STEP BY STEP UND CYBER-SICHERHEIT IN DER PRAXIS

ERFOLGREICHE UMSETZUNG IN DER KLÄRANLAGE UND ANWENDUNG IM LEITSYSTEM

In anspruchsvollen Betriebssituationen und Notfällen, wenn rasches und zielgerichtetes Handeln nötig ist, liefert das Handbuch «step by STEP» dem Kläranlagenpersonal einfache und anwenderfreundliche Anleitungen zum Vorgehen, so dass der Einsatz erfolgreich bewältigt werden kann. Damit die Dokumente des Handbuchs auch mittels Fernzugriff verfügbar sind, können sie ins Prozessleitsystem (PLS) integriert und mit dem STEP-Icon abgerufen werden. Die Cybersicherheit einer ARA lässt sich durch die Umsetzung des IKT-Minimalstandards Abwasser und durch Anwendung des Step-by-STEP-Handbuchs erhöhen.

Max Schachtler, step by STEP; Reto Steinemann, Chestonag Automation AG*
Thomas Bhend, ARA Wetzikon Flos; Lukas Studer, first frame networkers ag

RÉSUMÉ

STEP BY STEP ET LA CYBERSÉCURITÉ EN PRATIQUE – MISE EN ŒUVRE RÉUSSIE À LA STEP ET APPLICATION DANS LE SYSTÈME DE CONTRÔLE

Depuis sa parution en 2019, le manuel «step by STEP» a été utilisé avec succès par plusieurs stations d'épuration. La mise en œuvre du manuel visant à mieux gérer les situations d'urgence et dysfonctionnements critiques se déroule en sept étapes, tel qu'illustré ici par l'exemple de la STEP de Flos. L'accent principal du manuel porte sur la mise à jour des check-lists et des documents de la STEP en plus de la révision des ressources existantes pour la gestion des urgences. Afin de pouvoir utiliser ces documents avec succès en cas d'urgence, le personnel d'exploitation doit être familiarisé avec le manuel et formé aux différents scénarios. Dans les situations d'urgence réelles, les documents opérationnels de step by STEP à la station d'épuration de Flos ont permis de faire face aux événements rapidement et méthodologiquement.

En cas d'incident, le personnel doit pouvoir accéder rapidement aux formulaires de step by STEP ce qui est généralement le cas lorsque les employés sont sur le site. Mais si personne n'est sur site lors de l'incident, les documents doivent être facilement accessibles à distance. Ceci est rendu possible en intégrant le manuel step by STEP dans le système de supervision de la STEP. L'accès rapide aux formulaires de step by STEP est central car les

> S. 44

STEP BY STEP IN SIEBEN SCHRITTEN

Das Handbuch «step by STEP» [1] ist 2019 erschienen und kommt in vielen Kläranlagen (ARA) der Schweiz und auch in Industriebetrieben zum Einsatz. «Step by STEP» ist ein nützliches Hilfsmittel für Mitarbeitende und Betreiber einer ARA, um auf kritische Betriebszustände und Notfallsituationen vorbereitet zu sein. Dies hat sich deutlich am Beispiel der ARA Flos in Wetzikon gezeigt.

ANWENDUNGSBEISPIEL

Die Stadtentwässerung Wetzikon ist eine mittelgrosse ARA im Zürcher Oberland mit einer Kapazität von 37 500 EW. In den letzten Jahren kam es aufgrund kleinster Veränderungen im Zulauf, die durch verschiedene Einleiter verursacht wurden, immer wieder zu grösseren Problemen und Havarien. Aus diesen Gründen liess die ARA Flos bereits vor längerer Zeit ein eigenes Notfallkonzept erstellen. Damit sollte sichergestellt werden, dass die Mitarbeiter auf verschiedene Ernstfälle vorbereitet sind. In der Praxis zeigte sich jedoch, dass das Notfallkonzept zahlreiche Mängel aufwies. So wurden zum einen nur Notfallkonzepte für Strom- und Steuerungsausfälle sowie kleinere Öl-

** Kontakt: max.schachtler@neugut.ch*

unfälle im Netz festgelegt, zum anderen wiesen selbst diese noch erhebliche Mängel auf. Beispielsweise wurde bei einem Test mit simuliertem Stromausfall festgestellt, dass im Notfall die falschen Dokumente und Checklisten abgearbeitet und wichtige Personen nicht informiert oder alarmiert werden. Die Mitarbeiter mussten teils improvisieren, was zu Fehlern bei der Behebung der Notsituation führte. Und dies, obwohl vor Testbeginn alle Mitarbeiter im Notfallkonzept geschult und die nötigen Dokumente zentral in einem Notfallordner abgelegt worden waren.
Diese Erfahrung verdeutlichte, dass das vorhandene Notfallkonzept einer dringenden Überarbeitung bedurfte. Im Rahmen dieser Überlegungen wurde Anfang 2020 das Notfallkonzept der ARA Flos durch das Step-by-STEP-Handbuch abgelöst. Damit das Konzept bei den Mitarbeitenden auch gelebt wird, wurde entschieden, «step by STEP» Schritt für Schritt – in insgesamt sieben Schritten – einzuführen.

INHALT DES STEP-BY-STEP-HANDBUCHS

Das Handbuch wurde von Praktikern für Praktiker entwickelt und ist ein einfach handhabbares Arbeitsmittel, um in anspruchsvollen Betriebs- und Notfallsituationen schnell und richtig zu handeln. Als Nachschlagewerk enthält es Fachinformationen zu spezifischen Ereignissen sowie Hinweise zur Prävention. Ein Hauptbestandteil sind die Einsatzdokumente, in die jede ARA vor einem Ereignisfall ihre spezifischen Massnahmen eintragen kann, um vorbereitet zu sein und so bei Eintreten des Ereignisses die richtigen Entscheidungen zu treffen.

SCHRITTWEISE EINFÜHRUNG

Schritt 1: Grundlagen zusammentragen

Zunächst wurden die von «step by STEP» bereitgestellten Formulare und Checklisten auf die Situation der ARA Flos angepasst. Dazu wurden unter Einbezug der Mitarbeiter alle notwendigen Grundlagen zusammengetragen und vervollständigt. Die bereits vorhandenen Unterlagen waren an verschiedenen Orten auf der Anlage oder auf diversen Computern verteilt und nicht systematisch abgelegt. Da die Mitarbeiter bei der Zusammenstellung der Daten einbezogen wurden, wurden sie bereits in diesem ersten Schritt für die Ereignisplanung sensibilisiert und lernten die Struktur und den Inhalt des Step-by-STEP-Handbuchs kennen. Die folgenden Aspekte wurden in diesem ersten Schritt verbessert:

- Mehrfach vorhandene Dokumente mit zum Teil widersprüchlichen Vorgaben wie auch Dokumente mit Lücken, fehlenden Angaben oder veralteten Informationen wurden bereinigt, ergänzt oder entsorgt.
- Zusätzliche Pläne, wie etwa ein Fliesszeitenplan, wurden erstellt und unvollständige oder alte Pläne revidiert.
- Der Feuerwehreinsatzplan wurde komplett überarbeitet, übersichtlicher gestaltet und als Kernelement mit dem Kommandanten der Feuerwehr kontrolliert.
- Das Interventionsmaterial wurde überprüft und modernisiert (z. B. Erwerb von Bindemittel und Absperrvorrichtungen, Entsorgung einer alten defekten Pumpe, Bereitstellung von genügend Schlauchmaterial).
- Die Formulare im Step-by-STEP-Handbuch wurden ausgefüllt. Dazu gehört u. a. die Telefonliste «Einsatzkräfte» (wer ist wann bei welchen Ereignissen zu informieren).
- Die Inventarliste «Einsatzmaterial», in der festgehalten ist, wo welches Material abrufbar ist oder organisiert werden kann, wurde mit dem vorhandenen Material abgeglichen; fehlendes Material wurde beschafft.

Schritt 2: Mitarbeiter mit der Struktur des Handbuchs vertraut machen

In zwei Schulungseinheiten à 45 Minuten wurde den Mitarbeitern die Struktur des Handbuches mit den Checklisten und Formularen vertraut gemacht. Ziel war es, dass die Mitarbeiter die richtigen Formulare und Checklisten finden und bearbeiten können (sowohl elektronisch als auch von Hand).

Schritt 3: Schulung eines Ereignisses

Nachdem die Mitarbeiter mit dem Handbuch vertraut gemacht worden waren, mussten sie ein Ereignis eigenständig unter Zuhilfenahme des Handbuchs bewältigen. Diese Schulung erfolgte anhand eines vorgegebenen Fallbeispiels.
In der Vorbereitungszeit wurden alle Dokumente mithilfe der Step-by-STEP-Checklisten nochmals auf ihre Vollständigkeit geprüft. Durch die Schulung wurde erkannt, dass an potenziellen Gefahrenstellen eine rote Einsatzmappe mit den wichtigen Dokumenten deponiert werden sollte *(Fig. 1)*. Auch entsprechendes Interventionsmaterial (z. B. Reinigungsmaterial oder Absperr- und Abdichtungsmaterial) ist an einer übersichtlichen Stelle bereitzustellen. Kurz nach der Schulung kam es zu einem realen Ernstfall auf der ARA Flos, bei dem sich die Dokumente und Notfallmaterialien bewährten.

Schritt 4: Schulung weiterer Ereignisse in Etappen

In den nächsten Wochen wurden die weiteren Kapitel des Handbuchs inkl. Praxisteil geschult. Der Zeitaufwand pro Schulung betrug jeweils ca. zweimal 45 Minuten. Ein Terminplan für die verschiedenen Schulungen erwies sich als hilfreich.

Fig. 1 Stets griffbereit: Step-by-STEP-Notfallmappe mit allen notwendigen Formularen und Plänen (links) und Eisenfällmittelstation mit Notfallmappe (rechts).

Schritt 5: Training und Wiederholungen

Trainingseinheiten und Wiederholungen sind enorm wichtig. Kläranlagen testen regelmässig den Notstrommotor. Wie sieht es jedoch aus mit internen Havarien, auslaufendem Fällmittel, Leckagen von Flockungshilfsmittel, Cyberattacken, Bergung von Personen aus Schächten und Gruben? Auch die Bewältigung solcher Vorfälle muss periodisch geübt werden. Nur so kann sichergestellt werden, dass im Notfall richtig reagiert wird.

Schritt 6: Checklisten, Einsatzformulare und Dokumente aktuell halten

Das Handbuch empfiehlt, die Checklisten, Einsatzformulare und Dokumente jährlich zu überprüfen und zu aktualisieren. Beim alten Notfallkonzept der ARA Flos wurde dies stark vernachlässigt, was entsprechende Folgen für den Ernstfall hatte.

Schritt 7: Aufbieten Dritter

Im Ereignisfall ist es wesentlich zu erkennen, zu welchem Zeitpunkt welche Personen aufzubieten sind oder welches Hilfsmaterial bereitgestellt werden muss. Nur wenn jeder Mitarbeiter weiss, wie vorzugehen ist, und aktuelle Telefonnummern vorliegen, funktioniert dies auch im Ernstfall. Den Mitarbeitern muss klar sein, wo sie die wichtigen Informationen bei einem Ereignis abrufen können und welche vordefinierten Einsatzkräfte aufzubieten sind.

BEWÄHRUNG IM ERNSTFALL

Die ARA Flos konnte das Step-by-STEP-Handbuch nach seiner Einführung bereits bei folgenden realen Ereignissen anwenden:

- Grossbrand
- Schwerer Verkehrsunfall
- Interne Havarie mit Flockungshilfsmittel (Fehlfunktion Schlammentwässerung)
- Interne Havarie mit Fällmittel (Tankreinigung)
- Totaler Stromausfall in der ARA, inkl. Ausfall der unterbrechungsfreien Stromversorgung (USV) während rund 45 Minuten

Die Vorfälle konnten alle mithilfe der Step-by-STEP-Einsatzformulare gut bewältigt werden. Im Folgenden wird beschrieben, wie sich beim Brand im Einzugsgebiet der ARA das Handbuch bewährte.

Anwendung bei einem Grossbrand

An einem Mittwochnachmittag erreichte die ARA Flos die Meldung, dass in einem Ortsteil ihres Einzugsgebietes ein Grosseinsatz der Feuerwehr im Gange ist. Löschwasser drohte in ein Gewässer abzufliessen, die Einsatzkräfte vor Ort waren auf die Hilfe und Fachkenntnisse der ARA Flos angewiesen. Anhand der Einsatzdokumente wurde entschieden, dass zwei ARA-Mitarbeiter zusammen auf den Schadenplatz ausrücken. Die Löscharbeiten waren bereits in vollem Gange. Vor Ort anwesend waren: Ortsfeuerwehr, zwei Stützpunktfeuerwehren, Polizei, Sanität, AWEL, Staatsanwalt und Statiker.

Beim Einsatz war es von zentraler Bedeutung festzustellen, wie und wo das Löschwasser gefasst und allenfalls in die Kanalisation eingeleitet werden könnte. Die Step-by-STEP-Einsatzdokumente enthielten alle notwendigen Hinweise, welche Handlungen und Massnahmen möglich und notwendig sind. Im Laufe des Einsatzes zeigte sich, dass sich die Vorbereitung vor dem Ereignis und die in der Schulung gewonnenen Erfahrungen im Ernstfall auszahlen. So war beispielsweise bekannt, wo das Löschwasser entsorgt werden konnte. Dank des ebenfalls vorliegenden Fliesszeitenplans war es zudem möglich, das Eintreffen des Löschwassers auf der ARA zu bestimmen. Per Leitsystem wurden die Online-Werte im Zulauf überwacht. Dadurch bestand jederzeit die Möglichkeit, die nötigen Massnahmen in der ARA umzusetzen.

Während des Ereignisses wurde fortlaufend in den Einsatzformularen in der Spalte «Journal» *(Fig. 2)* die durchgeführten Handlungen von Hand eingetragen und dadurch auf dem neusten Stand gehalten. Dies wurde durch die Anwesenheit von zwei ARA-Mitarbeitern ermöglicht. Damit lagen direkt nach Ende des Einsatzes alle Dokumente ausgefüllt vor. Die Fragen der Blaulichtorganisation und der weiteren Einsatzkräfte konnten auf Grundlage der immer aktuellen Einsatzdokumente rasch und fachlich korrekt beantwortet werden.

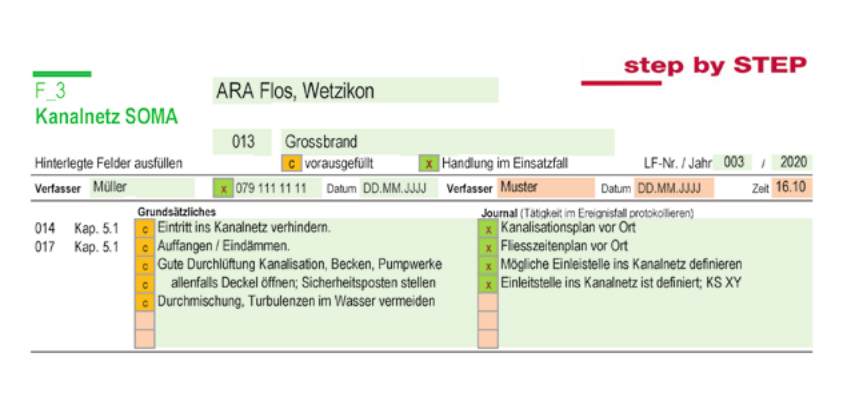
FAZIT AUS PRAXISEINSÄTZEN

Die Empfehlung von «step by STEP», die notwendigen Dokumente vor einem Ernstfall vollständig zusammenzustellen und regelmässig auf ihre Richtigkeit zu prüfen, erwies sich in der Praxis als äusserst wertvoll. Dadurch waren die Handlungen bereits vollständig geplant und im Einsatz-Notfall konnte rasch und richtig gehandelt werden.

Die Empfehlung, Einsätze nach Möglichkeit mit zwei Personen durchzuführen, hat sich ebenfalls bewährt. Dadurch kann sich ein Mitarbeiter auf den Einsatz konzentrieren, währenddessen der zweite das Journal in den Einsatzformularen führt, Material organisiert oder Abklärungen trifft. Sind Entscheidungen zu treffen, können diese miteinander besprochen und definiert werden. Je nach Ereignis oder notwendiger Handlung muss zwingend eine zweite Person anwesend sein (z. B. Einstieg in Schächte und Gruben, Gas-Alarme usw.).

STEP BY STEP – ANALOG UND DIGITAL

Das Step-by-STEP-Handbuch dient der schnellen Orientierung in kritischen Betriebszuständen. Bei einem Ereignis muss der Griff zu den Einsatzformularen rasch möglich sein, was in der Regel ge-


step by STEP

F_3
Kanalnetz SOMA

ARA Flos, Wetzikon

013 Grossbrand

Hinterlegte Felder ausfüllen | c vorausgefüllt | x Handlung im Einsatzfall | LF-Nr. / Jahr 003 / 2020

Verfasser Müller | x 079 111 11 11 | Datum DD.MM.JJJJ | Verfasser Muster | Datum DD.MM.JJJJ | Zeit 16.10

		Grundsätzliches	Journal (Tätigkeit im Ereignisfall protokollieren)
014	Kap. 5.1	c Eintritt ins Kanalnetz verhindern.	x Kanalisationsplan vor Ort
017	Kap. 5.1	c Auffangen / Eindämmen.	x Fliesszeitenplan vor Ort
		c Gute Durchlüftung Kanalisation, Becken, Pumpwerke	x Mögliche Einleistelle ins Kanalnetz definieren
		c allenfalls Deckel öffnen; Sicherheitsposten stellen	x Einleitstelle ins Kanalnetz ist definiert; KS XY
		c Durchmischung, Turbulenzen im Wasser vermeiden	

Fig. 2 Bei einem Grossbrand im Einzugsgebiet der ARA Flos wurde die Spalte «Journal» (rechts) des Step-by-STEP-Einsatzformulars F_3 bereits während des Einsatzes ausgefüllt. Namen und Telefonnummern sind unkenntlich gemacht.

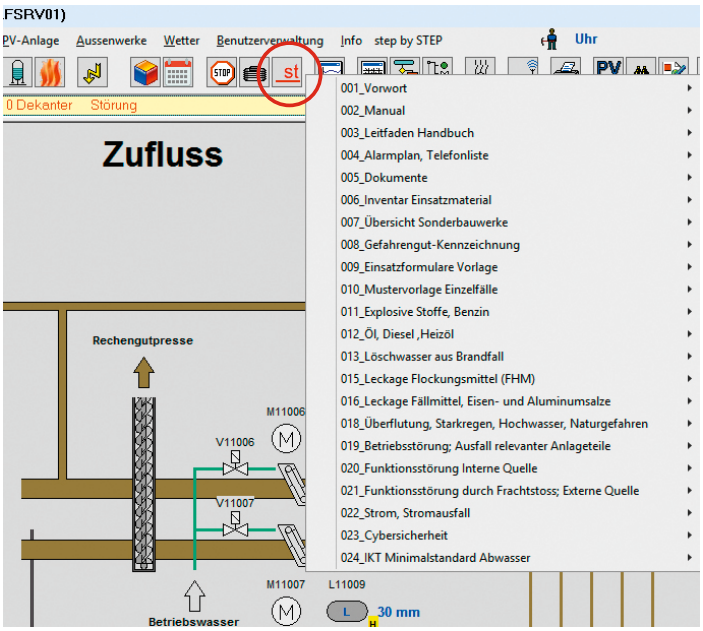


Fig. 3 STEP-Icon in der Icon-Liste des Leitsystems und dazu hinterlegte Step-by-STEP-Struktur.
(Bild: ARA Neugut; Chestonag Automation AG)

währleistet ist, wenn die Mitarbeitenden auf der Anlage sind. Ist es im Ereignismoment aber nur möglich, mittels Fernzugriff zu intervenieren, so bleibt der Ordner in Papierform in ungreifbarer Nähe. Daher muss eine Möglichkeit geschaffen werden, dass die Mitarbeitenden auch digital über das Leitsystem auf die Step-by-STEP-Dokumente zugreifen können.
Der Zugriff über das Leitsystem ist sinnvoll, weil die Mitarbeitenden damit täglich umgehen. Zudem ist während eines Pikettdienstes oder eines Notfalls der Zugriff auf das Leitsystem in der Regel möglich, auf einen Büro-PC hingegen nicht unbedingt.

ZUGRIFF MITTELS STEP-ICONS

Der Zugriff ins Step-by-STEP-Handbuch via Leitsystem muss klar und strukturiert sein. Dies ist vor allem in einem Ereignisfall wichtig, damit die vorgesehenen Schritte leicht erkennbar und somit umsetzbar sind. Die Mitarbeitenden müssen auf intuitive Weise zu den Einsatzdokumenten gelangen und ein gesuchtes Thema rasch finden. Dies lässt sich folgendermassen umsetzen: Das STEP-Icon *(Fig. 3)* ermöglicht über das Leitsystem den Schnellzugriff auf das gesamte Handbuch und die Einsatzformulare. Die Kapitelstruktur des Schnellzugriffs entspricht dem Handbuch in Papierform, wodurch der Wiedererkennungseffekt erhöht wird *(Fig. 3)*.

DIREKTER ZUGRIFF IM PROZESSBILD

Um den direkten Zugriff von einem Leitsystembild auf die Step-by-STEP-Dokumente zu ermöglichen, können an beliebigen Stellen im Prozessbild STEP-Icons platziert werden *(Fig. 4)*. So kann auf einen bestimmten Unterordner im Handbuch oder auf ein einzelnes Dokument direkt zugegriffen werden. Darüber hinaus können die Einsatzformulare spezifisch bei einzelnen Messwerten oder Maschinen hinterlegt werden *(Fig. 5)*. Das nachfolgende Beispiel zeigt die pH-Messung im Zulauf. Eine zu grosse Abweichung des pH-Wertes im Zulauf vom Sollwert ist ein Indikator für einen Störfall und hat einen Einsatz zur Folge. Wenn basierend auf der pH-Überwachung ein Alarm ausgelöst wird, erscheint das STEP-Icon bei der Meldung. Wird dieses angeklickt, so steht ein entsprechendes Einsatzformular mit den Schritt für Schritt abzuarbeitenden Massnahmen zur Verfügung.

ZENTRALE DOKUMENTENVERWALTUNG

Die Implementierung der Dokumente in das Leitsystem kann durch den Benutzer und den Leitsystemintegrator erfolgen. Alle Dokumente sind in der gleichen Step-by-STEP-Verzeichnisstruktur abgelegt wie im Ordner und können jederzeit ersetzt oder ergänzt werden. Die Aktualisierung im Leitsystem erfolgt unmittelbar und automatisch. Im Wesentlichen müssen folgende Aspekte bei der Pflege der Dokumente berücksichtigt werden:

- Aktualisierung/Ersetzen der Step-by-STEP-Dokumente und Einsatzformulare in der Verzeichnisstruktur
- Zuordnen der Einsatzformulare zu Messgeräten oder Maschinen
- Festlegung der benötigten STEP-Icons auf den Leitsystembildern (durch den Leitsystemintegrator)

FAZIT

Mit der PLS-Version des Step-by-STEP-Handbuchs und dem STEP-Icon steht den Mitarbeitern einer Kläranlage ein einfacher Zugriff auf die Einsatzdokumente auf der gewohnten PLS-Bedienebene zur Verfügung. Vorteilhaft ist zudem, dass mit der Ablage von step by STEP auf dem Leitsystem die Einsatzdokumente stets den gleichen Stand wie im Einsatzordner im Büro aufweisen, da ihre Verwaltung zentral erfolgt. Das Paket mit der aktuel-

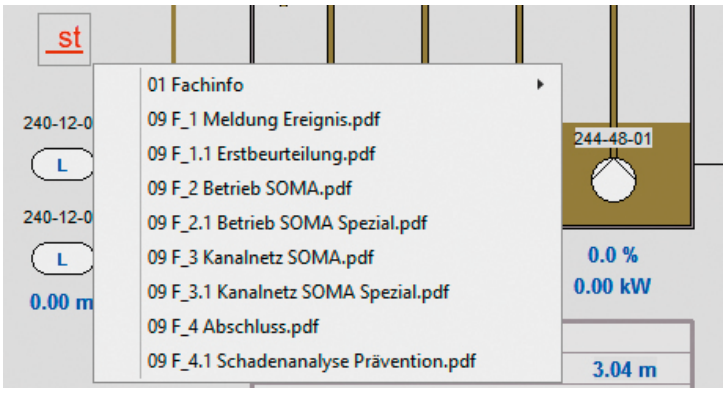


Fig. 4 STEP-Icon in einem Prozessbild und direkter Zugriff auf die Einsatzdokumente.
(Bild: ARA Neugut; Chestonag Automation AG)

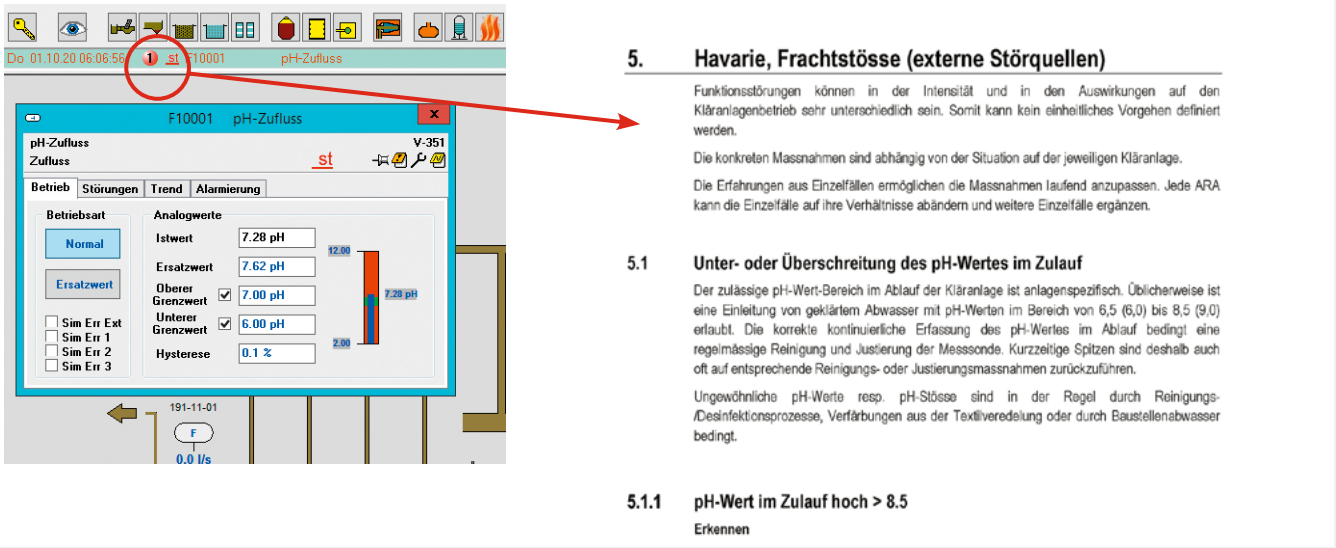


Fig. 5 Direkter Zugriff auf die Step-by-STEP-Einsatzdokumente im Falle einer Alarmmeldung. *(Bild: ARA Neugut; Chestonag Automation AG)*

len elektronischen Version kann bei den Leitsystemlieferanten bezogen werden, die Partner von «step by STEP» sind. Die aktuelle Liste der Partner-Leitsystemlieferanten ist auf *step-ara.ch* zu finden.

CYBERSICHERHEIT AUF KLÄRANLAGEN

Neben den meist bekannten Notfällen, die im Step-by-STEP-Handbuch beschrieben sind, gibt es inzwischen auch neue Risiken für Kläranlagen, nämlich die der Cyberkriminalität. Eine Kläranlage ist heute in der Regel eine hochautomatisierte Anlage und mit der zunehmenden Vernetzung, auch aufseiten der Cyberkriminellen, wächst die Gefahr eines Vorfalles (Notfall). Um möglichen Gefahren angemessen zu begegnen, verweist «step by STEP» auf den IKT-Minimalstandard Abwasser [2] des Bundesamts für wirtschaftliche Landesversorgung BWL.
Ziel des IKT-Minimalstandards Abwasser ist es, die Widerstandsfähigkeit der Leitsystemnetzebene (OT) und der Büro-Netzumgebung (IT) gegenüber Angriffen zu verbessern. Infolge der fehlenden Erfahrung im Bereich Cybersicherheit auf Kläranlagen ist die Umsetzung dieser Themen sowohl für Planer als auch Betreiber herausfordernd. Im Folgenden werden daher die Grundprinzipien erläutert, wie eine zeitgemässe Cybersicherheit auf Kläranlagen erreicht werden kann.

ANLAGENTYP UND RISIKOEXPOSITION

Um die Risikoexposition abzuschätzen, ist die Kläranlage zunächst zu kategorisieren. Normalerweise wird dazu die Kläranlagengrösse herangezogen. Hinsichtlich Risiken stellt diese allerdings meist keine ideale Kenngrösse dar. Als Beispiel kann der Umgang mit explosiven Stoffen angeführt werden. Die Gefahren, die der Einsatz explosiver Stoffe grundsätzlich mit sich bringt, sind für alle Anlagen dieselben. Die Schutzmassnahmen werden sich hingegen je nach Situation, Bau, Standort, Installation usw. unterscheiden. Ebenso verhält es sich mit den Cyberrisiken. Die Risikoexposition einer Kläranlage, deren System nicht mit dem Internet verbunden ist, ist deutlich kleiner als bei einer Anlage, die über das Internet ferngesteuert wird. Es ist sinnvoll, Kläranlagen anhand von drei Basis-Anlagetypen einzuordnen und so die Exposition gegenüber Cyberrisiken abzuschätzen. Diese Grundtypen werden im Folgenden dargestellt. In der Praxis ist die Typisierung von Kläranlagen nicht immer eindeutig.

Typ 1: Anlage nur mit Wartungszugriff auf das Leitsystem

Das Betriebspersonal hat keine Möglichkeit der Fernsteuerung, es besteht nur ein Wartungszugriff auf das Leitsystem durch den Lieferanten. Die einzige digitale Verbindung zum Betriebspersonal ist die Alarmierung via Pager resp. Natel. Die Anzahl der Benutzer ist gering. Dieser Anlagentyp *(Fig. 6)* weist das geringste Cyberrisiko im Vergleich mit den anderen beiden Typen auf.

Typ 2: Anlage mit Fernzugriff auf das Leitsystem

Dieser Anlagentyp *(Fig. 7)* kann durch das Betriebspersonal aus der Ferne gesteuert werden und der Leitsystem-Lieferant kann, wie bei Typ 1, Wartungsarbeiten aus der Ferne ausrichten. Allenfalls besteht zusätzlich noch die Möglichkeit, Betriebsdaten vom PLS auf einen Büro-PC zu übertragen. Der Büro-PC hat ebenfalls Internetanschluss. Die Anzahl der Benutzer und Verbindungen sind bereits grösser als bei Typ 1, wodurch das Cyberrisiko steigt.

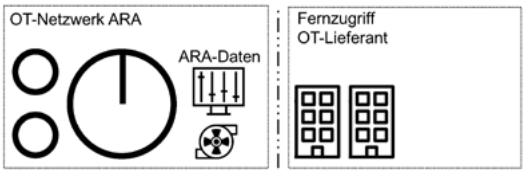


Fig. 6 Infrastruktur Typ 1: Keine Fernsteuerung, nur Fernwartungszugriff des OT-Lieferanten; Alarmierung via Pager oder Natel. *(Quelle: first frame networkers ag)*

Typ 3: Komplexe Anlage

Die komplexe Anlage *(Fig. 8)* ist mit all ihren Anlagenteilen hochgradig vernetzt. Diese umfassen einerseits die Kläranlage selbst und andererseits die Aussenbauwerke. Auch eine Vernetzung mit anderen Kläranlagen ist möglich. Die Benutzer sind vielfältig: Zusätzlich zum Betriebspersonal und dem PLS-Lieferanten können weitere Lieferanten, z. B. diejenigen eines Blockheizkraftwerks oder einer Photovoltaikanlage, direkten Zugriff auf Anlageteile haben. Allenfalls sind auch Gemeinden oder Dritte Benutzer des OT-Systems. Zudem ist die IT-Seite mit eigenem Server und den Zugriffen darauf zu berücksichtigen. Die Anzahl IT-Benutzer rangiert zwischen wenigen und sehr vielen. Für diesen Anlagentyp ist das Cyberrisiko am grössten.

RISIKOEXPOSITION NIMMT MIT STEIGENDER VERNETZUNG UND NUTZERZAHL ZU

Weist eine Kläranlage eine höhere Risikoexposition auf, hat dies direkte Auswirkungen auf die zu treffenden Cybersicherheitsmassnahmen. Eine Kläranlage des Typs 1 benötigt weniger Massnahmen und Aufwendungen als eine Kläranlage des Typs 3, um ein ähnlich hohes Cybersicherheitslevel zu erreichen. Folgende Gründe lassen sich dafür anführen:

- *Vernetzung*: Durch die stetig wachsende Vernetzung des Systems mit dem Internet wird die Angriffsfläche drastisch erhöht. Mit der Vernetzung steigen aber auch die Erwartungen der beteiligten Akteure. Jeder Akteur möchte von der Vernetzung profitieren und Zugriff auf die Anlage haben.
- *Schnittstellen*: Da OT- und IT-Umgebungen verschiedene Vorgaben bezüglich Sicherheit und Verfügbarkeit haben, muss den Schnittstellen zwischen diesen beiden Umgebungen besondere Aufmerksamkeit gewidmet werden. Es gilt, die zwei Netze klar voneinander zu trennen und nur die Datenflüsse zu erlauben, die für den ARA-Betrieb notwendig sind.
- *Verantwortungsbewusstsein*: Je umfangreicher und komplexer eine Infrastruktur und deren Betriebsabläufe sind, umso mehr involvierte Akteure gibt es. Das Verantwortungsbewusstsein des Einzelnen beschränkt sich verstärkt auf seinen Bereich. Dabei gerät der Blick für das grosse Ganze oft in den Hintergrund. Es wird schwieriger, allen Beteiligten die Cybersicherheitsvorgaben und -massnahmen zu erläutern und die einzuhaltenden Direktiven umzusetzen.
- *Akzeptanz*: Die Benutzer tragen wesentlich zur Cybersicherheit bei, wenn sie verstehen, dass Cybersicherheit Vorrang vor den eigenen persönlichen Bedürfnissen in der Bedienung des Systems hat. Dieser Lernprozess findet an vielen Orten erst noch statt. So dürfen beispielsweise nur jene Aufgaben im Leitsystem durchgeführt werden, für die es vorgesehen ist. Andere Verwendungen der Computer des Leitsystems sind nicht gestattet. Beispielsweise sind die Daten für eine Auswertung zentral anzufragen und auf einen geeigneten Computer zu transferieren. Dies kann den Benutzern mühsam erscheinen, ist jedoch der sichere Weg in Bezug auf Cyberrisiken.
- *Reduktion der Risiken*: Eine Reduzierung der Benutzeranzahl sowie getrennte OT- und IT-Systeme verbessert die Resilienz. Ebenso verhält es sich, wenn das OT-System keine IT-Anwendungen zulässt.
- *Erkennbarkeit von Risiken*: Je komplexer die Umgebungen sind, desto schwieriger ist es, Risiken zu erkennen und nachhaltig zu beheben.

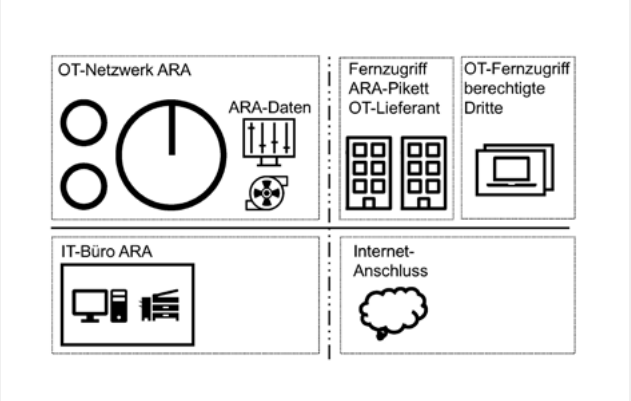


Fig. 7 Infrastruktur Typ 2 (in der Praxis häufig): Fernzugriff ausschliesslich durch ARA-Mitarbeiter; Alarmierung via Pager oder Natel; Fernwartungszugriff des OT-Lieferanten; Büro-PC.
(Quelle: first frame networkers ag)

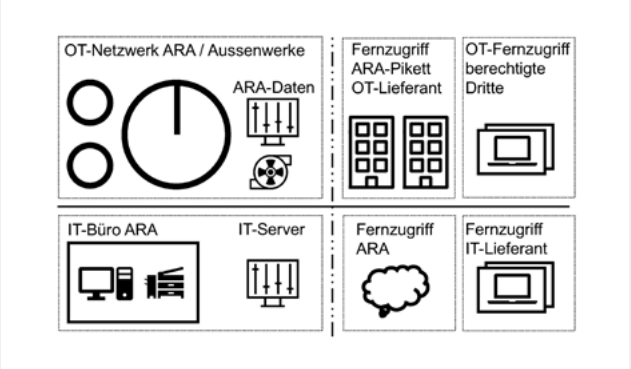


Fig. 8 Infrastruktur Typ 3 (komplexe Infrastruktur): OT- und IT-Netzwerk; OT-Fernzugriff für ARA-Mitarbeiter und Drittberechtigte; Alarmierung via Pager oder Natel; Fernwartungszugriff des OT-Lieferanten; IT-Fernzugriff für ARA-Berechtigte; Fernwartungszugriff des IT-Lieferanten. *(Quelle: first frame networkers ag)*

SIEBEN SCHRITTE ZUR CYBERSICHERHEIT

Zum Thema Cybersicherheit in Kläranlagen liegen erst wenige Erfahrungen vor. Daher ist es von Vorteil, die wenigen bisher gesammelten Erfahrungen anderer Kläranlagen aufzunehmen, um dadurch effizient und kostengünstig zu einer Ist-Bestandsaufnahme und einer massgeschneiderten Massnahmenplanung zu gelangen. Deshalb wurden die Erfahrungen von Cyberexperten sowie OT- und IT-Lieferanten zusammengetragen und in step by STEP integriert. Um das Thema der Cybersicherheit in Kläranlagen zu etablieren, haben sich die folgenden sieben Schritte bewährt:

Schritt 1: Self Assessment durchführen

Der IKT-Minimalstandard Abwasser bietet eine Checkliste für eine Selbsteinschätzung. Diese wird durch die Betriebsleitung mit minimalem Aufwand ausgefüllt (nur Ja/Nein-Antworten möglich). Anhand dieser Selbsteinschätzung zeigt sich, wo potenzielle Risiken auf der Kläranlage vorhanden sind.

Schritt 2: Ist-Zustand erfassen

Auf Basis der Selbsteinschätzung und der Step-by-STEP-Dokumentation der OT- und IT-Systeme werden gemeinsam mit einem Cyberexperten sowie den OT- und IT-Lieferanten Schwachstellen aufgedeckt. Die Ist-Zustandserfassung umfasst vier Haupt-

DANK
Ein grosser Dank geht an die Mitarbeiter der Kläranlagen Fällanden, Wetzikon und Neugut für ihre Unterstützung bei diesem Beitrag. Diese ARA sind Vorreiter in der Umsetzung von «step by STEP». Ein Dankeschön auch an *Johanna Otto* für das Lektorat dieses Beitrags.

schwerpunkte: Hardware, Software, Vernetzung, Datenbestände.

Schritt 3: Massnahmen erarbeiten
Der Cyberexperte schlägt Massnahmen zur Risikoreduktion vor und definiert gemeinsam mit der Betriebsleitung und den OT- und IT-Lieferanten, wie diese umgesetzt werden können. Die Ergebnisse hält der Cyberexperte zusammen mit seinen Feststellungen und Empfehlungen in einem Bericht für den Betreiber fest.

Schritt 4: Betreiber definiert Restrisiko
Der Betreiber definiert das Restrisiko, welches er einzugehen bereit ist. Die Betriebsleitung spricht die nötigen Mittel zur Risikoreduktion und definiert Verantwortlichkeiten und Aufgaben.

Schritt 5: Massnahmenumsetzung in Etappen
Gemeinsam mit Cyberexperte, den OT- und IT-Lieferanten definiert die Betriebsleitung einen Massnahmenplan. Sie legt fest, welche organisatorischen, technischen und auf das persönliche Verhalten wirkenden Massnahmen durch wen und bis wann umgesetzt werden. Die Betriebsleitung oder der Planer nehmen die Kosten in die Budget-Position auf und lassen die Wirksamkeit der umgesetzten Massnahmen durch den Cyberexperten prüfen.

Schritt 6: Prozess aufrechterhalten
Cybersicherheit ist kein Zustand, sondern ein Prozess. Die Bedrohungen wie auch die zu schützende Anlage verändern sich mit der Zeit. Daher müssen neue Risiken erkannt und allenfalls neue Massnahmen getroffen werden. Die Schritte 2 und 3 sind deshalb jährlich zu wiederholen.

Schritt 7: Direktiven erlassen
Um die Sicherheit zu erhöhen, erlässt die Betriebsleitung Direktiven, die Kontrollmechanismen umfassen. Diese Direktiven gilt es auf allen Ebenen einzuhalten, von den Mitarbeitern bis hin zu Externen und Lieferanten, denen ein Zugriff ermöglicht wird.

SCHLUSSFOLGERUNGEN

Das Step-by-STEP-Handbuch hat sich dank seiner unkomplizierten Anwendung bereits auf diversen Kläranlagen und in unterschiedlichen Situationen bewährt. Das Beispiel der ARA Flos zeigt, dass die korrekten Vorgehensweisen im Notfall, die im Handbuch beschrieben sind, geübt und bereits mehrfach unter realen Bedingungen erfolgreich umgesetzt werden konnten. Durch seine klare Struktur und die regelmässige Überprüfung der Dokumente kann im Notfall durchdacht und auf das Wesentliche konzentriert gehandelt werden. Damit das Step-by-STEP-Handbuch sowohl direkt auf der Anlage als auch über Fernzugriff verfügbar ist, bietet sich der Zugriff über das Leitsystem mit dem STEP-Icon an. Auf der ARA Neugut wurde dies erstmals in die Praxis umgesetzt. Der Zugriff kann benutzerfreundlich und anlagenspezifisch gestaltet werden. Die periodische Erinnerung der Wartung der Dokumente erfolgt über das Leitsystem.
Überdies ist step by STEP zusammen mit dem IKT-Minimalstandard Abwasser ein gutes Werkzeug, um Kläranlagen in Fragen der Cybersicherheit zu unterstützen. Angriffe von Cyberkriminellen nehmen zu und die Komplexität der eingesetzten Technologien führt zu einer grösseren Fehleranfälligkeit. Cybersicherheit ist heute ein Thema, das jede Kläranlage betrifft. Der IKT-Minimalstandard Abwasser hilft dabei, Experten dort einzusetzen, wo sie wirklich benötigt werden, um passende Massnahmen zum Schutz vor Cyberrisiken zu erarbeiten. Zusätzlich sind Cyberexperten in der Lage, mithilfe des Minimalstandards die Wirksamkeit und Angemessenheit dieser Massnahmen zu prüfen.

BIBLIOGRAPHIE

[1] *M. Schachtler et al. (2019): Handbuch step by STEP. Dübendorf. https://step-ara.ch*
[2] *Bundesamt für wirtschaftliche Landesversorgung BWL (2019): Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben. https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html*

> SUITE DU RÉSUMÉ

instructions de procédure pré-remplies sont l'outil qui permettra une action ciblée et méthodologique en cas d'incident. De plus, le personnel d'exploitation travaille au quotidien avec le système de supervision qui lui est donc très familier.
La cybersécurité d'une station d'épuration peut être renforcée de par la mise en œuvre de la norme minimale TIC (Technologies de l'Information et de la Communication) sur les eaux usées et du manuel step by STEP. Sur la base de ces documents, les risques pour la station d'épuration peuvent être évalués et des mesures appropriées peuvent être mises en place en collaboration avec des cyber-experts. Les objectifs de sécurité et la portée des mesures sont à être déterminées au cas par cas par les exploitants.