Remote Access Gateway (RAG)
mit SSV/SecSetup

Funktionsübersicht

SSV Software Systems GmbH
Dünenweg 5
D-30419 Hannover
Tel.: +49 (0)511/40 000-0
Fax: +49 (0)511/40 000-40
E-Mail: sales@ssv-embedded.de

Handbuch Revision: 1.0
Datum: 11.06.2014

www.ssv-embedded.de

INHALT

1 EINFÜHRUNG 3
1.1 Systemübersicht 3

2 FERNZUGRIFFSBETRIEB 6
2.1 Verbindungen und IT-Sicherheit 6

3 KONFIGURATIONSBETRIEB 8
3.1 Verbindungen und PC-Browserzugriff 8

4 HILFREICHE LITERATUR 10

KONTAKT 10

DOKUMENT HISTORIE 10

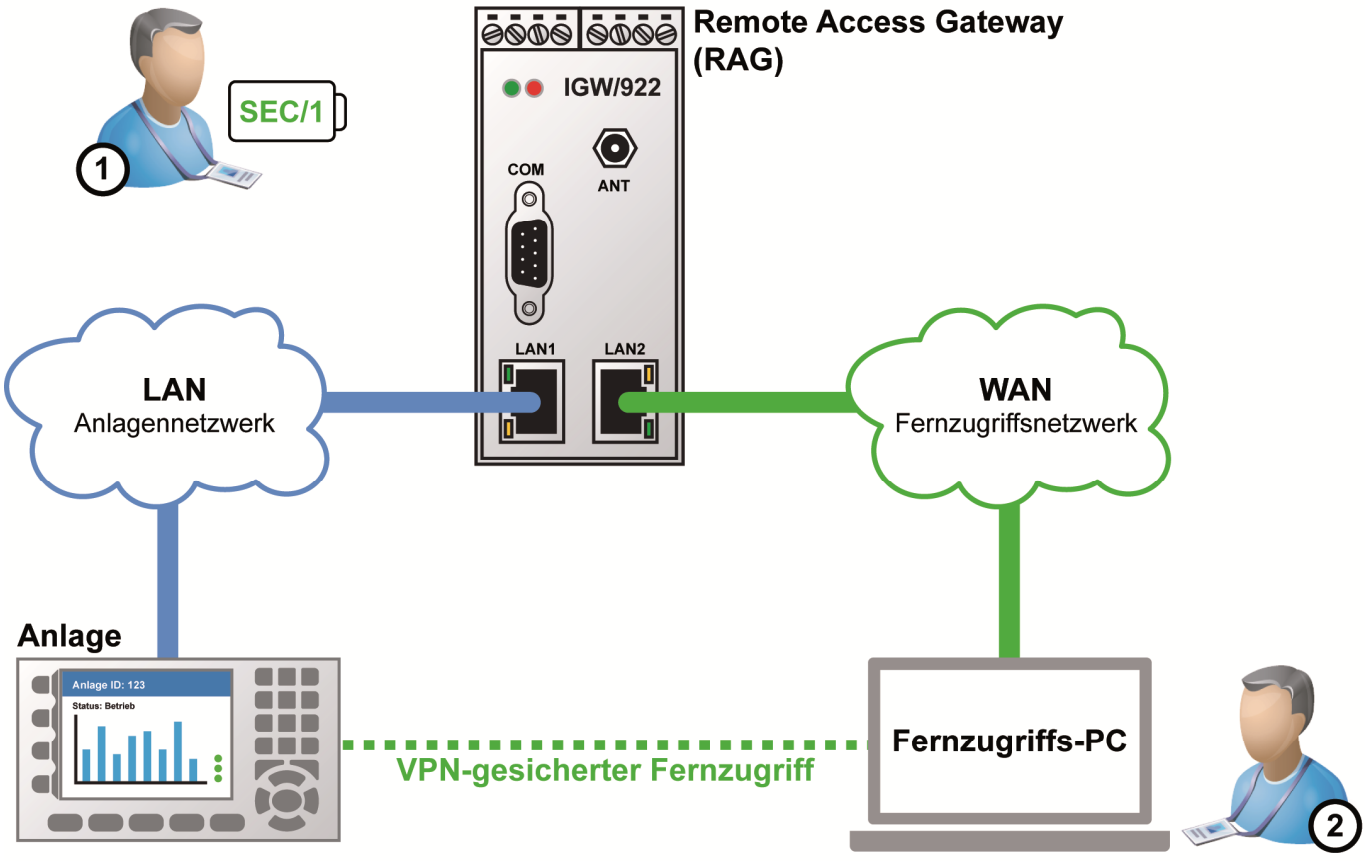
1 EINFÜHRUNG

Diese Dokumentation beschreibt den Anschluss eines Remote Access Gateway (RAG) an eine Anlage und einen Internet-Router sowie die Vorbereitungen für den VPN-gesicherten Fernzugriffsbetrieb am Beispiel eines RAG IGW/922.

Ein anwendungsbezogener **SSV Security Setup** (**SSV/SecSetup**) für ein bestimmtes Fernzugriffs-VPN (VPN = Virtual Private Network) ist im RAG bereits ab Werk voreingestellt. Das bedeutet, das System wird in einem sicheren Zustand ausgeliefert und muss vor Ort nur noch mit zwei Netzwerken und einer Spannungsversorgung verbunden werden. Durch den werkseitigen SSV Security Setup ist das RAG bereits so eingerichtet, dass es sich automatisch über einen Internet-Router mit einem vordefinierten SSV-VPN-Server verbindet und dort anmeldet.

1.1 Systemübersicht

Ein RAG mit einem SSV/SecSetup ermöglicht einem Servicetechniker über einen entsprechend vorbereiteten Fernzugriffs-PC den Internet-basierten Fernzugriff auf eine Anlage mit beliebigem Standort. Das RAG ist dafür gleichzeitig in zwei Netzwerke – dem LAN (Local Area Network) und WAN (Wide Area Network, in der Regel das Internet) – eingebunden.



(1) **Fachhandwerker:** Besitzt den SEC/1, installiert das RAG und führt die Inbetriebnahme durch.

(2) **Servicetechniker:** Kann von einem PC aus per Internet auf die Anlage zugreifen.

Abb. 1: Systemübersicht – VPN-gesicherter Anlagenfernzugriff und die Akteure

Bitte beachten Sie, dass die „Netzwerkwolke“ des Anlagen- und Fernzugriffsnetzwerks aus der Abbildung 1 in einfachen Anwendungsfällen jeweils durch eine direkte Kabelverbindung ersetzt werden kann.

Der gesamte Fernzugriff wird durch ein Virtual Privat Network (VPN) gesichert, das für die Authentifizierung, Verschlüsselung und Signierung sorgt. Der VPN-gesicherte Fernzugriff entspricht einer speziell gesicherten Punkt-zu-Punkt-Verbindung. Einen VPN-Endpunkt bildet der Fernzugriffs-PC, den anderen das RAG.

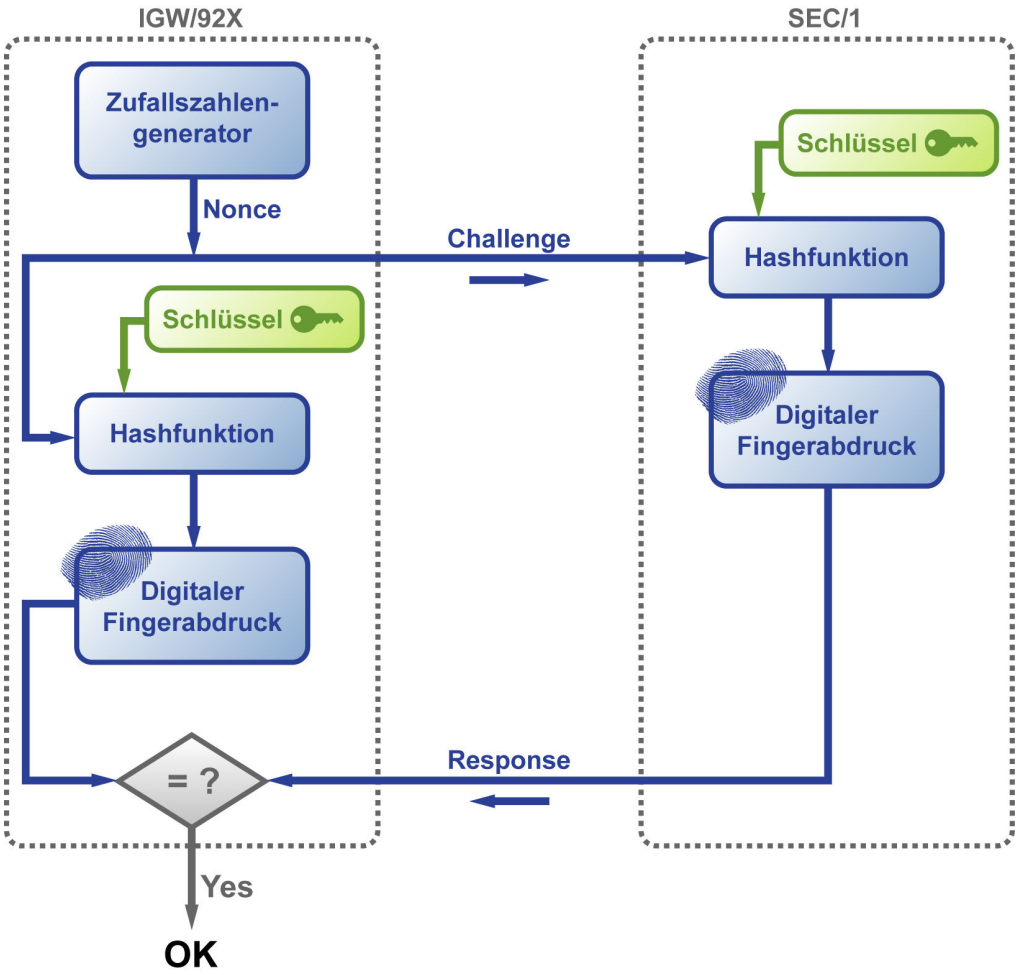


Abb. 2: Zwischen RAG und SEC/1 findet eine Challenge-Response-Authentifizierung statt

Für die Vor-Ort-Installation und den Betrieb eines RAG sind zwei entsprechend geschulte Akteure erforderlich (siehe Abbildung 1).

1. **Ein Fachhandwerker:** Er installiert das RAG vor Ort und sorgt dafür, dass sowohl die LAN-Anlagenverbindung als auch die WAN-Internetanbindung funktionieren. Der Fachhandwerker ist eine Vertrauensperson mit weitreichenden Befugnissen. Er ist darüber hinaus mit einem speziellen elektronischen Sicherheitsschlüssel ausgestattet – siehe **SEC/1** in der **Abbildung 1**. Über diesen Schlüssel kann der Fachhandwerker die RAG-Konfigurationseinstellungen und somit auch den SSV Security Setup verändern, um zum Beispiel die Standard-Werkseinstellungen den Besonderheiten einer Umgebung anzupassen. Darüber hinaus kann der Fachhandwerker mit Hilfe des SEC/1 einen Internet-Verbindungstest – also den Test der WAN-Fernzugriffsverbindung – durchführen und die Verbindung zum SSV-VPN-Server prüfen.

2. **Der Servicetechniker:** Dieser Akteur kann über einen speziellen PC – dem Fernzugriffs-PC in der **Abbildung 1** – auf die Anlage zugreifen. Der Fernzugriff erfolgt per Internet und wird durch ein VPN gesichert. Daher müssen auf dem Fernzugriffs-PC die entsprechenden VPN-Treiber und ein X.509-Sicherheitszertifikat vorhanden sein. Der Servicetechniker ist in der Regel für eine Gruppe von Anlagen zuständig. Neben dem völlig transparenten Anlagenfernzugriff besitzt der Servicetechniker die Möglichkeit, den aktuellen Status des VPNs in Hinblick auf die Anlagen aus seinem Verantwortungsbereich zu prüfen. Dazu gehört die Abfrage, welche Anlage per VPN erreichbar ist und welche nicht, bzw. wann eine Anlage zuletzt im VPN angemeldet war.

Neben den zuvor beschriebenen Akteuren spielt der elektronischen Sicherheitsschlüssel SEC/1 eine wichtige Rolle. Über diesen Schlüssel kann der Fachhandwerker den Zugriff auf die webbasierte RAG-Konfigurationsschnittstelle (**SSV Web ConfigTool**) freischalten. Dafür muss der SEC/1 einfach auf den COM-Port in der RAG-Frontplatte gesteckt werden.

Vor dem Benutzerzugriff eines Fachhandwerkers auf das SSV Web ConfigTool ist zunächst eine erfolgreiche Challenge-Response-Authentifizierung erforderlich. Wie in der **Abbildung 2** dargestellt, erzeugt ein RAG sofort nach dem Aufstecken des SEC/1 eine einmalige Zufallszahl (Nonce) und überträgt diese als Challenge an den SEC/1.

Dieser ermittelt aus der Zufallszahl und einem hinterlegten Schlüssel über eine geeignete Hashfunktion einen digitalen Fingerabdruck. Der wird als Response vom SEC/1 an das RAG IGW/922 zurückgeschickt. Das IGW/922 kennt ebenfalls den Schlüssel und die Hashfunktion des SEC/1. Somit kann ein IGW/922 selbst den digitalen Fingerabdruck für die Challenge erzeugen und das Ergebnis mit der vom SEC/1 erhaltenen Response vergleichen.

Sind beide Fingerabdrücke identisch, wird die Authentifizierung erfolgreich abgeschlossen. Danach muss der Fachhandwerker auf der ersten Webseite des SSV Web ConfigTool noch ein spezielles Passwort eingeben. Erst dann ist der Zugriff auf die RAG-Konfigurationsschnittstelle möglich. Ohne eine erfolgreiche Challenge-Response-Authentifizierung wird dem Fachhandwerker die Webseite zur Passworteingabe nicht angezeigt, weil die dafür erforderlichen Softwarekomponenten im RAG gesperrt sind.

Vor der Auslieferung wird für ein RAG der werksseitige SSV Security Setup (SSV/SecSetup) durchgeführt. Dieser besteht aus den folgenden Arbeitsschritten:

- RAG-Sicherheitseinstellungen für das WAN Fernzugriffsnetzwerk in der **Abbildung 1** vornehmen
- RAG-Sicherheitseinstellungen für das LAN Anlagennetzwerk in der **Abbildung 1** durchführen
- Zugriffsberechtigungen für einen SSV-VPN-Server im RAG hinterlegen
- Adressinformation für die Erreichbarkeit eines SSV-VPN-Servers im RAG konfigurieren
- Sicherheitsinformationen für den Zugriff auf das SSV Web ConfigTool im RAG hinterlegen
- Hardware-Sicherheitskonfiguration für die RAG-Firmware durchführen
- Datenbankeintrag mit den erforderlichen SSV/SecSetup-Managementinformationen auf einem SSV-Server erzeugen
- Passwortversand, um dem zuständigen Fachhandwerker den Zugriff auf die RAG-Konfigurationsschnittstelle zu ermöglichen

Der SSV/SecSetup darf nur durch einen entsprechend autorisierten SSV-Mitarbeiter durchgeführt werden. Der gesamte Vorgang unterliegt SSV-internen Sicherheitsauflagen und wird durch das ISO 9001:2008-basierte Qualitätsmanagementsystem der SSV Software Systems GmbH überwacht.

2 FERNZUGRIFFSBETRIEB

Die IT-Sicherheit (Security) des VPN-Fernzugriffsbetrieb eines RAG IGW/922 basiert auf gewissen Annahmen. Sie ist von folgenden Voraussetzungen abhängig:

- Ein RAG befindet sich zusammen mit der Anlage innerhalb eines zutrittsgesicherten Bereichs (zum Beispiel in einem Schaltschrank) und nur das Netzwerkkabel an **LAN2** ist nach außen geführt.
- Der zutrittsgesicherte Bereich wird nur von vertrauenswürdigen Personen – zum Beispiel dem Fachhandwerker – betreten.
- Ein RAG ist mit einer unterbrechungsfreien Stromversorgung verbunden.
- Alle Grenzwerte hinsichtlich Spannungsschwankungen, Betriebstemperaturbereich, max. Kabellängen an LAN1 und LAN2, EMV-Störgrößen usw. werden gemäß den Vorgaben eingehalten.

2.1 Verbindungen und IT-Sicherheit

Die **Abbildung 3** zeigt, wie ein RAG für den Fernzugriffsbetrieb verkabelt wird. Die physikalische Schnittstelle zum WAN Fernzugriffsnetzwerk der **Abbildung 1** bildet in der Praxis ein Internet-Router. Durch den SSV Security Setup erwartet ein RAG, dass dieser Internet-Router einen internen **DHCP-Server** besitzt, der auf Anforderung eine IP-Adresse zur Verfügung stellt.

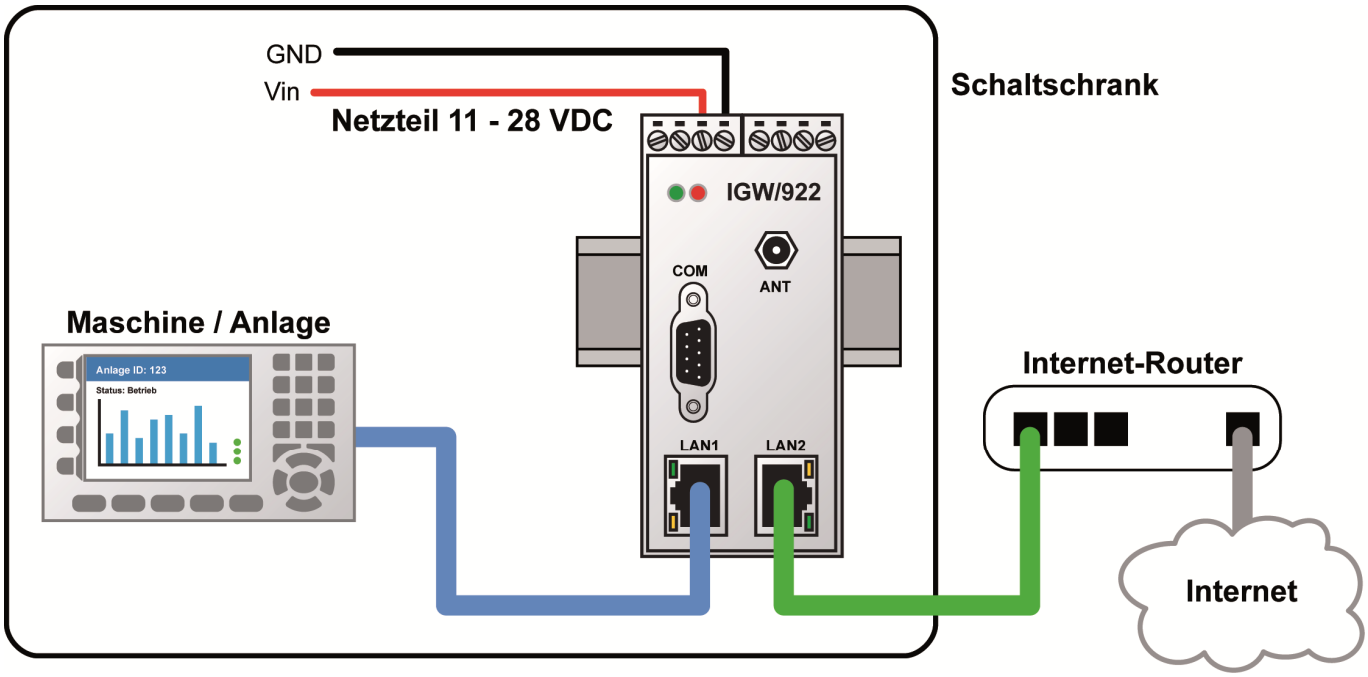


Abb. 3: Verbindungen für den Fernzugriffsbetrieb

Wird ein RAG in einer solchen Umgebung erstmals mit Spannung versorgt, erfolgt innerhalb des Startvorgangs der Bezug einer IP-Adresse vom DHCP-Server des Internet-Routers. Sofort danach baut das RAG IGW/922 per Internet eine Verbindung zu einem vordefinierten SSV-VPN-Server auf und meldet sich auf diesem Server an (die Serveradresse und Anmeldedaten stammen aus dem SSV/SecSetup).

Nach **ca. 35 bis 45 Sekunden** sollte die **rote LED** in der RAG-Frontplatte dauerhaft leuchten. Sie signalisiert die erfolgreiche Anmeldung auf dem VPN-Server.

Im **Fehlerfall blinkt die rote LED** in der RAG-Frontplatte. Die möglichen Ursachen für eine blinkende LED sind im Einzelnen:

- Das RAG hat keine IP-Adresse per DHCP vom Internet-Router erhalten.
- Es konnte keine Verbindung zum Internet aufgebaut werden.
- Es konnte keine Verbindung zum SSV-VPN-Server aufgebaut werden.
- Die Anmeldung auf dem SSV-VPN-Server ist fehlgeschlagen.

Die weitere Ursachendiagnose und Fehlerbehebung müssen durch einen Fachhandwerker erfolgen, der im Besitz eines für das jeweilige IGW/922 vorkonfigurierten Sicherheitsschlüssels SEC/1 und eines entsprechenden Passworts für den Zugriff auf die RAG-Konfigurationsschnittstelle ist (siehe **Kapitel 3**).

In Bezug auf die IT-Sicherheit ist davon auszugehen, dass ein RAG im Fernzugriffsbetrieb von einem potenziellen Angreifer oder einem PC mit entsprechender Schadsoftware über die LAN2-Schnittstelle direkt oder indirekt attackiert wird. Dabei sind folgenden Szenarien denkbar:

- Ein Angreifer befindet sich im gleichen LAN wie der Internet-Router und die LAN2-Schnittstelle des RAG.
- Ein PC mit einer Schadsoftware befindet sich im gleichen LAN wie der Internet-Router und die LAN2-Schnittstelle des RAG.
- Der Internet-Router besitzt eine WLAN-Schnittstelle und einen internen Access Point (AP). Ein Angreifer oder ein PC mit einer Schadsoftware ist als Client mit dem AP verbunden und kann daher auf die LAN2-Schnittstelle des RAG zugreifen.
- Der Internet-Router besitzt eine Backdoor, die von einem Angreifer ausgenutzt werden kann.
- Ein Angreifer oder ein durch Schadsoftware verseuchtes Rechnersystem greift ein RAG direkt über den Router aus dem Internet an (der Router muss für den VPN-Fernzugriffs-betrieb eines RAG keine zusätzlichen Firewall-Funktionen besitzen).
- Der Router könnte mit einem Port Forwarding und einem dynamischen DNS Account konfiguriert sein. Dadurch wäre die LAN2-Schnittstelle des RAG unter Umständen weltweit für jeden möglichen Angreifer erreichbar.

Es ist allerdings denkbar, dass sich ein Angreifer unberechtigterweise Zutritt zum RAG verschafft, um zum Beispiel die RAG-VPN-Identität zu entwenden. Um einen solchen Identitätsdiebstahl zu verhindern, besitzt ein RAG mit SSV/SecSetup keinerlei frei zugängliche Benutzerschnittstellen zur Betriebssystemebene.

Ein RAG IGW/922 im Fernzugriffsbetrieb ist innerhalb des VPNs nicht weiter geschützt. Es ist dafür zu sorgen, dass im VPN nur vertrauenswürdig Benutzer auf ein RAG zugreifen können.

3 KONFIGURATIONSBETRIEB

Diese Betriebsart ist nur im Fehlerfall erforderlich (**rote LED in der RAG-Frontplatte blinkt** – es ist somit kein Fernzugriffsbetrieb möglich). Folgende Annahmen werden für den Konfigurationsbetrieb vorausgesetzt:

- Ein Fachhandwerker ist vor Ort und hat Zutritt zu dem gesicherten Bereich, in dem RAG und Anlage betrieben werden.
- Der Fachhandwerker besitzt einen Sicherheitsschlüssel SEC/1 und ein entsprechendes Passwort, um sich den Zugriff zur RAG-Konfigurationsschnittstelle zu verschaffen und das SSV Web ConfigTool nutzen zu können.
- Der Fachhandwerker ist mit einem PC ausgerüstet, auf dem ein geeigneter Webbrowser (zum Beispiel Firefox) installiert ist.
- Der Fachhandwerker besitzt ein LAN-Crossoverkabel für die Verbindung zwischen PC und RAG.

3.1 Verbindungen und PC-Browserzugriff

Die **Abbildung 4** zeigt, wie das RAG für den Konfigurationsbetrieb verkabelt wird. Die Kabelverbindung zur Anlage wird aus dem LAN1-Stecker des RAG herausgezogen. Stattdessen wird eine Verbindung mit Hilfe des Crossoverkabels zwischen dem IGW/922-LAN1-Stecker und dem PC hergestellt.

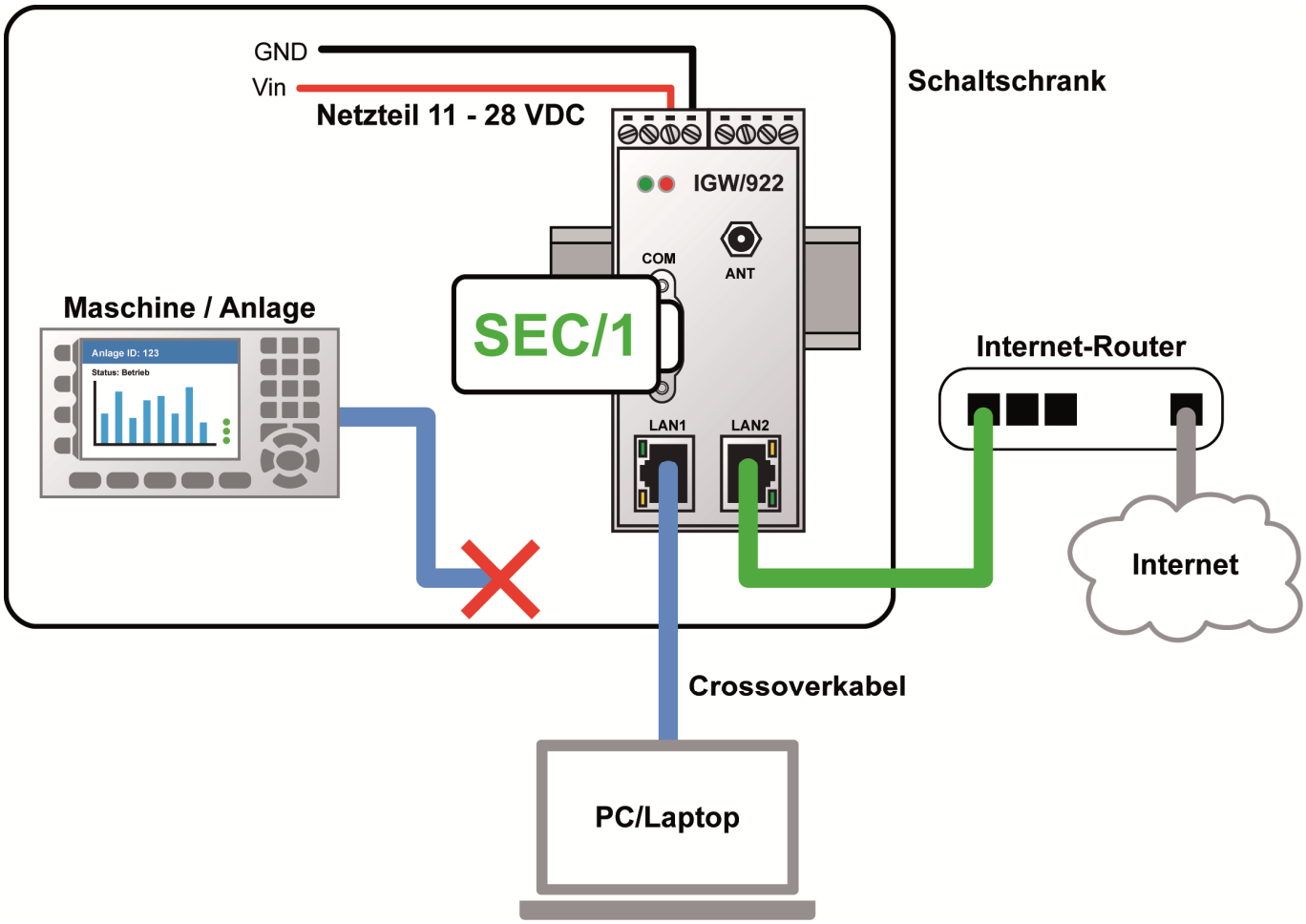


Abb. 4: Verbindungen für den Konfigurationsbetrieb

Nachdem die erforderliche Verkabelung für den Konfigurationsbetrieb hergestellt wurde, sollte der Fachhandwerker wie folgt vorgehen:

- Sicherheitsschlüssel SEC/1 auf den COM-Steckverbinder in der RAG-Frontplatte stecken.
- LAN-Schnittstelle des PCs mit der IP-Adresse **`192.168.19.10`** konfigurieren.
- Verbindung zum RAG vom PC aus mit einem **`ping 192.168.19.126`** testen.
- Webbrowser auf dem PC starten und **`http://192.168.19.126:7777`** als URL eingeben.
- Passwort in der ersten Webseite des SSV Web ConfigTools eintippen, um den Zugriff auf die weiteren Webseiten des SSV Web ConfigTool in der RAG-Konfigurationsschnittstelle freizuschalten. Bitte bei der Passworteingabe unbedingt zwischen Groß- und Kleinbuchstaben unterscheiden.

Danach kann der Fachhandwerker über den Browser durch die einzelnen Webseiten des SSV Web ConfigTools navigieren.

Wenn die rote LED in der RAG-Frontplatte dauerhaft blinkt, sind zur Fehlerursachenbehebung folgende Möglichkeiten vorgesehen bzw. hilfreich:

- DHCP-Adressbezug prüfen: Wenn dem RAG von Internet-Router eine IP-Adresse zugewiesen wurde, werden unter dem Menüpunkt „**Status**“ für LAN2 die Informationsfelder **Status VPN**, **Status DNS** und **Status route** angezeigt. Des Weiteren sollte die IP-Adresse **ungleich** **`192.168.1.126`** sein. Ist der DHCP-IP-Adressbezug fehlgeschlagen, besitzt LAN2 die Default-IP-Adresse **`192.168.1.126`** und die zuvor angesprochenen Felder werden nicht angezeigt.
- Verbindung zum Internet prüfen (nur sinnvoll, wenn der DHCP-Adressbezug erfolgreich war): Unter dem Menüpunkt „**Network > Internet**“ kann über die Schaltfläche **[Check]** die Internetverbindung getestet werden. Das Ergebnis dieses Tests wird im Klartext angezeigt.
- Verbindung zum VPN-Server prüfen (nur sinnvoll, wenn die Verbindung zum Internet funktioniert): Unter dem Menüpunkt „**Services > OpenVPN**“ wird ein Feld mit dem Titel „**OpenVPN configuration**“ angezeigt. In diesem Feld muss der Text „**Status Connected**“ stehen. Dann besitzt ein RAG eine funktionierende Verbindung zu einem SSV-VPN-Server und ein Servicetechniker kann aus der Ferne zugreifen.

Falls der Internet-Router, mit dem ein RAG verbunden ist, über keinen (aktiven) DHCP-Server verfügt, können IP-Adresse, Netzwerkmaske, DNS-Serveradresse und IP-Adresse für ein Default-Gateway über das SSV Web ConfigTool auch manuell vergeben werden.

Der Servicetechniker kann vom Fernzugriffs-PC aus jederzeit auf das SSV Web ConfigTool zugreifen. Ein aufgesteckter SEC/1 ist für diesen Zugriff nicht erforderlich, da der Konfigurationszugriff per Fernzugriff und somit innerhalb des VPNs erfolgt.

4 HILFREICHE LITERATUR

- IGW/922 Hardware Reference Manual
- IGW/925 Hardware Reference Manual
- SSV Web ConfigTool User Manual

KONTAKT

SSV Software Systems GmbH
Dünenweg 5
D-30419 Hannover

Tel.: +49 (0)511/40 000-0
Fax: +49 (0)511/40 000-40
E-Mail: sales@ssv-embedded.de

Internet: www.ssv-embedded.de
Forum: www.ssv-comm.de/forum

DOKUMENT HISTORIE

Revision	Datum	Bemerkungen	Name	Review
1.0	11.06.2014	Erste Version	WBU	KDW

Die Informationen in diesem Dokument können jederzeit ohne Ankündigung geändert werden. Die SSV Software Systems GmbH übernimmt keine Verantwortung für jegliche Art von Fehlern oder Schäden, die aus dem Gebrauch dieses Dokumentes und der darin enthaltenen Informationen resultieren. Produktnamen anderer Unternehmen können Warenzeichen dieser Gesellschaften sein.

© 2014 SSV Software Systems GmbH. Alle Rechte vorbehalten.