Saia PCD® Supervisor

Sicherheitshandbuch

Dokument 26-624 | Ausgabe GER03 | 2019-11-21

0

0

0.1 Dokumentenrevision

Version	Änderungen	Geändert	Kommentare
GER01	2019-07-01	komplett	- Auszug aus Handbuch 27-651 GER01
GER02	2019-07-02	Kap. 3.13	- Neues Unterkapitel: Einrichten der Google 2-Faktorauthentifizierung
GER03	2019-07-02	Kap. 3.15	- Neues Unterkapitel hinzugefügt: Datenschutz-Grundverordnung (DSGVO)

0.2 Warenzeichen

Saia PCD® ist ein eingetragenes Warenzeichen der Saia-Burgess Controls AG.

Technische Änderungen folgen dem Stand der Technik.

Veröffentlicht in der Schweiz

3 Sicherung von Saia PCD® Supervisor

3.1 Einführung

Der Zweck dieses Abschnitts ist die Bereitstellung der notwendigen Informationen für diejenigen, die an der Installation und Verwaltung eines Produkts oder Systems beteiligt sind, um die Anforderungen zur Konfiguration und Verwaltung der Sicherheit des Produkts oder Systems zu verstehen.

Allgemeine optimale Verfahren für Saia Burgess Controls IP-basierte Produkthandbücher „26-776_Manual_TCP-IP-Ethernet“ und „26-867_Manual_TCP-IP-Enhancements“.

Beide Dokumente sind auf der Saia Burgess Controls-Support-Webseite www.sbc-support.com verfügbar.

3.2 Notfallwiederherstellungsplanung

Hierbei handelt es sich um einen dokumentierten Vorgang oder eine Reihe von Vorgängen zur Wiederherstellung und zum Schutz einer geschäftlichen IT-Infrastruktur im Notfall. Solch ein Plan legt Vorgänge fest, die ein Unternehmen im Notfall befolgen soll.

Stellen Sie beim Entwickeln des Notfallwiederherstellungsplans sicher, dass er ALLE zur Wiederherstellung des Systembetriebs erforderlichen Daten beinhaltet, inklusive:

- Konfigurationsdateien für Plattform(en) und Station(en).
- Datenbankobjekte
- Lizenz- und Zertifikatsdateien
- Stationssicherung
- Stationskopien

Einzelheiten finden Sie Handbuch 27-651 im Kapitel *„6.8 Sicherung und Wiederherstellung“*.

3.3 Physische und umwelttechnische Berücksichtigungen

Der Saia PCD® Supervisor ausführende PC sollte nach Möglichkeit gegen ungenehmigten physischen Zugriff geschützt werden.

3.4 Sicherheitsaktualisierungen und Servicepakete

Stellen Sie sicher, dass auf dem Saia PCD® Supervisor ausführenden PC und jeglichen Client-Geräten die neueste Version des Betriebssystems installiert ist und die neueste Version von Saia PCD® Supervisor verwendet wird.

Saia Burgess Controls-Software wird zum Zeitpunkt der Veröffentlichung mit den neuesten Servicepaketen und entsprechenden Aktualisierungen getestet. Schlagen Sie bei Kompatibilitätsproblemen mit wesentlichen Aktualisierungen/Servicepaketen des Betriebssystems und von Java auf der Saia Burgess Controls-Webseite www.sbc-support.com nach.

3.5 Virenschutz

Stellen Sie sicher, dass der Saia PCD® Supervisor ausführende PC und jegliche Client-Geräte über Virenschutz-Software verfügen und die Virusdefinitionen aktuell gehalten werden.

Bestimmte Virenschutz-Software kann negative Auswirkungen auf die Leistung von Saia PCD® Supervisor haben. In solchen Fällen können Sie beantragen, dass das Saia PCD® Supervisor-Verzeichnis von der Zugriffsprüfung ausgenommen wird.

Weitere Einzelheiten finden Sie auf der Saia Burgess Controls-Support-Webseite www.sbc-support.com.

3.6 Netzwerkplanung und Sicherheit

Es wird empfohlen, das vom Gebäudemanagementsystem (*Building Management System*, BMS) verwendete Ethernet-Netzwerk durch einen Luftspalt vom normalen Büronetzwerk getrennt (separate Verkabelung und Geräte oder Layer 3-Schalter oder virtuelles privates Netzwerk (*virtual private network*, VPN) zu betreiben. Physischer Zugriff auf die Ethernet-Netzwerkinfrastruktur muss eingeschränkt werden. Sie müssen außerdem sicherstellen, dass die Installation in Einklang mit den IT-Richtlinien ihres Unternehmens steht.

Die Verwendung von Firewall und Einbruchserkennungssystem (*Intrusion Detection System*, IDS) eines zuverlässigen Anbieters von Sicherheitsprodukten wird für alle Installationen von Saia PCD® Supervisor empfohlen. Befolgen Sie die optimalen Verfahren für die ausgewählten Produkte sowie jegliche Unternehmens-IT-Richtlinien am Ort der Installation. Weisen Sie die Produkte dem bestimmten Port zu, den Sie für Saia PCD® Supervisor HTTPS und HTTP konfiguriert haben.

Befolgen Sie stets die Richtlinien der PDF-Dokumente:

Handbuch	26-776_Manual_TCP-IP-Ethernet
Handbuch	26-867_Manual_TCP-IP-Enhancements.
Handbuch	26-620_Manual_Security-Rules
Handbuch	Niagara^{AX} Hardening Guide
Anweisung	30-002_Internet-Security-Instructions_SBC
Anweisung zur Verwendung des VPN-Routers	30-004_VPN-Router

Sie müssen außerdem Schritte unternehmen, um die Sicherheit anderer mit Saia PCD® Supervisor verbundener Netzwerke (z. B. BACnet) sicherzustellen.

3.7 Virtuelle Umgebungen

Befolgen Sie die optimalen Verfahren für die ausgewählten Produkte sowie jegliche Unternehmens-IT-Richtlinien am Ort der Installation.

3.8 Sicherung drahtloser Geräte

Wird ein drahtloses Gerät verwendet, muss es in Einklang mit den IT-Richtlinien Ihres Unternehmens gesichert sein.

3.9 Systemüberwachung

Saia Burgess Controls empfiehlt für alle Installationen von Saia PCD® Supervisor die Verwendung eines Einbruchserkennungssystems (IDS) eines namhaften Anbieters von Sicherheitsprodukten, insbesondere wenn eine Verbindung zum Internet besteht. Befolgen Sie die optimalen Verfahren für die ausgewählten Produkte sowie jegliche Unternehmens-IT-Richtlinien am Ort der Installation.

Saia PCD® Supervisor protokolliert (Audit-Verlauf) Änderungen an seiner eigenen Konfiguration und Änderungen am Saia Burgess Controls-Kontrollsystem. Viele Einbruchserkennungssysteme und Firewall-Produkte bieten eine komplette Lösung zur Aufzeichnung des gesamten beim Saia PCD® Supervisor-PC eingehenden und ausgehenden Traffic, was es den Anwendern ermöglicht, alle Aktivitäten auf den untersten Ebenen aufzuzeichnen.

3.10 Sicherung des Zugriffs auf das Betriebssystem

Stellen Sie sicher, dass der Saia PCD® Supervisor ausführende PC und alle für Saia PCD® Supervisor-Clients verwendeten PCs in Einklang mit der IT-Richtlinie Ihres Unternehmens gesichert sind.

3.11 Zugriffskontrolle

Alle Saia PCD® Supervisor-Dateien sollten vor Lese- und Schreib-Zugriff von nicht genehmigten Anwendern und Software geschützt werden. Saia Burgess Controls empfiehlt die Befolgung der optimalen Vorgehensweisen für die Sicherung von System-objekten wie Dateien und die entsprechende Verwendung der Zugriffskontrolle.

Erhalten Windows-Anwender Zugriff auf den Standort des Ablagesystems des Saia PCD® Supervisor-Projekts, ist es möglich, dass sie versehentlich (oder absichtlich) unabhängig von ihren Saia PCD® Supervisor-Arbeitsgruppeeinstellungen Konfigurationsdaten und Dateien öffnen, löschen oder bearbeiten.

Sicherung von Saia PCD® Supervisor

3.12 Sicherung von Saia PCD® Supervisor

Die Saia PCD® Supervisor-Software sollte während der Installation konfiguriert werden und unter Befolgung der optimalen Vorgehensweise bedient werden. Befolgen Sie den in diesem Handbuch beschriebenen Installationsvorgang. Beachten Sie außerdem das Niagara 4-Hilfesystem und die Niagara 4-Sicherheitsrichtlinien.

3.12.1 Standard-Admin-Benutzer einer Station

Erstkonfiguration des Systems wird mithilfe eines standardmäßigen Admin-/Technischer Anwender-Kontos durchgeführt, welches bei der Erstellung der Station mit einem starken Kennwort eingerichtet wird.

3.12.2 Passwort

Das während des Installationsvorgangs des Saia PCD® Supervisor festgelegte Passwort schützt empfindliche Daten auf allen Stationen, die Sie erstellen und ist erforderlich, wenn die Saia PCD® Supervisor-Station auf einen anderen PC umzieht, z. B. zum Standort-PC oder nach einem PC-Fehler wiederhergestellt wird.

3.12.3 Einrichtung anderer Anwender für die Station

Nach Abschluss der Konfiguration (durch den Standard-Admin-Anwender) müssen weitere Anwenderkonten hinzugefügt werden, die verschiedenen Anwendern je nach Rolle spezifische Zugriffsrechte einräumen. Saia PCD® Supervisor erfordert die Verwendung starker Kennwörter.

Weitere Einzelheiten finden Sie im Handbuch 27-651 im Kapitel „*7 Verwendung von Saia PCD® Supervisor*“.

3.13 Einrichten der Google 2-Faktorauthentifizierung

Das Google-Authentifizierungsschema ist ein Zwei-Faktor-Authentifizierungsmechanismus, bei dem der Benutzer sein Kennwort sowie ein Einmal-Token eingeben muss, wenn er sich bei einer Station anmeldet. Dies schützt das Konto eines Benutzers, auch wenn sein Kennwort manipuliert wurde.

Dieses Authentifizierungsschema basiert auf TOTP (Time-based One Time Password) und der Google Authenticator-App auf dem Mobilgerät des Nutzers, um einmal verwendbare Authentifizierungstoken zu generieren und zu überprüfen. Die Google-Authentifizierung ist zeitbasiert, sodass keine Abhängigkeit von der Netzwerkkommunikation zwischen dem Mobilgerät des Nutzers, der Station oder externen Servern besteht. Da der Authentifikator zeitbasiert ist, müssen die Uhrzeit in der Station und die Uhrzeit im Telefon relativ synchron bleiben. Die App bietet einen Puffer von plus oder minus 1,5 Minuten, um den Zeitversatz zu berücksichtigen.

Voraussetzungen:

Für das Mobiltelefon des Nutzers ist die Google-Authentifizierungs-App erforderlich.

Sie arbeiten in der Workbench.

- Der Benutzer ist in der Stationsdatenbank vorhanden.

Führen Sie die folgenden Schritte aus:

1. Öffnen Sie die GAuth-Palette und fügen Sie das *GoogleAuthenticationScheme* zum Knoten **Dienste > Authentifizierungsdienst** in der Navigationsstruktur hinzu.
2. Klicken Sie mit der rechten Maustaste auf **Userservice**, und doppelklicken Sie auf den Benutzer in der Tabelle.
   Die Bearbeitungsansicht für den Benutzer wird geöffnet.
3. Konfigurieren Sie die Eigenschaft Name des *Authentication Scheme Name* zu *GoogleAuthenticationScheme* und klicken Sie auf **Save**.
4. Klicken Sie auf die Schaltfläche neben dem *secret Key* unter dem Authentifikator des Benutzers und befolgen Sie die Anweisungen.
5. Um die Konfiguration abzuschließen, klicken Sie auf **Save**.
   Je nachdem, welche Ansicht Sie verwenden, müssen Sie den Benutzer möglicherweise erneut öffnen oder aktualisieren nach dem Speichern.

3.14 Saia PCD® Supervisor-Sicherheits-Checkliste

- ❑ Neueste Version von Saia PCD® Supervisor wird verwendet.
- ❑ Saia PCD® Supervisor-Installationsdateien, Konfigurationsdateien (inklusive Stations-Sicherung), Zertifikate und Lizenzen sind im Notfallwiederherstellungsplan enthalten.
- ❑ Der Saia PCD® Supervisor ausführende PC sollte nach Möglichkeit gegen ungenehmigten physischen Zugriff geschützt werden.
- ❑ Das Ethernet-Netzwerk (und alle anderen Netzwerke), mit dem der PC verbunden ist, ist gesichert, z. B. durch die Verwendung von Firewalls und Einbruchserkennungssystemen.
- ❑ Auf dem PC läuft die aktuellste Version des Windows-Betriebssystems, mit allen Aktualisierungen und Servicepaketen.
- ❑ Auf dem PC ist Virenschutz-Software installiert.
- ❑ Auf dem PC sind entsprechende Anwenderkonten eingerichtet und der Zugriff auf Dateien ist auf genehmigte Personen beschränkt.
- ❑ Saia PCD® Supervisor ist zur Verwendung von HTTPS mithilfe eines Zertifikats von einer vertrauenswürdigen Zertifizierungsstelle konfiguriert.
- ❑ Saia PCD® Supervisor-Anwender werden nach Bedarf konfiguriert.
- ❑ Stellen Sie sicher, dass Saia PCD® Supervisor entsprechend konfiguriert ist, um Daten regelmäßig in Einklang mit den Sicherungsrichtlinien Ihres Unternehmens an einem sicheren Standort zu sichern.

3.15 Datenschutz-Grundverordnung (DSGVO)

Englisch: General Data Protection Regulation (GDPR)

Die Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) ist eine Verordnung im EU-Recht über Datenschutz und Privatsphäre für alle einzelnen Bürger der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR). Sie befasst sich auch mit der Übermittlung personenbezogener Daten außerhalb der EU und des EWR-Raums. Die DSGVO enthält Bestimmungen und Anforderungen im Zusammenhang mit der Verarbeitung personenbezogener Daten von Einzelpersonen (betroffenen Personen) innerhalb des EWR und gilt für jedes Unternehmen mit Sitz im EWR oder (unabhängig von seinem Standort und der Staatsangehörigkeit der betroffenen Personen), das die personenbezogenen Daten von betroffenen Personen innerhalb des EWR verarbeitet.

Gemäß den Bestimmungen der DSGVO enthalten personenbezogene Daten alle Informationen, die zur Identifizierung einer Person verwendet werden können. Dazu gehören (ist aber nicht beschränkt auf):

Benutzernamen,

Passwörter,

Telefonnummern,

E-Mail-Adressen,

- Arbeits- oder Wohnadressen

Alle in Saia PCD® Supervisor eingegebenen Informationen werden verschlüsselt und auf dem PC gespeichert, auf dem die Saia PCD® Supervisor-Anwendung beim Kunden installiert ist. Weder Honeywell noch Saia Burgess Controls sind an der Speicherung und/oder Verarbeitung personenbezogener Daten innerhalb von Saia PCD® Supervisor beteiligt.

Die Verantwortung für die Einhaltung der Anforderungen der DSGVO liegt in vollem Umfang beim Systemintegrator oder beim Systemadministrator. Als solcher müssen sie sicherstellen, dass angemessene technische und organisatorische Systeme vorhanden sind, um :

von jeder betroffenen Person die ausdrückliche Zustimmung einholen, dass personenbezogene Daten gespeichert, verwendet und / oder verarbeitet werden,

den Einzelnen den Zugang zu ihren personenbezogenen Daten zu ermöglichen, die Richtigkeit zu überprüfen

Einzelpersonen jederzeit die Möglichkeit geben, ihre Einwilligung zu widerrufen und ihre personenbezogenen Daten dauerhaft löschen zu lassen,

die Sicherheit und Integrität der Datenspeicherung und des Zugriffs jederzeit gewährleisten,

alle Verstöße gegen die Datensicherheit (die die Privatsphäre der Nutzer beeinträchtigen können) innerhalb von 72 Stunden nach auftretender Verletzung an die zuständige Behörde zu melden.

3

A Anhang

A.1 Symbole

In Handbüchern verweist dieses Symbol den Leser auf weitere Informationen, die in diesem oder anderen Handbüchern oder technischen Unterlagen enthalten sind. In der Regel gibt es keinen direkten Link zu solchen Dokumenten.

Diese zu diesem Zeichen gehörenden Anweisungen müssen jederzeit befolgt werden.

A.2 Sofware-Versionen

Buch	Auszug aus Buch	Saia PCD® Superrvisor	Niagara
26-624 GER01	**27-651 GER01**	Version V1.1	Basierend auf Niagara V4.3
26-624 GER02	**27-651 GER02**	Version V1.2	Basierend auf Niagara V4.7
26-624 GER03	**27-651 GER05**	Version V2.0	Basierend auf Niagara V4.7U1

A

A.3 Kontakt

Saia-Burgess Controls AG
Bahnhofstrasse 18
3280 Murten
Schweiz

Telefon ..... +41 26 580 30 00
Telefonischer Support ..... +41 26 580 31 00
Fax ..... +41 26 580 34 99

E-Mail-Support: ..... support@saia-pcd.com
Supportseite: ..... www.sbc-support.com
SBC-Seite: ..... www.saia-pcd.com

Internationale Repräsentanten und
SBC-Vertriebsgesellschaften: ..... www.saia-pcd.com/contact

Der technische Support von Saia Burgess Controls ist nur in der Lage, Support für Saia PCD® Supervisor und die in diesem Handbuch beschriebenen Treiberfunktionen zu leisten. Er kann keinen Support für Dritt-Treiber und undokumentierte Aspekte von Saia PCD® Supervisor anbieten.

Technische Publikationen
Bitte senden Sie jegliche Kommentare hierzu oder zu anderen technischen Publikationen von Saia Burgess Controls an support@saia-pcd.com.

A