

Safety Approaches in Water Utilities and Systems Safety Engineering: A Comparison

Dr. Ioannis M. Dokas

2009



Forward

This technical report is a research deliverable of the project 'Supporting the Concept of Early Warning Analysis - SCEWA'. SCEWA is a 5 year research project, funded by the Irish Environmental Protection Agency under the DERP grant scheme, which began on January 2008. The ultimate objective in the SCEWA is to support organisations and states agencies in providing early warning services. One goal in SCEWA project is to develop a prototype web based early warning system for water treatment plant operations. The prototype Early Warning System will be delivered to the Irish Environmental Protection Agency in order to set the foundations for early warning services in this domain.

This report explores the concept of safety from the view point of two scientific domains, namely the water utilities and system safety engineering. The report is based on the hypothesis that the advancements in systems safety engineering domain can be used as a benchmark in comparing the state of the art approaches for safety used by researchers and practitioners in the water utilities sector. In this report, we review safety approaches in both domains and identify methodological gaps.

Acknowledgments

I would like to acknowledge the Irish Environmental Protection Agency for supporting this research. Very special thanks go out to John Feehan and Gordon Rios. I would like to thank John for providing his material on hazard analysis and critical control point method and Gordon for his review and comments on the draft version of this document.

Table of Contents

Forward.....	1
Acknowledgments.....	2
1. Introduction	4
1.1. Adverse Effects.....	5
1.2. Report Objectives.....	6
2. Definitions	6
2.1. Definitions in the Water Utility Sector.....	6
2.2. System Safety Engineering Definitions	8
3. Safety Approaches in the Water Utility Sector	10
3.1. Monitoring	10
3.2. Multiple barrier approach.....	11
3.3. Water Safety Plans and HACCP	14
4. System Safety Engineering Approaches.....	16
4.1 Domino Model	16
4.2. Normal Accident Theory	17
4.3. The “Swiss Cheese” Model	17
4.4. The Rasmussen Framework	18
4.5. STAMP.....	19
5. Methodological Gaps and Conclusions	20
Bibliography	21

1. Introduction

Water safety issues are growing in importance among professional and general public, fuelled by the publicity given to some waterborne disease outbreaks that have affected communities in many parts of the world. During 2005, for example, 7,960 confirmed cases of cryptosporidiosis were reported in Europe. Ireland with 13.75 and UK with 9.26 per 100,000 cases have reported the highest incidence rates (Semenza, et al., 2007). In the republic of Ireland in particular, in 2007, the city of Galway experienced the adverse effects of having drinking water contamination due to cryptosporidium parasite caused by human sewage (Bradley, 2007) resulting in at least 180 serious cases of cryptosporidiosis. In late 2008 the Irish Environmental Protection Agency reported that 339 public water supplies, representing 36% of public drinking water supplies, required detailed profiling to ensure that it was providing clean and wholesome drinking water (Page, et al., 2009). These water supplies were included in a remedial action list. The remedial action list includes only supplies where the primary issue is the water treatment plant.

In North America, a significant number of waterborne disease outbreaks were recorded. Specifically, from 1991 to 2000, 155 outbreaks and 431,846 cases of illness in public and individual water systems were recorded in the U.S. (CCDACC, 2003). The most dramatic case of waterborne disease outbreak in Canada was that of Walkerton in May 2000 where more than 2,300 people became ill and seven died. In addition to the adverse effects on public health, the Walkerton outbreak had a significant economic cost, estimated at over 65 \$ million (CAD) including a cost of 9.5 \$ million (CAD) for a public inquiry to investigate the event (Rizak, et al., 2007). Clearly, the contamination of drinking water has been identified as a major problem in many countries. It has attracted the attention of the public giving rise to the discussions about issues of drinking water safety and risk management of water utilities.

The recent discussions on risk management and drinking water safety are usually focused on the performance of water supply systems from the catchment of the water source to the consumers tap. Basic elements of a water supply system are the source, the treatment plant, and the distribution system. Shallow wells, rivers, natural lakes, springs, artificial lakes and reservoirs are common water sources. A water distribution system is usually composed of three major components: pumping stations, distribution storage, and distribution piping (Mays, 2004). Water treatment plants are engineering systems purifying raw water to specific safety levels defined by regulations. Raw water passes through a series of treatment phases wherein it is processed and purified to meet existing safety standards. After purification, water is distributed to the consumers through a network of pipes, pumps and reservoirs.

The purification phases in a typical surface water treatment plant are shown in Figure 1. In raw water entering the water treatment facility, small particles of solids and organic matter as well as other impurities are suspended. During coagulation, a flocculating agent is thoroughly mixed with the water and this causes colloidal particles to coagulate, forming larger particles which are known as “flocs”. The water containing “flocs” is passed to large settlement/sedimentation tanks. This occurs slowly in order to allow heavy solid particles and “flocs” to settle to the bottom of the tanks. This process is known as sedimentation, where clear water continues its route within the plant and the remaining sludge is handled and disposed of according to regulations.

After sedimentation, any small quantities of solids remaining are removed by sand filters. A typical sand filter consists of layers of gravel, coarse sand, sand and fine sand. The water may contain some harmful bacteria or micro-organisms. During disinfection, a sufficient quantity of chemicals, usually chlorine or chlorine compounds, are added to kill most pathogenic micro-organisms in the water and to prevent recontamination before the water reaches the taps. Finally, for water supplies, fluoride is added to the water with the main aim to reduce tooth decay of consumers.

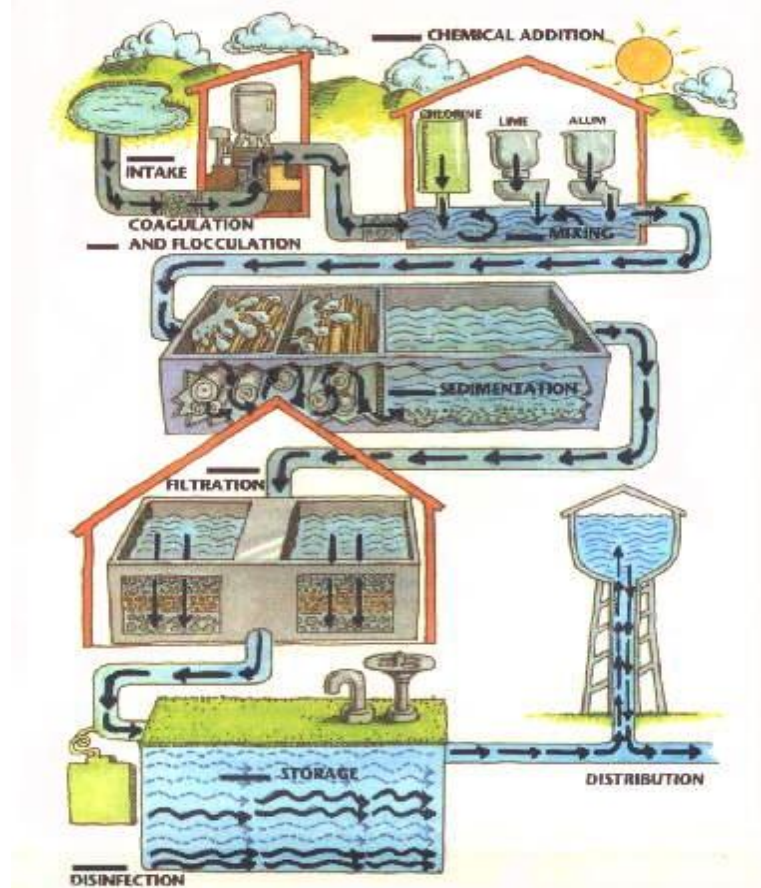


Figure 1: Surface Water Treatment Plant [Source: <http://www.geocities.com/CapeCanaveral/>]

1.1. Adverse Effects

Statistical analysis of recorded waterborne disease outbreaks illustrates the importance of undisturbed and safe operation of water treatment plants to drinking water safety. In a surveillance study of waterborne disease outbreaks in the U.S. for the years 2005 – 2006, 20 cases were found to be associated with inferior drinking water quality (Yoder, et al., 2008). The analysis identified 23 deficiencies of water supplies systems. The most frequently cited deficiencies were associated with a treatment deficiency (e.g. temporary interruption of disinfection, inadequate or no filtration, chronically inadequate disinfection) or with the absence of any type of treatment.

In addition, the importance of water treatment safety has been underlined by the 1993 cryptosporidium outbreak in Milwaukee, Wisconsin in the USA caused by cryptosporidium oocysts that passed through the filtration system of one of the city's water-treatment plants (Mac Kenzie, et al., 1994). It was estimated that over the span of approximately two weeks 403,000 residents in the Milwaukee area became ill with stomach cramps, fever, diarrhoea and dehydration caused by the

pathogen with 69 deaths attributed to this outbreak (Hoxie, et al., 1997). The cost of illness for the Milwaukee outbreak was estimated at \$ 96.2 million (USD) (Corso, et al., 2003).

1.2. Report Objectives

Unquestionably, water treatment plants are important components of a water supply system. This report is focused on safety of this critical infrastructure. The report reviews the approaches used in water utilities and systems safety engineering sectors and compares them to identify similarities, differences, and “methodological gaps”.

The basic finding of this report is that the risk management philosophy in water utilities is transitioning towards a multiple barrier - proactive approach, while in systems safety engineering a multiple barrier approach to assess safety is not something new. In the latter, the state of the art attempts are seen accidents as non-linear emerging phenomena. This indicates that there is a “methodological gap” in the research agenda between the two domains, based on the hypothesis that the system safety engineering domain is a benchmark allowing for comparisons of this kind.

2. Definitions

Some terms like “safety”, “risk” and “hazard” are widely used in everyday language as well as in many scientific domains. However, the meaning of these terms could be different, depending on the background of the listener. For example, the term “accident” can refer to either an event, the outcome of an event, or the possible cause (Hollnager, 2004). It is important to provide a list of definitions that specify the meaning of those terms in both drinking water supply and systems safety engineering domains.

2.1. Definitions in the Water Utility Sector

In the water utilities sector the term “safe” is mainly used to indicate a state of water quality that accords with predefined standards. “Safe water” means that potential harmful substances, depending on their nature and characteristics, are either absent from the water or their quantities falls below safety standards. The standards for safety levels are updated periodically. For example, new substances can be included in the standards or alternatively the values indicating the accepted amount of the substances in the water could be updated. In the Republic of Ireland for example, the latest water quality standards have been defined in the 2007 Drinking Water Regulations (SI, 2007) and are shown in Table 1: Parameters and parametric values.

One notion of “safety” is given by Hrudey et al. (2006) defined as “*a level of risk so negligible that a reasonable, well-informed individual need not be concerned about it, nor find any rational basis to change his/her behaviour to avoid such a small, but non-zero risk. This notion of safe drinking water should mean that we do not expect to die or become seriously ill from drinking or using it*”.

Drinking-water safety includes also monitoring the efficiency of control measures using appropriately selected determinants and a final verification of microbial and chemical quality (WHO, 2004). Safety of drinking water supplies in Ireland, for example, is determined by comparing the results of numerous tests carried out on water supplies, and public group water schemes against water quality standards (Page, et al., 2009).

Table 1: Parameters and parametric values			
MICROBIOLOGICAL PARAMETERS			
	Parameter	Parametric value	Unit
1	Escherichia coli (E.coli)	0	(number/100 ml)
2	Enterococci	0	
CHEMICAL PARAMETERS			
3	Acrylamide	0.10	µg/l
4	Antimony	5.0	µg/l
5	Arsenic	10	µg/l
6	Benzene	1.0	µg/l
7	Benzo(a)pyrene	0.010	µg/l
8	Boron	1.0	mg/l
9	Bromate	10	µg/l
10	Cadmium	5.0	µg/l
11	Chromium	50	µg/l
12	Copper	2.0	mg/l
13	Cyaniade	50	µg/l
14	1,2 dichloroethane	3.0	µg/l
15	Epichlorohydrin	0.10	µg/l
16	Fluoride (a) fluoridated supplies (b) supplies with naturally occurring fluoride, not needing further fluoridation	0.8 1.5	mg/l mg/l
17	Lead • until 24 December 2013 • from 25 December 2013	25 10	µg/l µg/l
18	Mercury	1.0	µg/l
19	Nickel	20	µg/l
20	Nitrate	50	mg/l
21	Nitrite	0.50	mg/l
22	Pesticides	0.10	µg/l
23	Pesticides Total	0.50	µg/l
24	Polycyclic aromatic hydrocarbons	0.10	µg/l
25	Selenium	10	µg/l
26	Tetrachloroethene and Trichloroethene	10	µg/l
27	Trihalomethanes	100	µg/l
28	Vinyl chloride	0.50	µg/l
INDICATOR PARAMETERS			
29	Aluminium	200	µg/l
30	Ammonium	0.30	mg/l
31	Chloride	250	mg/l
32	Clostridium perfringens (including spores)	0	number/100 ml
33	Colour	Acceptable to consumers and no abnormal change	
34	Conductivity	2500	µS cm ⁻¹ at 20 °C
35	Hydrogen ion concentration	6.5 and 9.5	pH units
36	Iron	200	µg/l
37	Manganese	50	µg/l
38	Odour	Acceptable to consumers and no abnormal change	
39	Oxidisability	5.0	mg/l O ₂
40	Sulphate	250	mg/l
41	Sodium	200	mg/l
42	Taste	Acceptable to consumers and no abnormal change	
43	Colony count 22°	No abnormal change	
44	Coliform bacteria	0	Number/100 ml
45	Total organic carbon	No abnormal change	
46	Turbidity	Acceptable to consumers and no abnormal change	
RADIOACTIVITY			
47	Tritium	100	Bq/l
48	Total Indicative Dose	0.10	mSv/year

Based on the World Health Organisation (WHO), drinking-water safety is secured by the application of a *water safety plan*. A water safety plan is a collection of comprehensive risk assessment and risk management approaches that encompass all steps in water supply from catchment to consumer (WHO, 2004) (i.e. the maintenance of safe water state by looking at what *may* go wrong in the water supply system).

The WHO drinking water regulations (WHO, 2004) are providing the following useful definitions:

- a *hazard* is a biological, chemical, physical or radiological agent that has the potential to cause harm;
- a *hazardous event* is an incident or situation that can lead to the presence of a hazard (what can happen and how);
- *risk* is the likelihood of identified hazards causing harm to exposed populations within a specified time frame, and include the magnitude of that harm and/or the consequences.

These concepts were illustrated with a specific pathogen by Hruday et al., (2006). *“Cryptosporidium is a hazard for any surface water system because it is always potentially present given its occurrence in human sewage and/or livestock wastes. A challenge to a water system by a waste source containing Cryptosporidium such as a sewage spill is a hazardous event. The risk associated with Cryptosporidium is the likelihood that this pathogen will pass through the treatment system to reach consumers in an infectious state and in numbers sufficient to cause illness”*.

2.2. System Safety Engineering Definitions

In systems safety engineering domain, *safety* is considered to be a property of a system that arises when the system components interact within an environment (Leveson, 2002). When a system is safe it is “free” from accidents or losses. Quoting Hollnager (2006), “safety is the sum of the accidents that do not occur”. *Accidents* are defined as being undesired and unplanned events that results in a loss. An accident need not involve loss of life, but it does result in some loss that is unacceptable to the customers or users (Leveson, 2002a). *Hazard* is defined as a state or set of conditions in the system that, together with other conditions in the environment, will lead to an accident or loss.

Taking for example the analysis of the Walkerton tragedy made by Leveson (2002), and Woo and Vicente (2003), the system level hazard that occurred was that “E-coli bacteria passed through the Walkerton municipal water treatment plant and entered the water supply system”. Based on their analysis, a set of unforeseen conditions and interactions between different system components and the environment made that system hazard possible. Some of the events and conditions that were considered as drivers in the Walkerton tragedy are:

- manure that had been spread on a farm near to the well of the water treatment plant some days before the tragedy;
- heavy rainfall in the area carrying bacteria from the farm in to the well of the water treatment plant;
- lack of chlorine residuals measurements even though daily checks were supposed to be carried out;
- irrational acts of the caretaker when he did not disclose to the health officials that laboratory test samples found positive for E.coli and total coliforms.

The above events and conditions were probably foreseen and identified as possible threats to the system independently to each other by the designers and decision makers. The tragedy is that the concurrence of these specific interactions between system’s components and the environment was not foreseen nor expected.

Clearly, the concept of safety, as given by systems safety engineering is not identical to the one used in the water utilities sector. In the Walkerton disaster for example, the laboratory confirmed the presence of bacteria (i.e. the hazard) in the samples and warned the caretaker that the water was not safe for consumption. This clearly shows that safety in the domain of drinking water supplies is an attribute of a system that consists among others of hardware, people, government agencies, procedures, laws and regulations. It is not only an attribute of the water substance, but also of a rather complex socio-technical system that includes, among others, human activities (e.g. farming, agriculture) at the catchment area, state agencies regulating the water treatment plants, the water service authorities which are responsible for water treatment plants operations.

A high level model of the socio-technical system for the provision of drinking water in the Republic of Ireland is depicted in Figure 2: Socio-technical System Model for the Provision of Drinking Water. Based on that model the public, group and private water supplies (i.e. the water treatment plants) are two out of ten components of the system. Other components are the Government Departments, the Environmental Protection Agency (EPA) and the Health Services Executive (HSE), which are involved in the provision and regulation of drinking water in the Republic of Ireland. Local Authorities and the National Federation of Group Water Schemes are two more components.

In Figure 2: Socio-technical System Model for the Provision of Drinking Water, the components of the socio-technical system are connected with arrows. The arrows indicate the types of interactions and dependencies between the components. For example, the Department of the Environment, Heritage and Local Government is funding the Water Services Authorities. Part of that funding goes to public water supplies and the water treatment plants. The EPA regulates the Water Services Authorities and conduct audits to the water treatment plants. Water Services Authorities are responsible for the operation of public water supplies and should notify EPA and consult HSE, whenever drinking water quality parameters are exceeded.

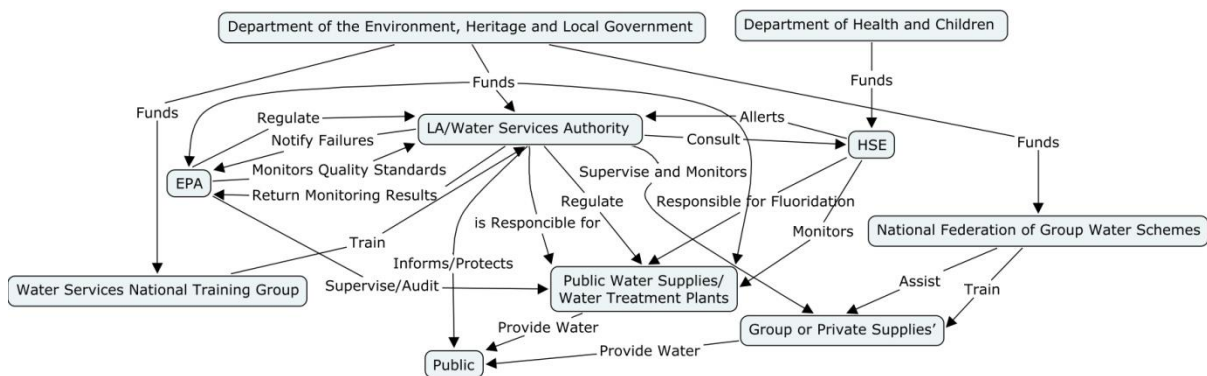


Figure 2: Socio-technical System Model for the Provision of Drinking Water

3. Safety Approaches in the Water Utility Sector

For many decades suppliers of drinking water were relying solely on the periodical testing of the end product to ensure that the distributed water was of good quality and safe for consumption. In many cases this approach proved to be ineffective because a problem with drinking water has only become obvious when consumers are seeking treatment for symptoms related to waterborne illnesses. However, over recent years, a transition seems to be happening in the water utility sector through the adaptation of more proactive approaches, aimed at the timely prevention of water quality problems. This section will introduce these approaches and will discuss some of their characteristics.

3.1. Monitoring

During the operation of water treatment plants several microbiological and non microbiological, parameters are monitored periodically (see for example Table 1). Some of these can be classified in to two main types namely the “index” and “indicator” parameters. The presence of an “index” parameter in a sample indicates that similar substances might be included in the water. The presence of an “indicator” parameter in a sample indicates that there was a failure in some stage of the water treatment process. For example, turbidity is used as an indicator of filtration efficiency. On the other hand, E.coli is an index of the purity of water based on a count of faecal bacteria. If E.coli is present in a sample, one can infer that the water has probably been exposed to faecal contamination. The main reason for monitoring these parameters is to verify whether the quality of the water is appropriate for human consumption.

Unquestionably, effective monitoring is an important component of a risk management approach. It improves understanding of the water treatment process and of its associated risks. However, in order to be truly sufficient and effective a monitoring programme has to address other issues such as:

- Parameters to be monitored
- Schedules, location and frequency of sampling
- Methods for quality assurance and validation of sampling
- A protocol for reporting and communicating results.

Some researchers and practitioners such as Rizak and Hruday (2007) argued that there is often a lack of a fully informed strategic basis to the design of drinking water quality monitoring programs. Usually in practice the monitoring programme within a water treatment plant conforms to a two phased process approach. During the first phase, continuous real time monitoring detects deterioration in the quality of drinking water. At the second phase of the monitoring process, drinking water samples are sent to laboratories for a more detailed analysis. During this phase a set of more sensitive contaminant tests are conducted using more sensitive identification technologies. However, the laboratory tests cannot be delivered immediately to decision makers, due to technological limitations.

Continuous real time monitoring of some physical and chemical parameters can be achieved with the use of systems known as Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are composed of software and hardware components pulling real time data, controlling processes, and monitoring equipment from remote locations to permit operators to monitor and

control facilities such as water treatment plants and water distribution systems. The data are collected by sensors. Sensors are devices able to measure and convert the values of critical parameters to signals in real or near-real time. For example, sensors are widely used to monitor the values of water quality parameters such as turbidity, UV absorbance, conductivity, and chlorine residual.

In addition to SCADA systems, Laboratory Information Management Systems (LIMS) are yet another type of important information technology infrastructure within the water utility sector. LIMS are used in the laboratories for monitoring and management of water samples. A LIMS enables its users to track water test samples during each step of their analysis. LIMS are also used to record, manage, and organise large collections of water analysis data and to facilitate rapid search and retrieval of water quality data.

In many countries, monitoring now includes not just the microbiological and chemical characteristics of the water but also a wide range of periodic checks aiming at verifying that the system and its barriers as a whole are working effectively and based on predefined specifications. For example, in Australia the monitoring includes (Australian, 2004) :

- *Operational monitoring*, which is used to check that the processes and equipment to protect and enhance water quality are working properly.
- *Drinking water quality monitoring*, which is a wide-ranging verification of the quality of water in the distribution system and as supplied to the consumer.
- *Monitoring of consumer satisfaction*, which is an assessment of consumer comments and complaints.
- *Investigative and research monitoring*, which includes strategic programs designed to increase understanding of a water supply system, to identify and characterise potential hazards, and to fill gaps in knowledge.

In short, over the years it has become obvious that sample testing and water quality monitoring on their own do not guarantee the safety of water supplies, and that there is a need to extend the role of monitoring from the narrow chemical and microbiological view towards a more systemic and holistic view. This has been embraced by the multiple barrier approach, which will be described in the following section.

3.2. Multiple barrier approach

The term *multiple barrier approach*, applied to the task of providing clean, safe drinking water, is the ability of the water industry to maintain a protected water source, to provide appropriate and adequate treatment, to provide, operate and maintain a distribution system and to provide adequate monitoring of regulated contaminants (Awwa, 2003). It was introduced as legislation by the 1996 Safe Drinking Water Act (EPA, 1996). In order to ensure a safe supply of drinking water a multiple barrier approach must have a coordinated set of programmes, an appropriate set of requirements as well as technical and managerial barriers between the potential threats and the consumer. This is graphically depicted in Figure 3.

Technical equipment for monitoring and reducing contamination in watersheds, appropriate water treatment technologies, properly trained and certified operators, and properly designed and constructed facilities are types of barriers between potential threats and consumers. Beyond the technological barriers, surveys and performance evaluation programs assessing the adequacy of a

water system's facilities and identifying potential improvements in the system are additional activities that ensure the integrity the acceptable performance of technological barriers. In addition, design and construction standards as well as education and training courses for personnel and managers contribute to the safety of water supplies.

Risk prevention is first in a multiple barrier approach to protecting a water supply system. It focuses on issues related to selection and protection of the drinking water sources. When selecting a water source it has to be examined first for quality of its raw water and for capacity to meet the current and future quantity needs. In addition, the risk of raw water contamination has to be assessed by thoroughly considering potential contaminations from man-made and natural factors in the catchment area. This means that the sources of contamination, together with the conditions under which risks may be realised, have to be identified and to be controlled by appropriate protection strategies. Thus, monitoring for conditions that could increase the risk of contamination through implementation of source water protection strategies is an important aspect of the risk prevention barrier.

Risk management is the second barrier of the approach. It focuses on the water treatment process of the water supply. Based on it, the facilities of the treatment process have to meet at least the minimum design and construction standards. In addition, the treated water has to meet the water quality standards defined by the regulations. Thus, a sound and reasonable asset management plan is required. Further, the operators of the water treatment plants must be certified and trained properly. Plant security issues should also be considered with development of emergency management and response plans and procedures.

The third barrier of the approach is monitoring and compliance. Systems and policies under this barrier aim to detect and fix problems by collecting data and information about the presence of contaminants within the water supply system and by assessing the effectiveness of the treatment process. Monitoring programs are components of this barrier and help to maintain performance of water supply systems, physical integrity of its components, and assess if adjustments need to be made.

Individual action is the last barrier of the approach and is focused mainly on the consumers. Specifically, consumer awareness and participation are the goals of this barrier. These goals can be achieved by periodic quality and performance reports that illustrate the condition of the entire water supply system starting from the source water to the quality of the water reaching the tap. Early notifications of potential public health risks by the local authorities as well as reports by the general public on identified problems with potential problems of drinking water could be considered as activities under this barrier.

After its introduction in the U.S., the multiple barrier approach attracted the attention of the water supply community on a global scale. In Australia for example, the importance of relying on more than one treatment barrier to contamination was emphasised in the final report of the 1998 Sydney Water Inquiry by Pet McClellan QC in which it concluded: "There is general agreement that the most effective approach to keeping *Cryptosporidium* and *Giardia* from a water supply is to adopt a multiple barrier approach" (Hellier, 2000).

Safe Drinking Water Act - Protecting America's Public Health



Figure 3: The Multiple Barrier Approach
 (After U.S. EPA http://www.epa.gov/safewater/publicoutreach/landscape_1200x776.jpg)

In Canada, the O'Connor Inquiry (O'Connor, 2002) who investigated the events that led to the Walkerton tragedy made more than 90 recommendations on a multiple barrier approach to managing drinking water. The Inquiry concluded that a multiple barrier approach is necessary for providing safe drinking water, consisting of effective and robust measures dealing with the following main elements:

- source: the best possible raw water quality should be maintained and protected;
- treatment: effective treatment should be designed, operated, and maintained;
- distribution: secure storage and distribution of treated water should be provided;
- monitoring: appropriate and effective monitoring should be performed;
- response: appropriate and effective responses to adverse monitoring or adverse circumstances are needed.

As a result, the Ontario Ministry of Environment has embarked on legislative approaches to drinking water safety, such as the 2002 Ontario Safety Water Act (OME, 2002).

3.3. Water Safety Plans and HACCP

In 2004, the WHO outlined a preventive management framework for safe drinking water. The framework is composed of 5 components (WHO, 2004):

1. health-based targets based on an evaluation of health concerns;
2. system assessment to determine whether the drinking-water supply (from source through treatment to the point of consumption) as a whole can deliver water that meets the health-based targets;
3. operational monitoring of the control measures in the drinking-water supply that are of particular importance in securing drinking-water safety;
4. management plans documenting the system assessment and monitoring plans and describing actions to be taken in normal operation and incident conditions, including upgrade and improvement, documentation and communication; and
5. a system of independent surveillance that verifies that the above are operating properly.

Three out of five components, namely the system assessment, monitoring and the management and communication, when combined together form the Water Safety Plans (WSP). WSP are management plans developed by the water supplies. These plans address important aspects of the normal and safe operation of water supplies with emphasis on assessing and controlling the hazards at different phases of the treatment process. Recently, the WHO has issued a practical guidance to facilitate WSP development and implementation and has introduced the following development approach (WHO, 2009):

1. set up a team and decide a methodology by which a WSP will be developed;
2. identify all the hazards and hazardous events that can affect the safety of water supply from catchment through treatment and distribution to consumer's point of use;
3. assess the risk presented by each hazard and hazardous event;
4. consider if controls or barriers are in place for each significant risk and if these are effective;
5. validate the effectiveness of controls and barriers;
6. implement an improved plan when necessary;
7. demonstrate that the system is consistently safe;

8. regularly review the hazards risks and controls;
9. keep accurate records for transparency and justification of outcomes.

Points 2,3,4,5 of the approach constitute the system assessment of the water supply identifying the potential hazards events and assessing their risks in each phase of the water supply chain, as well as the appropriate measures to control these risks (i.e. here, the concepts of hazard and risk are defined as in Section 2.1. Definitions in the Water Utility Sector). The proposed approach for implementing a WSP indicates a shift within the water supply sector towards a more proactive and precautionary approach and against monitoring only the finished water quality.

The elements of a WSP build on the multiple-barrier principle, the principles of hazard analysis and critical control points (HACCP) and other systematic management approaches (WHO, 2008). The HACCP concept and acronym was first conceived in the US in the 1959 by the Pillsbury Company to improve food safety for manned space missions by the National Aeronautics and Space Administration (Martel, et al., 2007). Over the years HACCP improved and evolved and was adopted internationally by the food industry as a food quality and risk management system to prevent or reduce the health risks from hazards associated with food processing. By the early 90s HACCP was applied in the drinking water sector to support a more proactive risk management strategy.

Based on the Codex Alimentarius Commission there are seven key principles for implementing a HACCP (CAC, 2003):

1. conduct a hazard analysis;
2. determine the critical control points (CCP);
3. establish critical limits;
4. establish a system to monitor control of the CCP;
5. establish the corrective action to be taken when monitoring indicates that a particular CCP is not under control;
6. establish procedures for verification to confirm that the HACCP system is working effectively;
7. establish documentation concerning all procedures and records appropriate to these principles and their application.

The hazard analysis principle includes the process of identification and assessment or evaluation of hazards and hazardous events. The concepts of hazard and hazardous event were described in Section 2.1. Definitions in the Water Utility Sector. Criteria used for assessing the hazards are the frequency of its occurrence and the severity of its consequence. For all identified hazards a risk score or ranking is assigned to each possible combination of frequency and severity. Based on the risk score a decision can be made about the hazards that should be included in a HACCP plan.

A critical control point is a step or an operating procedure of the water purification process necessary in maintaining safe drinking water levels in which a control can be applied. Ideally, all hazards with a significant risk score can be addressed, monitored or controlled effectively with a critical control point. The critical limits are measurable parameters indicating whether the water at a specific critical control point is safe or not. For example, a critical limit could be a value, maximum or minimum, to which a biological, chemical or physical parameter of the water must be controlled. In fact, the identification of critical limits are the skeleton of a monitoring system for assessing whether system performance is within specifications, identifying when critical limits are reached, and providing records of historical data that can be used for future analysis and evaluation.

Given that a monitoring system is established, it is necessary under the HACCP principles to define corrective actions for the case when the critical limits have been exceeded. This is the goal of corrective actions. The next HACCP principle states that a verification procedure is needed based on which objective evidence should be collected indicating potential problems or deficiencies with the HACCP system. The last HACCP principle, the documentation, indicates the importance of recordkeeping as a means of insuring compliance and traceability that facilitate the continuous improvement of the water supply.

4. System Safety Engineering Approaches

Based on systems safety engineering point of view safety is seen as an emergent property of a system. The term “*system*” denotes a collection of parts (equipment, infrastructure, people, regulations, agencies, subsystems, recourses etc.) designed to achieve specific goals. The concept of emergence then denotes that a value of a specific property of the system (i.e. in this case of safety) cannot be measured or estimated just by summing the value of the property for all systems components and subsystems. Indeed, Pariès (2006) states that “*emergence*” is what happens when we try to understand the properties of a system that exceeds the level of size and complexity that our intellect can grasp at once, so we decompose the system into interacting component parts.

Safety in a system is realised through the elimination of accidents and the prevention of their unwanted events. Unquestionably, there is a strong relation between safety and accidents. In order to maintain safety it is important to know *how* accidents occur and from *which threats* a system must be protected from. Accident investigations are used to provide answers to these questions. Over the years, the study of accidents has brought to light different schools of thought about the conceptual elements, which can explain the phenomenon of accidents. These schools of thought are known as *accident models*. Some accident models will be described below to better explain how the ideas on the aetiology of accidents have evolved in systems safety engineering domain.

4.1 Domino Model

One of the first recognised approaches to explain accidents introduced by Heinrich (1931) and originates from the domain of industrial safety. His approach is known as the Domino Theory or Domino Model. The model implies that accidents result due to the occurrence of factors that are propagating in a fixed and sequential logical order, similar to a chain of dominos. The five factors of Domino Theory are:

- social environment and ancestry;
- fault of person;
- unsafe act or mechanical or physical hazard (unsafe condition);
- accident;
- injury.

Based on the Domino Theory, any injury is the result of an accident. The cause of any accident is driven by unsafe acts of workers, or, by unwanted mechanical or physical hazards. The unsafe acts and hazardous conditions are caused only by acts of workers that are not correct. The unsafe acts are caused only by workers with undesirable features in their personality created by the environment or were passed to them through heredity.

The focus of this model on unsafe acts and personal fault has greatly influenced safety professionals and marked the beginning of significant research within safety science in directions such as human factors and human error. In addition, it has reinforced the belief that accidents have only one root cause emphasising human error and unsafe acts and defining them as categories of accident causes.

4.2. Normal Accident Theory

The Normal Accident Theory was introduced by Perrow (1984). The theory says in brief that in high risk organisations like nuclear power plants, chemical plants, aircrafts, dams, nuclear weapons, independent failures sooner or later will escalate to system accidents due to unexpected interactions and tight-coupling. Because the failures are interacting in an unexpected way, (e.g. nobody ever thought for example that when component X failed the alarm system Y would be off due to maintenance etc.) their escalation will not be expected by members of the organisation and any emergency response or recovery process might be impossible or less effective. In short, if a system is both complex and tightly-coupled, accidents are inevitable and one can call such accidents “normal”.

Based on Normal Accident Theory, interactive complexity and tight coupling are characteristics of the system and are not attributes of the workers or of the components of the system. Tight coupling means that some or all system processes are happening fast and there are few alternative ways to be performed, or to be turned off. Interactive complexity is a term introduced by Perrow to denote the unexpected interactions of independent failures. Interactive complexity is more likely to be present in systems where components have multiple functions and many control parameters.

4.3. The “Swiss Cheese” Model

On 1997, Prof. Reason in his attempt to define some underlying principles of accident causation in organisational accidents has introduced the “Swiss Cheese” Model. The main assumption of this model is that all organisational accidents entail the breaching of barriers and safeguards that separate damaging and injurious hazards from vulnerable people or assets (Reason, 1997). He also proposed three sets of factors, human, technical and organisational that, most likely, are implicated when barriers and safeguards of an organisation are breached. These factors are governed by production and protection; two processes which according to Reason are common to all organisations.

The defences are designed to serve one or more functions such as containing and eliminating the hazards, interposing safety barriers between the hazards and the potential losses, providing alarms and warnings when danger is imminent. The defences can also be “hard” or “soft”: physical barriers, alarm and warnings mechanisms, personal protective equipment are considered “hard” defences, whereas regulatory surveillance, administrative control and legislation are considered “soft” defences.

Reason hypothesizes that accidents and disturbances occur due to breach or bypass of a set of defences that separate hazards from vulnerable environments, people or assets. Based on the “Swiss Cheese” model depicted in Figure 4 the defences form successive layers of protection, each guarding against the possible breakdown of the one in front. However, due to errors and violations committed by front line personnel and latent conditions such as poor design, lack of training or insufficient procedures, “holes” are formed in the defences that are in constant flux. The necessary

condition for organisational accident is the conjunction of a set of holes in successive defences allowing hazards to come into damaging contact with people or assets.

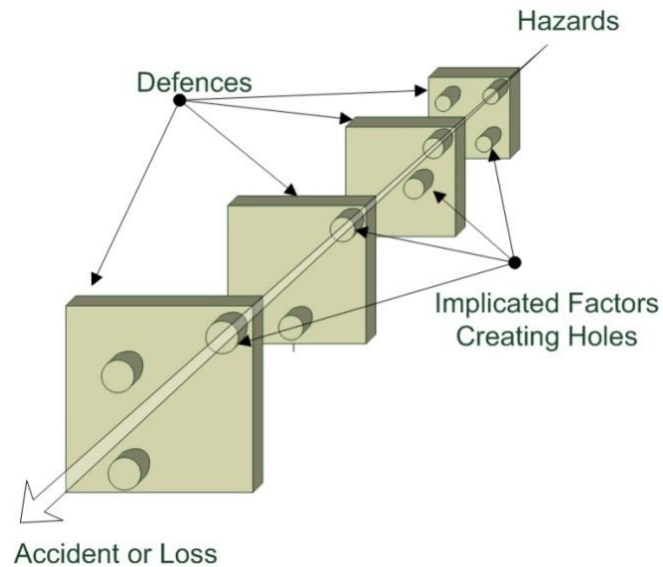


Figure 4 The “Swiss Cheese” Model

4.4. The Rasmussen Framework

A proactive risk management approach was proposed by Rasmussen (1997) and Rasmussen & Svedung (2000), emphasising the identification of boundaries of safety performance and how these can be made visible to the decision makers at all levels of the organisation. The main thesis of this framework is that risk management is a control problem where many levels of politicians, managers, safety officers, and work planners are involved in safety by means of laws, rules, and instructions for control of a hazardous physical process (Rasmussen, et al., 2000).

Based on this framework an organisation is a hierarchical socio-technical system like the one shown in Figure 5. Each level of the organisation, due to exoteric and esoteric pressures and continuous technological advancements, behaves differently and influences the performance and behaviour of the entire system. This generates the need to control safety at each level of the organisation through control constraints that are enforced from levels located above and below. It also means that decisions taken at higher levels in the organisation should be visible and propagate down the hierarchy, whereas reports and information about the current state of each level and their dependences on other levels should propagate up the hierarchy.

The proposed framework is composed of the following components:

- a study of the normal activities of the actors at all hierarchical levels of the organisations,
- a study of the present statue, information environment and information flow of the actors within the organisation,
- a review of the potential for improvement through changing the present environment,
- a set of guidelines for improving these aspects in practical work environments.

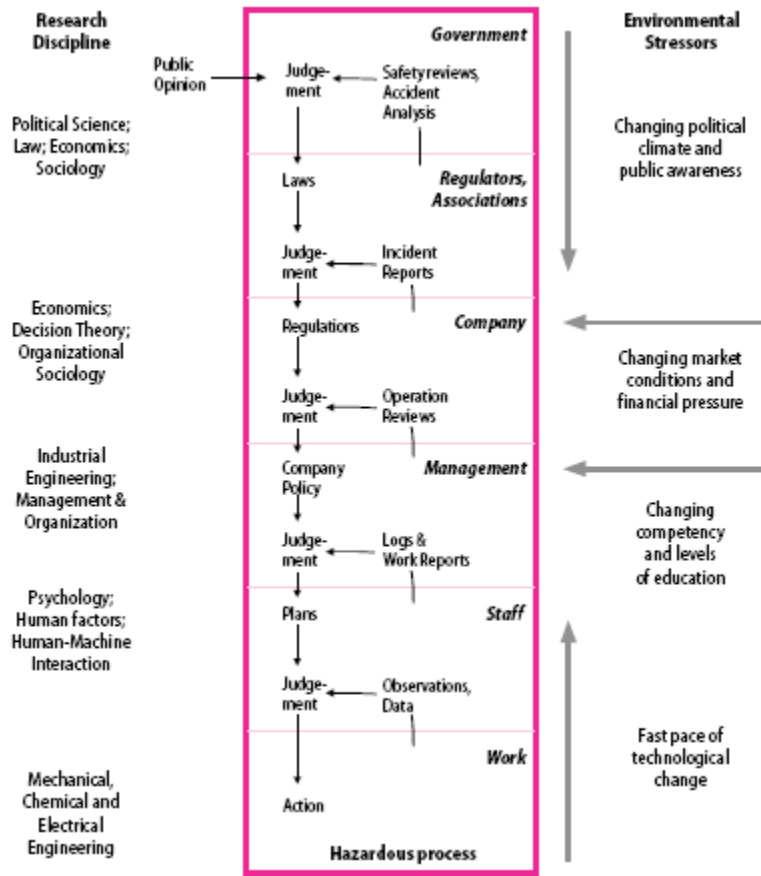


Figure 5: Hierarchical Levels of Socio-Technical Systems: An Example, After (Rasmussen, et al., 2000)

4.5. STAMP

In early 2000, Prof. Leveson introduced the Systems-Theoretic Accident Modeling and Process (STAMP), an accident model based on systems theory (Leveson, 2002). Based on STAMP, safety is an emergent property of a system due to the interaction of system components. Accidents occur when constraints and controls imposed on system design and components are not capable of effectively handling the dysfunctional interactions of system components. In short, accidents result from interactions among components that violate the safety constraints—in other words, from a lack of appropriate control actions to enforce the constraints on the interactions (Leveson, 2004). In this accident model, events are not considered a basic concept for explaining accidents. On the contrary, the concept of “*safety constraint*” is considered one of the most important.

Other important concepts in STAMP are the “*controllers*” and the “*process models*”. A controller is responsible for enforcing the safety constraints in the system. For example, a controller can be a sensor, an electronic device, a human etc. or a combination of these. A process model contains information on the current state of the system, relations of different variables of the system, rules on how the state of the system can change. Thus, based on the STAMP model the factors leading to accidents could be categorised as:

- inadequate enforcement of safety constraints;
- inadequate execution of control action;
- missing or inadequate feedback.

5. Methodological Gaps and Conclusions

In order to maintain safety it is required to know two things: the *threats* from which a system must be protected from and *how* accidents occur. It can be argued that in the water utility sector work on safety is mainly focused on understanding the former. Unquestionably, advancements in technology allowed for significant improvements in monitoring and understanding the hazardous physical, chemical, microbiological and radiological agents in water. An indicator of this is the periodic updates of the parameters and their values in regulations and guidelines defining the safety levels of drinking water quality. Another indicator is the number of early warning systems that monitor the presence of hazardous agents in water. For instance, a report by the U.S. EPA (2005) on the existing early warning systems has listed a significant number of technologies and techniques for integrated early warning systems for drinking water infrastructure, particularly for finished water supplies and distribution systems. These technologies would not have been implemented without knowing and understanding threats. In addition, by looking at the current trend in the water utilities literature on the adverse effects of Trihalomethans and Nitrates in the water, one will understand how effective and advanced the water utility sector is in generating new knowledge about the threats to water utility systems and to public health.

On the other hand, water utility sector is not so advanced in approaches and methods that provide systematic analysis and insights into how tragedies and accidents can occur. As it was mentioned in this report, only recently has the water utility sector begun to look at how accidents and unwanted events in water utilities may lead to tragedies. This has been driven primarily through the adaptation of a multiple barrier approach to risk management. For instance, the WHO has recently published the water safety plan manual (WHO, 2009), which provides guidance on how to perform a proactive risk management approach at the operational level of water treatment plants. Unquestionably, the multiple barrier approach and the proposed water safety plan manual by WHO are significant advancements towards achieving a more “complete” proactive safety approach.

However, this report has also shown that there is still plenty of work to be done. That conclusion is based on the hypothesis that the advancement in systems safety engineering domain can be used as a benchmark to compare state of the art approaches for safety used by researchers and practitioners in the water utilities sector. Looking at the safety approaches in these domains one can argue that the multiple barrier approach, which recently has been adopted by many countries, have many similarities to the Swiss cheese model. For example, the main thesis of the multiple barrier approach is that a coordinated set of programs, requirements, technical and managerial barriers should be established between the potential threats at the water source and the consumer. The necessary programs, requirements, technical barriers, and monitoring activities in the multiple barrier approach are identical to the concepts of “soft” and “hard” barriers defined by Reason in the Swiss cheese model.

While the similarities are quite obvious, the differences are not quite so. One difference is that in systems safety engineering there is significant effort in explaining the dynamic creation of the holes in the barriers and in understanding the role of interactive complexity between system components in accidents. In water utilities domain there seems to be a tendency to define the barriers and the mechanism, which monitor the presence of hazards between the defences. Another difference is that social and organisational factors are considered as drivers to accidents based on the systems safety engineering point of view. In the water utility sector, however these factors have not yet been

addressed through a systematic safety approach. There is neither a recommendation nor a unified methodology for how to assess the safety of water utilities as socio-technical systems that are composed of technical and social elements. In addition, there is no work on unsafe acts at the operational level in the water treatment plants or on dysfunctional interactions at the high levels of organisations, for example on dysfunctional interactions between state agencies and between state agencies and local authorities.

The recent approaches for safety in the water utilities sector unquestionably constitute a big step forward. However, there is plenty of work that needs to be done. One way to speed up the evolution of the safety methods in this domain is to look at the approaches used in the systems safety engineering domain. Some ideas could be reused and configured appropriately in order to meet the safety requirements of the water utilities sector in full. In this report, a step towards understanding the similarities and the differences between the safety approaches in these sectors has been made. More steps towards this direction are planned as results of future work in the SCEWA research project.

Bibliography

Australian Government Australian Drinking Water Guidelines (ADWG) [Online] // Australian Government, National Health and Medical Research Council. - 2004. - August 2009. - <http://www.nhmrc.gov.au/publications/synopses/eh19syn.htm>.

Awwa Water treatment: Principles and Practices of Watter Treatment Operations [Book]. - Denver : Awwa, 2003.

Bradley R. Cryptosporidium-Who is responsible? [Online]. - 2007. - June 2009. - <http://www.mlaw.ie/news/cryptosporidium-who-is-responsible>.

CAC CAC/RCP 1-1969, Rev.4- 2003 Codex Alimentarius Commission [Online]. - 2003. - September 2009. - http://www.codexalimentarius.net/web/index_en.jsp.

CCDACC Drinking Water Chlorination: A Review of Disinfection Practices and Issues [Online] // Chlorine Chemistry Division of the American Chemistry Council . - April 2003. - June 2009. - http://www.c3.org/chlorine_issues/disinfection/c3white2003.html.

Corso P S [et al.] Cost of Illness in the 1993 Waterborne Cryptosporidium Outbreak, Milwaukee, Wisconsin [Journal]. - [s.l.] : Emerging Infectious Diseases, 2003. - 4 : Vol. 9. - pp. 426-431.

EPA U.S. Safe Drinking Water Act (SDWA) [Online] // EPA. - 1996. - August 2009. - <http://www.epa.gov/OGWDW/sdwa/>.

EPA US Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State-of-the-Art Review [Book]. - Washington, DC : [s.n.], 2005. - Vols. EPA/600/R-05/156.

Heinrich H. W. Industrial accident prevention [Book]. - New York : McGraw-Hill, 1931.

Hellier Kevin Hazard Analysis and Critical Control Points for Water Supplies [Conference] // 63rd Annual Water Industry Engineers and Operators' Conference. - Warrnambool : [s.n.], 2000.

Hollnagel E, Woods D D and Leveson N Resilience engineering: Concepts and precepts. [Book]. - Aldershot, UK: : Ashgate, 2006.

Hollnager E Barriers and Accident Prevention [Book]. - [s.l.] : Aldershot, UK: Ashgate, 2004.

Hoxie N J [et al.] Cryptosporidiosis-associated mortality following a massive waterborne outbreak in Milwaukee, Wisconsin. 1997;87:2032–5. [Journal]. - [s.l.] : Am J Public Health, 1997. - Vol. 87. - pp. 2032–5.

Hrudey S E, Hrudey E J and Pollard S J.T. Risk management for assuring safe drinking water [Journal]. - [s.l.] : Environment International, 2006. - Vol. 32. - pp. 948-957 .

Leveson N Model-Based Analysis of Socio-Technical Risk [Report] / Engineering Systems Division. - Cambridge, MA. : Massachusetts Institute of Technology, 2002.

Leveson N System Safety Engineering: Back to the Future [Book]. - Cambridge, MA. : Massachusetts Institute, 2002a. - <http://sunnyday.mit.edu/book2.pdf>.

Leveson N. G. A New Accident Model for Engineering Safer System [Article] // Safety Science. - 2004. - 4 pp. 237-270 : Vol. 42.

Mac Kenzie W [et al.] A massive outbreak in Milwaukee of cryptosporidium infection transmitted through the public water supply [Journal]. - [s.l.] : The New England Journal of Medicine, 1994. - 3 : Vol. 333. - p. 161:7.

Martel K [et al.] Application of HACCP for Distribution System Protection [Book]. - [s.l.] : IWA, 2007.

Mays L. W. Water Supply Systems Security [Book]. - New York : McGraw-Hill Professional Engineering, 2004.

O'Connor D R Report of the Walkerton Inquiry: Part Two, A Strategy For Safe Drinking Water [Report]. - Ontario : Ontario Ministry of the Attorney General, 2002.

OME Clean Water Act [Online] // Ontario Ministry of the Environment. - 2002. - August 2009. - <http://www.ene.gov.on.ca/en/water/cleanwater/index.php>.

Page Darragh [et al.] The Provision and Quality of Drinking Water in Ireland A Report for the Years 2007 - 2008 [Report] / Office of Environmental Enforcement. - [s.l.] : Environmental Protection Agency, 2009.

Pariès Jean Complexity, Emergence, Resilience ... [Book Section] // Resilience engineering: concepts and precepts / book auth. Erik Hollnagel David D. Woods,Nancy Leveson. - Aldershot : Ashgate, 2006.

Perrow C. Normal accidents: Living with high risk technologies [Book]. - New York : Basic Books, Inc, 1984.

Rasmussen J. and Svedung I. Proactive risk management in a dynamic society [Book]. - Karlstad : Swedish Rescue Services Agency, 2000.

Rasmussen J. Risk Management in a Dynamic Society [Article] // Safety Science. - 1997. - 183-213. - 2 : Vol. 27.

Reason J. T. Managing the risks of organizational accidents [Book]. - Aldershot : Ashgate, 1997.

Rizak Samantha and Hrudehy Steve Strategic Water Quality Monitoring for Drinking Water Safety [Report] : Research Report No37. - [s.l.] : Cooperative Research Centre for Water Quality and Treatment, 2007.

Semenza J. C. and Nichols G. Cryptosporidiosis surveillance and water-borne outbreaks in Europe [Journal] = Euro Surveill // Eurosurveillance. - May 1 2007. - 5 : Vol. 12. - p. (5):pii=711. - Retrieved June 2009 from <http://www.eurosurveillance.org/ViewArticle.aspx?ArticleId=711>.

SI European Communities (Drinking Water) (No. 2) Regulations 2007. - 2007.

WHO Guidelines for Drinking-water Quality (Third Ed.) [Report]. - Geneva : WHO, 2004.

WHO Guidelines for drinking-water quality, third edition, incorporating first and second addenda [Online] // World Health Organization. - 2008. - September 2009. - http://www.who.int/water_sanitation_health/dwq/gdwq3rev/en/.

WHO Water Safety Plan Manual: Step-by-step risk management for drinking-water suppliers [Online] // World Health Organization. - 2009. - September 2009. - http://www.who.int/water_sanitation_health/publication_9789241562638/en/.

Woo D M and Vicente K J Sociotechnical systems, risk management, and public health: comparing the North Battleford and Walkerton outbreaks [Journal]. - [s.l.] : Reliability Engineering and System Safety, June 2003. - 3 : Vol. 80 . - pp. 253-269(17).

Yoder J [et al.] Surveillance for waterborne disease and outbreaks associated with drinking water and water not intended for drinking --United States, 2005-2006 [Journal]. - [s.l.] : MMWR Surveillance Summaries, 12 September 2008. - (SS09) : Vol. 57. - pp. 39-62.