

ERZ-PLS-Sicherheitsrichtlinie

Prozessleitsysteme

Zürich, 17. August 2009

Herausgeberin

Stadt Zürich

ERZ Entsorgung + Recycling Zürich

Klärwerk Werdhölzli

Tel. +41 44 645 55 55

Fax +41 44 645 55 59

Kehrichtheizkraftwerke

Tel. +41 44 645 77 77

Fax +41 44 645 77 78

Fernwärme

Tel. +41 44 645 88 88

Fax +41 44 645 88 89

Informatik

Tel. +41 44 645 55 55

Fax +41 44 645 55 56

www.erz.ch

Redaktionelle Bearbeitung

Philipp Sigg

Verfasser/in

Hans Andres, Philipp Sigg, Roland Gantenbein

Version

V03.00

Die wesentlichen Sicherheitsrichtlinien und -anforderungen für den Remote- und Lokal-Zugriff, zur Realisierung des VPN-Tunnels

Inhalt

1	Ausgangslage	4
2	Ziele	4
3	Datenschutz	4
4	Zuständigkeiten	4
5	Sicherheitsrichtlinien	4
5.1	Prozessbedienung verfahrenstechnischer Prozesse	4
5.2	Virenprüf- und Security-Programme	4
5.3	Internetverbindung	5
5.4	Zugriff auf die Prozessleitsysteme	5
5.5	Firewall	5
5.6	Datenfluss zwischen den Werken	5
5.7	Technische Sicherheit	5
5.8	Anpassung an technische Entwicklungen	5
6	Graphische Darstellung der Anbindung	6

1 Ausgangslage

Die Prozessleitsysteme, im speziellen die Server, können aus Gründen der Performance nicht mit Virenschutzsystemen ausgerüstet werden. Deshalb gelten bei Arbeiten am gesamten Prozessleitsystem sowohl lokal intern (bei ERZ) als auch bei externem Zugriff (Remote) adäquate Vorsichtsmassnahmen.

2 Ziele

Dieses Dokument regelt die Anforderungen und Sicherheitsrichtlinien für den Zugriff auf ein Prozessleitsystem im ERZ mit den Zielen:

- Gewährleistung der Sicherheit für die Prozessleitsysteme in ERZ beim Zugriff:
 - Fernzugriff
 - Fernwartung
 - Zugriff lokal
- Die Prozessleitsysteme in ERZ sind vor dem Eindringen aller unerwünschten Daten zu schützen
- Die Verfügbarkeit der Prozessleitsysteme in ERZ darf nicht beeinträchtigt werden und muss jederzeit gewährleistet sein.

3 Datenschutz

Es gelten die allgemeinen gesetzlichen Bestimmungen des Datenschutzes, insbesondere:

- Daten dürfen ohne schriftliche Zustimmung von ERZ nicht weiterverwendet oder publiziert werden

4 Zuständigkeiten

- Der ERZ Projektleiter ist die primäre Ansprechperson für externe Firmen
- Die externen Firmen stellen einen Antrag mit dem Formular «Zugriff auf ERZ-Prozessleitsysteme» beim ERZ Projektleiter bzw. beim PLS-Verantwortlichen.
- Die PLS-Verantwortlichen der Werke sind zuständig für die Bewilligungserteilung, den Zugriff auf ihr Prozessleitsystem, die Installation und für die Verwaltung des Prozessleitsystems ihres Werkes.
- Die ERZ-IT ist zuständig für die Installation, die Abwicklung und die Verwaltung des Fernzugriffs.
- Die externen Firmen sind für ihre Geräte, Installationen, sowie deren Unterhalt und Betrieb selbst zuständig.

5 Sicherheitsrichtlinien

5.1 Prozessbedienung verfahrenstechnischer Prozesse

Die Prozessbedienung sowohl lokal als auch via Fernzugriff wird werkspezifisch festgelegt.

5.2 Virenprüf- und Security-Programme

Als Virenprüf- und Security-Programme werden gängige lizenzierte, professionelle, in der IT-Branche verwendete Programme betrachtet.

Die Virenprüf- und Security-Programme müssen auf dem aktuellen Tages-Stand sein.

5.3 Internetverbindung

Betreiben von Geräten am Prozessleitsystem mit gleichzeitiger Internetverbindung ist sowohl lokal als auch per Remote strengstens verboten.

5.4 Zugriff auf die Prozessleitsysteme

- Sämtliche Geräte, welche ans PLS angeschlossen werden, müssen vor dem Anschliessen geprüft und virenfrei sein.

Das Prüfprotokoll ist auf Verlangen vorgängig dem PLS-Verantwortlichen vorzuweisen.

- Externe Firmen dürfen Arbeiten am Prozessleitsystem nur in Absprache mit ERZ-Verantwortlichen vornehmen.

Verantwortliche Personen sind: PLS Verantwortliche, Schichtverantwortliche, Pikett-Verantwortliche

- Der Zugriff auf das Prozessleitsystem von Aussen erfolgt über einen gesicherten VPN-Tunnel mittels RDP-Protokoll auf einen Terminal-Server. Die Authentifizierung am Terminalserver erfolgt über ein persönliches Benutzerkonto:

Jeder Nutzer ist mittels unterschriebenem Formular: «Zugriff auf ERZ-Prozessleitsysteme» registriert.

- Für den Fernzugriff wird keine Hochverfügbarkeit garantiert
- Der Terminal-Server schliesst die Verbindung nach 1 Stunde im Leerlauf automatisch
- In den Werken von ERZ ist der Zugriff auf das Prozessleitsystem nur mit den dafür zugelassenen, geprüften Quellen (PC, USB-Stick, CD usw.) erlaubt.
- Werksspezifische PC's sind entsprechend den Verwendungen zu schützen.
- Passwort und Benutzerkonto sind persönlich, vertraulich und gegen Missbrauch zu sichern.
- Softwares und Datensicherungen sind in Datensicherungsschränken aufzubewahren.

5.5 Firewall

Als Grundkonfiguration der Firewall gilt generell: **ALLE Ports sind geschlossen.** Für jeden zu öffnenden Port muss der Bedarf nachgewiesen werden und mit dem werkszuständigen PLS-Verantwortlichen und der ERZ-IT abgesprochen und dokumentiert werden.

5.6 Datenfluss zwischen den Werken

- Zwischen den Prozessleitsystemen der Werke erfolgt keine Datenkommunikation.
- Aus der ERZ Büromatik erfolgt kein Zugriff auf die Prozessleitsysteme. Für die Auswertung der Betriebsdaten steht ein zentraler Datenbankserver «PLS DWH» in einer geschützten Zone. Die Nutzung ist im «ERZ-PLS-Prozessdatenkonzept» beschrieben.

5.7 Technische Sicherheit

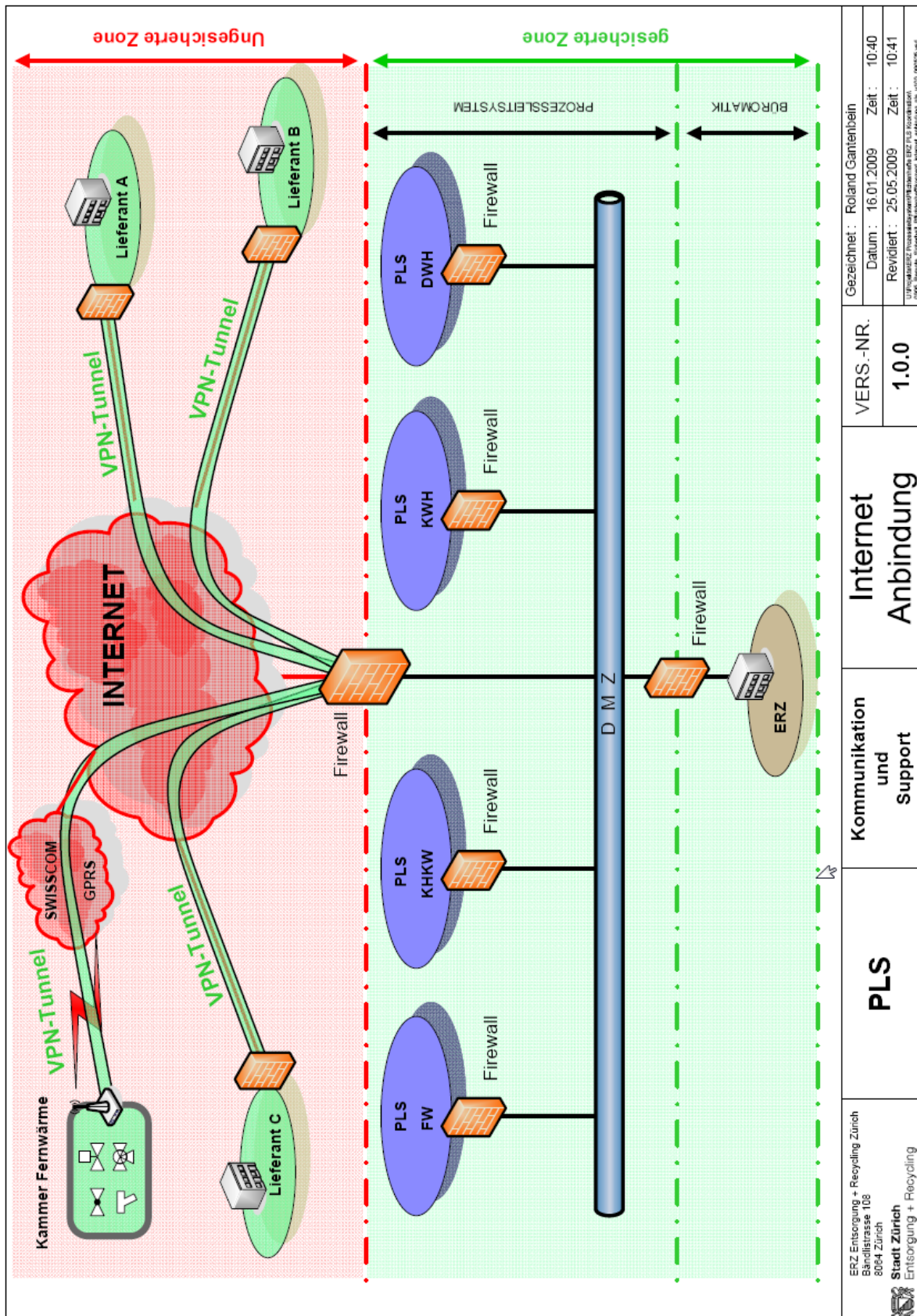
Die technische Sicherheit ist durch die Zuständigen gemäss (Kap. 4) sicherzustellen:

- Beschriftung aller Installationen (insbesondere Kabel, Switches, Hub, Router usw.) müssen verständlich, eindeutig, dauerhaft, der Funktion entsprechend beschriftet sein.
- Die Installationen und Konfigurationen sind geeignet zu dokumentieren.

5.8 Anpassung an technische Entwicklungen

Bei weitergehenden Schutzanforderungen oder neueren technischen Entwicklungen (z.B. automatische Prüfungen) behalten wir uns vor, den Schutz der Prozessleitsysteme auszubauen.

6 Graphische Darstellung der Anbindung



Dieses Dokument unterliegt dem Mutationswesen der ERZ-IT.