SAIA BURGESS CONTROLS

Saia PCD® Supervisor

Manuale di sicurezza

Documento 26-624 | Edizione ITA03 | 2019-11-21

0

0

0.1 Cronologia del documento

Versione	Data di pubblicazione	Modifiche	Note
ITA01	2019-07-01	Documento intero	- Estratto dal manuale 27-651 ENG01
ITA02	2019-07-02	Cap. 13.13	- Nuovo sottocapitolo “Impostazione dell’autenticazione dei fattori di Google 2”
ITA03	2019-11-21	Cap. 13.15	- Nuovo sottocapitolo “Regolamento generale sulla protezione dei dati (GDPR)”

0.2 Marchi registrati

Saia PCD® è un marchio registrato di Saia-Burgess Controls AG.

Le modifiche tecniche sono vincolate al livello della tecnologia.

Pubblicato in Svizzera

3 Protezione di Saia PCD® Supervisor

3.1 Introduzione

In questa sezione vengono fornite le informazioni necessarie affinché l'operatore addetto all'installazione e manutenzione di un prodotto o sistema conosca i requisiti per la configurazione e la gestione della sicurezza di tale prodotto o sistema.

Manuali con prassi comuni di sicurezza generale per prodotti basati su IP di Saia Burgess Controls "26-776_Manual_TCP-IP-Ethernet" e "26-867_Manual_TCP-IP-Enhancements".

Entrambi i documenti sono disponibili sul sito Web del supporto Saia Burgess Controls www.sbc-support.com.

3.2 Pianificazione di un ripristino d'emergenza

È un processo documentato o una serie di procedure documentata per ripristinare e proteggere un'infrastruttura IT aziendale in caso di emergenza. Tale piano specifica le procedure che un'organizzazione deve seguire in caso di emergenza.

Quando si sviluppa un ripristino d'emergenza, assicurarsi di includere TUTTI i dati richiesti per ripristinare il funzionamento del sistema, inclusi:

- File di configurazione per piattaforme e stazioni
- Oggetti del database
- File di licenze e certificati
- Backup delle stazioni
- Copie delle stazioni

Per dettagli, vedere il manuale 27-651 capitolo "*6.8 Backup e ripristino*".

3.3 Considerazioni fisiche e ambientali

Il PC in cui viene eseguito Saia PCD® Supervisor deve, dove possibile, essere protetto contro qualsiasi accesso fisico non autorizzato.

3.4 Aggiornamenti della sicurezza e Service Pack

Assicurarsi che nel PC in cui viene eseguito Saia PCD® Supervisor ed eventuali dispositivi client siano installati gli ultimi aggiornamenti del sistema operativo e che venga utilizzata l'ultima versione di Saia PCD® Supervisor.

Il software di Saia Burgess Controls software viene testato sui più recenti Service Pack e aggiornamenti applicabili al momento del rilascio. Per Service Pack/aggiornamenti Java e del sistema operativo significativi, visitare il sito Web del supporto Saia Burgess Controls www.sbc-support.com per eventuali problemi di compatibilità.

3.5 Protezione antivirus

Verificare che nel PC in cui viene eseguito Saia PCD® Supervisor ed eventuali dispositivi client sia installato un software di protezione antivirus e che le definizioni dei virus siano aggiornate.

Alcuni tipi di software di protezione antivirus possono avere un impatto negativo sulle prestazioni di Saia PCD® Supervisor. In tali casi, richiedere che la directory di Saia PCD® Supervisor venga esclusa dalla scansione sempre attiva.

Per ulteriori dettagli, visitare il sito Web del supporto Saia Burgess Controls www.sbc-support.com.

3.6 Sicurezza e pianificazione della rete

È consigliabile che la rete Ethernet utilizzata dal sistema di gestione edifici (*Building Management System*, BMS) sia separata dalla normale rete dell'ufficio mediante un air gap (cablaggio e dispositivi separati o switch di livello 3 o rete virtuale privata (*Virtual Private Network*, VPN)). L'accesso fisico all'infrastruttura di rete Ethernet deve essere limitato. È inoltre necessario verificare che l'installazione venga eseguita in conformità alla politica IT aziendale.

L'uso di un firewall e di un sistema di rilevamento delle intrusioni (*Intrusion Detection System*, IDS) di un fornitore rispettabile di prodotti per la sicurezza è consigliato per qualsiasi installazione di Saia PCD® Supervisor. Seguire le migliori prassi per i prodotti scelti così come ogni politica IT aziendale quando si esegue l'installazione. Bloccare i prodotti alla porta specifica che è stata configurata per i protocolli HTTPS e HTTP di Saia PCD® Supervisor.

Seguire sempre le linee guida contenute nei seguenti documenti PDF:

manuale	26-776_Manual_TCP-IP-Ethernet
manuale	26-867_Manual_TCP-IP-Enhancements
manuale	26-620_Manual_Security-Rules
manuale	Niagara^{AX} Hardening Guide
istruzioni	30-002_Internet-Security-Instructions_SBC
istruzioni per l'uso del router VPN	30-004_VPN-Router

È inoltre necessario adottare misure per garantire la sicurezza di eventuali altre reti connesse a Saia PCD® Supervisor (ad es. BACnet).

3.7 Ambienti virtuali

Seguire le migliori prassi per i prodotti scelti così come ogni politica IT aziendale quando si esegue l'installazione.

3.8 Protezione di dispositivi wireless

Se si utilizza una rete wireless, è necessario proteggerla in base alla politica IT aziendale.

3.9 Monitoraggio del sistema

Per qualsiasi installazione di Saia PCD® Supervisor, specialmente quando il sistema è connesso a Internet, Saia Burgess Controls consiglia di utilizzare un sistema di rilevamento delle intrusioni (IDS) di un fornitore rispettabile di prodotti software. Seguire le migliori prassi per i prodotti scelti così come ogni politica IT aziendale quando si esegue l'installazione.

Saia PCD® Supervisor registra (cronologia di controllo) le modifiche apportate alla propria configurazione e le regolazioni effettuate nel sistema di controllo Saia Burgess Controls. Molti prodotti IDS e firewall offrono una soluzione completa per la registrazione di tutto il traffico in entrata e in uscita dal PC con Saia PCD® Supervisor, consentendo agli utenti di tener traccia di tutte le attività al livello più basso.

3.10 Protezione dell'accesso al sistema operativo

Assicurarsi che il PC in cui viene eseguito Saia PCD® Supervisor ed eventuali PC utilizzati per i client con Saia PCD® Supervisor siano protetti in base alla politica IT aziendale.

3.11 Controllo dell'accesso

Tutti i file di Saia PCD® Supervisor devono essere protetti dall'accesso in lettura e scrittura da parte di persone e software non autorizzati. Saia Burgess Controls consiglia di attenersi alle seguenti migliori prassi per la protezione degli oggetti del sistema, come i file, e di utilizzare il controllo dell'accesso in modo appropriato.

Se agli utenti Windows viene concesso l'accesso alla posizione del sistema di archiviazione del progetto Saia PCD® Supervisor, possono aprire, eliminare o modificare inavvertitamente (o deliberatamente) uno qualsiasi dei file di dati e di configurazione indipendentemente dalle loro impostazioni dei gruppi di lavoro di Saia PCD® Supervisor.

Protezione di Saia PCD® Supervisor

3.12 Protezione di Saia PCD® Supervisor

Il software di Saia PCD® Supervisor deve essere configurato durante l'installazione e il funzionamento seguendo le migliori prassi indicate. Attenersi alla procedura di installazione descritta in questo manuale. Inoltre, fare riferimento al sistema di guida di Niagara 4 e alle linee guida per la sicurezza di Niagara V4.7U1.

3.12.1 Utente amministratore predefinito di una stazione

La configurazione iniziale del sistema viene eseguita utilizzando un account utente di amministrazione/progettazione predefinito che viene impostato con una password complessa quando la stazione viene creata.

3.12.2 Passphrase

La passphrase, specificata durante la procedura di installazione di Saia PCD® Supervisor, protegge i dati sensibili in qualsiasi stazione creata e verrà richiesta qualora la stazione di Saia PCD® Supervisor dovesse essere spostata in un altro PC, ad es. spostata nel PC del sito, o ripristinata dopo un guasto al PC.

3.12.3 Impostazione di altri utenti per la stazione

Una volta completata la configurazione (utilizzando l'utente amministratore predefinito), è necessario aggiungere altri account utente che concedono a utenti differenti diritti di accesso specifici in base ai loro ruoli. Saia PCD® Supervisor impone l'utilizzo di password complesse.

Per ulteriori dettagli, vedere il 27-651 capitolo "*7 Utilizzo di Saia PCD® Supervisor*".

3.13 Impostazione dell’autenticazione a 2 fattori di Google

Lo schema di autenticazione di Google è un meccanismo di autenticazione a due fattori che richiede all’utente di immettere la propria password e un token una tantum quando si connette a una stazione. Questo protegge l’account di un utente anche se la sua password è compromessa.

Questo schema di autenticazione si basa su TOTP (password una tantum basata sul tempo) e sull’applicazione Google Authenticator sul dispositivo mobile dell’utente per generare e verificare token di autenticazione una tantum. Poiché l’autenticazione di Google è basata sul tempo, non vi è alcuna dipendenza dalla comunicazione di rete tra il dispositivo mobile dell’utente, la stazione o i server esterni. Poiché l’autenticatore si basa sull’ora, l’ora nella stazione e l’ora nel telefono devono rimanere relativamente sincronizzate. L’applicazione fornisce un buffer di più o meno 1,5 minuti per tenere conto del cambio di orario.

Prerequisiti:

Il telefono cellulare dell’utente richiede l’app di autenticazione di Google.

Lavori in Workbench.

- L’utente esiste nel database della stazione.

Effettuare le seguenti operazioni:

1. Apri la palette GAuth e aggiungi il programma **GoogleAuthenticationScheme** al nodo **Services > Authenticationservice** nella struttura di navigazione.
2. Fare clic con il pulsante destro del mouse su **Userservice** e fare doppio clic sull’utente nella tabella.
   Si apre la vista Modifica utente.
3. Impostare la proprietà *Authentication Scheme Name* su *GoogleAuthenticationScheme* e fare clic su Salva **“Save”**.
4. Fai clic sul pulsante accanto a *secret Key* sotto l’autenticatore dell’utente e segui le istruzioni.
5. Per completare la configurazione, fai clic su Salva **“Save”**.
   A seconda della vista in uso, potrebbe essere necessario riaprire l’utente o aggiornare dopo il salvataggio.

3.14 Elenco di controllo per la sicurezza di Saia PCD® Supervisor

- ❑ Viene utilizzata la versione più recente di Saia PCD® Supervisor.
- ❑ I file di installazione, i file di configurazione (compreso il backup delle stazioni), i certificati e le licenze di Saia PCD® Supervisor sono inclusi nella piano del ripristino di emergenza.
- ❑ Il PC in cui viene eseguito Saia PCD® Supervisor deve, dove possibile, essere protetto contro qualsiasi accesso fisico non autorizzato.
- ❑ La rete Ethernet (ed eventuali altre reti) connessa al PC è protetta, ad es. mediante l'uso di firewall e sistemi di rilevamento delle intrusioni.
- ❑ Nel PC viene eseguita la versione più recente del sistema operativo Windows, con tutti gli aggiornamenti e i Service Pack.
- ❑ Nel PC è in esecuzione un software di protezione antivirus.
- ❑ Nel PC sono stati impostati gli account utente appropriati e l'accesso ai file è limitato ai soli utenti autorizzati.
- ❑ Saia PCD® Supervisor è configurato per l'uso di HTTPS utilizzando un certificato di un'autorità di certificazione attendibile.
- ❑ Gli utenti di Saia PCD® Supervisor sono stati configurati come richiesto.
- ❑ Verificare che Saia PCD® Supervisor sia configurato per eseguire il backup regolare dei dati in una posizione sicura in base alla politica di backup dell'azienda.

3.15 Regolamento generale sulla protezione dei dati (RGPD)

Inglese: General Data Protection Regulation (GDPR)

Il regolamento generale sulla protezione dei dati (UE) 2016/679 (RGPD) è un regolamento della legislazione UE sulla protezione e la privacy dei dati per tutti i cittadini dell'Unione europea (UE) e dello Spazio economico europeo (SEE). Si occupa anche del trasferimento di dati personali al di fuori delle aree UE e SEE. La RGPD contiene disposizioni e requisiti relativi al trattamento di dati personali di soggetti (soggetti interessati) all'interno del SEE e si applica a qualsiasi impresa stabilita nel SEE o (indipendentemente dalla sua posizione e dalla cittadinanza degli interessati) che sta elaborando il personale informazioni degli interessati all'interno del SEE.

Secondo i termini del RGPD, i dati personali includono qualsiasi informazione che può essere utilizzata per identificare una persona. Questo include (ma non è limitato a):

nomi utente,

le password

numeri di telefono,

indirizzi email,

- indirizzi professionali o residenziali.

Tutte le informazioni inserite in Saia PCD® Supervisor verranno crittografate e archiviate sul PC in cui l'applicazione Saia PCD® Supervisor è installata sul sito del cliente. Né Honeywell né Saia Burgess Controls sono coinvolti nella conservazione e/o nell'elaborazione dei dati personali all'interno di Saia PCD® Supervisor.

La responsabilità del rispetto dei requisiti del RGPD spetta interamente all'integratore di sistema o all'amministratore di sistema, che deve quindi garantire che siano predisposti adeguati sistemi tecnici e organizzativi per:

ottenere il consenso esplicito di ciascuna persona interessata a conservare, utilizzare e / o elaborare i dati personali,

consentire alle persone di avere accesso ai propri dati personali per verificarne l'accuratezza,

consentire alle persone di ritirare il loro consenso in qualsiasi momento ed eliminare definitivamente i propri dati personali,

mantenere la sicurezza e l'integrità dell'archiviazione e dell'accesso ai dati in ogni momento,

segnalare eventuali violazioni dei dati (che possono influire sulla privacy degli utenti) all'autorità competente entro 72 ore dal verificarsi di una violazione.

3

A Appendice

A.1 Icone

Nei manuali, questo simbolo rimanda il lettore ad altre informazioni contenute in capitoli diversi dello stesso o in altri manuali o documenti tecnici. Di regola, non ci sono collegamenti diretti a tali documenti.

Questo simbolo accompagna le istruzioni da seguire sempre.

A.2 Versioni del software

Versione del libro	Estratto dal manuale	Saia PCD® Supervisor	Niagara
26-624 ITA01	**27-651 ITA01**	Versione V1.1	Basato su Niagara V4.3
26-624 ITA02	**27-651 ITA02**	Versione V1.2	Basato su Niagara V4.7
26-624 ITA03	**27-651 ITA05**	Versione V2.0	Basato su Niagara V4.7U1

A

A.4 Contatti

Saia-Burgess Controls AG
Bahnhofstrasse 18
3280 Murten
Svizzera

Telefono ..... +41 26 580 30 00
Supporto telefonico ..... +41 26 580 31 00
Fax ..... +41 26 580 34 99

Supporto e-mail: ..... support@saia-pcd.com
Sito del supporto: ..... www.sbc-support.com
Sito di SBC: ..... www.saia-pcd.com

Rappresentanti internazionali
e aziende rivenditrici SBC: ..... www.saia-pcd.com/contact

Il supporto tecnico Saia Burgess Controls può fornire assistenza solo per le funzioni dei driver Saia Burgess Controls e Saia PCD® Supervisor descritte in questo manuale. Non è in grado di fornire assistenza per driver di terze parti e per aspetti non documentati del funzionamento di Saia PCD® Supervisor.

Pubblicazioni tecniche
Inviare eventuali commento al riguardo o qualsiasi altra pubblicazione tecnica su Saia Burgess Controls all'indirizzo support@saia-pcd.com.

A