Weiterbildungskurse 2018

Schweizerischer Brunnenmeister-Verband

www.brunnenmeister.ch

Blackout – wenn nichts mehr geht

Von:

Damian Kempter
Geschäftsleitung, Kundenberatung
Kempter Meile AG, Engineering Leitsysteme
Churfirstenstrasse 54
9500 Wil

KEMPTER MEILE
ENGINEERING · LEITSYSTEME

https://www.kempter-meile.ch

damian.kempter@kempter-meile.ch

Veranstaltungsort:
CAMPUS SURSEE
Lernen / Leben / Erleben

Blackout – wenn nichts mehr geht

Autor / Referent: Damian Kempter

Inhalt

1 Einleitung

1.1 Über Kempter Meile AG, Engineering Leitsysteme

Kempter Meile AG ist ein lieferantenunabhängiges und produkteneutrales Ingenieurbüro, welches seit 1984 Energie- und Wasserversorgungsunternehmen bei der Spezifikation, Beschaffung und Realisierung von Steuerungen und Leitsystemen berät. Zu unseren Kunden zählen schweizweit sowohl örtliche Versorgungen wie Korporationen, Stadtwerke als auch überregionale Versorgungen wie Gruppenwasserversorgungen, Zweckverbände oder Wasserverbunde.
Unsere 13 Mitarbeiter und Mitarbeiterinnen packen mit Freude an, sei es in einer kurzen Stellungnahme in Form einer Zweitmeinung, bei einer einfachen Offertanfrage, bei einer Submission eines Leitsystems oder bei der Gesamtprojektleitung und technischen Begleitung Ihres Steuerungsprojektes.

1.2 Blackout

„Blackout“ stammt aus dem Englischen und wird im Deutschen in bestimmten Zusammenhängen gebraucht. In verschiedenen Wörterbüchern wird Blackout wie folgt übersetzt:

- Ausfall, Totalausfall, Gesamtausfall
- Infrastrukturausfall
- Programmausfall
- Stromausfall
- Schwarzfall
- Verdunkelung
- Blockierung, Sperre
- Ohnmachtsanfall
- Gedächtnisstörung
- Aussetzer

Es geht also nicht nur um einen Stromausfall, sondern allgemein um das plötzliche Versagen eines Zustandes. In diesem Beitrag beziehen wir uns nebst dem Stromausfall auch auf den Totalausfall, Infrastrukturausfall, Programmausfall sowie auf die Blockierung und Sperre immer in Bezug auf die Steuerung und das Leitsystem. Wir werden nicht auf hydraulische oder chemische Schadenpotentiale eingehen.

1.3 Hierarchischer Aufbau des Steuerungs- und Leitsystems

Ein Steuerungs- und Leitsystem ist hierarchisch in verschiedene Steuerungsebenen gegliedert. Um die Tragweite eines Teil- oder Totalausfalls beurteilen zu können, ist es wichtig, die Aufgaben der einzelnen Steuerungsebenen zu kennen.

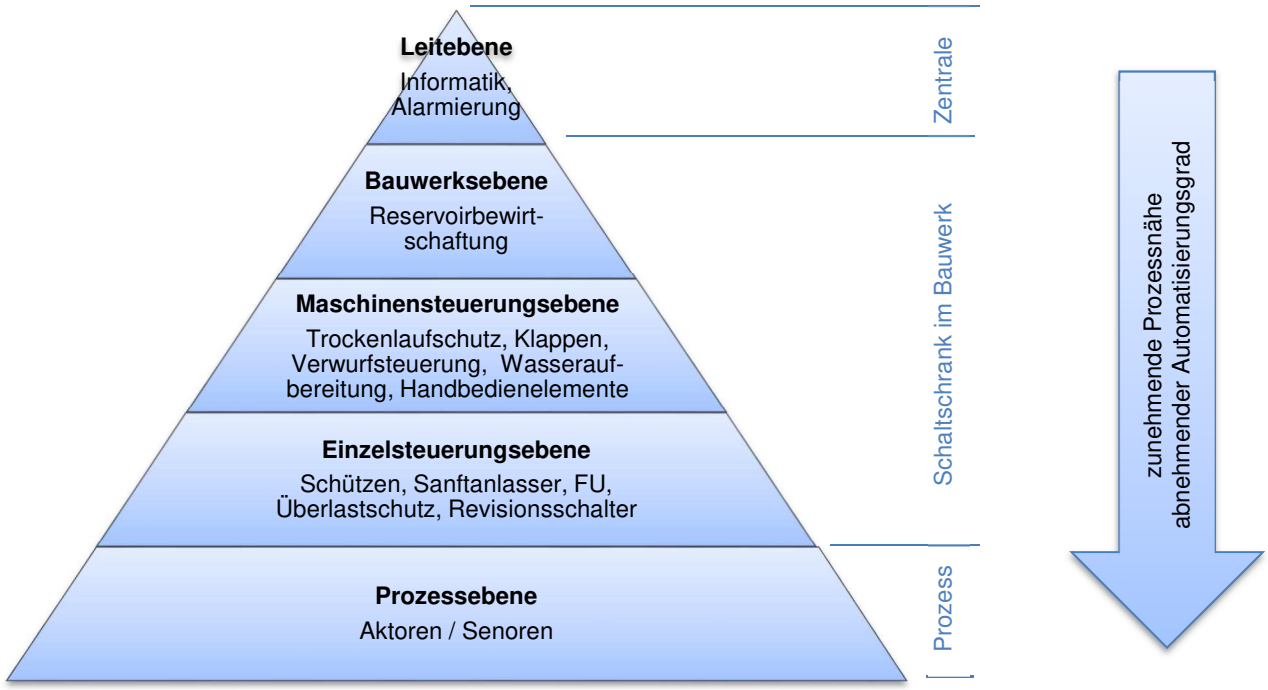

Abbildung 1: Hierarchischer Aufbau des Steuerungs- und Leitsystems

Prozessebene

Zur Prozessebene gehören die Sensoren und Aktoren. Dies sind in einer Wasserversorgung z.B. Wasserzähler, Durchflussmesser, Wasserstandsonden, Drucksonden, Temperaturfühler, Wasser-qualitätsmessgeräte, Türkontakte, Schalter, Taster, Motoren, Klappen, Ventile, Signalleuchten etc.

Einzelsteuerungsebene

In der Einzelsteuerungsebene werden die einzelnen Aggregate angesteuert. Bei Wasserversorgungen sind dies mehrheitlich Motoren von Pumpen und Klappen. Angesteuert werden diese Motoren aus der Maschinensteuerungsebene über Schützen, Sanftanlasser oder Frequenzumformer. In der Einzelsteuerungsebene sind nur Noteingriffe über Revisionsschalter oder die Unterbrechung von Sicherungselementen möglich. Es findet in dieser Ebene keine Überwachung des Prozesses statt. Einzig werden die Motoren und Kabel gegen Überstrom und Überlast geschützt. In bestimmten Situationen werden Verriegelungen bereits in dieser tiefen Ebene realisiert. Beispielsweise werden zwei Pumpen gegenseitig verriegelt, wenn für den gleichzeitigen Betrieb beider Pumpen die Anschlussleistung nicht ausreichte oder wenn durch den gleichzeitigen Betrieb von zwei Pumpen die Gefahr eines Leitungsbruches entstünde.

Maschinensteuerungsebene
Auf der Maschinensteuerungsebene werden Funktionseinheiten aus einzelnen Aggregaten und Sensoren gebildet. Typische Funktionseinheiten in einer Wasserversorgung sind beispielsweise Wasserförderungseinheiten, Quellwassereinläufe, Trinkwasserkraftwerke, Wasseraufbereitungen etc. Eine Wasserförderungseinheit besteht in der Regel aus einer Pumpe, Saugschutz, Strömungsüberwachung, Anlaufdrosselklappe und Handbedienelementen. In der Maschinensteuerungsebene wird die Wasserförderung angesteuert und überwacht. Erhält die Wasserförderungseinheit einen EIN-Befehl zur Förderung entweder aus der übergeordneten Steuerungsebene oder ab dem Handbetriebsschalter, so prüft die Maschinensteuerung (Pumpenautomat) vor dem Einschalten der Pumpe, ob saugseitig genügend Wasser vorhanden ist und ob die Anlaufdrosselkappe geschlossen ist. Ist eine der beiden Bedingungen nicht erfüllt, wird eine Störung signalisiert. Sind beide Bedingungen erfüllt, so wird die Pumpe eingeschaltet, deren Betrieb an die nächst höhere Steuerungsebene signalisiert und der AUF-Befehl an die Anlaufdrosselkappe gegeben. Wird nicht innert einer definierten Zeit eine Strömung gemessen, so wird die Anlaufdrosselklappe wieder geschlossen, die Pumpe abgestellt und eine Störung signalisiert. Wird eine Strömung gemessen, so ist der Förderbetrieb erfolgreich gestartet. Die Strömung wird während dem Pumpeneinsatz dauernd überwacht. Dies ist nur ein ausführlich beschriebenes Beispiel für eine Funktionseinheit Auf der Maschinensteuerungsebene. Genauso sind weitere Funktionseinheiten mit ihren spezifischen Funktionsabläufen zum Beispiel für das Abschalten einer Turbine oder das Überwachen einer Ultrafiltrationsanlage denkbar. Die Maschinensteuerungsebene gehört, wie es ihr Name schon ausdrückt, zur Maschine. Sind Maschinen wie beispielsweise Pumpen aus Redundanzgründen mehrfach vorhanden, so macht dies nur Sinn, wenn auch deren Maschinensteuerung redundant aufgebaut ist.

Bauwerksebene
In der Industrieautomation wird diese Ebene Zellenebene genannt. Auf die Wasserversorgung bezogen, wird hier sinnbildlich von der Bauwerksebene gesprochen. In der Bauwerksebene wird dafür gesorgt, dass die einzelnen Maschinen zum richtigen Zeitpunkt eingesetzt werden. Dies ist zum Beispiel bezogen auf die Wasserversorgung die Reservoirbewirtschaftung, also die Wasserförderung in Abhängigkeit eines Sollwasserstandes (Füllstandskurve) in ein Zielreservoir oder der Kraftwerkseinsatz nach einem Produktionsfahrplan. Weiter gehören in diese Ebene bauwerksbezogene Überwachungen zum Beispiel für den Gebäudezutritt, Überflutung, Kommunikation, Stromversorgung, Batterien etc.

Leitebene
In der Leitebene befindet sich das Leitsystem, welches auf Servern entweder physisch, virtualisiert oder in der Cloud betrieben wird. Die Aufgabe des Leitsystems ist die Visualisierung des Prozesszustandes, die Fernsteuerung der Aggregate und Maschinen, die Überwachung des Prozesses und der Maschinen, die Alarmierung im Störungsfall sowie Protokollierung der Betriebsmeldungen und Messwerte und Archivierung der Prozessdaten.
Durch die Verwendung der klassischen IKT-Infrastrukturen ist die Bedienung der Leitebene nicht mehr örtlich begrenzt. Via Internet kann auch von Ferne auf die Leitebene zugegriffen werden. Wasserversorgungen gehören zu den kritischen Infrastrukturen eines Landes. Daher sollten deren Systeme erhöhte Standards betreffend IT-Sicherheit erfüllen.

2 Blackout-Szenarien

2.1 Lokaler Stromausfall

Unsere Verteilnetzbetreiber leisten sehr gute Arbeit. Trotzdem kommt es immer wieder zu Zwischenfällen beispielsweise bei Netzausbauarbeiten, durch defekte Spannungswandler, Unwetter, Überschwemmungen etc.


MÄNNEDORF

Ein Teil Männedorfs blieb noch länger ohne Strom

Vorderhand bezieht ein Teil Männedorfs seinen Strom über eine provisorische Trafostation. Diese Gebiete blieben noch länger dunkel, als der Stromausfall vom Samstagabend im Grossteil der Gemeinde behoben war.

Abbildung 2: Zürichsee-Zeitung vom 11.12.2017

Stromausfälle wegen des Sturms in verschiedenen Landesteilen:
Im Gebiet der Centralschweizer Kraftwerke waren rund 6000 Kunden betroffen, im Kanton Bern etwa 14 000 Stromabnehmerinnen und -abnehmer, vor allem im Berner Jura, im Emmental und im Oberland.

Mehrere Tausend Menschen hatten am rechten Zürichseeufer keinen Strom, weil Bäume auf eine Hochspannungsleitung gestürzt waren. Auch im Neuenburger Val-de-Travers traf ein Stromunterbruch ungefähr 10 000 Personen.

Abbildung 3: NZZ-Online vom 04.01.2018 berichtet über Sturm „Burglind“

Meistens können die Verbraucher nach solchen Fehlern innert einigen Stunden wieder mit Strom versorgt werden. Dies gelingt dank Redundanzen im Stromnetz und umgehend erstellter Provisorien. Besonders bei Verbrauchern ausserhalb dicht besiedelter Orte sind die Möglichkeiten für eine provisorische Wiederversorgung oft eingeschränkt, wodurch Stromunterbrüche länger dauern können.

2.2 Mehrtägiger flächendeckender Stromausfall

Bis vor wenigen Jahren wurde ein mehrtägiger flächendeckender Stromausfall von der Mehrheit der Bevölkerung und der Fachleute als sehr unwahrscheinliche beurteilt. Erst im Dezember 2016 sprach Swissgrid die nationale Netzgesellschaft von einer Stromknappheit. Der milde Winter wendete einen Strom-Blackout in der Schweiz ab.

Milder Winter wendet Strom-Blackout ab
Letzten Dezember sah es noch so aus, als gehe der Schweiz im Frühling der Strom aus. Jetzt gibt Swissgrid eine «umfassende Entwarnung».

Abbildung 4: Tagesanzeiger vom 06.04.2016

Swissgrid hat diverse Vorkehrungen getroffen und für den Winter 2017/18 Entwarnung gegeben. Dennoch sind der steigende Stromkonsum, die Zunahme an volatilen Einspeisungen aus Photovoltaik und Wind, Abschaltung von Grosskraftwerken, weniger Wasserkraft wegen Trockenheit und zunehmende Abhängigkeit von Internet und Informatik nicht unbedingt Faktoren, welche für eine stabilere Stromversorgung sprechen.

2.3 Hardwaredefekt

Von den namhaften Steuerungslieferanten wird zum Glück robuste Industrie-Elektronik eingesetzt. Dadurch sind Hardwareausfälle eher selten. Dennoch gibt es sie, wie es die folgende Schlagzeile zeigt.

Neues Leitsystem erhöht Versorgungssicherheit
Update Die Folgen des Totalausfalls der Steuerung in der Betriebswarte der Wasserversorgung Degersheim im Jahr 2015 waren fatal. Wiederholen wird sich Vergleichbares kaum. Die Installation eines neuen, modernen Leitsystems ist weitgehend abgeschlossen.

Abbildung 5: Wiler Zeitung vom 11.02.2017

Durch geschickte Aufteilung der Steuerungskomponenten und gezielte Redundanzen können Sie Blackouts, bedingt durch Hardwareausfall, weitgehend vermeiden.

2.4 Breit gestreute Schadsoftware

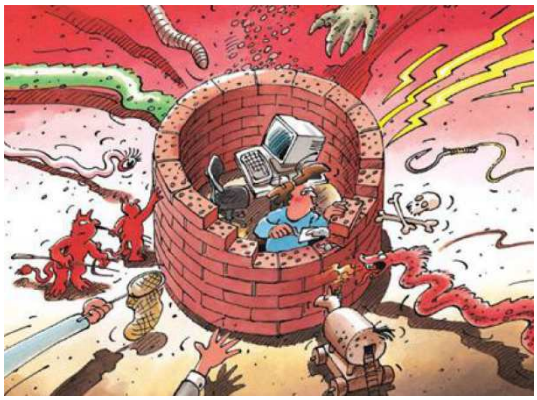

Abbildung 6: www.melani.admin.ch

Im Halbjahresbericht 2017 (Januar - Juni) widmet sich MELANI (Melde- und Analysestelle Informationssicherung des Bundes) im Schwerpunktthema der Verschlüsselungssoftware wie „WannaCry“ oder „Petya“. Vom Verschlüsselungstrojaner „WannaCry“ waren in 150 Ländern mindestens 200‘000 Rechner betroffen. Von betroffenen Rechnern wurden alle sichtbaren Laufwerke verschlüsselt und von den Opfern wurde für den Entschlüsselungscode eine Lösegeldsumme verlangt.
Ist ein Versorgungsunternehmen Opfer von einer Schadsoftware geworden, wird es damit kaum freiwillig an die Öffentlichkeit gelangen. Vielmehr wird es versuchen Schadensbegrenzung zu betreiben, bevor der Vorfall publik wird. Es ist daher nicht erstaunlich, wenn über solche Vorfälle wenig zu hören oder zu lesen ist.
Aus zuverlässiger Quelle ist uns jedoch ein Fall eines Schweizer Energieversorgungsunternehmens bekannt, welches Opfer eines Verschlüsselungstrojaners wurde. Das ganze Netzleitsystem war verschlüsselt und unbrauchbar. Dank einer funktionierenden Datensicherung und eines Sondereinsatzes des Leitsystemlieferanten konnte das Leitsystem innert nützlicher Frist wieder hergestellt werden.

2.5 Gezielte Cyber-Attacke

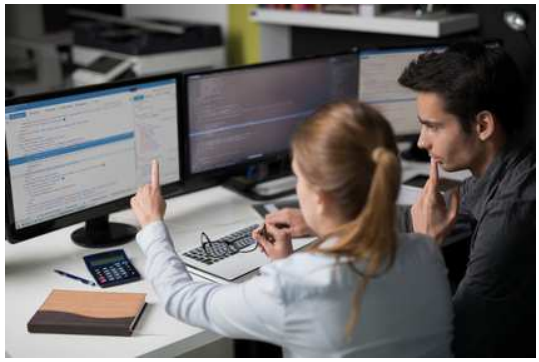

Abbildung 7: www.fotolia.de

Auch wenn es über gezielte Cyber-Angriffe keine genauen Angaben sondern nur grobe Schätzungen gibt, ist die Tendenz der letzten Jahre unbestritten und eindeutig: Vorfälle, bei denen Staaten, Unternehmen und Individuen via Datennetzwerke angegriffen und geschädigt werden, nehmen zu, in Anzahl und Qualität[1]. Der Bundesrat hat im April 2017 dazu eine Nachfolgestudie in Auftrag gegeben. Das Bundesamt für wirtschaftliche Landesversorgung BWL analysierte 2016 die Risiken und Verwundbarkeit der Stromversorgung und erarbeitete dazu einen Massnahmenkatalog. Eine Massnahme daraus ist die Erarbeitung von IKT-Minimalstandards für die Strombranche. Dies zeigt, dass sich andere Bereiche der kritischen Infrastrukturen intensiv mit dem Thema Cyber-Sicherheit beschäftigen und Massnahmen treffen, um den Schutz zu erhöhen. Für gezielte Cyber-Attacken betreiben die Angreifer unter Umständen viel Aufwand. Die Angreifer sind professionelle Organisationen, welche ein Ziel verfolgen und dieses Ziel mit möglichst geringem Aufwand erreichen wollen. Wenn es in einigen Bereichen der kritischen Infrastrukturen, wie der Stromversorgung aufwändiger wird das Ziel zu erreichen, werden die Angreifer auf einfachere Ziele ausweichen. Gezielte Cyber-Attacken können nur sehr schwer verhindert werden. Die Wasserversorgungen können aber mit einigen gezielten Massnahmen in Ihren Anlagen den Wirkungsraum allfälliger Angreifer stark eingrenzen und eine sichere Wasserversorgung gewährleisten.

2.6 Weitere Blackout-Szenarien

Abbildung 8: www.fotolia.de

Es sind durchaus noch weitere Blackout-Szenarien denkbar. Inzwischen sind einige Wasserversorgungen bei der Versorgungssicherheit von Mobilfunk-, Internet-Providern oder von anderen Kommunikationsdienstleistungen abhängig.

[1] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (19.06.2012 rev.) vom VBS

3 Beurteilung von Risiken

Risiken sind latent vorhanden. In der Regel können Wasserversorgungen gut damit umgehen. Dazu müssen sie die Risiken kennen und angemessene Massnahmen dagegen ergriffen haben. Jede Wasserversorgung hat ihre individuellen Voraussetzungen und Gegebenheiten. Daher muss auch jede Wasserversorgung für sich selbst ihre Risiken einschätzen.
Mit dem Werkzeug der Risikoanalyse können Sie Risiken identifizieren, bewerten und gezielt dagegen vorgehen.

3.1 Risikoidentifikation

Bei der Risikoidentifikation werden alle erkennbaren Risikofaktoren bezüglich des Schadenpotentials und der Eintrittswahrscheinlichkeit beurteilt. Jede Wasserversorgung hat andere Voraussetzungen und Rahmenbedingungen, daher ist die Beurteilung der Risiken individuell für jede Wasserversorgung. Wenn etwa in einer Wasserversorgung Quellwasser ins Versorgungsgebiet hineinläuft, ist das Schadenspotential bei einem Stromausfall wesentlich kleiner, als bei einer Wasserversorgung, welche auf einen Pumpbetrieb angewiesen ist.
Bei einer Wasserversorgung ist das Schadenspotential bei einem Versorgungsunterbruch vermutlich weniger monetärer oder existenzieller Art. Vielmehr sind es die Anzahl betroffener Verbraucher und der Imageschaden, welche das Schadenspotential schnell mittel oder hoch werden lassen.

Risikofaktoren	**Schaden-potential** [1-3]	**Eintrittswahr-scheinlichkeit** [1-3]
1. Mehrtägiger flächendeckender Stromausfall	3	1
2. Lokaler Stromausfall	2	2
3. Hardwaredefekt	2	1
4. Breit gestreute Schadsoftware	1	3
5. Gezielte Cyber-Attacke	3	2
6. ...		
7. ...		

Tabelle 1: Risikoidentifikation

3.2 Risikobewertung

Mit der Risikomap kann anhand des Schadenpotentials und der Eintrittswahrscheinlichkeit das Risikoniveau der einzelnen Risikofaktoren ermittelt werden.

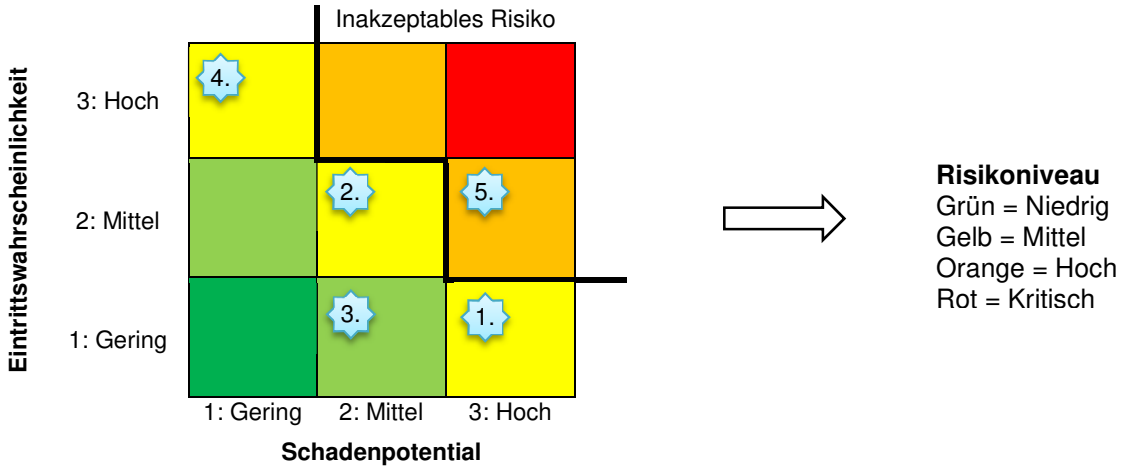

Abbildung 9: Risikomap zur Risikobewertung

3.3 Risikomanagement

Beim Risikomanagement geht es darum durch gezielte Massnahmen und Vorkehrungen entweder das Schadenspotential oder die Eintrittswahrscheinlichkeit und dadurch das Risikoniveau zu reduzieren. In Kapitel 5 werden wir ein paar Beispiele aufzeigen, wie Sie Ihre Steuerung und Ihr Leitsystem sicherer und widerstandsfähiger machen können und dadurch ihr Risikoniveau senken können.

4 Blackouts und Ihre Auswirkungen auf den Betrieb

Um die Beeinträchtigung des Betriebs und das Schadensausmass für die verschiedenen Blackout-Szenarien abschätzen zu können, müssen Sie sich vor Augen führen, welche Systemteile betroffen und nicht mehr einsatzfähig sind. In der Einleitung unter Kapitel 1.3 wurde der hierarchische Aufbau eines Steuerungs- und Leitsystem aufgezeigt. Anhand dieses Modells wird nachfolgend aufgezeigt, welche Systemteile von einem Blackout betroffen sind und welche Massnahmen Sie ergreifen können.

4.1 Bei Stromausfall

Sie erhalten vom Leitsystem den Alarm, dass in einem oder mehreren Bauwerken die Stromversorgung ausgefallen ist. Als erstes dürfte es Sie als Brunnenmeister interessieren, welche Bauwerke betroffen sind und für wie lange die Wasservorräte ausreichen, um die Versorgung sicherzustellen. Diese Information erhalten Sie am schnellsten und übersichtlichsten vom Leitsystem. Dort sehen Sie die Alarmzustände, die aktuellen und historischen Verbräuche sowie die aktuellen Wasserstände. In der Regel werden Ihre Wasservorräte für mehrere Stunden ausreichen und Sie können sich in Ruhe beim EVU erkundigen, wie lange der Stromunterbruch voraussichtlich dauern wird. In regelmässigen Abständen 30‘, 1 h, 2 h möchten Sie sich versichern, wie es um Ihre Wasserreserven steht. Dabei sind Sie darauf angewiesen, dass von der Prozessebene bis zur Leitebene alle Steuerungsteile inkl. Klappen ab Batterie versorgt und in Betrieb sind. Aufgrund der hohen Leistungen können Pumpen und Wasseraufbereitungsanlagen kaum über Batterien mit Notstrom versorgt werden. Dauert der Stromunterbruch voraussichtlich länger, als Ihre Wasservorräte ausreichen werden, so müssen Sie sich um Notstromaggregate für die Pumpwerke und Wasseraufbereitungsanlagen bemühen. Bei einem lokalen Stromausfall wird Ihnen vermutlich das EVU, die Feuerwehr oder ein Bauunternehmen mit einem Notstromaggregat aushelfen können. Oft ist es jedoch so, dass mobile Notstromaggregate für hohe Leistungen, wie sie für Pumpwerke benötigt werden - wenn überhaupt - nur bei EVUs vorhanden sind.

Ist ein Stromausfall grossflächig und von längerer Dauer, so dürfte es für Sie schwierig werden, spontan ein passendes Notstromaggregat auftreiben zu können. Die Batterien der Notstromversorgungen fürs Leitsystem und die Steuerungen in den Bauwerken entleeren sich allmählich und Sie verlieren zunehmend die Informationen aus den Bauwerken. Statt periodisch im Leitsystem nach den Wasservorräten zu schauen, müssen Sie dies vor Ort in den Reservoirs tun. Jetzt wird es zeitaufwändig: Notstromaggregat inkl. Treibstoff organisieren, Wasserstände kontrollieren, Notstromaggregate verschieben und anschliessen, Handpumpbetrieb, etc. Unter Umständen bricht das Mobilfunk-Netz zusammen und Sie können nicht mehr mit Ihren Arbeitskollegen telefonieren.

4.2 Bei Hardwaredefekt

Fällt eine zentrale Steuerungskomponente aus, über welche grosse Teile der Wasserversorgung gesteuert werden, und wenn auch noch die Alarmierung darüber läuft, kann es für den Anlagenbetreiber sehr ungemütlich werden. Reservoir-Tiefstände werden nicht mehr rechtzeitig erkannt und Sie erhalten keinen Alarm. Die Alarmierung übernimmt dann der Kunde, welcher über die Pikettnummer seinen Wassermangel meldet. Der Anlagenbetreiber muss sich gleichzeitig um die Wiederversorgung, die Ursachenermittlung und um die Schadensbehebung kümmern. Kann der Schaden nicht unmittelbar behoben werden, folgt ein aufwändiger Handbetrieb der Anlage. Unter Umständen müssen Sie während längerer Zeit rund um die Uhr die Wasserstände der Reservoirs vor Ort manuell überprüfen und die Pumpen von Hand bedienen. In etwa so war das Szenario, welches schlussendlich zur Schlagzeile in Abbildung 5 führte.

In der Praxis sind oft die Maschinensteuerungsebene und die Bauwerksebene (vergleiche Kapitel 1.3) aus Kostengründen auf ein und derselben Steuerungshardware realisiert (siehe rote Einrahmung in Abbildung 10). Fällt diese Hardware aus, so fällt nicht nur die automatische Reservoirbewirtschaftung aus, sondern auch der Trockenlaufschutz der Pumpen, die Ansteuerung der Anlaufdrosselklappen, die Verwurfsteuerung des Quelleinlaufs etc. Dies bedeutet, dass Sie das Bauwerk in der Einzelsteuerungsebene im Nothandbetrieb bedienen müssen und nebst der manuellen Reservoirbewirtschaftung auch die Schutz- und Sicherheitsfunktionen der eingesetzten Aggregate überwachen müssen. Die Folgen allfälliger Kosteneinsparungen zeigen sich erst im Notfall.

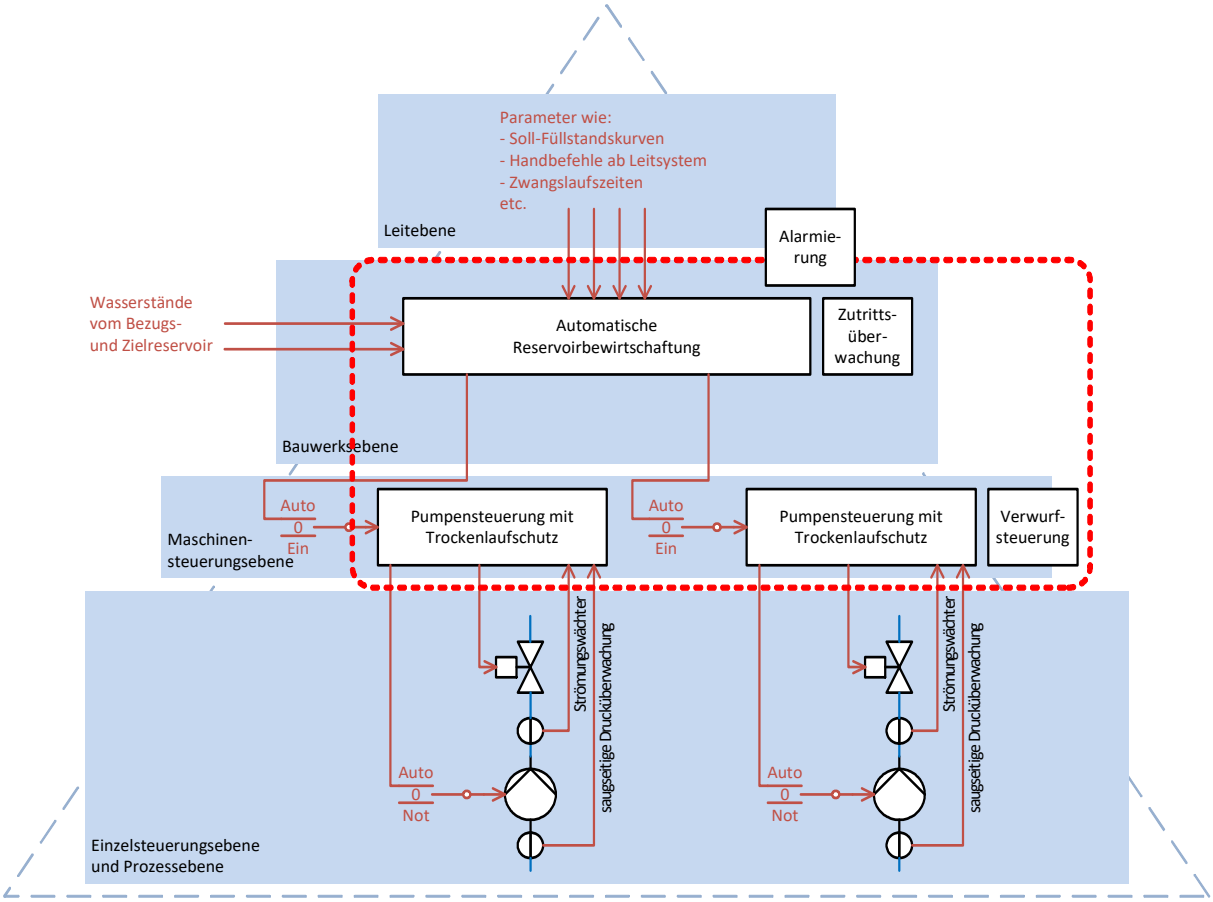

Abbildung 10: Sämtliche Steuerungsfunktionen eines Bauwerks auf derselben Hardware

4.3 Bei breit gestreuter Schadsoftware

Breit gestreute Schadsoftware ist so ausgelegt, dass sie auf möglichst vielen Rechnern ihre Wirkung entfalten kann. Sie ist nicht dazu entwickelt, gezielt in einer Wasserversorgung maximalen Schaden anzurichten. Mit grösster Wahrscheinlichkeit werden deshalb die Windows-Rechner und selten die Steuerungskomponenten in den Bauwerken befallen sein. Im Schadenfall sind ganze Rechner nicht mehr einsatzfähig, da sie verschlüsselt oder gelöscht sind. In den meisten Trinkwasserversorgungen laufen die Steuerungsfunktionen in Steuerungskomponenten der Bauwerksebene ab und funktionieren vorübergehend weiter, auch bei einem Ausfall der Leitebene. Der Brunnenmeister verliert aber die Visualisierung und Fernsteuerung seiner Anlagen, die Protokollierung von Prozessdaten und unter Umständen auch die Alarmierung. Während der Zeit, bis die Rechner neu aufgesetzt und die Datensicherung eingespielt sind, können Sie Ihrer Steuerung blind vertrauen oder Sie müssen sich vor Ort in den Reservoirs einen Überblick über die Wasserstände und Betriebszustände verschaffen.

4.4 Bei gezielter Cyber-Attacke

Ganz anders ist die Situation, wenn Sie mit einer gezielten Cyber-Attacke angegriffen werden. In diesem Fall ist die kriminelle Energie auf Sie gerichtet (vergleichbar mit einem Scharfschützen). Im Extremfall wird sich der Angreifer Zeit lassen und möglichst viele Informationen über die Unternehmen, die Belegschaft und die eingesetzten Systeme sammeln. Je nachdem, welche personellen und technischen Schutzvorkehrungen von Ihnen getroffen wurden, wird der Angreifer mehr oder weniger Zeit benötigen, bis er in die von extern erreichbaren Systeme vorgedrungen ist. Ich wage zu behaupten, dass für Systeme mit Internetverbindung kein 100%-iger Schutz gegen Cyber-Attacken möglich ist.

Ist ein Angreifer nun mal im System drin, so kann er theoretisch alles anstellen, was der Servicetechniker vom Systemlieferanten auch von extern machen kann. Er kann das Leitsystem und die Programmierung auf den Steuerungen löschen oder verändern. Er kann falsche Prozesswerte vorgaukeln, so dass der Betreiber im ersten Moment nicht bemerkt, dass etwas nicht in Ordnung ist. Den Möglichkeiten sind praktisch keine Grenzen gesetzt.

Die Auswirkungen sind ähnlich, wie bei einem Hardwaredefekt (siehe Kapitel 4.2) nur können sie sich gleichzeitig über die ganze Versorgung erstecken oder sie sind perfider, weil falsche Prozesswerte angegeben werden. Je mehr Funktionalitäten in Steuerungskomponenten integriert sind, welche über Fernwartung erreichbar sind, auf umso mehr Funktionalitäten kann ein Angreifer Einfluss nehmen.

5 Vorkehrungen zur Trinkwasserversorgung in Notlagen

Bezogen auf die oben beschriebenen Blackout-Szenarien und ihren Auswirkungen für die Wasserversorgung werden in diesem Kapitel mögliche Massnahmen aufgezeigt, wie Sie trotz den latent vorhandener Risiken Ihre Wasserversorgung aufrechterhalten können.

5.1 Notstromversorgungen gegen Stromausfälle

Lokale Stromausfälle sind oft innert 1-2 Stunden vom Energieversorgungsunternehmen wieder behoben. In der Regel ist in den Reservoirs genügend Wasser vorhanden, so dass ein solcher Ausfall ohne Pumpbetrieb nicht zu einem Versorgungsengpass führt.
Dauert jedoch ein Stromausfall länger oder ist er sogar flächendeckend, so wird die Aufrechterhaltung der Wasserversorgung komplex und sehr zeitaufwändig. Mit folgenden Massnahmen können Sie sich optimal auf einen solchen Blackout vorbereiten:

- Batteriegestützte Notstromversorgungen (24 VDC) in jedem Bauwerk für die Kommunikation, Steuerung, Sensoren, Klappen, Wasserqualitätsmessung für mind. 12 h (in versorgungsrelevanten Bauwerken besser für 24 h)
- Wenn Sie auf fremde Infrastrukturen von Dienstleistern vertrauen, prüfen Sie, wie diese Ihre Notstromversorgung sicherstellen.
- Batteriegestützte, unterbruchsfreie Stromversorgung (USV 230 VAC) für das Netzwerk und Rechner des Leitsystems für mind. 2 h, danach kontrolliertes Herunterfahren der Rechner
- Vorbereiteter Einspeisepunkt aus einem mobilen Notstromaggregat für die Versorgung der Leitstelleninfrastruktur
- Jährlicher Test der Batteriekapazitäten
- 3x400 VAC Noteinspeisungen mit Netzumschalter in Pumpwerken und Wasseraufbereitungsanlagen vorsehen
- Eigene fix installierte oder mobile Notstromaggregate beschaffen oder sich ein mobiles Notstromaggregat für den Krisenfall vertraglich zusichern lassen
- Treibstoffreserve sicherstellen
- Regelmässiger Pumpbetrieb mit Notstrom als Test und zur Ausbildung des Personals. Es gibt bei den Notstromaggregaten und in den Bauwerken verschiedene Erdungssysteme, die zusammen passen müssen. Ohne vorgängigen Test gibt es keine Gewähr, dass die Notstromversorgung im Krisenfall tatsächlich funktioniert.
- Krisenorganisation für einen länger andauernden Stromausfall aufstellen. Kann der Brunnenmeister die Krisensituation alleine bewältigen oder braucht er Unterstützung? Wer kümmert sich um was? Wie arbeiten die Personen zusammen? Wie werdend die Informationen über Wasserstände, Verbräuche, Fördermengen etc. gesammelt und festgehalten? Wie wird kommuniziert, falls das Mobilfunknetz ausfällt? usw.

5.2 Redundanzen gegen defekte Hardware

Im Kapitel 4.2 haben wir aufgezeigt, dass wenn viele Funktionsblöcke auf ein und derselben Hardware ausgeführt werden, beim Ausfall dieser Hardware auch viele Funktionen dem Bediener nicht mehr zur Verfügung stehen. Durch Redundanzen sollen im Falle eines Hardwaredefektes die Grundfunktionalitäten, wie Pumpenschutz, Bewirtschaftungen, Verwurfsteuerung, etc. weiter zur Verfügung stehen.
Pumpwerke haben aus Redundanzgründen häufig mehr als eine Pumpe. Eine echte Pumpenredundanz ist nur dann gegeben, wenn auch je Pumpe ein autonomer Pumpenautomat für den Pumpenschutz installiert ist (siehe Abbildung 11). Dadurch steht trotz eines Hardwareausfalls mindestens eine Pumpe mit den Überwachungsfunktionen zur Verfügung.
Wird die Verwurfsteuerung in der Maschinensteuerungsebene durch Verknüpfung der Betriebsmeldungen aus der Trübungsmessung und der Wasseraufbereitungsanlage (z.B. UV-Entkeimungsanlage) gelöst, so kann mit der Steuerungshardware in der Bauwerksebene die Funktion der Verwurfsteuerung überwacht werden.

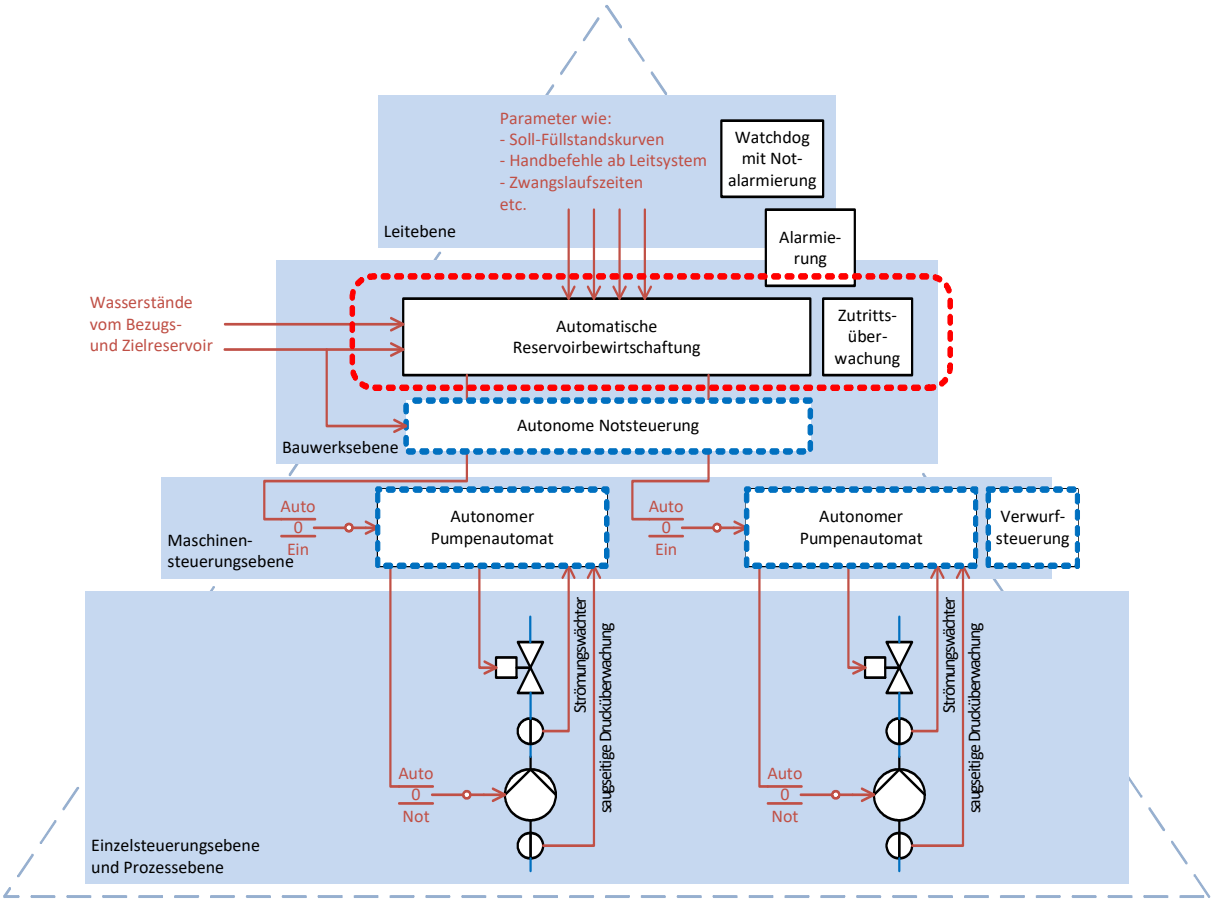

Abbildung 11: Versorgungsrelevante Steuerungsfunktionen eines Bauwerks auf redundanter Hardware

Als Redundanz zur automatischen Reservoirbewirtschaftung empfehlen wir in der Bauwerksebene bei den versorgungsrelevanten Pumpwerken eine autonome Notsteuerung. Die autonome Notsteuerung ist eine eigene kleine Hardware, welche den Wasserstand des Zielbauwerkes auf Hochstand und Tiefstand überwacht und notfalls die Steuerhoheit der Pumpen übernimmt. In Abbildung 12 ist die Funktionsweise einer autonomen Notsteuerung dargestellt.

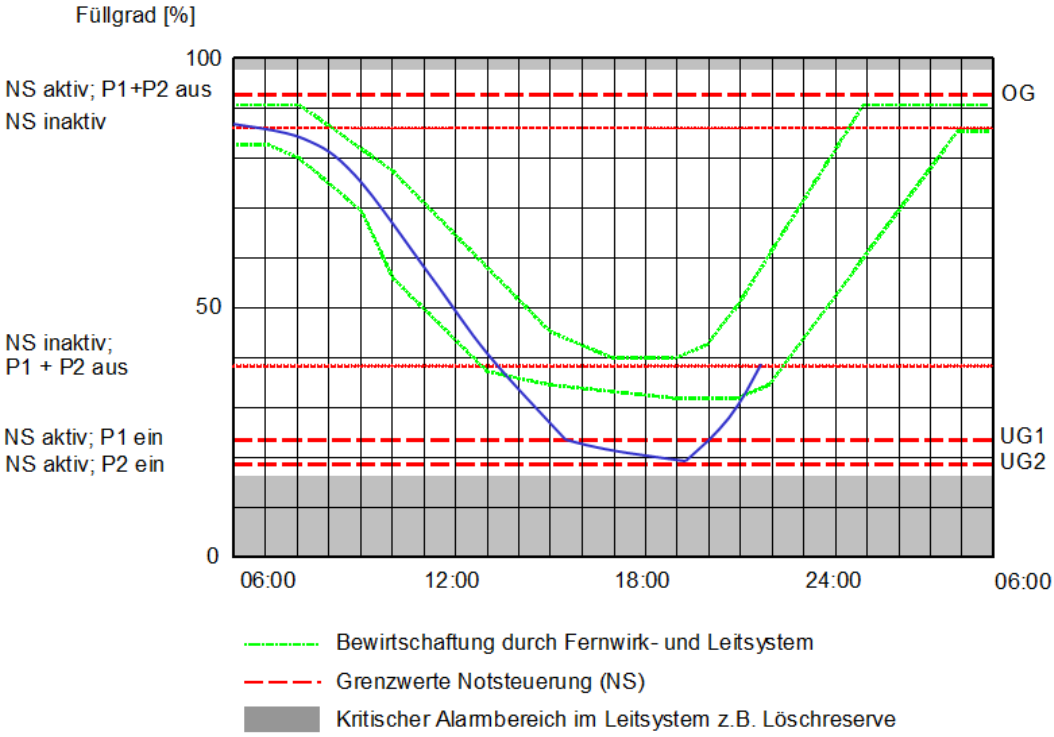

Abbildung 12: Funktionsweise einer autonomen Notsteuerung

In Grün ist das Zielband des Wasserstandes über einen Tag dargestellt, welche im Leitsystem eingestellt ist. Die automatische Reservoirbewirtschaftung sorgt mit Einschalten der Pumpen dafür, dass der effektive Wasserstand (blau) nie unter die untere grüne Sollwertkurve fällt. Sie schaltet die Pumpen wieder aus, wenn der Wasserstand höher ist, als die obere grüne Sollwertkurve.
Fällt die Hardware (SPS) der automatischen Reservoirbewirtschaftung aus, so fällt nach einer gewissen Zeit der Wasserstand unter die grüne Sollwertkurve. In Abbildung 12 ist dies ca. 13:30 Uhr der Fall. Um 15:30 Uhr unterschreitet der Wasserstand die 1. Untergrenze (UG1) der autonomen Notsteuerung. Die autonome Notsteuerung wird aktiv und schaltet eine Pumpe ein. Sinkt der Wasserstand trotz Förderung mit einer Pumpe weiter, so schaltet die autonome Notsteuerung beim Erreichen der 2. Untergrenze (UG2) eine weitere Pumpe zu. Sobald der Wasserstand wieder ein gewisses Niveau erreicht hat, schaltet die autonome Notsteuerung die Pumpen wieder aus und wird inaktiv.
Auf gleiche Art überwacht die autonome Notsteuerung die Obergrenze (OG) des Wasserstandes und schaltet beim Versagen der automatischen Reservoirbewirtschaftung die Pumpen aus, bevor ein Reservoir überläuft.

Eine weitere wichtige Redundanz bildet Notalarmierung. Diese erkennt einen Totalausfall des Systems mittels Watchdog und alarmiert. Sie wird auch angestossen, wenn das Leitsystem nicht mehr mit der Alarmierungseinrichtung kommunizieren kann oder die Alarmierungseinrichtung kein Signal mehr vom Telefonprovider erhält. Idealerweise wird für die Notalarmierung eine andere Kommunikationstechnologie verwendet, als bei der Hauptalarmierung.

Redundanzen sind nicht gratis, aber im Verhältnis zu den Gesamtinvestitionen einer Steuerung und eines Leitsystems auch nicht teuer. Wenn Ihnen Redundanzen wichtig sind, müssen Sie diese bei Ihrem Systemlieferanten explizit anfordern.

5.3 Vorkehrungen gegen Schadsoftware wie Viren, Trojaner etc.

Um sich gegen breit gestreute Schadsoftware zu schützen gelten die allgemeinen Regeln der IT-Sicherheit. Nachfolgend einige empfohlene Massnahmen:

- Aktuelle, zuverlässige und getestete Datensicherung mit alternierend eingesetzten Datenträgern. Ein Datenträger mit der Datensicherung ist immer vom Strom und Netzwerk getrennt und ist extern aufbewahrt.

- Sensibilisierung und regelmässige Schulung der Mitarbeiter auf die verschiedenen Verbreitungsarten von Schadsoftware
- Betriebssystem aktuell halten (Windows-Patches zeitnah einspielen)
- Aktueller Virenschutz
- Unterbindung der Internet-Nutzung ab den Leitsystemrechnern
- Unterbindung des E-Mail Empfangs auf den Leitsystemrechnern
- Keine Software ohne Rücksprach mit dem Systemlieferanten installieren
- System härten d.h. keine USB-Sticks, Memory-Cards, CDs; DVDs, etc. zulassen
- Keine Dateien z.B. mit Fernwartungssoftware auf die Leitsystemrechner kopieren
- Keine Administrator-Rechte für Systemdienste und Leitsystembenutzer
- Standardbenutzer wie Gast, Admin, User, etc. deaktivieren
- Starke Passwörter (mind. 10 Zeichen lang mit Gross-, Kleinbuchstaben, Zahlen und Sonderzeichen)
  Anmerkung: Ein schneller Einzel-PC kann heute ca. 2.15 Milliarden Schlüssel pro Sekunde generieren. So ein Rechner benötigt für die Entschlüsselung eines 10-stelligen Passwortes mit a-z, A-Z, 0-9 und Sonderzeichen ca. 980 Jahre. Im Vergleich entschlüsselt er ein 8-stelliges Passwort bestehend nur aus Gross- und Kleinbuchstaben in 6.9 Stunden und einen 6 stelligen Zahlencode in nur 5 Millisekunden.
- *Segmentierung des Systems in verschiede Netzwerkzonen*
- Regelmässige externe Audits durch neutrale und unabhängige IT-Security Spezialisten

5.4 Vorkehrungen gegen Cyber-Attacken

Wie bereits erwähnt, bin ich der Meinung, dass sich ein mit dem Internet verbundenes System nicht 100%-ig gegen einen gezielten Cyber-Angriff schützen lässt. Sie können jedoch den Angreifern mit ein paar Vorkehrungen den Aufwand massiv erhöhen, so dass sie sich doch lieber eine andere Anlage aussuchen.
Generell gelten zuerst wieder die allgemeinen Regeln der IT-Sicherheit, wie sie in Kapitel 5.3 bereits beschrieben wurden.
In Kapitel 5.2 haben wir die Vorkehrungen gegen defekte Hardware beschrieben. Wenn nun ein Angreifer Steuerungskomponenten von extern manipulieren kann, sind die Auswirkungen sehr ähnlich, wie wenn die Hardware ausgefallen ist. Redundanzen wie autonome Pumpenautomaten und autonome Notsteuerungen müssen mit eigener Hardware ausgeführt werden, welche nur vor Ort konfiguriert werden kann. Dadurch hat ein Angreifer keinen Zugriff auf die redundanten Systeme. Eine einfache Reservoirbewirtschaftung über die autonome Notsteuerung und die autonomen Pumpenautomaten ist immer gewährleistet. Die Funktionalität der autonomen Notsteuerung und der autonomen Pumpenautomaten ist derart einfach und standardisiert, dass sie keine Fernwartungsmöglichkeiten erfordern.

6 Fazit

Blackouts können nicht immer vermieden werden, doch durch die richtigen Vorkehrungen und regelmässiger Anwendung dieser Massnahmen können Wasserversorgungen damit umgehen und ihren Versorgungsauftrag erfüllen.

7 Abkürzungen

BWL	Bundesamt für wirtschaftliche Landesversorgung
EVU	Elektrizitätsversorgungsunternehmen
IKT	Informations- und Kommunikationstechnologie
MELANI	Melde- und Analysestelle Informationssicherung des Bundes
NS	Notsteuerung
OG	Obergrenze
SBV	Schweizerischer Brunnenmeister-Verband
SPS	Speicher programmierbare Steuerung
UG	Untergrenze
USV	Unterbruchsfreie Stromversorgung
VAC	Wechselspannung
VDC	Gleichspannung