren*, *UBoot freischalten*, *Konsole freischalten* - Optionen sind für fortgeschrittene Benutzer gedacht und ermöglichen es, das Verhalten der Fernwirkkarte zu ändern, um die Sicherheit der Datenübertragung zu erreichen, indem die entsprechenden Dienste aktiviert bzw. deaktiviert werden oder indem die angegebenen Aktionen ausgeführt werden.
- *IP-Einstellungen der Karte ändern* - diese Taste wechselt zur Seite *REG-PE(D) IP-Einstellungen der Karte*.
- *Run RPL* - diese Schaltfläche führt die REG-PEX-Lader-Konfigurationssoftware aus, mit der eine REG-PE(D)-Karte konfiguriert werden kann, falls die Firmware auf der Karte für die Erkennung durch WinConfig nicht ausreicht. Die Verwendung von RPL erfordert eine serielle Verbindung zwischen dem PC und der zu konfigurierenden Karte.
- *Zertifikate einreichen* - diese Schaltfläche wechselt zur Seite *Zertifikate einreichen*.
- *Verfügbare Board-Dienste* - Check-Buttons zum Aktivieren/Deaktivieren von Board-Diensten
  - *www-Seiten aktivieren* - diese Option aktiviert bzw. deaktiviert die im Board installierte Online-WinConfig. Wenn www-Seiten deaktiviert sind, kann der Benutzer das Board über ein Menüsystem verwalten.
  - *SSH/SFTP aktivieren* - diese Option aktiviert die Online-Konsole (Zugriff auf das Board über das Menüsystem).
  - *UBoot freischalten - Option zum Aktivieren/Deaktivieren des Benutzerzugriffs durch Unterbrechen des Bootvorgangs, bevor der UBoot ausgeführt wird.*

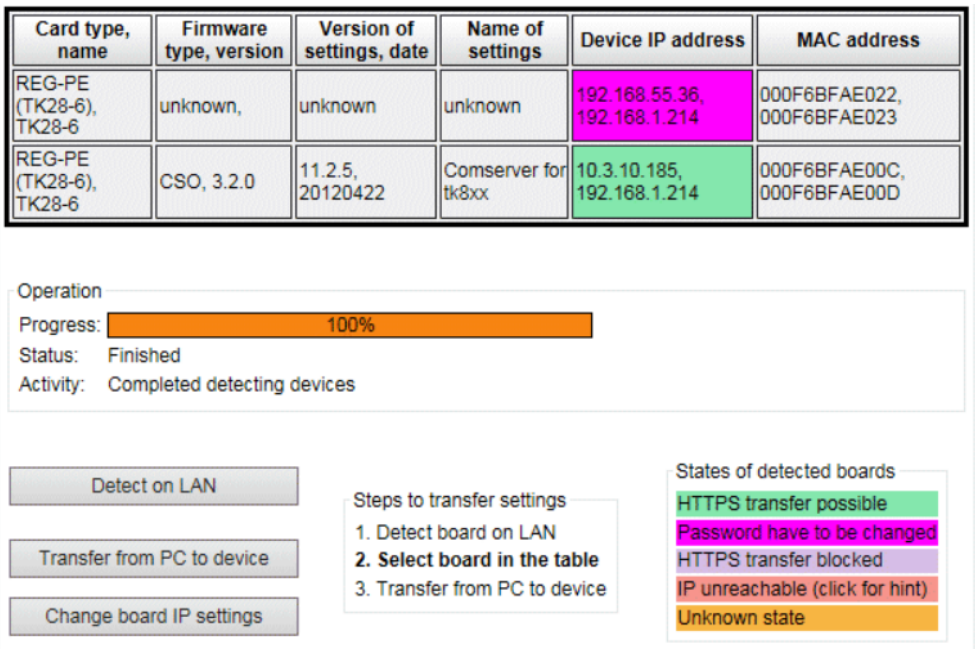
- *Konsole freischalten - Diese Option aktiviert den SSH-Zugriff auf die Konsole anstelle des Benutzermenüs. Diese Option ist für die Fernwirkkarten TK28x und TK102 nicht verfügbar, bei denen der Konsolenzugriff immer gesperrt ist.*

0 *Zustände der erkannten Boards*

- *HTTPS-Übertragung möglich* - die Karte ist bereit für den Datentransfer.
- *HTTPS-Übertragung gesperrt* - Die Übertragung ist nicht möglich. Wahrscheinlicher Grund dafür ist die Einstellung von Firewalls im Benutzer-PC oder nicht verfügbarer WEB-Server im Board.
- *IP-Adresse unerreichbar* - Wenn die IP-Adresse der Karte außerhalb des Bereichs der vom Benutzer-PC aus sichtbaren IP-Adressen liegt. Klicken Sie auf dieses Element, um Hinweise zur Lösung dieses Problems durch Ändern der IP-Adresse des PCs anzuzeigen. Eine weitere Möglichkeit besteht darin, dass die WinConfig die Adresse der Fernwirkkarte vorübergehend ändern kann; diese Option gilt nur für die Fernwirkkarten TK8xx.
- Der *nicht erreichbare IP-Zustand* kann auch dann auftreten, wenn im Benutzer-PC eine Ethernet-Schnittstelle mit korrekter IP-Adresse vorhanden ist, diese Schnittstelle jedoch getrennt oder mit einem falschen Netzwerk verbunden ist. In diesem Fall überprüfen Sie bitte den korrekten Anschluss der Ethernet-Schnittstellen.
- *Unbekannter Zustand* - Die Karte kann von der Detect-Funktion nicht gelesen werden.

6.5.4.1 Fernwirkkarten REG-P (TK28-4), REG-PE (TK28-6) und REG-PED^{SV} (TK102) erstmals erkannt

Wie im obigen Kapitel *Funktionskonzepte* beschrieben, muss der Benutzer bei der ersten Erkennung der Karte das Notfallpasswort ändern. Der Zustand der erkannten Karte ist mit der Farbe *Password has to be changed* board state gekennzeichnet.



Card type, name	Firmware type, version	Version of settings, date	Name of settings	Device IP address	MAC address
REG-PE (TK28-6), TK28-6	unknown,	unknown	unknown	192.168.55.36, 192.168.1.214	000F6BFAE022, 000F6BFAE023
REG-PE (TK28-6), TK28-6	CSO, 3.2.0	11.2.5, 20120422	Comserver for tk8xx	10.3.10.185, 192.168.1.214	000F6BFAE00C, 000F6BFAE00D

Figure 14: Erste Erkennung von TK28x- und TK102-Boards

6.5.4.2 Fernwirkkarten REG-P (TK28-4), REG-PE (TK28-6) und REG-PED^{SV} (TK102) mit erstmals angeschlossener Online-WinConfig

Die gleiche Regel gilt auch für das erstmals verbundene Online-WinConfig, wenn das Notfallpasswort vor der Verwendung von offline WinConfig nicht geändert wurde. In diesem Fall erscheint der folgende Dialog:

Figure 15: Erste Verbindung mit online WinConfig

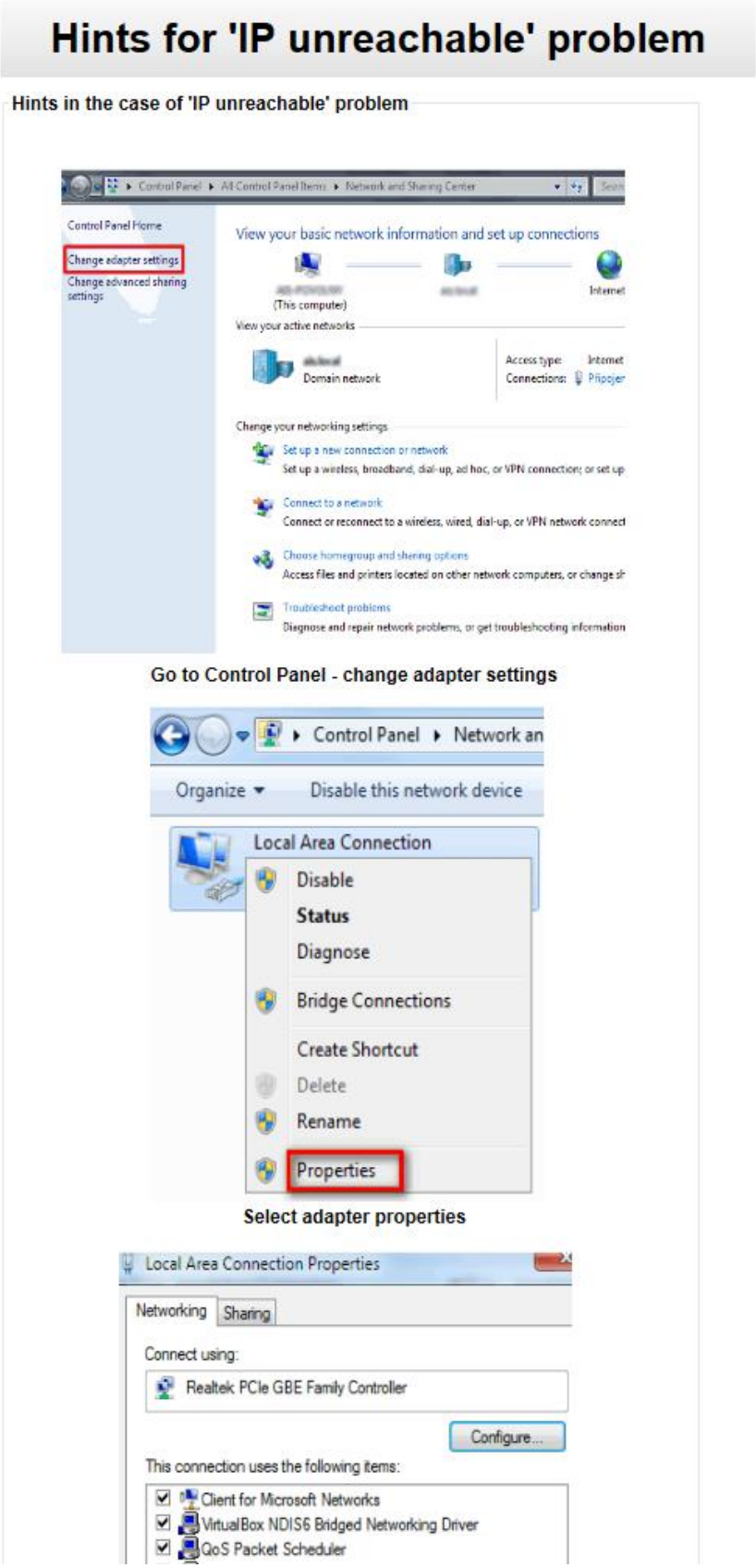


Figure 16: Hinweise auf "IP unreachable" Probleme

6.5.5 Änderung der IP-Einstellungen für REG-PE(D) Fernwirkkarten

Um die IP-Einstellungen für die Fernwirkkarte vom Typ REG-PE(D) (TK8xx TK28-x) zu ändern, klicken Sie auf die Schaltfläche *IP-Einstellungen der Karte ändern*, die auf dem Bildschirm erscheint, wenn die erfolgreiche Erkennung der Karte im LAN durchgeführt und die entsprechende Karte ausgewählt wird. Die Erkennung kann vor der Datenübertragung entweder vom oder zum PC erfolgen. Die IP-Einstellung der Fernwirkkarte ist protokollunabhängig. Das folgende Fenster erscheint auf dem Bildschirm:

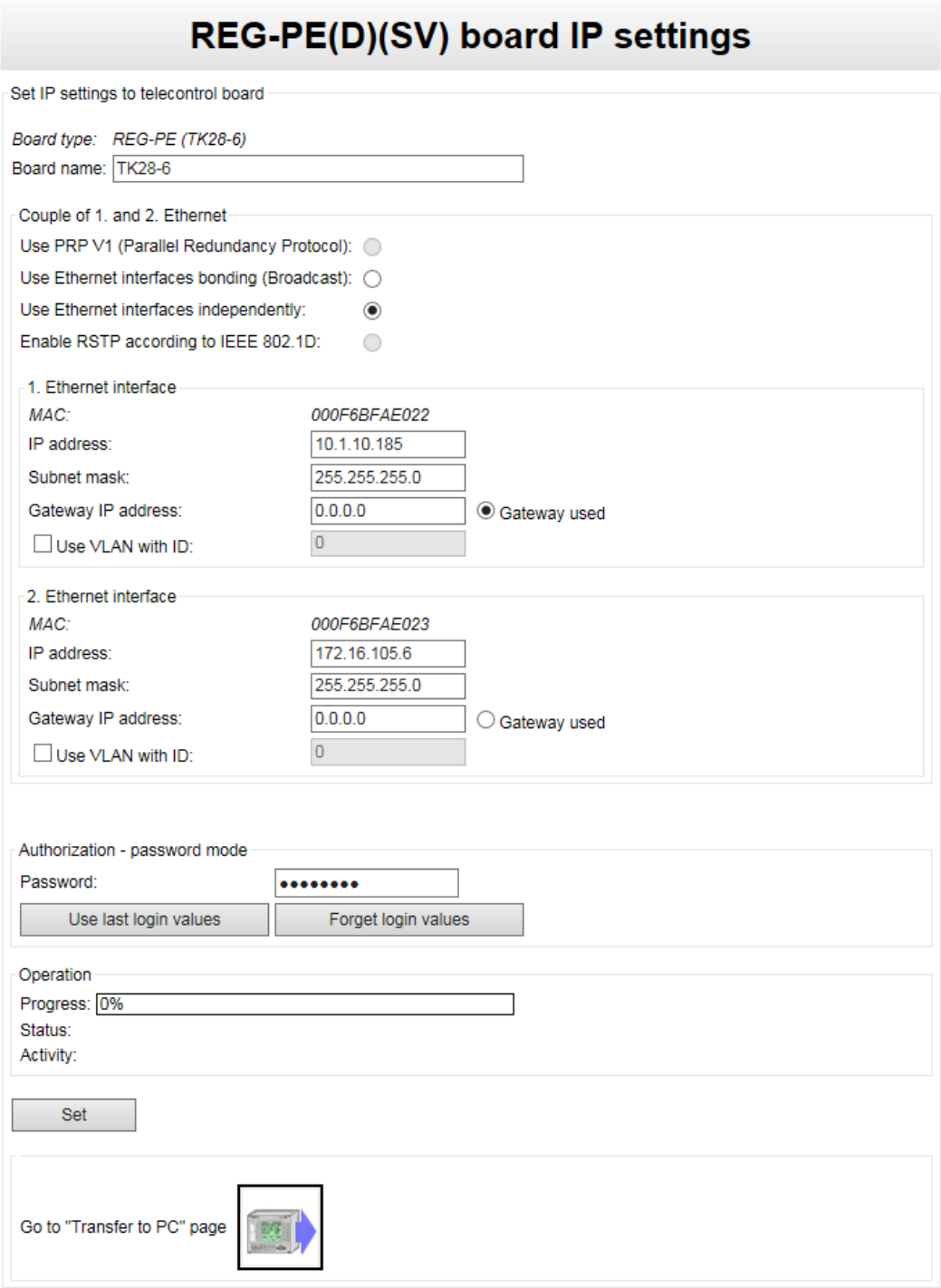


Figure 17: REG-PE(D) Karte IP-Einstellungen

Geben Sie neue Werte ein und klicken Sie auf die Schaltfläche *Set, um die* IP-Einstellungen der Ethernet-Schnittstellen zu ändern.

Wenn Sie einen Ausfall einer Ethernet-Schnittstelle verhindern möchten, aktivieren Sie die Kontrollbox *Ethernet-Schnittstellen verbinden*, um Ethernet-Schnittstellen zu verbinden und die Richtlinie "Aktives Backup" zu verwenden.

Die zweite Ethernet-Schnittstelle ist nur für den Kartentyp REG-PED (TK885) verfügbar. Eines der definierten Gateways kann über den *verwendeten* Auswahlknopf *Gateway* als Standard-Gateway ausgewählt werden.

Um die Verbindung von Ethernet-Schnittstellen auszuschalten, aktivieren Sie die Kontrollbox *Ethernet-Schnittstellen unabhängig verwenden*.

Um PRP V1 (Parallel Redundancy Protocol) zu verwenden, aktivieren Sie die Kontrollbox *PRP verwenden*.

Um RSTP zu aktivieren, das gemäß IEEE 802.1D definiert ist, aktivieren Sie die Kontrollbox *RSTP aktivieren*.

Um die Verwendung der Ethernet-Schnittstelle im VLAN zu aktivieren, aktivieren Sie die Kontrollbox VLAN mit ID verwenden und geben Sie die VLAN-ID-Nummer ein.

6.5.6 Änderung der IP-Einstellungen für Fernwirkkarten REG-PED^{SV} (TK102)

Das Board TK102 kann mit einem Erweiterungsmodul ausgestattet werden, welches zwei weitere Ethernet-Ports enthält. Diese Erweiterung kann während des Erkennungsprozesses erkannt werden. Die *Seite REG-PE(D) IP-Einstellungen* wird in diesem Fall um die Parameter des dritten und vierten Ethernet-Ports erweitert.

Es gibt eine Beschränkung der Konfigurationen der beiden Ethernet-Paare. Wenn das erste Paar auf Parallel Redundancy Protocol (PRP) oder Ethernet-Verbindung eingestellt ist, muss das zweite Paar als zwei unabhängige Ethernet-Ports eingestellt werden.

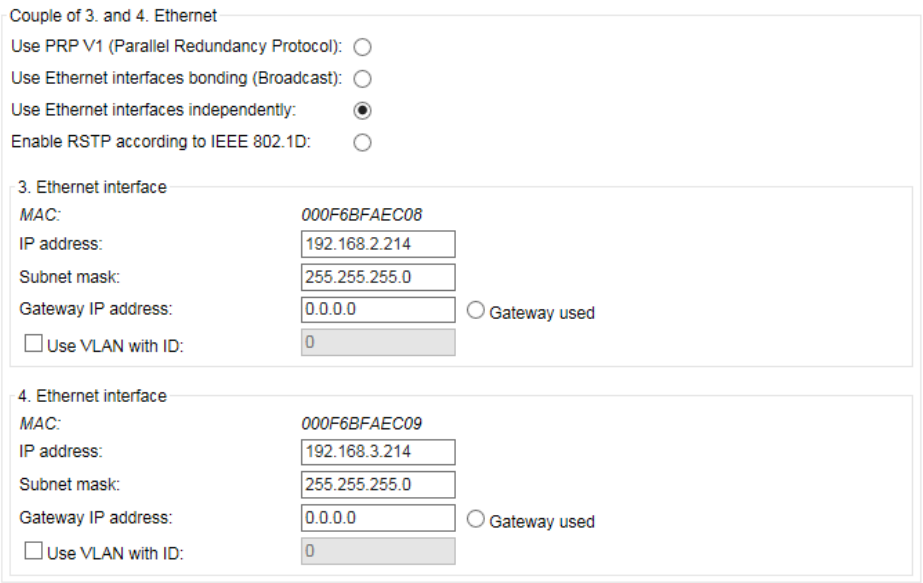


Figure 18: Paar von 3. und 4. Ethernet (TK102)

6.5.7 Zertifikate für Fernwirkkarten TK28-4, TK28-6, TK860 und TK885, TK102 einreichen

Sicherheitszertifikate werden für die HTTPS-Kommunikation mit der Fernwirkkarte REG-PEx verwendet. Fernwirkkarten werden mit werkseitigen Standard-Zertifikaten geliefert, die mit Benutzerzertifikaten neu geschrieben werden können.

Das Benutzerzertifikat kann bei der Certification Authority (CA) angefordert oder durch ein spezielles Programm (z.B. OpenSSL) generiert werden. Die Zertifikate müssen im PEM-Format (Privacy Enhanced Mail) vorliegen; andere Formate können mit einem entsprechenden Programm in das PEM konvertiert werden.

Das Zertifikat besteht typischerweise aus einer *Zertifikatsdatei* und einer *Schlüsseldatei*. Wenn das Zertifikat von der CA ausgestellt wird, dann gibt es auch die *CA-Zertifikatsdatei* und eventuell auch eine *Zwischenzertifizierungsdatei,* falls die Zwischenzertifizierungsstelle von der CA verwendet wird. Die *Schlüsseldatei* darf nicht passwortgeschützt sein, um vom REG-PEx akzeptiert zu werden.

Für den Fall, dass ein spezielles Programm zur Generierung von Zertifikaten verwendet wird, ist es möglich, die CA zu generieren oder die bereits vorhandene CA zu verwenden (3 erstellte Dateien) oder ein selbstsigniertes Zertifikat zu generieren (2 erstellte Dateien).

Weitere Informationen zu Zertifikaten finden Sie in den öffentlich zugänglichen Informationen im Internet.

Alle notwendigen Aktionen zum Umschreiben der Standard-Zertifikate können auf der Seite *Zertifikate* durchgeführt werden.

Um Benutzerzertifikate zu übermitteln, durchsuchen Sie die Zertifikatsdateien und übertragen Sie diese über die Schaltfläche *Senden* an die Fernwirkkarte.

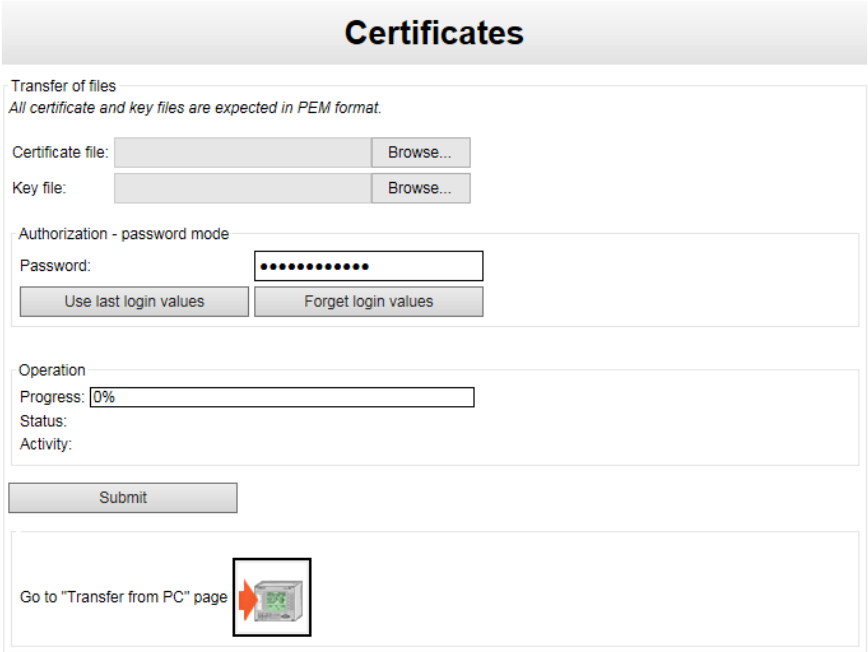


Figure 19: REG-PE(D) Board Zertifikate

6.5.8 Verbindung

Die Ethernet-Schnittstellenanbindung ist eine Softwarefunktion, um eine höhere Sicherheit zu erreichen. Wenn die Funktion aktiviert ist, haben die Ethernet-Schnittstellen die gleichen MAC- und IP-Adressen. Dies führt zu Redundanz bei einem gebrochenen Ethernet-Kabel.

Wenn die Verbindungsoption eingeschaltet ist, verwendet die Firmware die Ethernet-Schnittstelle, über welche die Verbindung hergestellt wurde, und im Falle eines Verbindungsabbruchs (die Verbindung ist wegen eines gebrochenen oder abgetrennten Ethernet-Kabels unterbrochen) schaltet die Firmware automatisch auf die zweite Verbindungs-Schnittstelle um, die als Backup dient.

Die Option *Use Ethernet interface bonding* und die beiden Ethernet-Ports sind nur für den Kartentyp TK885 verfügbar, die Kartentypen TK860 und TK885-1 haben nur eine Ethernet-Schnittstelle zur Verfügung.

Darüber hinaus gibt es weitere Bedingungen im Zusammenhang mit der Verbindungsoption:

Das TK885-Board mit 2x Glasfaser-COM-Ports hat immer den COM-4-Port deaktiviert und Verbindungen verfügbar.

Andere Versionen des TK885-Boards verwenden je nach Verbindungsfunktion zwei verschiedene Firmware-Versionen (Linux-Kernel). Die Kontrollbox Ethernet-Schnittstellen-Verbindungen verwendet auf der Seite REG-PE(D) der IP-Einstellungen der Karte von Win-Config wird entsprechend der Kernel-Version der REG-PED-Karte aktiviert bzw. deaktiviert, die in den vorherigen Übertragungseinstellungen auf der PC-Seite erkannt und ausgewählt wurde.

Wenn die Verbindung benötigt wird, aber nicht vom aktuellen Kernel unterstützt wird, der in die Karte geladen ist, gehen Sie zu den Übertragungseinstellungen von der PC-Seite und übertragen Sie die Einstellungen zusammen mit der Firmware und der richtigen Version der REG-PED-Karte.

Wenn die Verbindungs-Option in der Firmware vorhanden ist, kann der COM 4 Port nicht verwendet werden.

Bei der Verwendung der Verbindungsfunktion ist immer zu beachten, dass für Boards mit elektrischen oder elektrischen/optischen Ethernet-Schnittstellen die richtige Version der Firmware mit Verbindungs-Option ausgewählt werden muss und die Verbindungs-Option auf der IP-Einstellungsseite der RED-PED-Karte eingeschaltet werden muss. Beachten Sie auch, dass die serielle Schnittstelle COM4 bei Firmware mit der Option Verbindung nicht verwendet werden kann.

6.5.9 PRP - Paralleles Redundanzprotokoll

Eine Netzwerkredundanz bedeutet, dass zwei unabhängige aktive Pfade zwischen zwei Geräten vorhanden sind. Die Sender REG-PED (TK885) und REG-PED^{SV} (TK102) verwenden zwei unabhängige Netzwerkschnittstellen, welche die gleichen Daten gleichzeitig übertragen. Dann stellt das Redundanzüberwachungsprotokoll sicher, dass der Empfänger nur das erste Datenpaket verwendet und das zweite verwirft. Wenn nur ein Paket empfangen wird, weiß der Empfänger, dass auf dem anderen Weg ein Fehler aufgetreten ist. Das parallele Redundanzprotokoll ist in der Norm IEC 62439-3 beschrieben.

Die Fernwirkkarte REG-PED^{SV} (TK102) kann mit zwei Paar Netzwerkschnittstellen ausgestattet werden. In diesem Fall gibt es eine Einschränkung. Nur ein Paar Netzwerkschnittstellen kann auf das PRP-Protokoll oder andere verfügbare Verbindungs-Funktionen eingestellt werden. Ein weiteres Paar Netzwerkschnittstellen muss als zwei unabhängige Ports betrieben werden. Weitere Informationen finden Sie in Kapitel 6.5.6 *Änderung der IP-Einstellungen für Fernwirkkarten REG-PED^{SV} (TK102)*.

7. Unterstützung für skriptbasiertes Upgrade-Verfahren für Fernwirkkarten TK28-4, TK28-6 und TK102 und A-Eberle Geräte-Firmware

7.1 Konzepte

7.1.1 SW-Architektur

Die REG-P(E)(D)(SV) vom Typ TK28-x oder TK102 Fernwirkkarten (Karten) haben ein Embedded-Linux-basiertes Betriebssystem. Die unterstützten aktualisierbaren Teile sind:

- SYSTEM.FIT image - Dateisystem des Betriebssystems (in der Linux-Umgebung manchmal rootfs oder ramdisk genannt). Es beinhaltet z.B. eingebettete Webserver-Binärdateien, SSH-Server-Binärdateien usw.
- TKxxxxx.TGZ - Anwendungs-Tarball. Es umfasst Anwendungen (Protokolle) Binärdateien und WinConfig Online-Dateien (Skripte, Webseiten usw.). Es enthält keine Einstellungsdateien.
- YYY.XML - Einstellungsdatei (auch Template genannt) - Parametrierdatei für Anwendungen. Sie wird im Paar mit der entsprechenden ICD-Datei bei der Anwendungsart IEC61850 verteilt.

7.1.2 Konzept des Upgrades

Die unterstützte Upgrade-Methode funktioniert in den folgenden Schritten:

- Der Benutzer erstellt *Verteilungsskripte* unter Verwendung des bereitgestellten *Vorbereitungsskripts* (*Verteilungsskripte* enthalten die gewünschten Dateien für das Upgrade, digitale Signatur und vorbereiteten skriptbasierten Aktualisierungscode).
- Der Benutzer führt das *Upgrade-Skript* mit den entsprechenden Parametern auf einer Zielkarte aus.
- Das *Upgrade-Skript* verbindet den SSH-Server auf der Karte und kopiert die *Verteilungsskripte* auf die Karte.
- Das *Upgrade-Skript* führt die *Verteilungsskripte,* die den Upgrade-Prozess starten, aus der Ferne aus. Der Prozess besteht typischerweise aus den folgenden Schritten:
  - Überprüfung der digitalen Signatur des Vertriebsskripts.
  - Überprüfung der Ziel-HW-Kompatibilität.
  - Stoppen und Blockieren von tatsächlich laufenden Anwendungen.
  - Neustart.
  - Übertragung des Verteilungsskripts.
  - Parsen des Verteilungsskripts auf die gezippten Upgrade-Dateien und das Upgrade-Skript.

- Upgrade.
- Neustart.

0 Während des gesamten Upgrade-Vorgangs werden zwei Neustarts angezeigt.

0 Der Prozess kann vom Anwender nach Bedarf automatisiert werden.

7.1.3 Sicherheitskonzept

Die folgenden Sicherheitsmaßnahmen sind implementiert:

0 Das Verteilungsskript wird mit einem speziell für diesen Zweck ausgestellten Zertifikat digital signiert. Dieser private Schlüssel wird im Upgrade-Support-Paket verteilt. Es gibt auch einen entsprechenden öffentlichen Schlüssel, der als Teil des TK-Kartensystems verteilt wird. Es wird zur Überprüfung der Signatur zu Beginn des Upgrade-Verfahrens verwendet.

0 Der Benutzer muss die richtigen Anmeldeinformationen verwenden, um den SSH-Server auf der Zielkarte zu verbinden. Es werden sowohl der RADIUS- als auch der Passwortmodus unterstützt.

0 Der Upgrade-Prozess verwendet die Backup/Upgrade/Wiederherstellungsmethode des Workflows, so dass der ursprüngliche Zustand wiederhergestellt wird, wenn das Upgrade fehlschlägt.

0 Die Firmware-Datei des A-Eberle-Geräts im **mot**-Format ist von A-Eberle digital signiert und der Endbenutzer verwendet diese signierte Datei für das Upgrade. Das TK-Kartensystem prüft die Signatur und stellt sicher, dass die Firmware von A-Eberle autorisiert ist. Der entsprechende öffentliche Schlüssel wird als Teil des TK-Kartensystems verteilt, der private Schlüssel verbleibt bei der A-Eberle Company zur Unterzeichnung.

7.1.4 Hosting-Umgebung

Die beiden Versionen der Upgrade-Support-Pakete für Windows- und Linux-Umgebungen sind verteilt. Beide Pakete enthalten ähnliche Tools und verwenden identische Methoden zur Vorbereitung und Aktualisierung.

7.2 Installation des Upgrade-Support-Pakets

7.2.1 Windows

Das Installationspaket sollte entpackt oder in den gewünschten Ordner kopiert werden. Das Paket enthält alle notwendigen Binärdateien (7z.exe, plink.exe, openssl.exe, tee.exe, wget.exe), statische Bibliotheken (7z.dll, libeay32.dll, ssleay32.dll, libiconv2.dll, libintl3.dll, libssl32.dll), Skripte (preparation.bat, run_upgrade.bat), Vorlagen (upg_restart.tpl, upg_system.tpl, upg_application.tpl, upg_settings.tpl, upg_firmware.tpl), Schlüssel (fd.key) und Unterordner (/UPG_RESTART, /UPG_SYSTEM, /UPG_APPLICATION, /UPG_SETTINGS, /UPG_FIRMWARE). Es sind keine weiteren Installationsschritte erforderlich und es muss keine andere Software installiert werden. Das Installationspaket ist kompatibel mit Windows 7 und höher, 64-Bit.

7.2.2 Linux

Das Installationspaket sollte entpackt oder in den gewünschten Ordner kopiert werden. Das Paket enthält alle notwendigen Skripte (preparation.sh, run_upgrade.sh), Vorlagen (upg_restart.tpl, upg_system.tpl, upg_application.tpl, upg_settings.tpl, upg_firmware.tpl), Schlüssel (fd.key) und Unterordner (/UPG_RESTART, /UPG_SYSTEM, /UPG_APPLICATION, /UPG_SETTINGS, /UPG_FIRMWARE). Die folgenden Softwarepakete müssen installiert sein:

- ssh
- sshpass
- wget

7.3 Vorbereitung des Upgrades

7.3.1 Windows

Das Vorbereitungsskript ist *preparation.bat*. Es muss mit dem Parameter "MODUS" laufen, der angibt, was vorbereitet werden soll. Die gültigen Parameterwerte folgen:

- "MODE=s" (Beispiel: C:\Upgrade\preparation.bat "MODE=s") zur Vorbereitung der Aktualisierung des Fernwirksystems.
- "MODE=a" (Beispiel: C:\Upgrade\preparation.bat "MODE=a") zur Vorbereitung des Upgrades von Fernwirkkartenanwendungen.
- "MODE=x" (Beispiel: C:\Upgrade\preparation.bat "MODE=x") zur Vorbereitung des Upgrades der Fernwirkkarteneinstellungen.
- "MODE=f" (Beispiel: C:\Upgrade\preparation.bat "MODE=f") zur Vorbereitung des Firmware-Upgrades von A-Eberle Geräten.

Entsprechende Dateien müssen in die Vorbereitungsordner kopiert werden, bevor das Vorbereitungsskript ausgeführt wird:

- Für ein System-Upgrade - Ordner /UPG_SYSTEM, system.fit und testimage.tgz werden benötigt.
- Für das Anwendungs-Upgrade - Ordner /UPG_APPLICATION, applications.tgz wird benötigt, settings.xml (und die entsprechende ICD-Datei im Falle der IEC61850-Anwendung) wird empfohlen.
- Für das Upgrade der Einstellungen - Ordner /UPG_SETTINGS, settings.xml (und die entsprechende ICD-Datei im Falle der IEC61850-Anwendung) wird benötigt.
- Für ein Firmware-Upgrade von A-Eberle - Ordner /UPG_FIRMWARE, Firmware. Smot wird benötigt (digital signierte Mot-Firmware-Datei).

Während der Vorbereitung werden im Installationsordner verschiedene temporäre Textdateien (*.txt) erstellt.

7.3.2 Linux

Das Vorbereitungsskript ist preparation.bat. Es muss mit dem Parameter "MODE" laufen, der angibt, was vorbereitet werden soll. Die gültigen Parameterwerte folgen:

- "MODE=s" (Beispiel: \upgrade\preparation.sh "MODE=s") zur Vorbereitung der Aktualisierung des Fernwirksystems.
- "MODE=a" (Beispiel: \upgrade\preparation.sh "MODE=a") zur Vorbereitung des Upgrades von Fernwirkkartenanwendungen.
- "MODE=x" (Beispiel: \upgrade\preparation.sh "MODE=x") zur Vorbereitung des Upgrades der Fernwirkkarteneinstellungen.
- "MODE=f" (Beispiel: \upgrade\preparation.sh "MODE=f") zur Vorbereitung des Firmware-Upgrades von A-Eberle Geräten.

Entsprechende Dateien müssen in die Vorbereitungsordner kopiert werden, bevor das Vorbereitungsskript ausgeführt wird:

- Für ein System-Upgrade - Ordner /UPG_SYSTEM, system.fit und testimage.tgz werden benötigt.
- Für das Anwendungs-Upgrade - Ordner /UPG_APPLICATION, applications.tgz wird benötigt, settings.xml (und die entsprechende ICD-Datei im Falle der IEC61850-Anwendung) wird empfohlen.
- Für das Upgrade der Einstellungen - Ordner /UPG_SETTINGS, settings.xml (und die entsprechende ICD-Datei im Falle der IEC61850-Anwendung) wird benötigt.
- Für das Firmware-Upgrade des A-Eberle-Geräts - Ordner /UPG_FIRMWARE, Firmware.Smot wird benötigt (digital signierte Mot-Firmware-Datei).

Während der Vorbereitung werden im Installationsordner verschiedene temporäre Textdateien (*.txt) erstellt.

7.3.3 Digitale Signatur der A-Eberle Geräte-Firmware-Datei

Die Dateien, die für die Unterstützung der digitalen Signaturen von A-Eberle-Geräte-Firmware-Dateien erforderlich sind, werden im Ordner /EBERLE verteilt. Dieser Ordner ist nicht für die Verteilung an den Endbenutzer bestimmt. Der Ordner enthält Skripte *sign_mot_udm.bat* für die digitale Signatur. Der Dateiname der Mot-Datei wird als Parameter des Skripts verwendet; Ergebnis ist die Datei *filename.smot*, die in den Ordner /UPG_FIRMWARE kopiert und in *firmware.smot* umbenannt werden soll. Das Skript verwendet die private Schlüsseldatei "fd.key".

7.4 Upgrade-Prozess

7.4.1 Windows

Das Upgrade-Skript ist *run_upgrade.bat*. Es muss mit 5 Parametern "MODUS", "SERVER", "BENUTZER", "PWD", "HW" laufen, die angeben, was zu aktualisieren ist und welche Verbindungsparameter.

Der Parameter "MODUS" Wertebereich ist:

- "MODE=s" für die Aktualisierung des Fernwirksystems.
- "MODE=a" für die Aktualisierung von Fernwirkkartenanwendungen.
- "MODE=x" für die Aktualisierung der Einstellungen der Fernwirkkarte.
- "MODE=f" für die Aktualisierung der Firmware des A-Eberle-Geräts.

Der Parameter "SERVER" ist die IP-Adresse oder der Hostname der Ziel-TK-Karte.

Die Parameter "USER" und "PWD" sind Benutzername und Passwort für die Anmeldung an der Ziel-TK-Karte nach dem Sicherheitsmodell - RADIUS oder Passwort. Alle Sicherheitsmodelle bieten Benutzern, die die Berechtigung haben, ein skriptbasiertes Remote-Upgrade durchzuführen.

Der Parameter "HW" gibt den Zielkartentyp an. Der zulässige Wertebereich ist "HW=TK28-4", "HW=TK28-6", "HW=TK28-8", "HW=TK102" und "HW=". Der letzte leere Wert sollte verwendet werden, wenn ein unerwarteter Zustand des Upgrades auftritt - z.B. unbeaufsichtigte Unterbrechung des Upgrade-Prozesses nach der ersten Stufe usw. In diesen Fällen bleibt die Karte ohne entsprechende HW-Versionsinformationen verfügbar. Der Wert von "HW=" deaktiviert die Überprüfung der HW-Versionskompatibilität und erzwingt das Upgrade ohne Kompatibilitätsprüfung. Dieses Upgrade kann riskant sein und sollte nur dann vorsichtig durchgeführt werden, wenn die HW-Informationen von der Karte nicht verfügbar sind. Der Wert "HW=" kann nicht im System-Upgrade- und A-Eberle-Geräte-Firmware-Upgrade-Modus verwendet werden.

Beispiel:

run_upgrade.bat "MODE=a" "SERVER=10.1.10.185" "PWD=password2" "USER=scripter" "HW=TK28-6".

Während des Upgrade-Vorgangs werden verschiedene temporäre Textdateien (*.txt) im Installationsordner erstellt. Einige temporäre "sedxxx"-Dateien werden ebenfalls erstellt und können gelegentlich gelöscht werden.

7.4.2 Linux

Das Upgrade-Skript ist run_upgrade.sh. Es muss mit 5 Parametern "MODUS", "SERVER", "BENUTZER", "PWD", "HW" laufen, die angeben, was zu aktualisieren ist und welche Verbindungsparameter.

Der Parameter "MODUS" Wertebereich ist:

- "MODE=s" für die Aktualisierung des Fernwirksystems.
- "MODE=a" für die Aktualisierung von Fernwirkkartenanwendungen.
- "MODE=x" für die Aktualisierung der Einstellungen der Fernwirkkarte.
- "MODE=f" für die Aktualisierung der Firmware des A-Eberle-Geräts.

Der Parameter "SERVER" ist die IP-Adresse oder der Hostname der Ziel-TK-Karte.

Die Parameter "USER" und "PWD" sind Benutzername und Passwort für die Anmeldung an der Ziel-TK-Karte nach dem Sicherheitsmodell - RADIUS oder Passwort. Alle

Sicherheitsmodelle bieten Benutzern, die die Berechtigung haben, ein skriptbasiertes Remote-Upgrade durchzuführen.

Der Parameter "HW" gibt den Zielkartentyp an. Der zulässige Wertebereich ist "HW=TK28-4", "HW=TK28-6", "HW=TK28-8", "HW=TK102" und "HW=". Der letzte leere Wert sollte verwendet werden, wenn ein unerwarteter Zustand des Upgrades auftritt - z.B. unbeaufsichtigte Unterbrechung des Upgrade-Prozesses nach der ersten Stufe usw. In diesen Fällen bleibt die Karte ohne entsprechende HW-Versionsinformationen verfügbar. Der Wert von "HW=" deaktiviert die Überprüfung der HW-Versionskompatibilität und erzwingt das Upgrade ohne Kompatibilitätsprüfung. Dieses Upgrade kann riskant sein und sollte nur dann vorsichtig durchgeführt werden, wenn die HW-Informationen von der Karte nicht verfügbar sind. Der Wert "HW=" kann nicht im System-Upgrade- und A-Eberle-Geräte-Firmware-Upgrade-Modus verwendet werden.

Beispiel:

\upgrade\run_upgrade.sh "MODE=a" "SERVER=10.1.10.185" "PWD=password2" "USER=scripter" "HW=TK28-6".

Während des Upgrade-Vorgangs werden verschiedene temporäre Textdateien (*.txt) im Installationsordner erstellt.

7.4.3 Sequentielles Upgrade

Der Upgrade-Prozess ermöglicht auch ein sequentielles Upgrade mehrerer TK-Boards. In diesem Fall führt der Benutzer das Vorbereitungsskript aus, erstellt die Datei *IP.txt* im Ordner mit Skripten und ändert die Skriptdatei *sample_loop.bat*.

Die Datei *IP.txt* enthält die IP-Adressen der Karten, die für das Upgrade vorbereitet sind. Die *sample_loop.bat* enthält eine Schleife mit Aktivierung von *run_upgrade.bat,* in der die entsprechenden Parameter eingegeben werden müssen (MODE, USER, PWD, HW). Das Skript übernimmt die IP-Adressen aus der Datei *IP.txt*. Die T-Stück-Umleitung kann zur Aufzeichnung aller Konsolenausgaben von der gesamten Schleife bis zur Ausgabetextdatei verwendet werden.

Beispiel:

- *IP.txt* Dateistruktur:
  - 10.1.10.55
  - 10.1.10.78
  - 10.1.10.48
  - .
  - .
- Änderung von *sample_loop.bat* (***fett*** markierte Parameter zum Ändern)

für /f %%x in (ip.txt) rufen Sie run_upgrade.bat "MODE=**f**" "SERVER=%%x" "PWD=**password**" "USER=**User**" "HW=**TK28-6**" | tee output.txt auf.

7.5 Hinweise

7.5.1 So stellen Sie die Kompatibilität sicher

Das einzige Tool, das die Kompatibilität zwischen Anwendung und Einstellungen gewährleistet, ist das Windows-basierte Offline-Programm WinConfig. Es ist notwendig, seine Funktionalität zu nutzen, um die Kompatibilität zwischen dem hochgeladenen Anwendungspaket und der Einstellungen-XML-Datei sicherzustellen.

Am besten ist es, die gewünschte XML-Einstellungsdatei in der WinConfig zu öffnen und wieder in der neuen Datei zu speichern. WinConfig nimmt notwendige Hintergrundänderungen in der Einstellungsdatei vor, um die Kompatibilität mit der im Paket enthaltenen Anwendungsversion sicherzustellen. Das Öffnen und Speichern der Einstellungsdatei gewährleistet die Anwendung notwendiger Änderungen, um die gleiche korrekte Einstellungs-datei zu erhalten, die WinConfig für den Download verwendet.

Es wird empfohlen, den Anwendungs-Upgrade-Modus mit vorbereiteter Einstellungs-Xml-Datei (und entsprechender ICD-Datei im Falle der IEC61850-Anwendung) im Ordner UPG_APPLICATION (als "settings.xml") zu verwenden. Dieses Verfahren kommt der Art und Weise nahe, wie WinConfig ein Upgrade durchführt.

7.5.2 Ausgabe von Skripten auf der Konsole

Es ist eine gute Vorgehensweise, die Konsolenausgabe von Upgrade-Skripten im Problemfall und in anderen Fällen zu analysieren.

7.5.3 Schutz von Produktionsdateien

Die Textskripte und Vorlagen sollten im Dateisystem als read-only gekennzeichnet bleiben, um ein versehentliches Überschreiben zu vermeiden. Die Skripte, die auf Linux abzielen (alle Shell-Skripte, Vorlagen unter Linux), sollten sorgfältig übertragen und kopiert werden, um ein Ändern der EOL-Zeichen zu vermeiden und sie im UNIX-Stil zu lassen.

7.5.4 A-Eberle Geräte-Firmware-Upgrade

Das Firmware-Upgrade dauert ziemlich lange (Minuten).

Hinweis:

- Es gibt einen langen Timeout (ca. 15 Minuten), bevor das A-Eberle-Gerät bei einer fehlgeschlagenen Übertragung der Firmware zum A-Eberle-Gerät in den Standard-Arbeitszustand zurückgesetzt wird. Das Gerät funktioniert und interagiert in diesem Intervall nicht.
- Der COM3-Anschluss (Fernwirkkarte) und der COM1S-Anschluss (A-Eberle-Gerät) werden für das Firmware-Update verwendet.

8. Demontage & Entsorgung

Die Entsorgung des LVRSys™ erfolgt durch die A. Eberle GmbH & Co. KG.

➲ Alle Komponenten an A. Eberle senden:

A. Eberle GmbH & Co. KG
Frankenstraße 160
D-90461 Nürnberg

9. Gewährleistung

A. Eberle GmbH & Co. KG. gewährleistet, dass dieses Produkt und Zubehör, für die Dauer von drei Jahren ab Kaufdatum, frei von Material- und Fertigungsdefekten bleibt.

Gewährleistung gilt nicht für Schäden durch:

- Unfälle
- Missbrauch
- abnormale Betriebsbedingungen

Um Gewährleistung in Anspruch zu nehmen, A. Eberle GmbH & Co KG in Nürnberg kontaktieren.

10. Abbildungsverzeichnis

11. Tabellenverzeichnis

Notizen

A. Eberle GmbH & Co. KG

Frankenstraße 160
D-90461 Nürnberg
Deutschland

Tel.: +49 (0) 911 / 62 81 08-0
Fax: +49 (0) 911 / 62 81 08 96
E-Mail: info@a-eberle.de

http://www.a-eberle.de

Präsentiert von:

_____