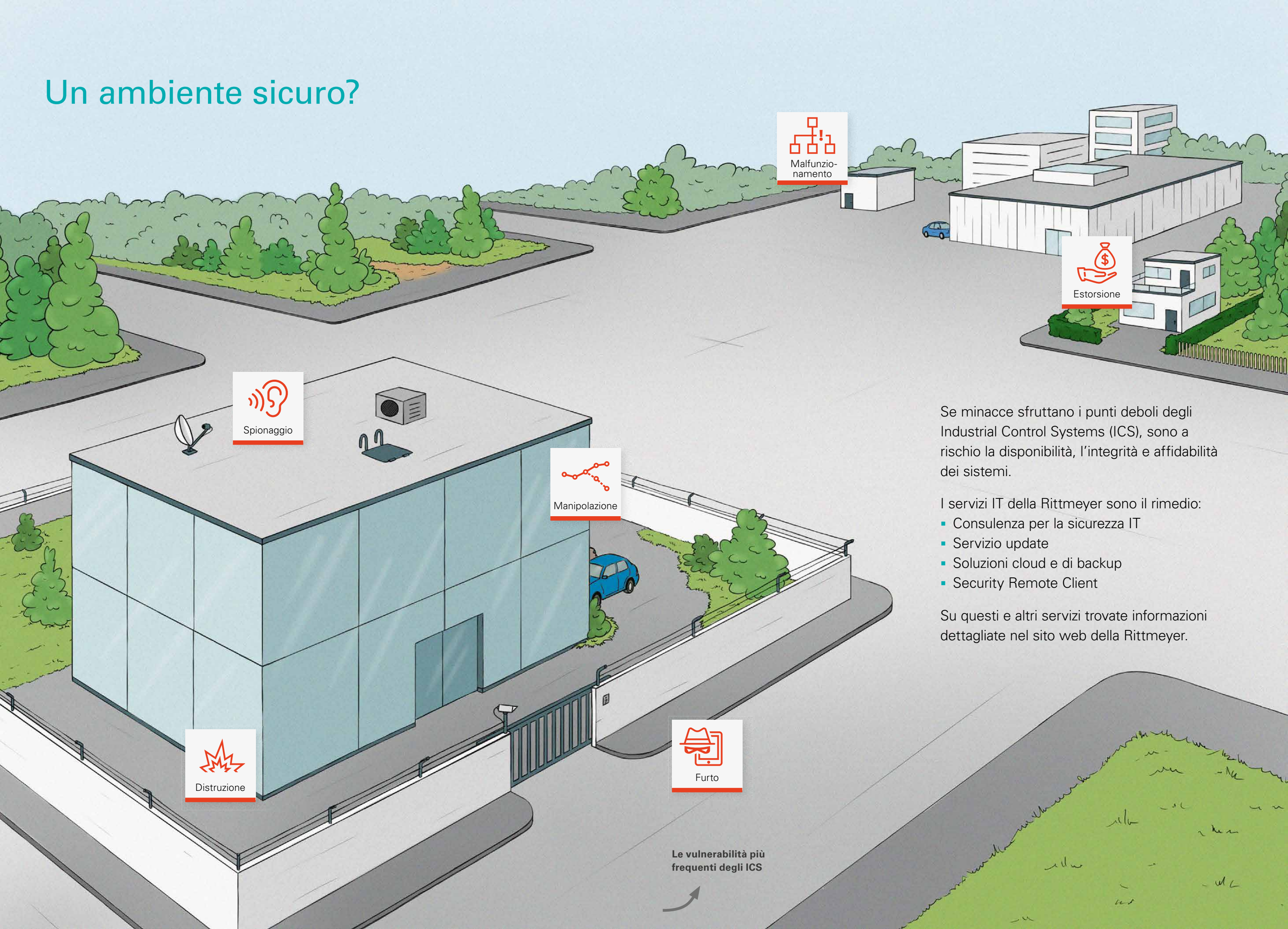
rittmeyer
BRUGG

RISCHI PER LA SICUREZZA NELLE INFRASTRUTTURE CRITICHE

Le più frequenti vulnerabilità degli Industrial Control Systems (ICS)

Un ambiente sicuro?



Se minacce sfruttano i punti deboli degli Industrial Control Systems (ICS), sono a rischio la disponibilità, l'integrità e affidabilità dei sistemi.

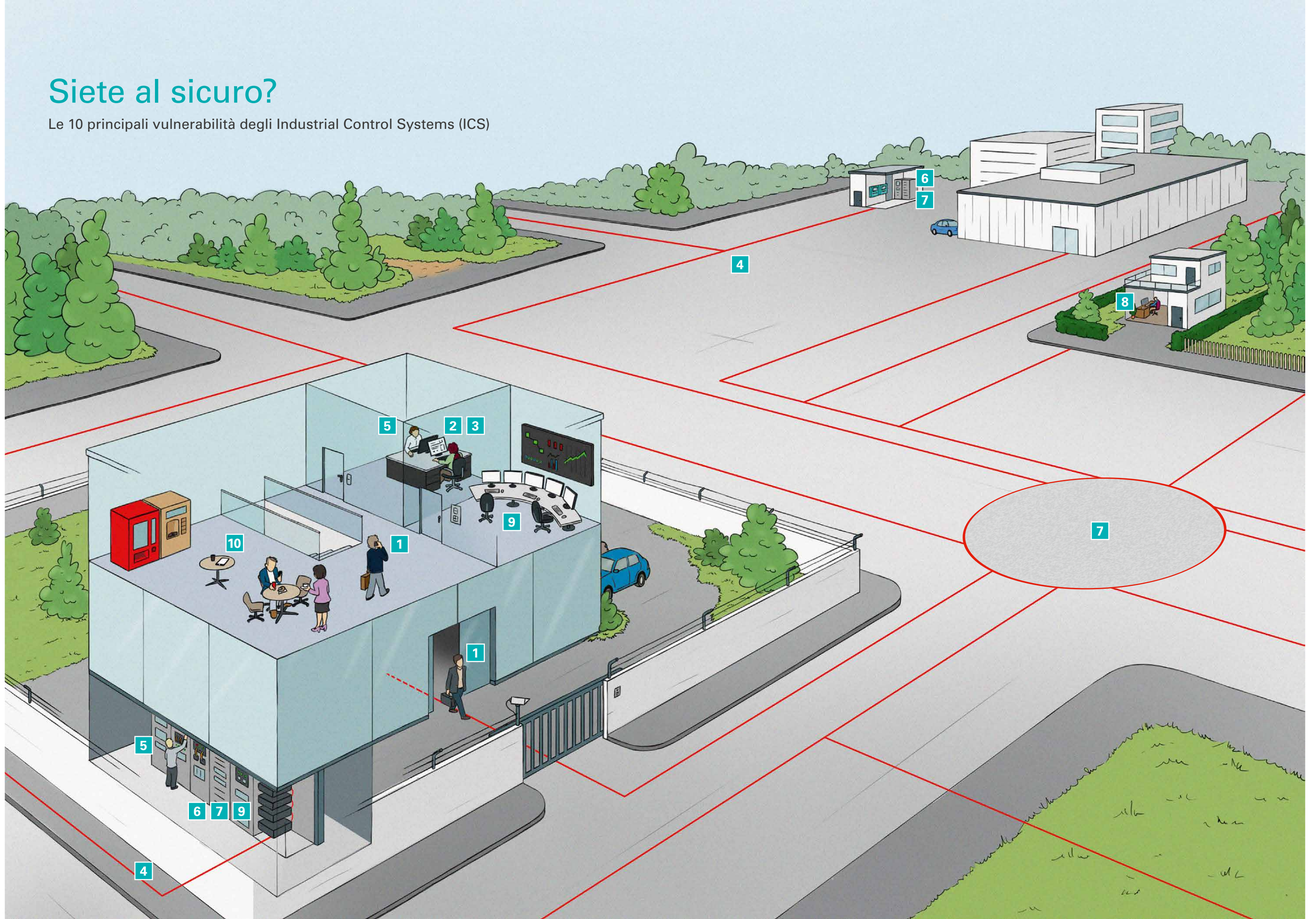
I servizi IT della Rittmeyer sono il rimedio:

- Consulenza per la sicurezza IT
- Servizio update
- Soluzioni cloud e di backup
- Security Remote Client

Su questi e altri servizi trovate informazioni dettagliate nel sito web della Rittmeyer.

Siete al sicuro?

Le 10 principali vulnerabilità degli Industrial Control Systems (ICS)



1 Social engineering

Con il ‹social engineering› si cerca di carpire dati rilevanti per la sicurezza sfruttando componenti umani. Gli uomini sono manipolabili e in generale sono l'anello più debole di una catena.

Protezione

- Addestramento alla consapevolezza della sicurezza
- Direttive di sicurezza
- Controlli di accesso
- Buonsenso
- Creazione di canali di allarme

2 Supporti dati amovibili: infiltrazione di software dannoso

I dipendenti utilizzano supporti dati amovibili e hardware esterno, come ad es. chiavette USB, oltre che in ufficio e nella rete ICS spesso anche nel privato.

Protezione

- Norme per gli utenti
- Protezione tecnica
- Antivirus
- Gestione dei diritti
- Indurimento del computer
- Salvataggio dei dati

3 Internet e Intranet: infezione con software dannoso

Browser e client di posta elettronica sono di regola connessi ad Internet.

Protezione

- Direttive per gli utenti
- Antivirus
- Aggiornamenti del software
- Gestione dei diritti
- Responsabilità
- Indurimento del computer
- Backup dei dati

4 Accessi per la manutenzione remota

Nelle installazioni ICS sono molto diffusi accessi esterni per scopi di manutenzione. Spesso vi sono a tal fine accessi di default con password standard o addirittura password codificate fisse. Questo facilita la penetrazione ai cybercriminali.

Protezione

- Firewall
- Codifica SSL/TLS
- Chiavi precondivise
- Certificati
- Accessi personalizzati
- Audit
- Modifica delle password standard
- Microsegmentazione delle reti
- Codifica di dati sensibili
- Abilitazione di accessi per la manutenzione remota da parte di personale interno
- Registrazione di accessi remoti

5 Errore umano e sabotaggio

L'ambiente di lavoro del personale ICT ha un'importanza particolare sotto l'aspetto tecnico della sicurezza. Le manipolazioni in questi ambienti sono possibili intenzionalmente o involontariamente.

Protezione

- Protezione fisica
- Direttive per gli utenti
- Corsi di formazione
- Gestione dei diritti
- Affermazione del principio ‹Need to know›
- Monitoraggio automatico degli stati e delle configurazioni del sistema

6 Con componenti di controllo connessi ad Internet

Spesso i componenti ICS, come ad esempio i controllori logici programmabili (PLC), vengono collegati direttamente ad Internet (Internet of Things, IoT).

Protezione

- Firewall
- Aggiornamenti del software
- Modifica delle password standard

7 Errore tecnico e forza maggiore

Gli errori del software in componenti specifici di sicurezza e componenti ICS, che causano un imprevisto errore di comportamento, sono altrettanto difficili da escludere quanto possibili difetti dell'hardware e le interruzioni di rete.

Protezione

- Protezione fisica
- Sistemi ridondanti
- Dispositivi di ricambio o sostitutivi
- Manutenzione
- Configurazione di una gestione delle emergenze
- Uso di interfacce standardizzate

8 Pregiudizio per Extranet e componenti cloud

La tendenza diffusa nell'IT convenzionale per l'outsourcing di componenti IT sta facendo il suo ingresso anche nell'ICS.

Protezione

- Accessi VPN
- Offerenti certificati
- Sistemi ridondanti
- Service Level Agreement
- Meccanismi crittografici

9 Attacco (D)DoS

La comunicazione fra componenti ICS può svolgersi attraverso collegamenti cablati e wireless. Se questi collegamenti vengono disturbati, non è più possibile la corretta trasmissione di dati, fra i quali i dati di misurazione e di controllo. Un componente può essere ad esempio sovraccaricato da un altissimo numero di richieste, in misura tale da rendere impossibile qualsiasi ulteriore tempestiva risposta.

Protezione

- Intrusion Detection (IDS)
- Connessioni ridondanti con diversi protocolli
- Connessioni cablate dedicate per funzioni critiche
- Indurimento degli accessi alla rete

10 Ambiente di produzione: pregiudizio per smartphone/tablet

La visualizzazione e modifica di parametri di funzionamento o di produzione su smartphone o tablet sono pubblicizzate e utilizzate come proprietà supplementare del prodotto per un numero sempre maggiore di componenti ICS.

Protezione

- Direttive per gli utenti
- Gestione dei diritti
- Accessi VPN
- Mobile Device Management
- Utilizzo di App Store certificati
- Nessuna App per l'accesso diretto a ICS

Rittmeyer è un'azienda del BRUGG GROUP che sviluppa e fornisce soluzioni di misura e controllo all'avanguardia per approvvigionamenti energetici e idrici, centrali idroelettriche e impianti di depurazione delle acque reflue. Dal 1904 il nome Rittmeyer è sinonimo di massima qualità del prodotto e delle prestazioni. Per Rittmeyer il cliente è come un partner e per questo viene accompagnato durante tutto il ciclo di vita del proprio impianto – dal concepimento alla progettazione, dall'installazione, alla messa in servizio, fino alla formazione dei tecnici e ad un servizio di assistenza completo. Rittmeyer è attiva nel mondo con sei consociate, un ufficio vendita e di rappresentanza, nonché agenzie in oltre 25 paesi.

www.rittmeyer.com

rittmeyer
BRUGG

Rittmeyer AG
Inwilerriedstrasse 57
C.P. 1660
CH-6341 Baar
+41 41 767 10 00
security@rittmeyer.com

82824.1.I | 1804 ERN