Hochschule Ostwestfalen-Lippe
University of Applied Sciences

NATO Workshop on Physical and Cyber Safety in Critical Water Infrastructure
Oslo, Norway, 8 - 11 October 2018

Overview: Preparedness in the European / German Water Supply Sector

Joachim Fettig

University of Applied Sciences Ostwestfalen-Lippe, Germany
Department of Environmental Engineering and Applied Informatics

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Table of Contents

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Introduction

The Water Supply Sector in Germany and Europe

Germany

Population → 82.8 Mio.
Drinking water production → 4.5 Bio. m^3/a
DW consumed in households → 3.6 Bio. m^3/a
No. of utilities → > 4,000 small + 1,700 medium/large suppliers

Europe (29 EurEau countries)

Population → ~ 525 Mio.
Drinking water production → 47.7 Bio. m^3/a
DW consumed in households → 22.8 Bio. m^3/a
No. of utilities → between < 100 (e.g. Bulgaria, UK) and several thousand (e.g. Czech Republic, Sweden)

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Physical Security: The Water Safety Plan Concept

→ A comprehensive risk assessment and risk management approach from water catchment to consumption

General idea

The **Water Safety Plan concept** was developed by the World Health Organization (WHO 2005). It is now included in the WHO Guidelines for Drinking Water Quality. A water safety plan consists of a comprehensive **risk assessment** and **risk management** approach that encompasses all steps in water supply from the catchment to the consumer.

The aim of a water safety plan is to **consistently ensure** the safety and acceptability of a drinking water supply.

Key requirement

In the utility, organizational structure or job descriptions must exist that determine **who is responsible** for which activity along the water supply steps.

Implementation

The development and implementation of water safety plans should fit in with the way a utility is organized and operates, otherwise it will not be accepted in the organization.

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Physical Security: The Water Safety Plan Concept

WHO has provided a manual to develop and implement water safety plans and recommends the following step-wise approach:

- Set up a team and decide on a methodology by which the water safety plan will be developed. It is important that this team has adequate experience and expertise to understand water abstraction, treatment and distribution, and the hazards that can affect safety through the supply system.
- Identify all the hazards and hazardous events that can affect the safety of a water supply from the catchment, through treatment and distribution to the consumer.
- Assess the risk presented by each hazard and hazardous event.
- Consider if controls or barriers are in place for each significant risk, and if these are effective.
- Validate the effectiveness of controls and barriers.
- Implement an improvement plan where necessary.
- Demonstrate that the system is consistently safe.
- Regularly review the hazards, risks and controls.
- Keep accurate records for transparency and justification of outcomes.

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Physical Security: The Water Safety Plan Concept

Implementation in Germany and Europe

2008

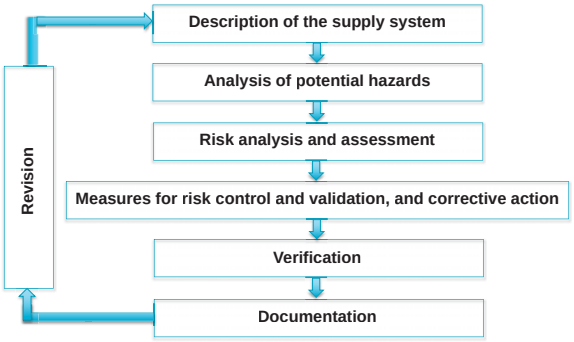
Technical code W 1001 “Secure Drinking Water Supply” developed and adopted by the German Water and Gas Association (DVGW)

2013

DIN EN 15975-2 “Security of Drinking Water Supply Systems – Guidelines for Risk and Crisis Management – Part 2: Risk Management”

→ Process oriented risk management

Physical Security: The Water Safety Plan Concept



Scheme of the risk management according to DIN EN 15975-2

Physical Security: The Water Safety Plan Concept

Experiences with risk management in Germany

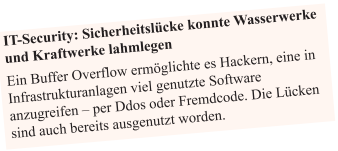
2016

- Certification of utilities according to the Technical code DVGW W 1000 "Requirements on the Qualification and Organization of Drinking Water Utilities"

2018

- Evaluation by the German Environmental Protection Agency (UBA)
  → questionnaires sent to water utilities, not finished yet
- Development of the web tool TRiM®online by the IWW Institute
  → support of small utilities with limited human resources
- Development of handbooks for **crisis management** in large utilities according to DIN EN 15975-1 "Security of Drinking Water Supply – Guidelines for Risk and Crisis Management - Part 1: Crisis Management"

IT Security: Precautions against Cyber Attacks


IT-Security: Sicherheitslücke konnte Wasserwerke und Kraftwerke lahmlegen

Ein Buffer Overflow ermöglichte es Hackern, eine in Infrastrukturanlagen viel genutzte Software anzugreifen – per Ddos oder Fremdcode. Die Lücken sind auch bereits ausgenutzt worden.


Cyber-Attacken kosten 43 Milliarden Euro

Erschreckend: Bei fast einem Viertel der Unternehmen sind digitale Daten abgeflossen

Estimated cyber crimes in German industries (Bitkom, 2018):

- 70% of all enterprises have been attacked in 2016-17.
- 25% of all companies have lost digital data (e-mails, customer files, financial data, R&D results).
- Current or earlier personnel is presumably involved in > 60 % of the attacks.
- Foreign intelligence services are involved in 11% of the attacks.
- The financial losses in two years are on the order of 43 Bio. €.

IT Security: Precautions against Cyber Attacks

Critical infrastructures in Germany: Overview

- Definition of 9 different sectors, where **water** is one sector
- Collaboration between operating companies, associations and authorities in the framework of the implementation plan UP KRITIS, since 2007
- Central goal of UP KRITIS is to increase the resilience of critical infrastructures where **cyber security** is an important aspect.

UP KRITIS

Sectors of critical infrastructure in Germany

IT Security: Precautions against Cyber Attacks

Critical infrastructures in Germany: Requirements on IT security

2009

- Act on the Federal Office for Information Security (BSI Act)
  → § 8a: Security of information technology in critical infrastructures

2016

- Ordinance for the definition of critical infrastructures (BSI KRITIS Ordinance)
  → Requirements set by the BSI Act have to be met within 2 years by all utilities which deliver > 22 Mio. m^3/a of water (equivalent to 500,000 people served); this applies to about 40 utilities (smaller ones are encouraged to join).

2017

- Development of an **industry-specific security standard** for water supply / waste-water utilities (**B3S WA**) by DVGW and DWA
  → Definition of the state-of-the-art regarding technical processes and organization by the DVGW code of practice W 1060 "IT Security"
  → Specification of cyber security by IT security guidelines

IT Security: Precautions against Cyber Attacks

Implementation of the requirements of the BSI Act

Deadline for the utilities: 3 May 2018, thereafter reporting every other year

Procedure:

- Hazard analysis and risk assessment for water abstraction, water treatment, waterworks, water distribution, and control units
- Implementation of basic and standard measures
- Proof for the Federal Office for Information Security by means of an audit or a certificate, e.g. according to ISO 27001 (Information security management systems)
- Specification of a contact point for the BSI for the exchange of relevant information

Support: Web-Application of the IT security guidelines (DVGW, 2017)

→ 22 case studies with different infrastructure configurations of the IT systems
→ Generation of the corresponding hazards regarding IT security
→ Suggestion of security measures to be taken

IT Security: Precautions against Cyber Attacks

Experiences of German water suppliers with the B3S approach

- Implementation by Berliner Wasserbetriebe (200 Mio. m^3/a):
  - → Human resources well qualified, also from contributing to the development of B3S WA
  - → Analysis and assessment of > 2000 different facilities and processes very time-consuming
- Offer of diagnosis and risk management software in order to assess the current status (Example: Software IRMA of Videc Data Engineering Co., offered by Phoenix Contact Co.)

Challenge: How can new tools, e.g. short-range wireless transmitted data from water meters to cars passing in the streets, be designed and applied with adequate safety standards?

IT Security: Precautions against Cyber Attacks

Status in Europe:

EU Directive 2016/1148 „Measures for a high common level of security of network and information systems across the Union"

- Obligation to adopt national strategies on the security of network and information systems
- Creation of a computer security incident response teams (CSIRTs) network
- Establishment of security and notification requirements for operators of essential services and for digital service providers
- Obligation to designate national competent authorities, single points of contact and CSIRTs
- Obligation to give the competent authorities the necessary powers and means to assess the compliance of operators of essential services
- Obligation to adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with the Directive

IT Security: Precautions against Cyber Attacks

Status in Europe:

The European Commission has the obligation to review the functioning of the directice and to submit a report to the EU Parliament and the EU Council by 9 May 2021

→ No information on the state of implementation available yet

Examples from two countries:

UK: Development of a water sector cyber security strategy 2017-2021

→ Vision for 2021 is a secure, effective, and confident water sector, resilient to the ever-evolving cyber threat.

The Netherlands: Definition of critical infrastructures where drinking water supply and water management belong to category A

→ Application of "testbeds", i.e. platforms where CI operators and manufacturers can test hardware and software in a protected simulation environment.

Conclusions and Outlook

1. In many European countries the water supply sector is very diverse, that is, there is a large variety of public and private companies of different size.
2. Based on WHO's water safety plan concept, the DIN EN 15975-2 provides a sound basis for establishing the physical security of water utilities. This is basically a process oriented risk management approach. In Germany it has been implemented by many large and medium-sized utilities while there is a backlog in small supply companies.
3. Regarding IT security, utilities which produce > 22 Mio. m^3/a of drinking water belong to the critical infrastructures in Germany. An industry-specific security standard (B3S WA) has been developed and implemented by the ~ 40 utilities concerned. Smaller companies are encouraged to follow up.
4. There are several ongoing research projects, e.g. the Stop-IT project presented by Rita Ugarelli, with four German partners.

STOP-IT

IT security will remain a big challenge in the years to come !