8-18-2016 12:00 AM

Automated Control Flaw Generation Procedure: Cheakamus Dam Case Study

Bogdan Pavlovic, *The University of Western Ontario*

Supervisor: Dr. Slobodan Simonovic, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Engineering Science degree in Civil and Environmental Engineering

Summary

This thesis deals with the problem of aging hydropower infrastructure systems and system components, a problem that is very common across Canada. Flaws of common risk analysis methods are noted, and the need for new risk analysis approaches is identified. System dynamics simulation method is introduced as an implementation mechanism for the System Theoretic Process Analysis (STPA). STPA and its adaptation to complex hydropower systems are explained thoroughly. Fuzzy logic is used to model operator's decision making. The main objectives of the research include the development of an automated generic approach that implements STPA and fuzzy logic for the investigation and identification of potentially hazardous actions and hazardous system states. The developed methodology is illustrated using a case study based on the BC Hydro's Cheakamus Dam, British Columbia, Canada.

Keywords

System dynamics simulation, Risk analysis, System Theoretic Process Analysis, Fuzzy logic, Systems approach

Acknowledgements

Special thanks to Dr. Slobodan P. Simonovic for supervising this research. This thesis would not be possible without the guidance of Dr. Simonovic, and I am grateful for the opportunity to study and conduct my research with him. I would like to thank BC Hydro for providing financial support and the necessary data used in this study. Special thanks to Dr. Desmond Hartford and Mr. Derek Sakamoto from BC Hydro for their much appreciated input, suggestions, and help.

I would like to thank Mr. Patrick Breach for his patience and assistance with programming and editing part of this research. He helped me integrate Python code in the process of creating context for the STPA.

I would like to thank my project research partners, Dr. Arunkumar Radhakrishnan and Ms. Leanna King for their valuable insight into the dam infrastructure systems and their continuous support during the research.

I would like to thank my stepfather Dr. Dusan Teodorovic for introducing me to fuzzy logic and for his insightful advice throughout my time as a student at the University of Belgrade and Western University. Without his, my mother's, and my father's support and assistance this thesis and my graduate studies at Western University would not have been possible.

I am also thankful to Dr. Vladimir Nikolic and my colleagues at the Facility for the Intelligent Decision Support for their support and friendship throughout my time as a graduate student. They helped me a lot during my first months in Canada and helped me get used to the Canadian way of life.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Risk of dam systems

Aging hydropower systems across Canada pose a serious threat to the Canadian economy. Many components of these systems are near the end of serviceable life and will require significant investments in order to be replaced or upgraded (if possible). Many components are old or have been poorly maintained, and require remedial attention. Technological advances over the past few decades have resulted in increasing complexity of integrated civil infrastructure systems, making management and operations of these systems more of a challenge (Leveson 2011). Constant upgrades and replacement of the components also add to the complexity of the infrastructure. Interdependencies of the system components are poorly understood in spite of the fact that system performance and reliability are the result of interactions between engineered, natural and human system components (Regan 2010; Leveson 2011; Thomas 2012; Baecher et al. 2013).

Risk is the combination of the probability of an event and its negative consequences. Risk assessment includes a review of the technical characteristics of hazards such as their location, intensity, frequency, and probability; the analysis of exposure and vulnerability including the physical social, health, economic and environmental dimensions; and the evaluation of the effectiveness of prevailing and alternative coping capacities in respect to likely risk scenarios. This series of activities is sometimes known as a risk analysis process. (UNISDR, 2009).

1.2. Traditional dam systems risk analysis

Traditional methods of dam systems risk analysis include Fault Tree Analysis, Event Tree Analysis, Dynamic Event Tree Analysis, Failure Modes and Effects Analysis, and Failure Modes Effects and Criticality Analysis. These methods have their disadvantages. Traditional methods of engineering analysis tend to decompose the system into smaller, more manageable components, which essentially ignore the interactions between them (Regan 2010; Leveson 2011; Thomas 2012). Limited emphasis is placed on events that could occur within the design envelope (Regan 2010). The dominant risks to be managed derive not from extreme events but adverse combinations of less severe events and/or unusual combinations of usual events (Baecher et al. 2012 It is established in the literature that traditional risk analysis methods cannot identify the hazards and initiating events. Even when these are considered, they focus on major hazards and do not provide a way to include all instigating events. Resulting scenarios that are analyzed do not cover unsafe situations when there were no component failures but the lack of safety results from control actions. Similarly, the failure of components or unsafe control actions might not result in a hazard. Traditional methods assume linear progression of events, though component interactions can lead to nonlinear behaviour of a system (Leveson 2011; Regan 2010; Thomas 2012). Traditional analysis methods overlook or oversimplify the role of humans. Quantitative predictions of human behaviour in complex systems are hard to generate. Human behaviour is unpredictable and depends on the context in which the action is taken. In addition, the new technology is changing the role of humans in systems from followers of procedures to supervisors of automation and high – level decision makers (Thomas 2012).

1.3. Systems approach to dam systems risk analysis

A system is defined as "a collection of various structural and nonstructural elements that are connected and organized in such a way as to achieve some specific objective through the control and distribution of material resources, energy, and information" (Simonovic 2009). Simulation is one of the techniques used in systems analysis. Simulation inputs may be varied to determine system behaviour under various conditions (Simonovic, 2009) and link system structure to its behaviour.

Many researchers advocate the application of systems analysis to risk analysis. Regan (2010), Baecher (2013) and Komey et al., (2015) advocate for the consideration of water flow – control dams as systems and using systems approach for risk analysis of dam systems. To deal with the aspect of control flaws in risk analysis, Regan (2010) and Baecher et al. (2013) point to control systems theory. Control systems theory is an interdisciplinary approach that involves the use of feedback to determine how systems behave in response to inputs and as a result of system structure (Leveson 2011). The primary differences between traditional techniques and a systems approach are: (1) the traditional approach relies on top-down systems thinking rather than bottom-up; (2) the traditional view has a reliability engineering focus (Dulac, 2007).

In order to deal with the disadvantages of traditional methods, systems approach was taken through the use of system dynamics simulation. In system dynamics, the behaviour of the system is linked to its underlying structure (the relationships between system components) and the dynamics of how the system changes over time can be investigated by changing either the inputs or the structure (Simonovic, 2009).

System Theoretic Process Analysis (STPA), a hazard analysis method based on System-Theoretic Accident Model and Processes (STAMP) is used to investigate the impacts of control actions in the system. The term hazard can be defined as a dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage (UNISDR, 2009). Hazard analysis is the first step in the risk analysis process. STAMP treats safety as a control problem, rather than as component failure problem. STPA can be used to derive causal factors related to human controllers within the context of the system and its design.

1.4. Research objective

This research focuses exclusively on risk analysis of dam systems. There are many different dam types, and each type has different risks to consider. Concrete dams (gravity and arch dams) have risks related to overtopping, sliding, overturning and foundation erosion. Embankment dams have risks related to slope instability and internal erosion in addition to those of concrete dams. Most of these risks can be attributed to poor design or other factors. This research focuses on the risk of dam overtopping due to both control flaws and component failures under a range of conditions and external disturbances. The focus is not on the extreme conditions and events as in the traditional dam risk analysis methods.

The main objective of this research is to develop a tool that will investigate all of the possible scenarios in which the system may encounter a hazardous state. A system is said to be in a "hazardous state" when a threat exists that a hazard may occur now or in the near future. Many factors can lead to hazardous system states such as component failure, software errors, or control

actions. It is possible that component failure or unsafe control actions might not result in a hazard. Therefore, there is a need for a tool that will continuously investigate the system states. This procedure is a part of the risk analysis project "Systems Engineering Approach to the Reliability of Complex Civil Infrastructure" supported by BC Hydro and Natural Sciences and Engineering Council of Canada and lead by Dr. Simonovic. The main project tasks involve: creation of hydropower dam hazardous states (research presented in this thesis), hydropower dam system safety simulation and system resilience assessment. Hazardous system states are recorded and may be used as input for system safety simulation that will provide system operating conditions and assess them using resilience metric. Resilience is a dynamic quantitative measure of system performance that covers the time from the beginning of an undesirable event to full system recovery from it (Simonović and Peck, 2013).

A fuzzy logic controller is developed to model the dam operator's decision – making and control actions. The control strategies of the dam's operator can be put together in terms of numerous descriptive rules. When describing different decisions made at various stages of a process, human beings have a preference to use qualitative expressions instead of quantitative ones. The dam operator's behavior and decision making are modelled using the approximate reasoning algorithm developed in this thesis. It is well-known that operators of many systems have a fuzzy notion of various quantities. Human operators use their subjective knowledge or linguistic information on a daily basis when making decisions. Human beings are capable of processing such information and, based on it, make subsequent decisions. The operation of reservoirs and dam spillway gates are inherently nonlinear, and cannot be represented exactly by linear models used in conventional system identification. As such, the fuzzy logic based approach is a powerful expert system

technique to effectively control real, complex and unpredictable processes with nonlinear and time-varying properties (Ross, 2010). Fuzzy control can be considered one of the most suitable for mathematical modelling of a process that is (a) deficient or complicated, (b) nonlinear or time-dependent, or (c) difficult to control with the conventional methods. Fuzzy control grants effective solutions for nonlinear and partially unknown processes, mainly because of its ability to combine information from different sources, such as available mathematical models and experience of operators (Bagis, 2004). The environment in which operators make decisions is most often complex, making it difficult to formulate a suitable mathematical decision-making model. Thus, the development of fuzzy logic systems seems justified in such situations.

1.5. Organization of the thesis

Traditional dam risk analysis methods and the dam accident reports are covered in Chapter 2, literature review. Basics of STPA are covered in the systems approach part of the literature review, Section 2.3. Basics of fuzzy logic and fuzzy inference are covered in Section 2.4.

STPA formulation, system dynamics simulation and automated generation and failure states are covered in the methodology section of the thesis presented in Chapter 3. Data used and the results are presented in the Cheakamus Dam case study section, Chapter 4. The document ends with conclusions and future work in Chapter 5.

2. Literature Review

It is documented in the literature that there is a need for automated generation and investigation of scenarios that will describe hazardous states of a system originating from the failure of

components, control actions and the combination of the two. Hydropower systems are complex systems that are sensitive to component failures and unsafe control actions that can result in major disasters. Component failures, component interactions, human behavior, and control actions should be evenly investigated in the hazard analyses. This chapter will cover the basics and issues of traditional dam systems risk analysis methods. Two historical dam accident reports that highlight the need to examine dams as systems are presented.

2.1. Traditional dam safety risk analysis methods

Traditional dam safety risk analysis methods include Fault Tree Analysis, Event Tree Analysis, Dynamic Event Tree Analysis, Failure Modes and Effects Analysis and Failure Modes Effects and Criticality Analysis.

The Fault Tree Analysis (FTA) begins with an undesirable event but does not provide means to identify undesirable events. Figure 1 shows an example fault tree of the Minuteman missile system gas valve from the original Bell Laboratory Study (Ericson, 1999).

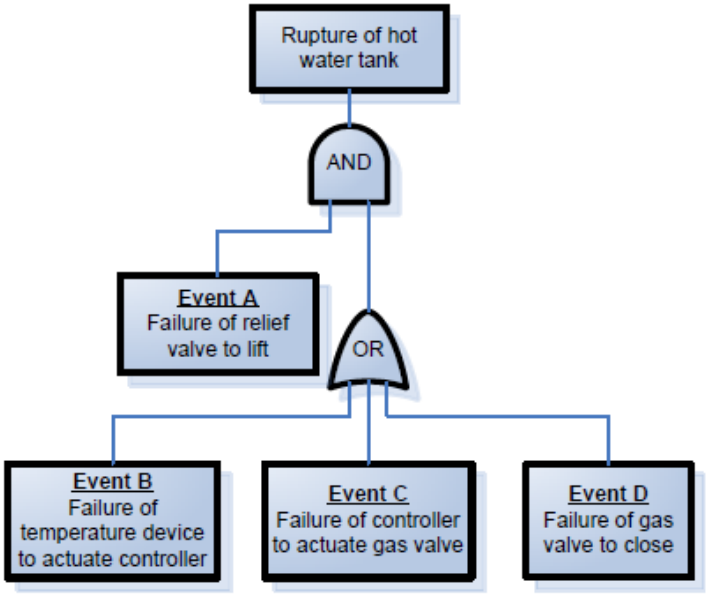

Figure 1. Fault tree example gas valve from the original Bell Laboratory study (after Thomas, 2012).

The undesirable event is shown in the top rectangle. The analysis proceeds in a top-down fashion to identify the causes of the undesirable event, as in the case where a system component does not operate in accordance with its specification. The analysis must also be based on an existing model of the system. Logic gates (OR and AND) are used to connect the events. When the fault tree is complete, it can be analyzed to determine combinations of component failures sufficient to cause a top-level undesirable event.

The FTA does not include any standard system model. Expert judgement has been used as a way to identify and quantify operator errors in a fault tree (Thomas, 2012) which is subjective. Event trees also begin with an initiating event but do not provide a way to identify systematically the initiating events or how to include all relevant events. Human behaviour is reduced to a binary

decision that is connected to a context in which it occurs. Due to the top-down nature of the analysis fault trees can become quite large for complex systems and may be difficult to interpret. There is no way to verify that all of the event causes have been identified. There is no stopping rule when performing FTA. Failure and fault tree can usually be decomposed further.

The event tree analysis (ETA) graphically presents the propagation of events leading up to a failure (Hartford and Baecher 2004). A simplified event tree for a nuclear reactor failure is shown in Figure 2.

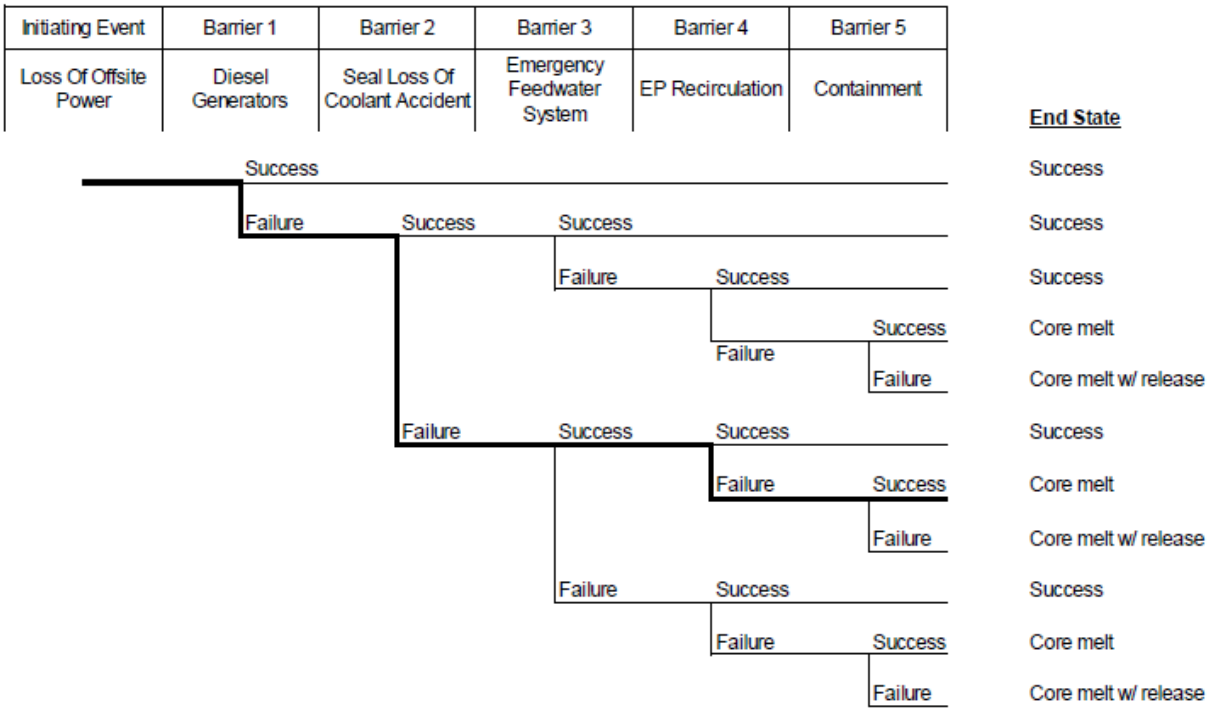

Figure 2. Simplified event tree for a nuclear reactor (after Thomas, 2012)

The first step is to identify an initiating event, shown in the first column in Figure 2. The event tree introduces a set of barriers or protective functions intended to prevent an event leading to an accident. Logical trees are created by tracking the initiating event forward in time and inserting

binary branches at each barrier to reflect the success or failure of that barrier (Thomas, 2012). Barriers in the event tree are often assumed to operate independently, while in practice that is often not the case, especially if human behaviour is involved. In the ETA, human behaviour is reduced to a binary decision. This simplification removes the context that explains why the operator would choose the given action. In the real world, human behaviour is associated with the context in which it occurs. Event trees also disregard high-level systemic causes, such as organizational, managerial, or political. ETA cannot analyze design errors and requirement flaws, which are critical factors. In the nuclear reactor example, operators were not aware of the coolant loss because indicator lamps suggested everything was in order. The instruments satisfied their requirements, but the design was flawed.

The dynamic event tree analysis method was created with the intention to examine more comprehensively the accident scenario space in traditional event tree analysis. The word "dynamic" can be used to describe periodic updates on the probabilistic risk analysis (PRA) to reflect any changes in the system configuration. Another use is when the PRA model is updated to account for equipment deterioration. (Hakobyan et al., 2008). In dynamic PRA analysis, event tree scenarios run simultaneously starting from a single initiating event. The branching occurs at user – specified times and/or when an action is required by the system and/or the operator, thus creating a sequence of events based on the time of their occurrence. For example, every time a system parameter exceeds a given threshold, branching takes place based on the possible outcomes of the system/component response. These outcomes then decide how the dynamic system variables will evolve over time for each branch. Since two different outcomes at a branching may lead to

completely different paths for system evolution, the next branching for these paths may occur not only at different times but also based on different branching criteria. (Hakobyan et al., 2008).

Failure Modes and Effects Analysis (FMEA) and Failure Modes Effects and Criticality Analysis (FMECA) were developed to evaluate the effect of component failures on system performance systematically. FMEA follows the bottom-up approach. Various components of the system are identified and then failure modes - mechanisms by which a component may fail to achieve its designed function, are investigated. FMECA follows the same process but assigns a criticality to each failure mode based on severity and probability of each identified effect. Resulting scenarios that are analyzed include both, hazardous and nonhazardous scenarios triggered by a failure. Unfortunately, a set of scenarios triggered by failure does not necessarily include all unsafe scenarios. FMECA does not capture nonlinear and feedback relationships and omits scenarios that result from a combination of several failures. FMECA also assumes a linear progression of events and does not capture nonlinear relationships. FMECA omits scenarios that result from a combination of several failures.

The “Bow-tie” model is the composition of fault and event tree. The illustration of the “bow-tie” model is shown in Figure 3.

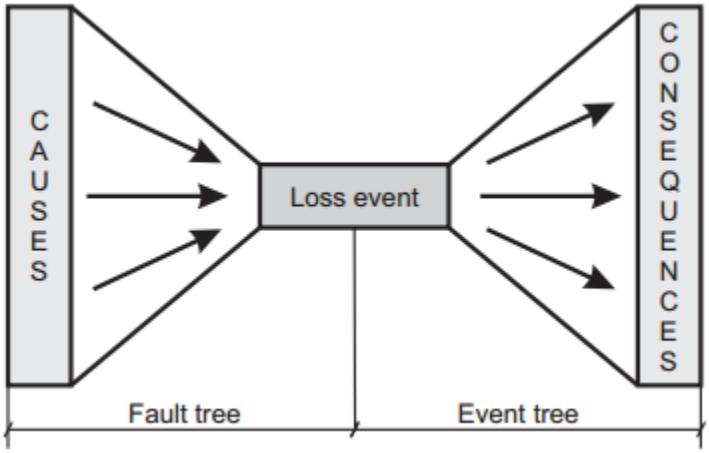

Figure 3. Illustration of the "Bow-tie" model (after Markowski et al., 2011)

The fault tree identifies causes of the top event, while the event tree presents consequences of the event. It is intended to prevent, control and mitigate undesired events through the development of a logical relationship between the causes and consequences of an undesired event (Dianous and Fiévez, 2006). The “Bow-tie” model follows the same assumptions of event and fault trees. The assumptions consider the crisp probabilities and independent relationships for the input events. The probabilities are often hard to obtain or are missing, which introduces data uncertainty (Ferdous et al., 2013). There have been some improvements to the “bow – tie” model recently with the use of fuzzy logic to negate data uncertainty and overcome missing data (Ferdous, 2013).

Event based techniques are not suited to handle complex software – intensive systems, complex human-machine interactions, and nested systems with distributed decision-making that cut across both physical and organizational boundaries (Dulac, 2007). To summarize, major disadvantages of the traditional methods are:

- Subjective judgement is required in selection of events and failure modes (Hartford and Baecher, 2004)
- Events are assumed to be independent
- Emphasis placed on component failures rather than design or control flaws which could be just as dangerous (Leveson, 2011)
- Assumption of linear progression of events, though component interactions can lead to nonlinear behaviour of the system (Leveson, 2011)
- Systems are decomposed into more manageable sub-systems (Leveson 2011; Regan 2010; Thomas 2012)
- Oversimplified human behaviour and limited ability to deal with software flaws (Thomas, 2012)

2.2. Historical dam accidents

Examination of the Taum Sauk Dam failure in the central US and the Sayano – Shushenskaya powerhouse incident in Siberia, Russia, highlights the need to examine dams as systems.

2.2.1. Taum Sauk Dam failure

The Taum Sauk pump storage plant is located in the St. Francois mountain region of the Missouri Ozarks. The Taum Sauk plant is pump – back only operation. There is no natural primary flow

available for power generation. Power is generated by water flowing from a reservoir on top of the Proffit Mountain into a lower reservoir on the East Fork of the Black River. Water is pumped back during the night when the electrical generation system is running at low – cost baseline capacity.

On December 14, 2005, the northwest side of the upper reservoir was overtopped. Overtopping led to the failure of the reservoir wall and the release of 3.8 million cubic meters of water. A combination of design and construction flaws, unsafe operation, and delayed maintenance caused the upper reservoir to overtop. State of the reservoir after the breach is shown in Figure 4.

Figure 4. Taum Sauk Dam and upper reservoir after the wall breach, Lesterville, Missouri, US. (https://commons.wikimedia.org/wiki/Category:Taum_Sauk_Reservoir_breach#/media/File:Taum_Sauk_upper_aerial-USGS-Picture037.jpg, last accessed on July 19, 2016)

Several investigation reports focus on the technical reasons for the breach (Regan, 2010). These reports present a clear picture of the mechanics of the failure of the Taum Sauk Dam. However, the reports do not provide a complete picture of the interactions, control actions and decisions, and design flaws that contributed to the failure.

Overtopping of the Taum Sauk occurred because of complex interactions of numerous decisions made over a period of time from the planning stage of the project (e.g. no spillway on the dam) and including actions during design, construction, operation and decisions made by the owner and society at large (Regan, 2010). The dam was constructed with uncompact rockfill which led to an excessive settlement. Operations staff lowered the allowable maximum water level because of the excessive settlement. Later, the retirement of the operations staff resulted in losing that knowledge, and the designers of the new water level monitoring system were unaware of the previous decision to lower the allowable water surface level. The designers instead referred to the original drawings to determine the normal maximum water level. This resulted in the normal maximum water level being set a few inches below the low point of the parapet wall. Settlement caused cracking in the impermeable water barrier for the dam. Cracking resulted in excessive leakage that was remediated by the installation of the geomembrane across the upstream face of the dam. Penetration of the geomembrane was not allowed in order to ensure its prevention of the excessive leaking. The inability to penetrate geomembrane required the water level monitoring system to be modified. The Modified system included PVC conduits for the sensors and the associated cables leading back to the top of the dam. In order to minimize costs, inlet/outlet of the water conduit was placed in the southern part of the dam, because it was the shortest path to the powerhouse. Also, the water level sensors were placed in the southern part of the reservoir to minimize cable length from the

instrument to the powerhouse. The design of the inlet/outlet resulted in swirling in the reservoir as water flowed through. The swirl caused vibrations in the instrumentation cables, which then loosened and ultimately broke apart the system that held PVC conduits. Swirling water deflected the unsupported PVC conduits. That deflection caused the water level sensors to move upward resulting in erroneous water level readings being sent to Supervisory Control and Data Acquisition system (SCADA). The operators were aware of the movement and adjusted the SCADA system. In addition, the high water level alarm and the "high – high" water level alarms, which should have automatically turn off the pumps, were also set incorrectly. The alarms were programmed not to alarm until the parapet wall was overtopping.

In December 2005, the Taum Sauk pumped storage hydropower system provided significant financial benefits to its owner (Regan, 2010). Utility profits were driven by market conditions. Planned maintenance and repair of the sensors system were delayed until a planned future outage. This is a case where reliability, safety, and profits come into conflict.

2.2.2. Sayano – Shushenskaya powerhouse accident

Sayano – Shushenskaya Dam (Russian: Саяно-Шу́шенская гидроэлектроста́нция, Sayano-Shushenskaya Gidroelektrostantsiya) is an arch – gravity dam located on the Yenisei River, near Sayanogorsk in Khakassia, Russia. Hydropower system consists of the 242 metres high, 1,066 metres long crest. The plant operated ten 640 MW turbines with total installed capacity of 6,400 MW.

On August 17, 2009, hydropower plant suffered a catastrophic failure of a turbine unit resulting in flooding of the powerhouse and loss of 75 lives. The main cause of the failure was the failure of

the bolts holding the turbine head cover to the scroll case on unit #2 (Regan, 2010). Unit #2 and state of the powerhouse after the accident are shown in Figure 5.

Figure 5. Sayano - Shushenskaya turbine unit #2 and the powerhouse after the 2009 accident (after Regan, 2010)

After the bolts failed the turbine was ejected vertically through the generator. Water flowing through the opening flooded the lower level of the powerhouse, trapping workers and causing extensive damage to the power plant. Power output fell to zero, resulting in a local blackout. It took over 3.5 hours to mobilize an auxiliary power source and close the penstock intake gates. During that time turbines continued to spin without load.

Tests of the Sayano – Shushenskaya turbine design at the time of manufacturing showed zones of water head to power combinations that should be avoided during operation due to unacceptably high vibrations (Regan, 2010). On the day of failure, the turbine was operated in a load – following manner and turbine #2 transitioned through the "not recommended", high vibration zone on at least six occasions (Regan, 2010). Investigations after the failure showed that 49 out of the 80 bolts holding the head cover showed signs of fatigue fracture. There is evidence that six bolts did not even have nuts on them at the time of the failure (Regan, 2010).

Design decisions were made to not install turbine shut – off valves or back – up power for the intake gates. This prevented shut – off of the unit #2 penstock after the head cover failed and led to flooding of the powerhouse. The project Commissioning Report recommended design and fabrication of new runners that would suffer less vibration but the privatization of the project led to an increased financial performance and design of the new runners was postponed. Unit #2 had been overhauled prior to the incident by a company closely allied with managers of the powerhouse, raising the question if the maintenance was adequate. The maintenance report does not mention inspection or replacement of any of the head cover bolts (ref.).

Before the failure, a fire occurred at another plant in the same electric system. A fire occurred at Bratskaya Powerhouse. Bratskaya was being utilized to stabilize the power production in the Unified Electric System of Siberia. The fire caused loss of communication between the control center and the Bratskaya powerhouse. The control center transferred load control responsibilities to Sayano – Shushenskaya. Operators at Sayano – Shushenskaya placed unit #2 in the load – following mode. The unit control system did not account for the high vibration operation zone. Unit #2 transitioned several times through this zone. Ultimately, enough clamping force was lost,

either through continuing fatigue fracture or loosening of the nuts and head cover failed, ejecting the turbine through the generator.

The accident analyses show that design flaws, software flaws (due to operator's adjustments), complex interactions, control actions, human behaviour and performance conditions interacted in unforeseen ways that allowed the failures to progress (Regan, 2010). The failures of Taum Sauk and Sayano – Shushenskaya were caused by a combination of mentioned factors and nonlinear interactions among system components that were partly unrecognized prior to the failures.

2.3. Systems approach to dam safety risk analysis

Systems analysis is defined as "the use of rigorous methods to help determine preferred plans, design and operations strategies for complex, often large-scale, systems" (Simonovic 2009). Techniques that can be used in systems analysis include simulation and optimization (with single and multiple objective functions). Simulation models describe how the system operates and are used to assess what changes in system behaviour will result from a specific course of action. Simulation models describe the state of the system in response to a change in system structure and various inputs but give no direct measure of what decisions should be taken to improve the performance of the system (Simonović 2009).

System-Theoretic Accident Model and Processes (STAMP) is an accident causation model (Leveson 2011; Thomas 2012) that is based on systems theory. STAMP treats safety as a control problem, rather than as a failure problem. Unsafe control includes inadequate handling of failures, software design errors, and erroneous human decision making. Accidents are viewed as the result of inadequate enforcement of constraints on system behaviour. The reason behind the inadequate

enforcement may involve classic component failures, but it can also result from unsafe interactions among components operating as designed or from erroneous control actions by software or humans (Thompson, 2012). STAMP is based on the observation that there are four types of hazardous control actions that need to be eliminated or controlled to prevent accidents:

- A control action required for safety is not provided or is not followed.
- An unsafe control action is provided that leads to a hazard.
- A potentially safe control action is provided too late, too early, or out of sequence.
- A safe control action is stopped too soon or applied for too long.

The process model contains the controller's understanding of (a) the current state of the controlled process, (b) the desired state of the controlled process, and (c) the ways the process can change the state. This model is used by the controller to determine what control actions are needed (Thompson, 2012).

System Theoretic Process Analysis (STPA) is a hazard analysis technique built on STAMP. It can be applied in order to derive causal factors related to human controllers within the context of the system and its design. The objective of STPA is to identify scenarios of inadequate control that could potentially lead to an accident.

STPA is performed using generic control system structure outlined by Leveson (2011). Schematic presentation of a generic control system is shown in Figure 6.

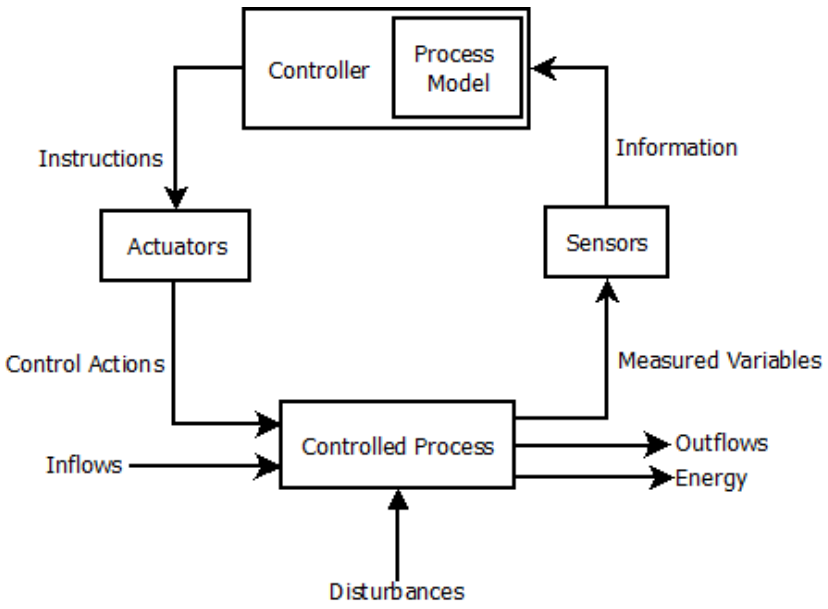

Figure 6. Schematic presentation of a generic control system (after Leveson 2011)

A stabilizing control loop includes a controller, actuators, a controlled process (the infrastructure), and sensors which relay information back to the controller. According to Leveson (2011), this high-level system structure represents a hierarchical system of systems, with each box representing its own system.

A generic control system structure is implemented to capture the hydropower dam safety context. The detailed control loop, as it relates to a hydropower dam safety is shown in Figure 7.

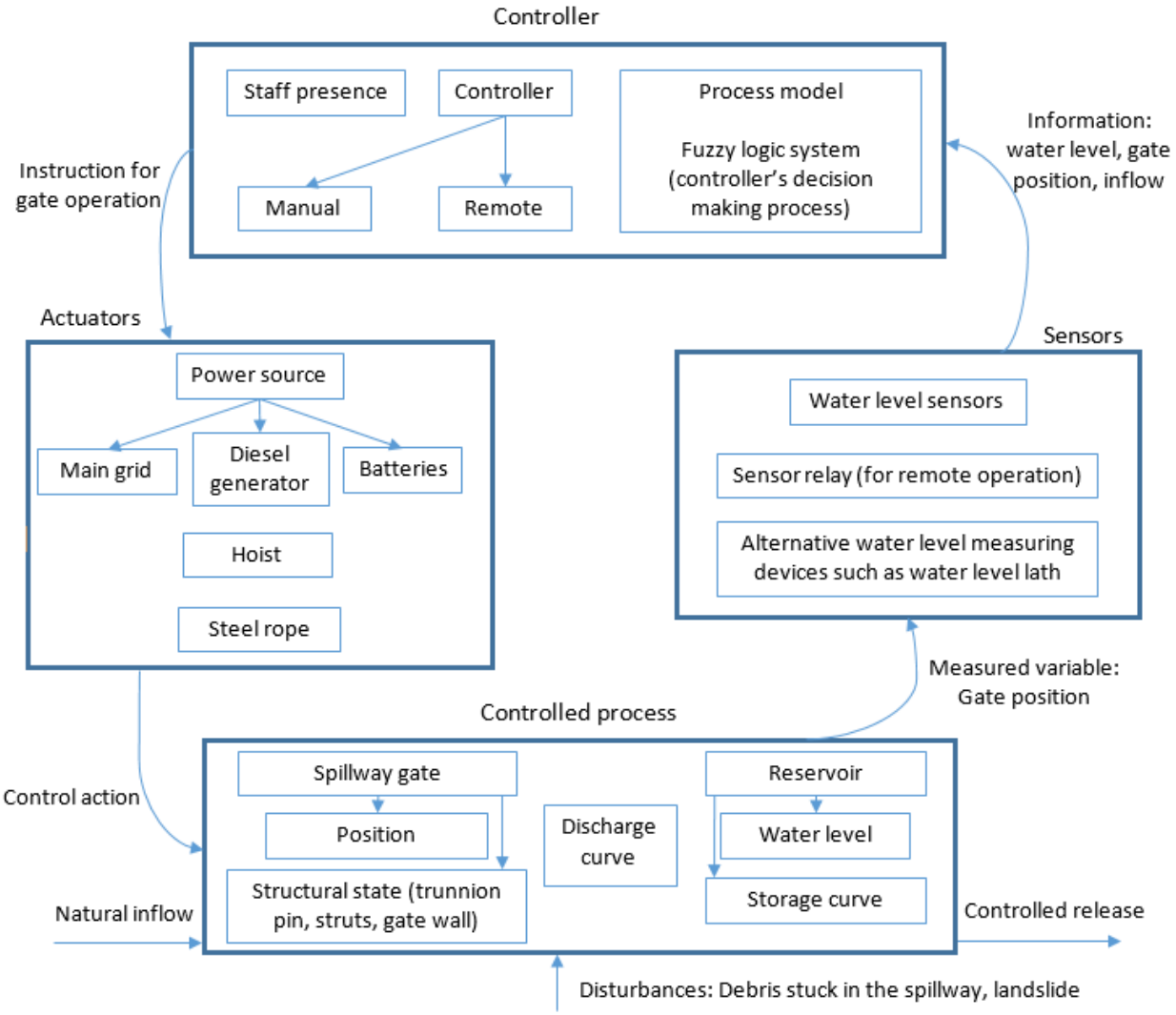

Figure 7. Detailed control feedback loop for a hydropower dam system

The controlled process is the operation of the spillway gate. States of all inflows, disturbances, and system components are automatically generated. Sensors relay system state information to the controller, part (a) of the process model. A fuzzy inference system (FIS) introduced below, is used to model the controller's decision-making at a particular state of the system. The controller issues instructions that are performed by actuators (if possible). System dynamics simulation is used to

simulate water level change in the reservoir over time. Sensors monitor the water level and relay information to the controller, closing the control feedback loop.

2.4. Fuzzy inference systems

To capture human component of the hydropower dam control feedback loop a fuzzy theoretic approach is used. The decisions made by the human operators are described using fuzzy inference system. Fuzzy inference is a part of the fuzzy logic controller. Mamdani inference system and Sugeno inference system are the two most commonly used inference systems (Teodorovic, 2012). This thesis will cover and use Mamdani inference in the fuzzy logic controller.

In certain cases, experienced operators achieve better results while operating complex systems than automated control systems. Operator's management strategies can be expressed as a set of heuristic rules that are difficult to express using traditional algorithms. These difficulties are caused by the fact that people mainly use qualitative expressions for a description of certain situations. Theory of fuzzy sets and fuzzy logic offers an approach to computing based on "degrees of truth" rather than the usual "true or false" (1 or 0) Boolean logic on which the modern computer is based. Fuzzy logic systems were created from the desire to incorporate human experience, intuition, and behaviour in the process of making decisions (Zimmermann, 1991). The idea of developing a model of decision making based on imprecise, qualitative data and descriptive linguistic rules that are combined using fuzzy logic comes from work of Lotfi Zadeh (1973).

2.4.1. Basics of fuzzy set theory

In classical set theory, membership of objects is assessed in binary terms. An object either belongs or does not belong to a set which is expressed with a 1 or a 0. Classical set membership function $\mu_{\tilde{A}}$ for an element x ∈ X can be expressed in mathematical form as:

$$\mu_{\tilde{A}}(x) = \begin{cases} 1, if\ x \in A \\ 0, if\ x\ \notin A \end{cases} \quad (2.1)$$

where $\mu_{\tilde{A}}(x)$ is the function denoting the membership of x in set A.

Fuzzy set theory permits intermediate membership classes to sets. Characteristic function takes values between 1 and 0, i.e. values in the real unit interval [0, 1]. If X is a universal set whose elements are {x}, then a fuzzy set is defined by its membership function:

$$\mu_{\tilde{A}}: X \rightarrow [0, 1], \quad (2.2)$$

which assigns a degree in the interval [0, 1] of membership to every element x.

Fuzzy set can be represented by a set of ordered pairs of elements, which present the element together with its membership value to the fuzzy set:

$$\tilde{A} = \{(x, \mu_{\tilde{A}}(x)) | x \in X\} \quad (2.3)$$

Membership functions can be generated using several methods: intuition, inference, rank ordering, neural networks, genetic algorithms and inductive reasoning (Ross, 2010).

A fuzzy set is normal fuzzy set if at least one of its elements has a membership value of 1.

2.4.2. Set-theoretic operations for fuzzy sets

Most common membership function shapes are presented in Figure 8.

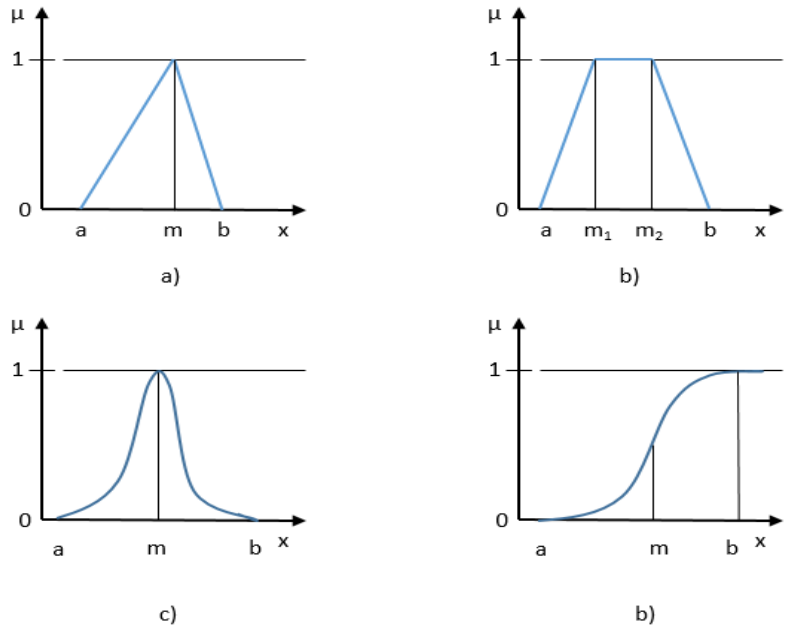

Figure 8. (a) triangular, (b) trapezoid, (c) Gaussian and (d) sigmoid membership functions

The basic operations of fuzzy sets include intersection and union. Intersection of fuzzy set Ã with B̃, C̃ = Ã ∩ B̃ is defined by:

$$\mu_{\tilde{C}}(x) = min\{\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)\}, x \in X \quad (2.4)$$

where:

$\mu_{\tilde{C}}(x)$ is the membership of the fuzzy intersection of Ã and B̃;

min ( ) is the ordinary minimum operator;

$\mu_{\tilde{A}}(x)$ is the membership of fuzzy set $\tilde{A}$; and

$\mu_{\tilde{B}}(x)$ is the membership of fuzzy set $\tilde{B}$.

Union of fuzzy set $\tilde{A}$ with $\tilde{B}$, $\tilde{C} = \tilde{A} \cup \tilde{B}$ is defined by:

$$\mu_{\tilde{C}}(x) = max\{\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)\}, x \in X \quad (2.5)$$

where:

$\mu_{\tilde{C}}(x)$ = the membership of the fuzzy union of $\tilde{A}$ and $\tilde{B}$;

max ( ) = the ordinary maximum operator;

$\mu_{\tilde{A}}(x)$ = the membership of fuzzy set $\tilde{A}$; and

$\mu_{\tilde{B}}(x)$ = the membership of fuzzy set $\tilde{B}$.

Graphical presentation of intersection and union are shown in Figure 9.

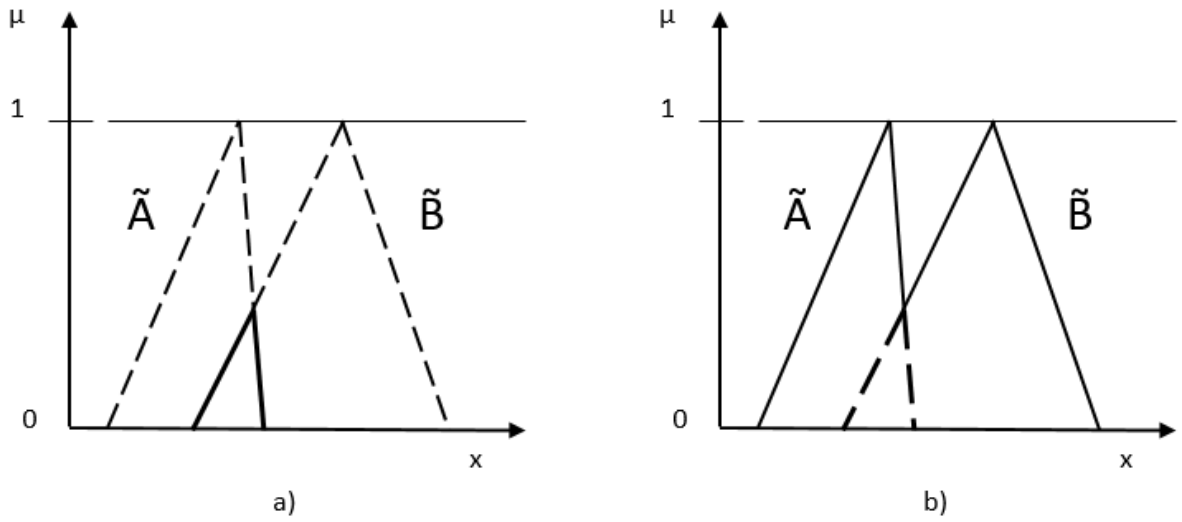

Figure 9. Union (a) and intersection (b) of fuzzy sets Ã and B̃

A fuzzy number is a special case of fuzzy set that has the following properties:

- it is defined in the set of real numbers;
- it is a normal fuzzy set; and
- it is convex.

Fuzzy number can be defined as follows:

$$\tilde{X} = \{(x, \mu_{\tilde{x}}(x)) : x \in R;\ \mu_{\tilde{x}}(x) \in [0,1]\} \tag{2.6}$$

where

$\tilde{X}$ is the fuzzy number;

$\mu_{\tilde{X}}(x)$ is the membership value of element x to the fuzzy number; and

R is the set of real numbers.

A Fuzzy set is convex if and only if it satisfies the following property:

$$\mu_{\tilde{A}}(\lambda x_1 + (1-\lambda)x_2) \geq \min(\mu_{\tilde{A}}(x_1), \mu_{\tilde{A}}(x_2)) \quad (2.7)$$

where λ is the interval [0, 1] and $x_1 < x_2$. Visually it is the same as a convex polygon.

At any α-level, the fuzzy number $\tilde{A}$ can be represented in the interval form as follows:

$$\tilde{A}(\alpha)=[a_1(\alpha), a_2(\alpha)] \quad (2.8)$$

where

$\tilde{A}(\alpha)$ is the fuzzy number at α-level;

$a_1(\alpha)$ is the lower bound of the α-level interval; and

$a_2(\alpha)$ is the upper bound of the α-level interval.

From here, the arithmetic operations of real numbers can be extended to the four main arithmetic operations with fuzzy numbers, i.e. addition, subtraction, multiplication, and division. The fuzzy operators of two fuzzy numbers $\tilde{A}$ and $\tilde{B}$ are defined at any α-level cut as follows:

$$\tilde{A}(\alpha)\ (+)\ \tilde{B}(\alpha)=[a_1(\alpha)+b_1(\alpha), a_2(\alpha)+b_2(\alpha)] \quad (2.9)$$

$$\tilde{A}(\alpha)\ (-)\ \tilde{B}(\alpha)=[a_1(\alpha)+b_2(\alpha),\ a_2(\alpha)-b_1(\alpha)] \tag{2.10}$$

$$\tilde{A}(\alpha)\ (*)\ \tilde{B}(\alpha)=[a_1(\alpha)*b_1(\alpha),\ a_2(\alpha)*b_2(\alpha)] \tag{2.11}$$

$$\tilde{A}(\alpha)\ (/)\ \tilde{B}(\alpha)=[a_1(\alpha)/b_2(\alpha),\ a_2(\alpha)/b_1(\alpha)] \tag{2.12}$$

Note that for multiplication and division:

$$(\tilde{A}\ (/)\ \tilde{B})\ (*)\ \tilde{B} \neq \tilde{A} \tag{2.13}$$

Also true for addition and subtraction:

$$(\tilde{A}\ (-)\ \tilde{B})\ (+)\ \tilde{B} \neq \tilde{A} \tag{2.14}$$

2.4.3. Mamdani inference system

Approximate or fuzzy reasoning involves combinations of imprecise logic rules into a single management strategy. Fuzzy logic allows processing of fuzzy data and making decisions based on inaccurate statements and inaccurate data (Ross, 2010). Because of these properties, fuzzy inference approach is used in this work to model the operator's decision making or control actions in a hydropower dam system.

Following up from Zadeh's approximate reasoning or fuzzy reasoning, a team from Queen Mary College, London, the UK, led by Mamdani (1974) worked on many applications of approximate reasoning for various industrial systems. Most famous is the fuzzy controller of a steam engine and boiler. The fuzzy controller was based on a set of linguistic control rules obtained from

experienced operators. Linguistic rules are representations of human knowledge in IF-THEN rule - based form. Using rule-based simulation, the inference of a conclusion (consequent) given an initially known fact (premise, hypothesis, antecedent) can be made (Ross, 2010). Typical form of IF-THEN rule (also referred to as deductive form) is:

IF *premise (antecedent)*, THEN *conclusion (consequent)* (2.15)

Mamdani inference method is a graphical technique that follows five main steps:

1. Development of fuzzy sets and linguistic rules.
2. Fuzzification of inputs.
3. Application of fuzzy operators.
4. Aggregation of all outputs.
5. Defuzzification of aggregated output.

Step 1. Development of fuzzy sets and linguistic rules

Fuzzy rules represent knowledge and experience of an experienced operator that controls certain system, process, or performs a certain task. Rules are created through interview or observation of the operator at work.

Mamdani form rules may be described by the collection of n linguistic IF-THEN expressions. Following expression shows a rule for the fuzzy inference system with two noninteractive inputs (antecedents) x_1 and x_2 and a single output (consequent) y:

$$\text{IF } x_1 \text{ is } \mathbf{A_1} \text{ AND (OR) } x_2 \text{ is } \mathbf{A_2} \text{ THEN y is } \mathbf{B} \quad \textbf{(}2.16)$$

where $\mathbf{A_1}$, $\mathbf{A_2}$, and **B** are the fuzzy sets representing the antecedent pair and consequent. These fuzzy sets may represent fuzzy linguistic concepts such as “large” or “small”, “hot” or “cold” and so forth.

Step 2. Fuzzification of inputs

Inputs to the system, x_1 and x_2 are scalar values. In order to proceed with the inference method, the corresponding degree to which the inputs belong to appropriate fuzzy sets via membership functions needs to be found. Fuzzification of the input thus requires the membership function of the fuzzy linguistic set to be created, and through function evaluation, the corresponding degree of membership for the scalar input belonging to the universe of discourse is then found. This is illustrated in Figure 10.

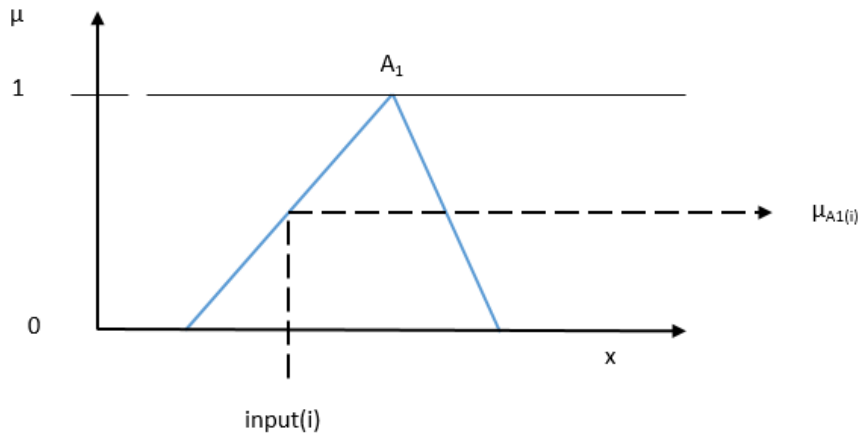

Figure 10. Fuzzification of scalar input using created membership function

Step 3. Application of fuzzy operators

Since there is usually more than one input for a rule, fuzzy operators are used to obtain one number that will represent premise for that rule. That number is applied to output function producing a single truth value for the rule. Usually used logical operators are AND and OR for conjunctive and disjunctive premises. For conjunctive premises we assume new fuzzy subset A_s as intersection:

$$A_S^k = A_1^k \cap A_2^k \qquad \text{for k=1,2, …, r} \tag{2.17}$$

expressed using membership function:

$$\mu_{A_s^k}(x) = \min\left[\mu_{A_1^k}, \mu_{A_2^k}\right] \qquad \text{for k=1,2, …, r.} \tag{2.18}$$

For disjunctive premises we assume a new fuzzy subset A_s as union:

$$A_S^k = A_1^k \cup A_2^k \qquad \text{for k=1,2, …, r} \tag{2.19}$$

expressed using membership function:

$$\mu_{A_S^k}(x) = \max\left[\mu_{A_1^k}, \mu_{A_2^k}\right] \qquad \text{for k=1,2, …, r.} \tag{2.20}$$

Given the above, rule may be rewritten as:

$$\text{IF } A_S^k \text{ THEN } B_s^k \quad \text{for k=1, 2, …, r} \tag{2.21}$$

where r is the number of rules. Graphical representation of operators' application is shown in Figure 11.

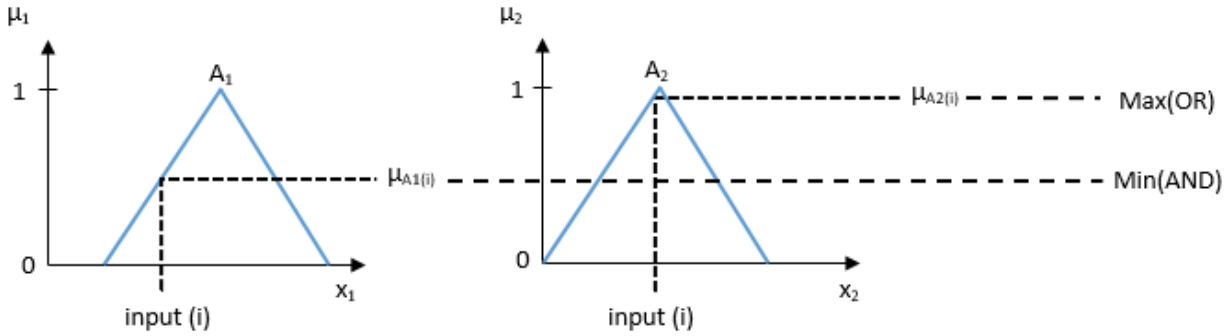

Figure 11. Graphical representation of operators' application

Step 4. Aggregation of outputs

Since it is common for fuzzy inference systems to have more than one rule aggregation of individual consequents contributed by each rule is required, so that all outputs are combined into a single fuzzy set that may be defuzzified in the final step to obtain a single scalar value.

There are two most often used ways of aggregating outputs, min-max truncation, and max-product scaling, and former will be presented. Min-max truncation is the process of propagation of

minimum or maximum membership function values from the premises (depending on the operator in each rule) through to the consequent and in doing so truncating the membership function for the consequent of each rule. Then, the truncated membership functions of each rule are combined. That is achieved through the use of disjunctive or conjunctive rules using the same fuzzy operators from the previous step. Disjunctive rules will be applied because of the nature of the inference system. Rules cannot be combined conjunctively. For example, there is a no way to have two states of hydrological data and consequences of those. We can have either one situation or another. Therefore disjunctive rules are applied in this work. Aggregation of the rule outputs is shown in Figure 12.

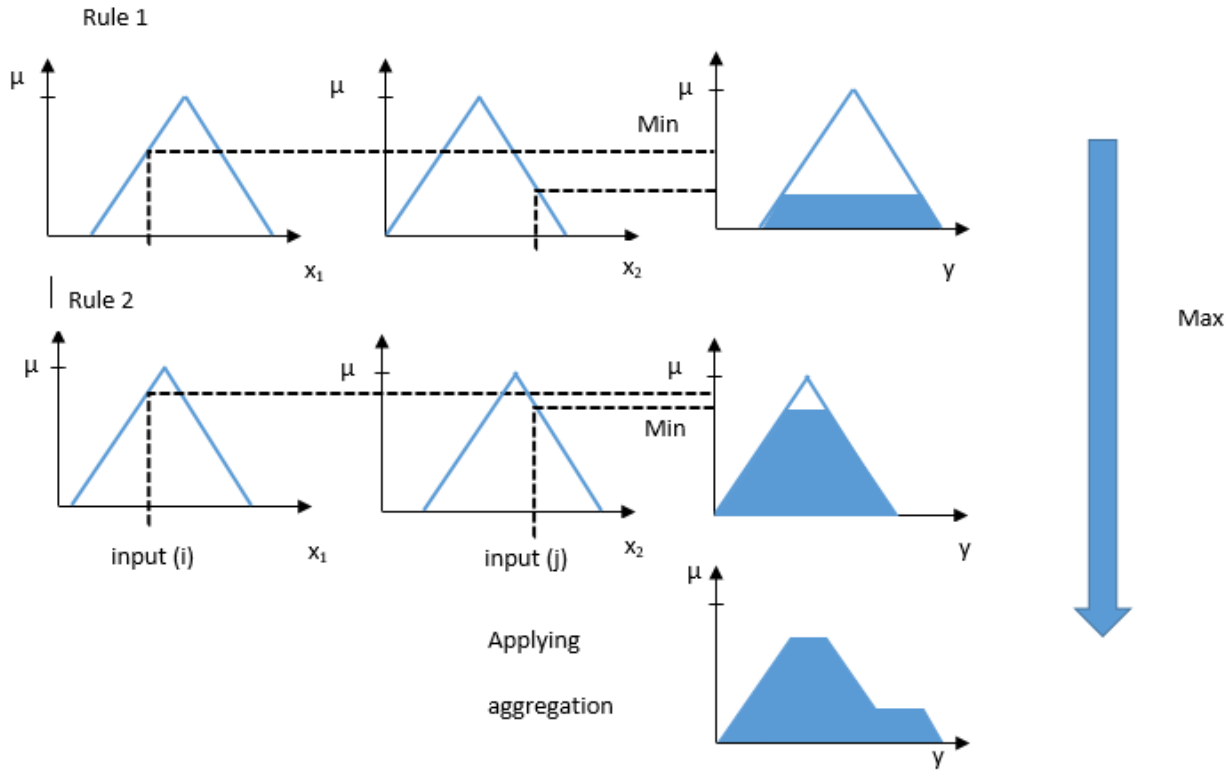

Figure 12. Aggregation of rule outputs into a single fuzzy membership function

Step 5. Defuzzification of aggregated result

The objective of the rule-based system is typically to reach a single value obtained from the defuzzification of the aggregated fuzzy set of all outputs. Defuzzification is the process, or method, of extracting a single value from the aggregated fuzzy set. There are many defuzzification methods: Max membership principle, centroid method, weighted average method and many others (Simonović, 2009, Ross 2010, Teodorović, 2012). There is not one most suitable method, depending on the shape of the premise, membership functions and problem under consideration, an appropriate method should be selected. The centroid method is used in this project. It is also referred to as the center of gravity, or center of an area. Its expression is given as:

$$y* = \frac{\int_{xmin}^{xmax} \mu(x) * x \, dx}{\int_{xmin}^{xmax} \mu(x) dx} \tag{2.22}$$

Graphical representation of the centroid method is shown in Figure 13.

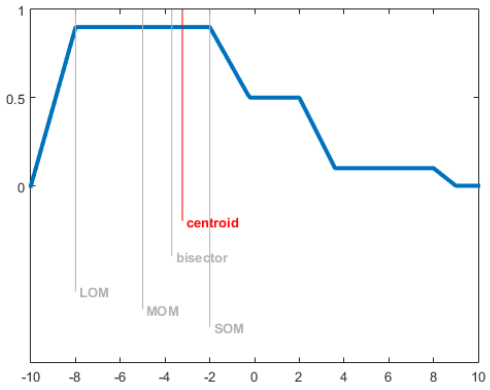

Figure 13. Defuzzification methods - centroid method result in red

An overview of defuzzification methods is available online http://www.mathworks.com/help/fuzzy/examples/defuzzification-methods.html (last viewed on 22/1/2016).

3. STPA methodology and automatic generation of control flaws

In this section of the thesis, the STPA steps are explained using a generic dam system. Additionally, formal specification for hazardous control actions (according to Thomas, 2012) and use of system dynamics simulation and fuzzy inference system to automate the generation of hazardous control actions, i.e., the scenarios for causing a hazard, are introduced.

System dynamics simulation method is introduced in this work as an implementation tool for STPA. Control actions, which are assigned by the fuzzy inference system, and investigation of the system states are achieved through system dynamics simulation. This procedure investigates all of the possible scenarios in which the system may encounter a hazardous state.

3.1. Introduction to STPA

STPA is introduced using a simplified dam system. Assume a dam system that consists of an arch dam with one spillway radial gate. Sensors read water level and relay information to operator's office that is located close to the dam. The operator manually controls the gate position. Hoist is used for lifting and lowering the gate. Hoist is powered by electric power from the existing power grid. Populated area is located downstream of the dam and reservoir is used for flood control. Reservoir water level is controlled by planned releases achieved by the operation of the spillway gate.

Before beginning STPA hazard analysis, potential hazards need to be identified. Take for example the previously described dam system Hazards in that simple system include:

- H-1: Dam overtopping and destruction
- H-2: Uncontrolled spill and downstream flooding

STPA Step One: The first step is to identify potentially unsafe control actions for the specific system being considered that can lead to one or more defined system hazards. STPA is performed on a functional control diagram. In this simple system, the control actions could be: open gate, stop opening the gate, close gate, stop closing gate. Control actions can be documented using a table like Table 1.

Table 1: Potentially hazardous control actions for a simple gate controller

Control Action	1. Not given	2. Given incorrectly	3. Wrong timing of order	4. Stopped too soon or applied for too long
Gate open command	Gate not open when the water level is high, and inflow is high (H1)	Gate open spilling more than inflow (H2)	Gate open and there is no risk of flooding (H2)	Stopped too soon can lead to (H1)
	Gate not open to release minimum flow requirements			Applied too long can drain the reservoir and cause (H2)
Gate close command	Gate is not closed after flood event is over leading to (H2)	Gate not fully closed leading to unnecessary spilling (may not be hazardous)	Gate closed during regular release. May not be hazardous or hazardous for downstream river ecosystem	Gate closed too soon when water level is high, and peak inflow still has not passed (H1)
				Gate closed too soon, but peak inflow passed (may not be hazardous)

STPA Step Two: The second step examines each control loop in the safety control structure to identify potential causal factor for each hazardous control action, i.e., a scenario causing a hazard. Figure 14 shows a generic control loop that can be used to guide this step.

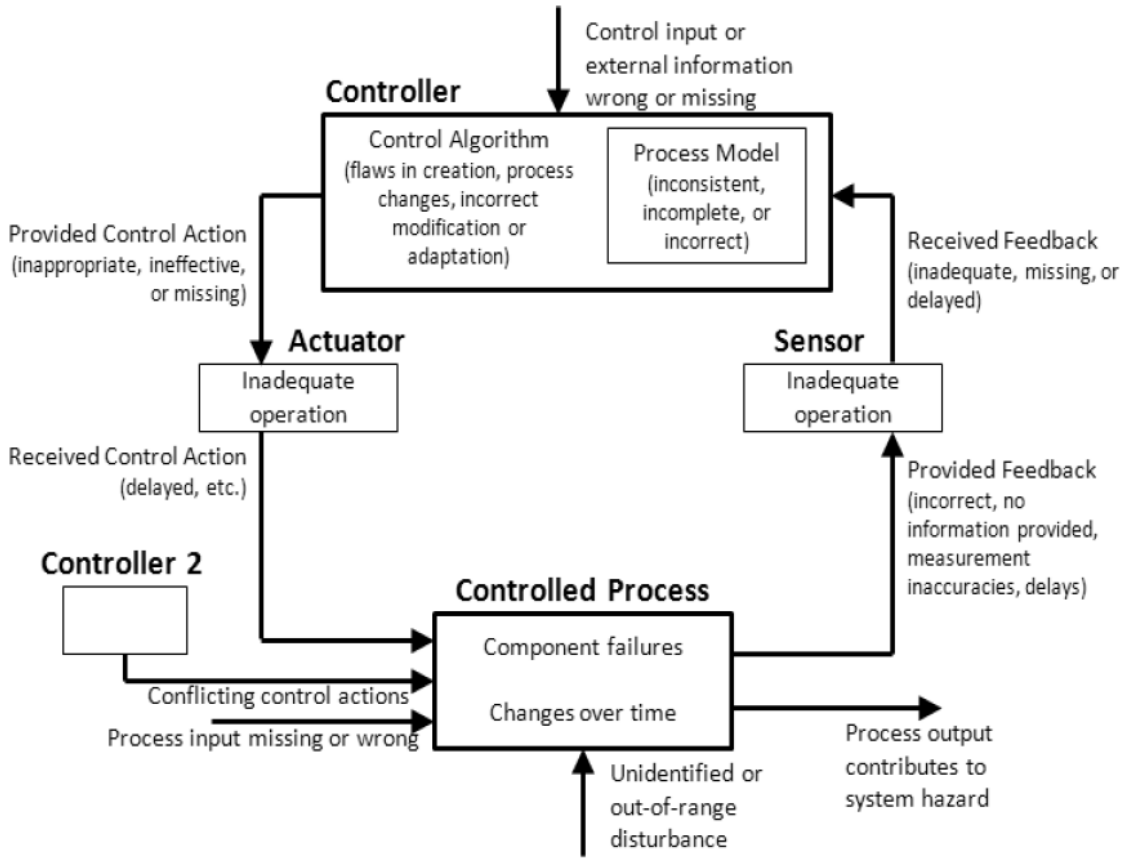

Figure 14. General control loop with causal factors (after Thomas, 2012)

Step one focuses on providing control actions while step two expands the analysis to consider causal factors along the rest of the control loop (Thomas, 2012). For example, if the gate is closed too soon, one of the causes may be the faulty feedback that controller received from the sensors. Once the second step is over, and potential causes are determined for each hazardous control, they should be eliminated or controlled in the design.

3.2. Formal specification of the hazardous control actions

Thomas provided a formal specification of hazardous control actions that is used during step one of STPA. This specification is used to develop an automated algorithm that assists in identifying the actions and generating requirements that enforce safe behaviour (Thomas, 2012). Hazardous control action in the STPA accident model can be expressed formally as a four-tuple (S, T, CA, C) where:

- S is a controller in the system that can issue control actions. The controller may be automated or human.

- T is the type of control action. There are two possible types: *Provided* describes a control action that is issued by the controller while *Not provided* describes a control action that is not issued.

- CA is the control action or command that is output by the controller, like an *Open gate*.

- C is the context in which the control action is or is not provided. Context C is further decomposed into:

    - V- a variable or attribute in the system or environment that may take on two or more values. For example, *water level* and *gate position* are two potential variables for a dam system.

    - VL- a value that can be assumed by a variable. For example, *closed* is a value that can be assumed by the variable *gate position*.

- CO - a condition expressed as a single variable/value pair. For example, the *gate is closed* a condition.

- The context C is the combination of one or more conditions and defines a unique state of the system or environment in which a control action may be given.

- To qualify as a hazardous control action, the event (S, T, CA, C) must cause a hazard H ∈ $\boldsymbol{H}$, where $\boldsymbol{H}$ is the set of system level hazards.

Each element of hazardous control action is a member of a larger set, i.e. the following properties must hold:

$$S \in \boldsymbol{\mathcal{S}} \tag{3.1}$$

where $\boldsymbol{\mathcal{S}}$ is the set of controllers in the system,

$$T \in \boldsymbol{\mathcal{T}} \tag{3.2}$$

where $\boldsymbol{\mathcal{T}}$ = {Provided, Not Provided},

$$CA \in \boldsymbol{\mathcal{CA}}(S) \tag{3.3}$$

where $\boldsymbol{\mathcal{CA}}$ (S) is the set of control actions that can be provided by controller S,

$$C \in \boldsymbol{\mathcal{C}}(S) \tag{3.4}$$

where $\boldsymbol{\mathcal{C}}$ (S) is the set of potential contexts for controller S. Context is further decomposed into:

$$V \in \boldsymbol{\mathcal{V}}(S) \tag{3.5}$$

where $\boldsymbol{\mathcal{V}}$ (S) is the set of variables referenced in the system hazards $\boldsymbol{\mathcal{H}}$,

$$\mathrm{VL} \in \boldsymbol{\mathcal{VL}}\,(\mathrm{V}) \tag{3.6}$$

where $\boldsymbol{\mathcal{VL}}$ (V) is the set of values that can be assumed by variable V,

$$\mathrm{CO} = (\mathrm{V}, \mathrm{VL}) \in \boldsymbol{\mathcal{CO}}\,(\mathrm{S}) \tag{3.7}$$

where $\boldsymbol{\mathcal{CO}}$ (S) is the set of conditions for controller S,

$$\mathrm{C} = (\mathrm{CO1}, \mathrm{CO2}, \dots) \tag{3.8}$$

where each CO_i is independent. That is, no two CO_i refer to the same variable V.

Finally, each hazardous control must be linked to a system-level hazard:

- Event (S, T, CA, C) must cause a hazard H ∈ $\boldsymbol{\mathcal{H}}$, where $\boldsymbol{\mathcal{H}}$ is the set of system hazards.

Using this formal specification is important for identifying hazardous control actions since the idea is that some actions are only hazardous in certain contexts. For example, opening the spillway gate is not hazardous by itself but in a certain context, it may be. Therefore, Thomas (2012) proposed a procedure that involves identification of potential control actions (presented by S, T, CA), potential hazardous states (presented by context C) and then analyzes which combinations yield a hazardous control actions. Using formal specification, the following example (of the previously described system) of the procedure is shown where action is expressed by following four-tuple:

- S = Human
- T = Not provided

- CA = open gate
- C:
    - V = Gate position, Water level, Inflows
    - VL = Closed, Partially open, Fully open, Normal operating range, Above spillway crest, Low, Normal, High
    - CO = Gate is Closed, Gate is Partially open, Gate is Fully open, so forth (each variable gets assigned a value, according to formal specification).

Results can be documented in tabular form. Table 2 shows context for the lack of an open gate control action.

Table 2: Contexts for the lack of an open gate control action

Control Action	Gate position	Water level	Inflows	Hazardous if not provided in this context?
Gate open command not provided	Closed	Above spillway crest	High	Yes
Gate open command not provided	Closed	Above spillway crest	Normal	Yes*
Gate open command not provided	Closed	Above spillway crest	Low	No
Gate open command not provided	Closed	Normal operating range	(does not matter)	No
Gate open command not provided	Partially open	Above spillway crest	High	Yes*
Gate open command not provided	Partially open	Above spillway crest	Normal	No
Gate open command not provided	Partially open	Above spillway crest	Low	No
Gate open command not provided	Partially open	Normal operating range	(does not matter)	No
Gate open command not provided	Fully open	(does not matter)	(does not matter)	No

Values of the variables in the previous example are intentionally provided in the verbal form to assist in the easy investigation if some actions are hazardous or not, depending on the context. Control actions that might be hazardous depending on the values behind verbal phrases are marked with an asterisk.

3.3. Implementation approach and computer programming

3.3.1. Generation of context

While the tabular presentation of actions and contexts is clear, another problem appears. Hydropower dams are complex systems, and high level of detail is needed to achieve proper analysis of the system, hazardous actions, and contexts (or scenarios). Therefore, contexts, C, will be automatically generated. To explain further, each system and its components in the control loop, hydrologic data, and disturbances are represented by several variables. Each variable, V, can have several values, VL, from two (binary 0 and 1) to multiple values. For example, hydrologic inflow has a range of values, from 0 or 1 m^3/s to the value of probable maximum flood (PMF). Sets V_1, V_2, …, V_n (where n is the number of variables) containing their values are multiplied using Cartesian product to create all the possible combinations of variables and their respective values, therefore creating all possible contexts:

$$V_1 = [\,VL_{11}, VL_{12}, \dots, VL_{1m1}] \tag{3.9}$$

$$V_2 = [VL_{21}, VL_{22}, \dots, VL_{2m2}] \tag{3.10}$$

.

.

$$V_n = [\,VL_{n1}, VL_{n2}, \dots, VL_{nml}] \tag{3.11}$$

where m_1 is the number of values variable V_1 can assume; m_2 is the number of values variable V_2 can assume, and m_l is the number of values variable V_n can assume.

Following simple combinatorics:

$$|S_1| \cdot |S_2| \cdot \ldots \cdot |S_n| = |S_1 \times S_2 \times \ldots \times S_n| \tag{3.12}$$

the context is then expressed as:

$$C = |V_1 \times V_2 \times \ldots \times V_n| \tag{3.13}$$

Automatic generation of the context has been achieved using Python programming language (Python org. 2016). Variables and their values are written in a table. Python code is then run which creates the table with complete context. The complete context table has $m_1 * m_2 * \ldots * m_l$ number of rows and n columns.

3.3.2. Development of fuzzy inference system

In order to successfully apply fuzzy logic, one must previously generate fuzzy rule base and determine shapes of membership functions. In a number of cases, membership functions are initially determined subjectively by an expert, decision maker, or analyst. The subjective way of determining membership functions is based on experience, intuition, and knowledge of the particular domain. Most frequently, the final set of fuzzy rules and the final choice of shapes of membership functions are determined by trial and error procedure (Ross, 2010). In other words, the majority of fuzzy logic systems set up the parameters of the membership functions arbitrarily.

This means, that the locations and spreads of the membership functions are chosen by the analyst without the help of the numerical training data (Teodorovic, 2012).

To provide the necessary control actions for the procedure, Mamdani fuzzy inference system (FIS) is created which describes operator decisions on how much to open (or close) the gate, depending on the inflow and reservoir water level with guidance not to spill more than inflow. Fuzzy inference systems like this are best created after series of interviews with experienced operators. For the purpose of testing the methodology, FIS is created on the basis of hydraulic capability of the spillway and guidelines for BC Hydro's operators not to spill more than inflow until peak inflow has passed. FIS consists of rules in the following format:

IF *water level* is "371" AND *inflow* is "1000", THEN *gate position* is "2" (3.14)

where "371" is the fuzzy set of reservoir elevation input, "1000" is the fuzzy set of inflow, and "2" is the fuzzy set of gate position output. Complete set of rules is shown in Appendix A. Input membership functions for both inputs (reservoir elevation and inflow), and outputs are triangular functions. Examples of the membership functions of the input and output fuzzy sets created based on spillway capability are shown in Figures 15, 16 and 17.

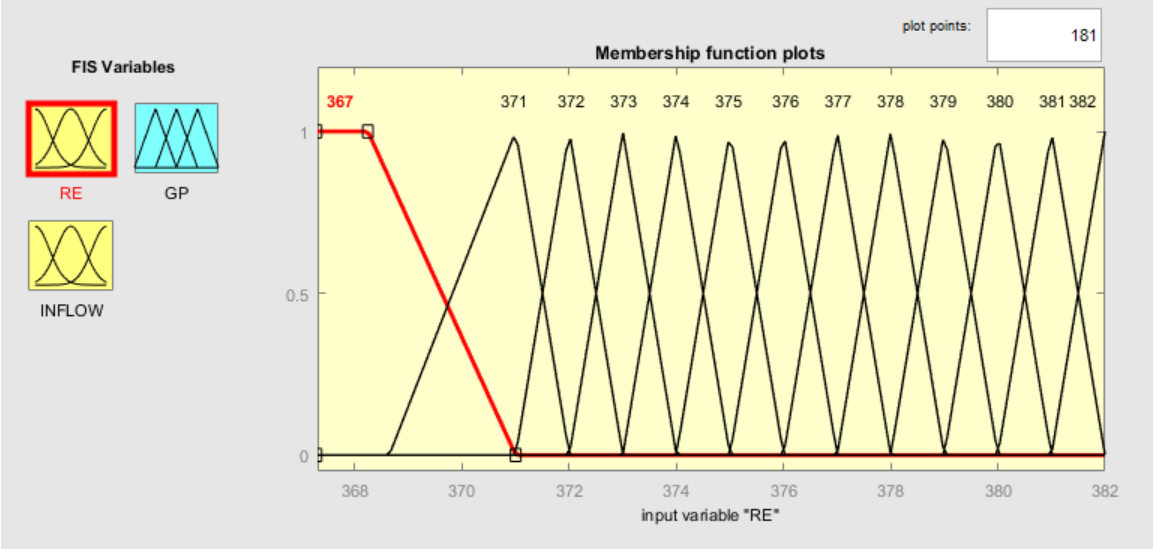

Figure 15. Membership functions of reservoir elevation fuzzy sets for the FIS.

The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the reservoir elevation in meters above sea level.

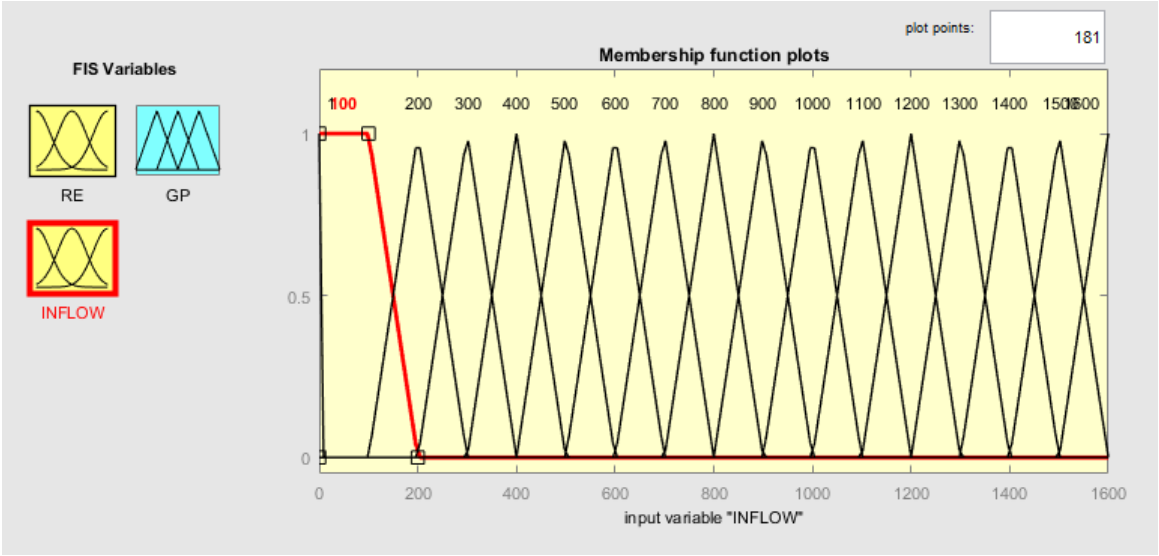

Figure 16. Membership functions of inflow fuzzy sets for the FIS.

The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the inflow in m^3/s.

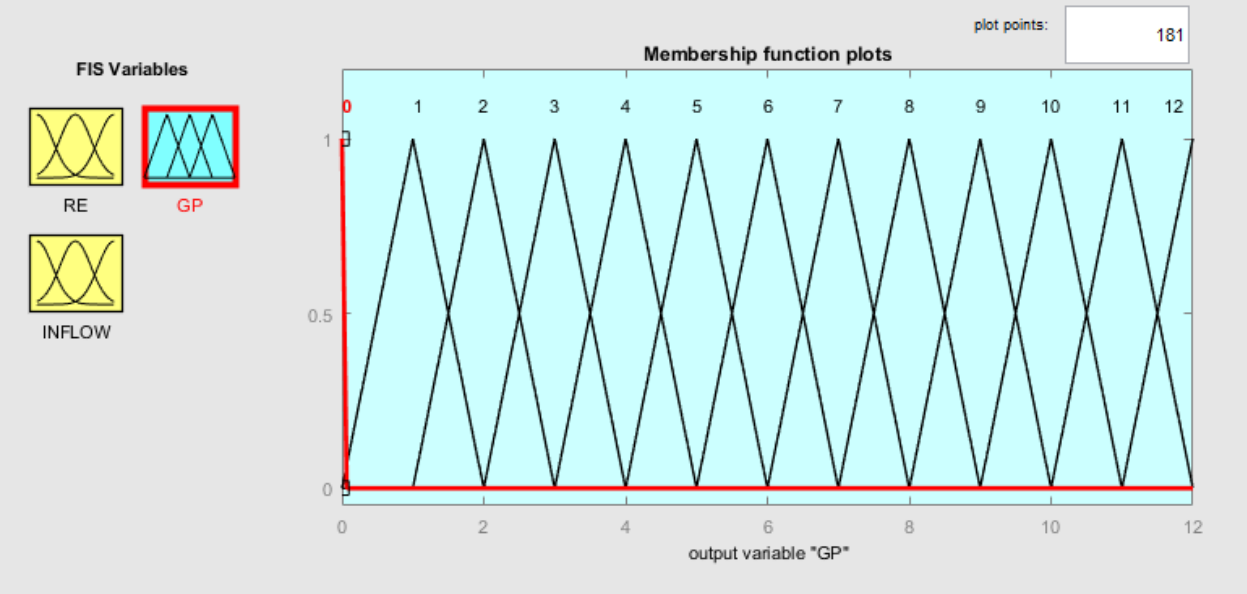

Figure 17. Membership functions of gate position fuzzy sets for the FIS

The vertical axis is the degree of membership, from 0 to 1. The horizontal axis is the gate position relative to the spillway sill, from 0 meters (closed) to 12 meters (fully opened).

Fuzzy sets usually have descriptive names, like “low”, “medium”, “high” but in this context, the number just represents closeness to that value. For example, inflow of 490 m^3/s will have very high degree of membership to “500” and very low degree of membership to “400”.

3.3.3. System dynamics simulation model

System state cannot be assessed from a single moment in time or single context and control action. System dynamics simulation model has been developed to investigate the behaviour of the hydropower dam system. The model is able to represent the system components, component interactions and control actions. The structure of the model used in the simulation is shown in Figure 18 using stock and flow diagram.

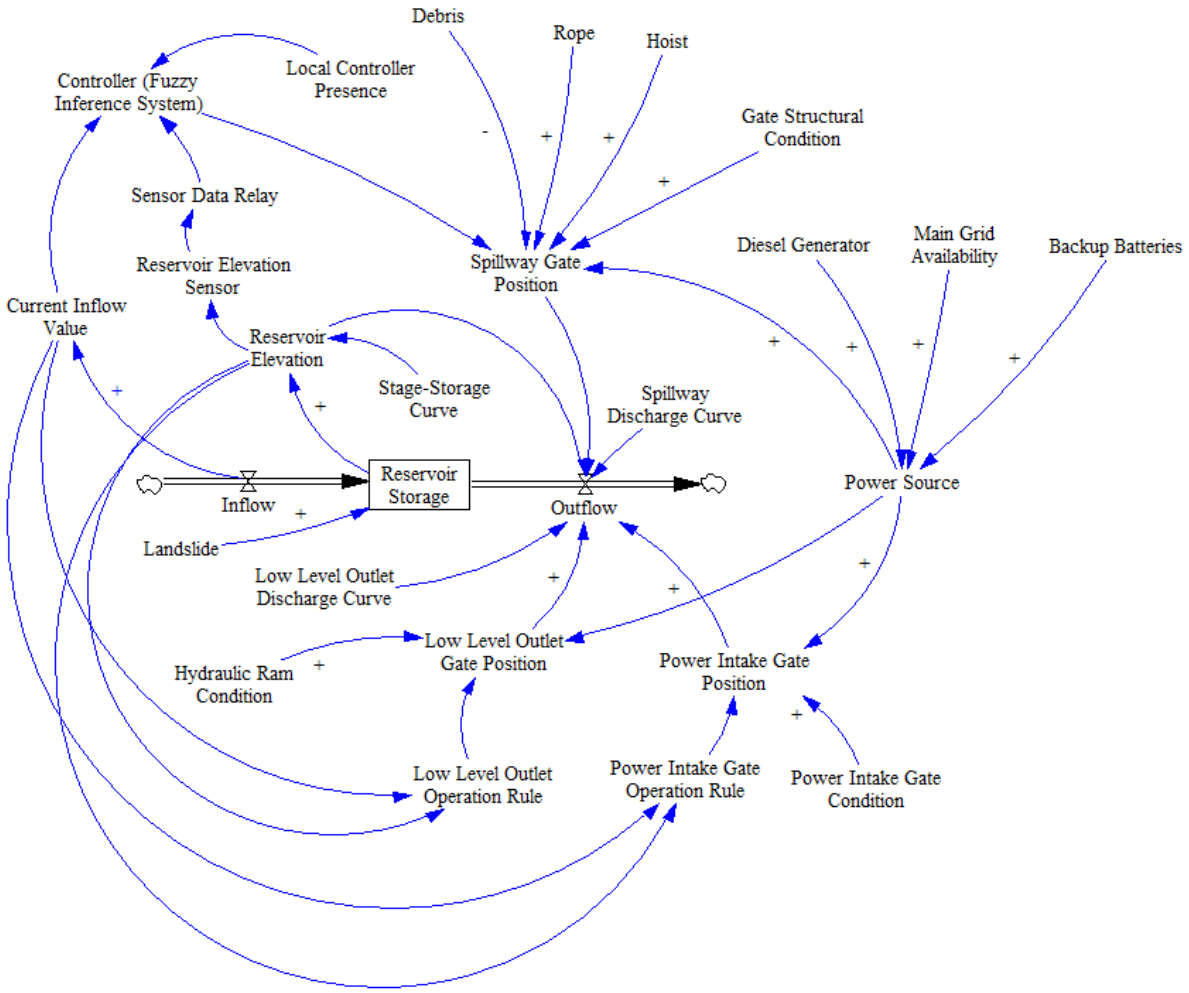

Figure 18. Stock and flow diagram of the hydropower dam system

Inflow and Outflow are the "flows", Reservoir Storage is the system stock. Other components are known as system variables.

The reservoir storage (volume of the water in the reservoir) accumulates or integrates the flows:

$$RS(t) = \int_{t_0}^{t} [Inflow(s) - Outflow(s)]ds + RS(t_0) \qquad (3.15)$$

where *RS(t)* is the reservoir storage in current time *t* in m^3, *Inflow(s)* is the value of the inflow at any time *s* between the initial time t_0 and the current time *t* in m^3/s, *Outflow(s)* is the value of the outflow at any time *s* between the initial time t_0 and current time *t* in m^3/s, and $RS(t_0)$ is the reservoir storage at initial time t_0 in m^3. The net rate of reservoir storage change can be presented by its derivative:

$$\frac{d(RS)}{dt} = Inflow(t) - Outflow(t) \tag{3.16}$$

The ordinary differential equation (1.2) is the basis of the system dynamics simulation. Euler integration is the most basic numerical integration method. Applying Euler integration and assuming constant flows during the time interval (3.16) transforms to:

$$RS_{t+dt} = RS_t + dt \times (Inflow_t - Outflow_t) \tag{3.17}$$

where *dt* is the time interval interval between simulation time steps. When *dt* becomes an infinitesimal moment of time, equation (3.17) reduces to the exact continuous-time differential equation:

$$\frac{\lim_{dt \to 0} S_{t+dt} - S_t}{dt} = \frac{dS}{dt} = Inflow_t - Outflow_t \tag{3.18}$$

Analytical and numerical solution of the differential equation vary because of the size of *dt*. Based on the usual dam operation and hourly inflow data available, time step of 1 hour is selected. Equation (3.17) becomes:

$$RS_{t+1} = RS_t + \Delta t \times (Inflow_t - Outflow_t) \tag{3.19}$$

where RS_{t+1} is the reservoir storage in the next time step, RS_t is the reservoir storage in the current time step t, Δt is the time step of 1 hour, $Inflow_t$ is the value of the inflow in the current time step, and $Outflow_t$ is the value of the outflow in the current time step t. $Outflow_t$ is a sum of following outflows:

$$SPOutflow_t = f(Gate\ position_t, Reservoir\ elevation_t) \tag{3.20}$$

$$PIOutflow_t = f(PI_t, Reservoir\ elevation_t) \tag{3.21}$$

$$LLOOutflow_t = f(Gate\ position_t, Reservoir\ elevation_t) \tag{3.22}$$

$$Overflowing_t = f(Reservoir\ elevation_t) \tag{3.23}$$

where $Gate\ position_t$ is the position of the main spillway gate in the current time step t, $Reservoir\ elevation_t$ is the elevation of the reservoir water surface elevation in the current time step t in meters above sea level, PI_t is the position of the power intake gate in the current time step t, LLO_t is the position of the low – level outlet gate in the current time step t. $SPOutflow_t$ is the spillway outflow in current time step t, $PIOutflow_t$ is power intake (intake from the reservoir, outflow through the turbines) in the current time step t, $LLOOutflow_t$ is the low – level outlet outflow in the current time step t, and $Overflowing_t$ is the overflowing of the reservoir free crest weirs, emergency ports and the dam itself. Therefore, $Outflow_t$ is:

$$Outflow_t = SPOutflow_t + PIOutflow_t + LLOOutflow_t + Overflowing_t \tag{3.24}$$

$SPOutflow_t$ is evaluated from the spillway discharge curve. An example of spillway discharge curve is shown in Figure 19.

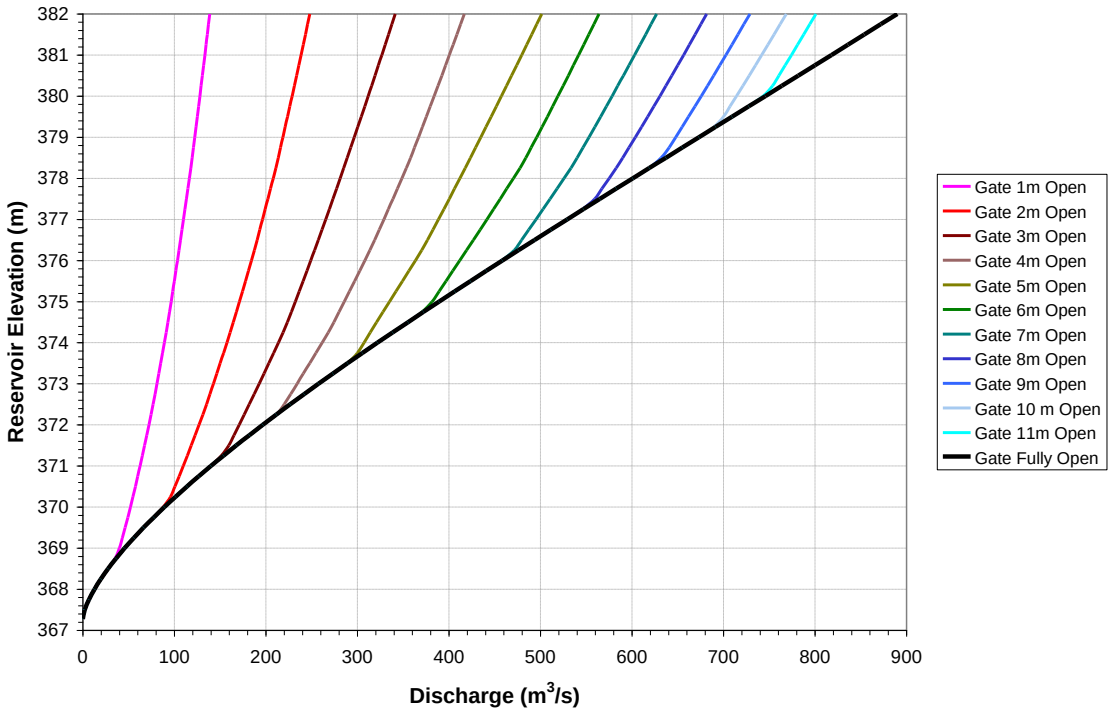

Figure 19. An example of the spillway gate discharge curve (after Kong, 2013)

The horizontal axis is the discharge under the spillway gate in m^3/s. Gate position is presented with series of curves. The vertical axis is the reservoir elevation in meters above sea level. Each of the $Outflow_t$ components is evaluated in the same way, using corresponding hydraulic curves.

Reservoir elevation is evaluated from the stage – storage curve. An example of stage – storage curve is shown in Figure 20.

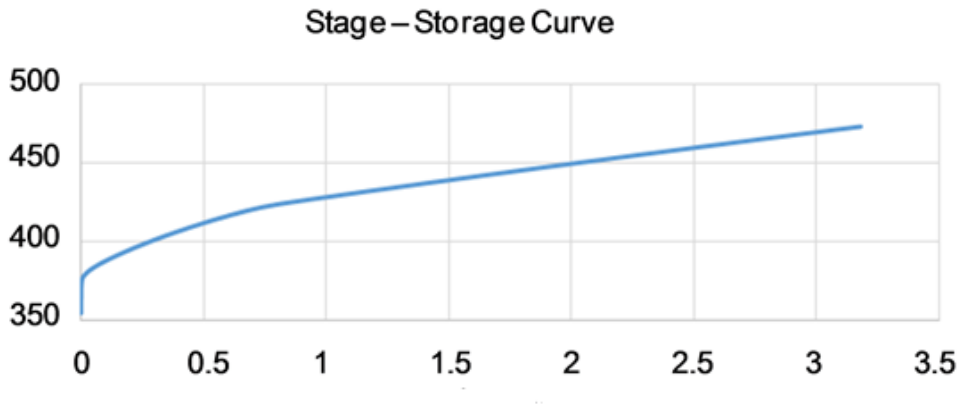

Figure 20. An example of the stage - storage curve

The horizontal axis is the volume in millions of m^3 and the vertical axis is the reservoir water surface elevation in meters above sea level.

Spillway gate position, power intake gate position, and low – level outlet gate position change in every time step based on the operational rules and system variables. Relationships between system variables, gate operational rules and gate positions can be very complex.

System variable conditions are stored in the automatically generated context. Variables used in the simulation are reservoir volume, inflow, spillway gate position, hoist condition, steel rope condition, structural gate condition, hydraulic ram condition (low – level gate actuator), power intake gate condition, main grid availability, backup power generator availability, backup batteries availability, sensors condition, sensor relay system condition, human presence, debris and landslide. Variables used in the model are shown in Figures 21 and 22.

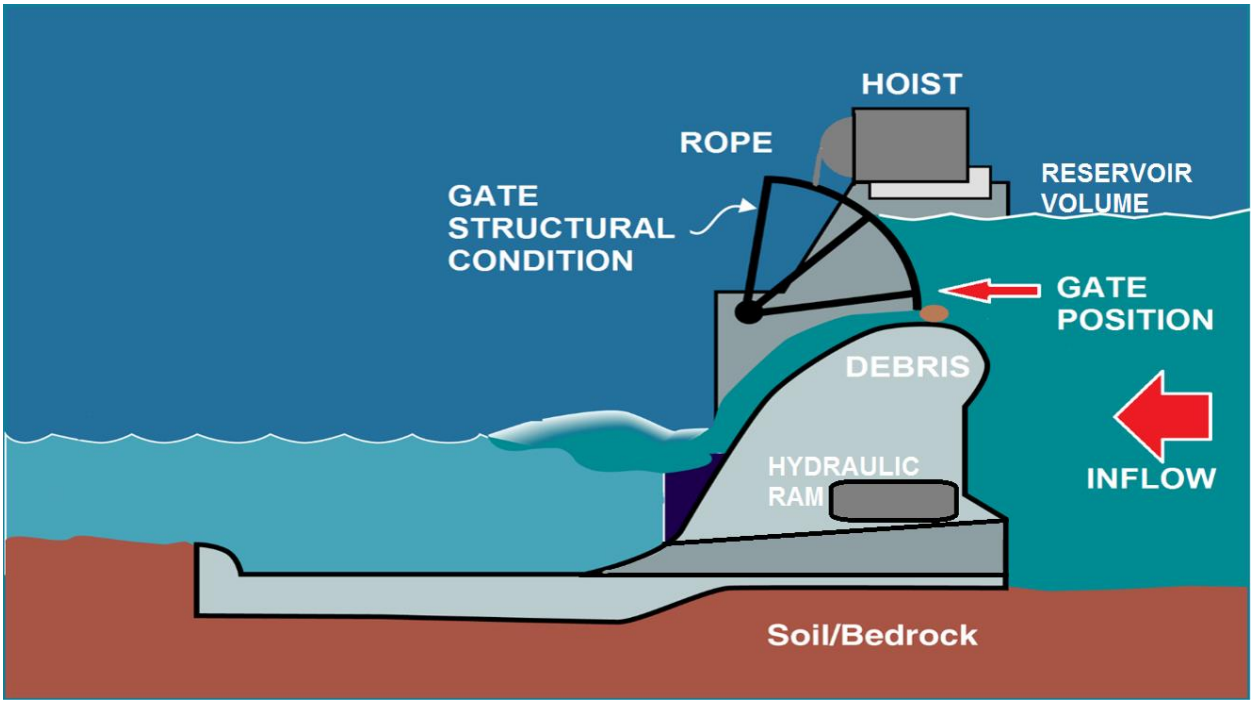

Figure 21. Cross section of a spillway section of a dam with system variables (U.S. Army Corps of Engineers, 29/11/2015.)

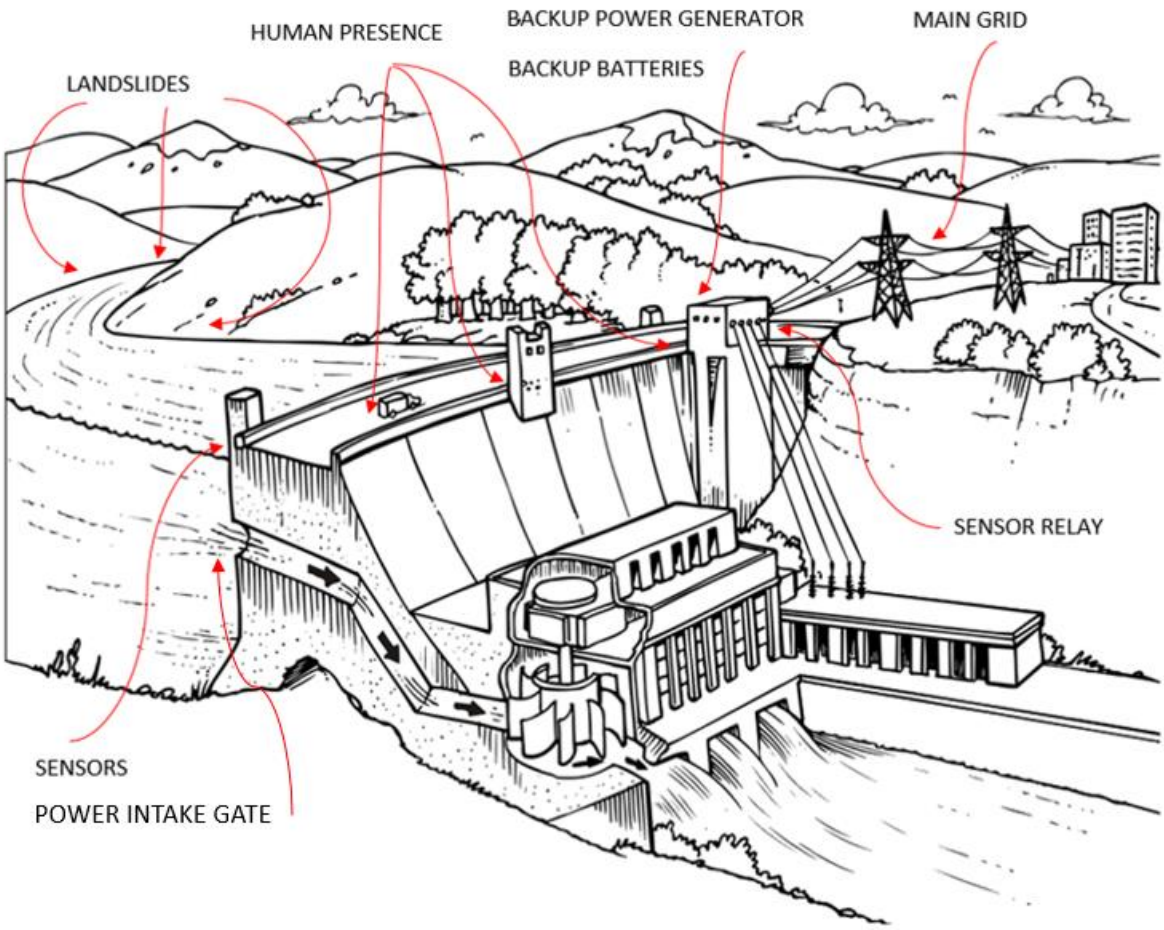

Figure 22. Dam and reservoir diagram with system variables (Summit Hydropower, Inc. 2015)

Starting conditions of the simulated system are represented by the variables from the context. Therefore, depending on the other variables, negative state of one variable will not necessarily mean that system is in a hazardous state. For example, if a gate cannot be opened, or due to faulty sensors operator decides not to open the gate, depending on the water level and inflow no harm may happen to the dam in the following hours. That time might be enough to eliminate the fault, or repair the critical system component.

Simulation software tools offer an intuitive interface for simulation model creation. However, this procedure was implemented in the MATLAB® (Matworks.com, 2016) software because of easy implementation of fuzzy interface system in the simulation model.

A continuous simulation approach is used for the determination of reservoir storage. Inputs for the simulation are (a) all the variables from the context; (b) storage curve, gate discharge curve and free crest weirs discharge curve; (c) FIS; and (d) simulation time horizon. The simulation time step is 1 hour. Data preparation and simulation flowchart is shown in Figure 23.

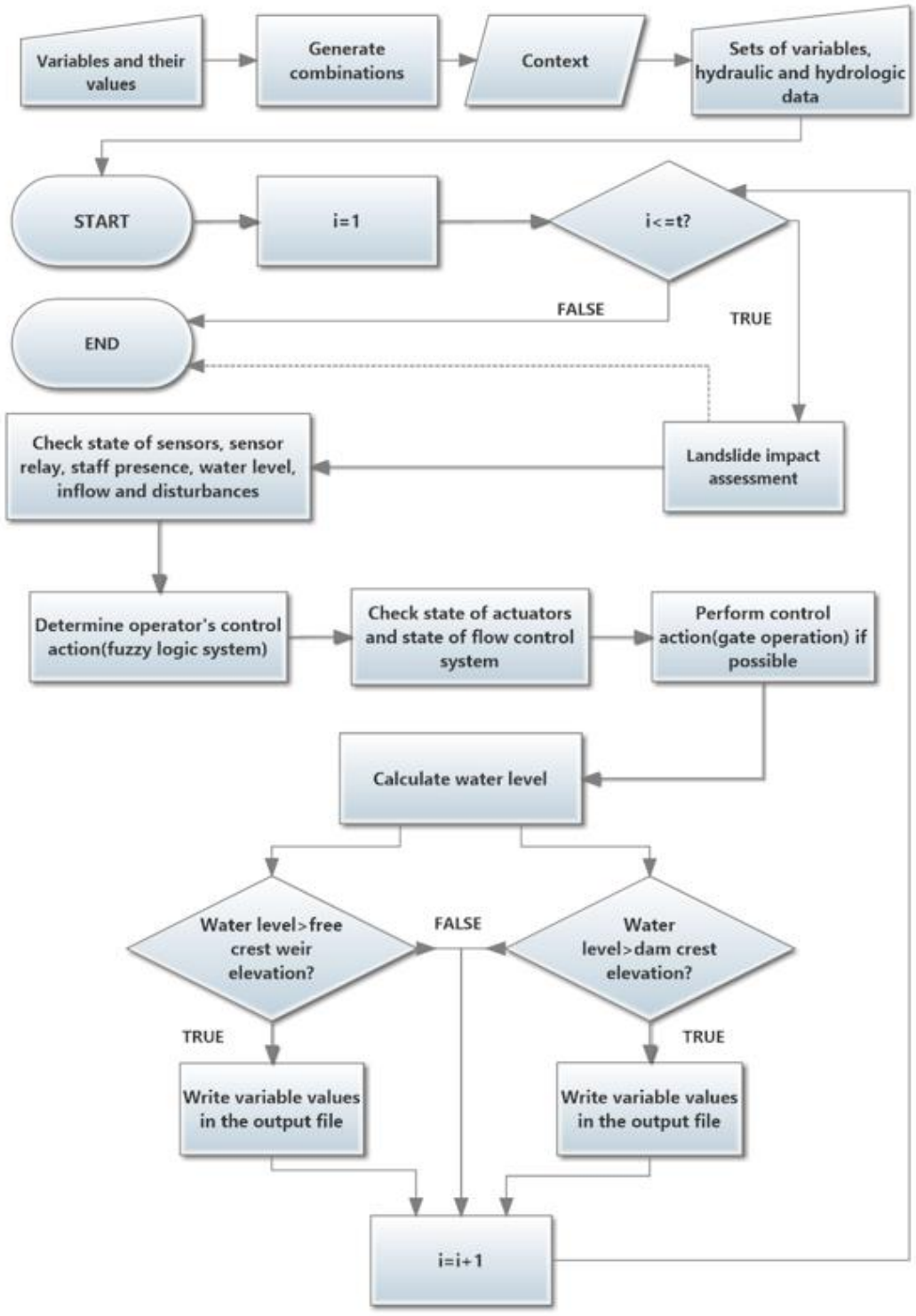

Figure 23. Simulation modelling procedure

The landslide impact is assessed at the beginning of each simulation step. If the volume of the landslide mass is significant compared to the reservoir size, the dam may be overtopped regardless of the dam state. Therefore, the simulation may end after landslide impact analysis. If that is not the case, next, the sensors are inspected. Availability of the sensor components is inspected because it influences operator's decisions. Fuzzy inference model based on information from the sensors provides operator's decision (shown in Figure 24).

```
if sensors are available then
      if CWL ≥ spillway sill elevation AND IN ≤ maximum gate discharge then
            set gate_position to output of FIS for inputs CWL and IN
      else if CWL ≥ spillway sill elevation AND IN ≥ maximum gate discharge then
            set gate_position to maximum gate elevation
      end
end
```

Figure 24. Pseudocode for sensors inspection and operator's decision (CWL - current water level or the reservoir elevation; IN - inflow)

After the operator's decision is determined, the state of the actuators and flow control system (gate) is investigated. The actuator system is divided in (a) power source: main power grid, backup generators (gasoline or diesel) and backup batteries; (b) mechanical component, the actual hoist machine and steel cable that lifts or lowers the gates; and (c) structural component, gate and its training wall and trunnions. State of the actuators and gates is determined and if possible, issued control action is performed. Using discharge curves (gate discharge, and free crest discharge) spillway and free crest discharge are calculated. Simulation revolves around single equation, based on (3.19):

$$RS_{t+1} = RS_t + 3600 \times (IN_t - SPO_t - PIO_t - LLOO_t - Overflowing_t) \quad (3.25)$$

where IN_t is the inflow in the current time step *t*, SPO_t is the spillway gate outflow in the current time step *t*, PIO_t is the power intake in the current time step *t*, $LLOO_t$ is the low-level outlet outflow in the current time step *t*, and $Overflowing_t$ is the free crests spill. It is assumed that there are no losses due to infiltration, leakage, and evaporation. At the end of each step, if the water level is higher than certain free crest weir and/or dam crest it means context is recorded in the output file and simulation ends since it reached hazardous state. Simulation runs until it reaches time horizon or until water level overtops free crest weirs and/or dam. Simulation is repeated for every combination of the starting conditions of the system.

Since water level change is simulated, only water level and gate position (if possible) change through the simulation. It is assumed that other system components' state (like sensors or hoist) cannot or do not change through the simulation. If the state of a system component can change in a short amount of time, that state of the system is described by another combination of variable values ("row" of context). Therefore, nothing is omitted from the final result.

The simulation is repeated for each combination of the variable values i.e. for each "row" of the context. This means that simulation is run *j* times for *k* hours, where *j* is the number of different combinations of variable values and *k* is the chosen simulation time horizon. Simulation time step is 1 hour.

3.4. Data

Because of the reservoir problem structure (components and their interactions), a lot of data is needed for model simulation.

- Hydrologic inflow data. The range of inflows from minimum to maximum inflow (probable maximum flood).
- Hydraulic data. Reservoir storage curve, spillway gate discharge curve, free crest and overtopping spill curves.
- Technical data: Information on actuator systems, power systems, sensors, and gates.
- Structural data: Locations of all the system components and their structure
- Geologic data: Landslide existence and their probable mass.

It is important to get the accurate hydrologic and hydraulic data for the simulation to have a realistic representation of the dam system and its behaviour. In order to have a clear picture of the state variables and connections between system components and how they influence each other, accurate mechanical and structural data is needed. If available, controller's experience can facilitate the development of fuzzy inference system.

4. Analysis and Results of Cheakamus Dam Case Study

The developed methodology has been implemented on a system based on the Cheakamus Dam in British Columbia. Cheakamus Dam is an earth dam with a concrete section where all the outlets are. It has several outlet structures including two 35 ft x 40 ft hoist operated spillway radial gates, lower level outlet gate, a hollow cone valve and three free crest weirs. A system dynamics

simulation model, presented ins Section 3.3, is based on the Cheakamus dam. The system representation has been simplified for model testing by combining radial gates into a single rating curve. Hollow cone is not incorporated in the model. All of the data has been provided by BC Hydro in the following documents: Local Operating Order 3G-CMS-06 (Wood, 2009) and Operations, Maintenance and Surveillance Manual for Dam Safety and Generation Operating Order CMS 4G-25 v2.2 (Oswell, 2009). Hazards that were investigated in this study are:

(H-1): Earth dam overtopping and destruction

(H-2): Uncontrolled spill over three separate free crest weirs (with same crest elevations).

Other hazards, like uncontrolled spill and downstream flooding, are not yet incorporated in the model.

The dam cross sections are shown in Figures 25, 26, and 27.

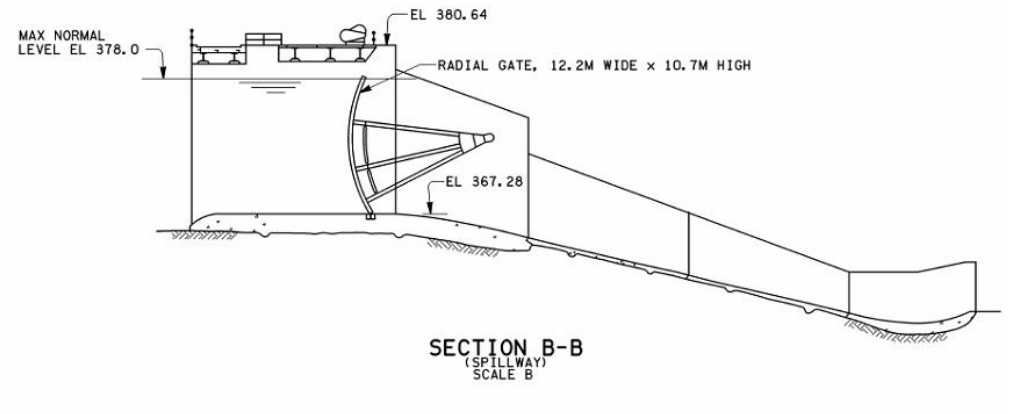

Figure 25. Spillway cross section – Cheakamus Dam (BC Hydro, 2009)

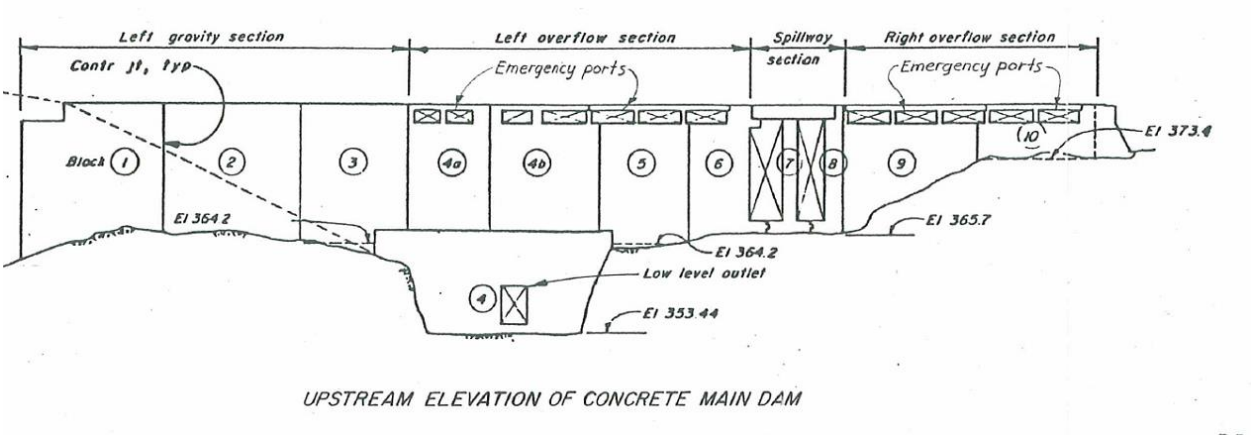

Figure 26. Upstream face of the concrete dam – Cheakamus Dam (BC Hydro, 2009)

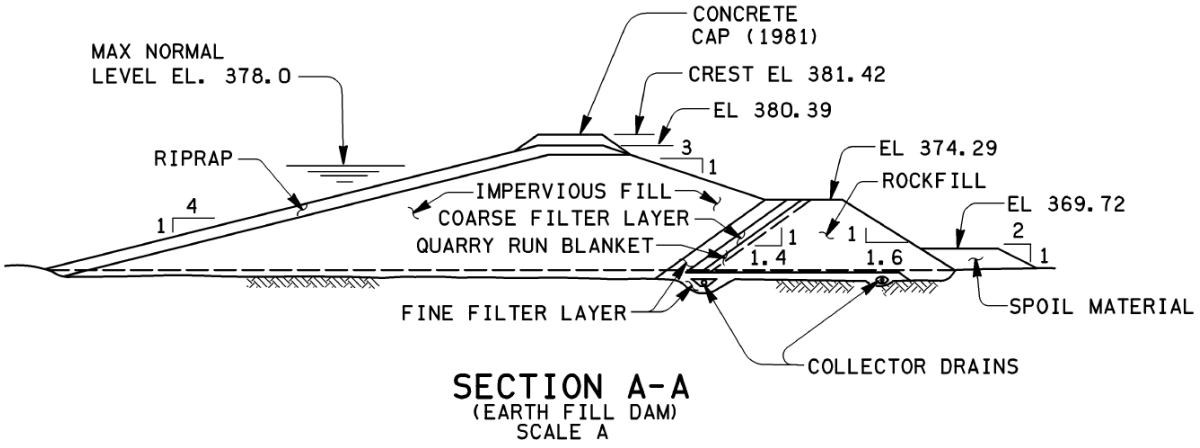

Figure 27. Cheakamus Dam earth fill cross – section (BC Hydro, 2009)

Figures 28, 29, and 30 show hydraulic capabilities of the main spillway, low level outlet gate and overflow facilities. Figure 31 shows the stage – storage curve for the Cheakamus Dam reservoir.

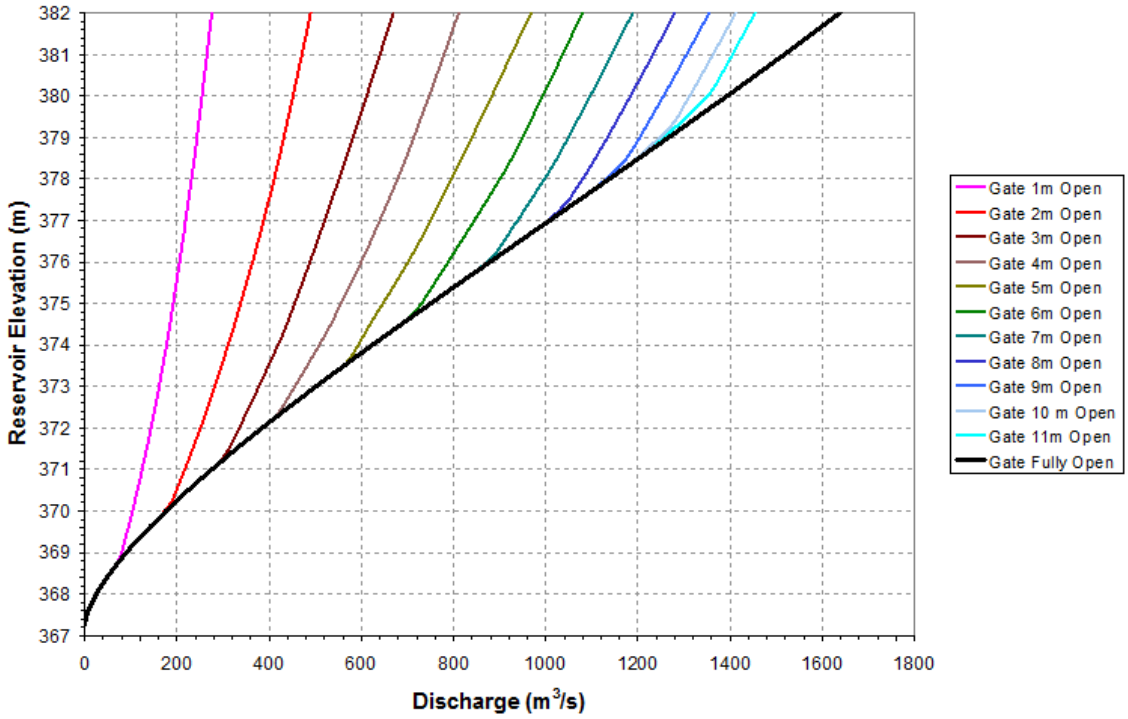

Figure 28. Spillway discharge curve for both spillway gates – Cheakamus dam (after Kong, 2013)

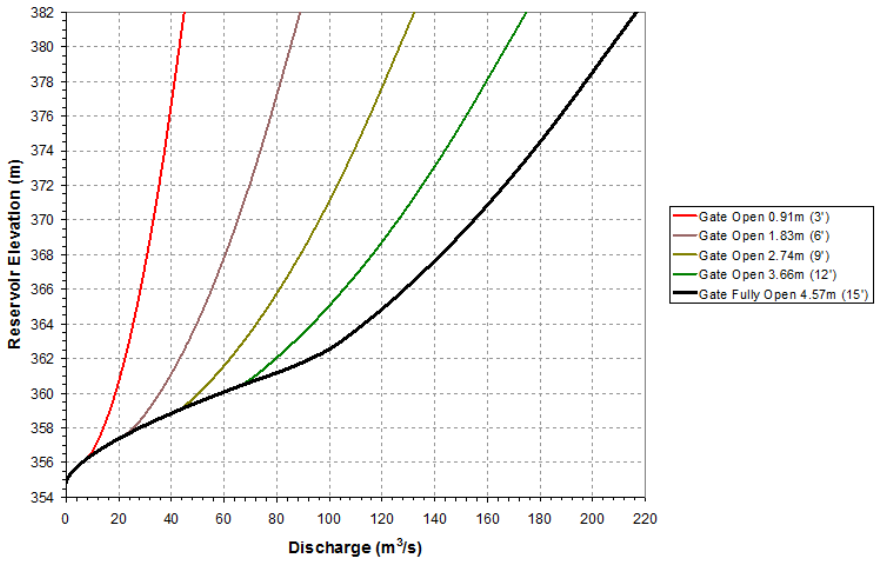

Figure 29. Discharge curve for low level outlet gate – Cheakamus dam (after Kong, 2013)

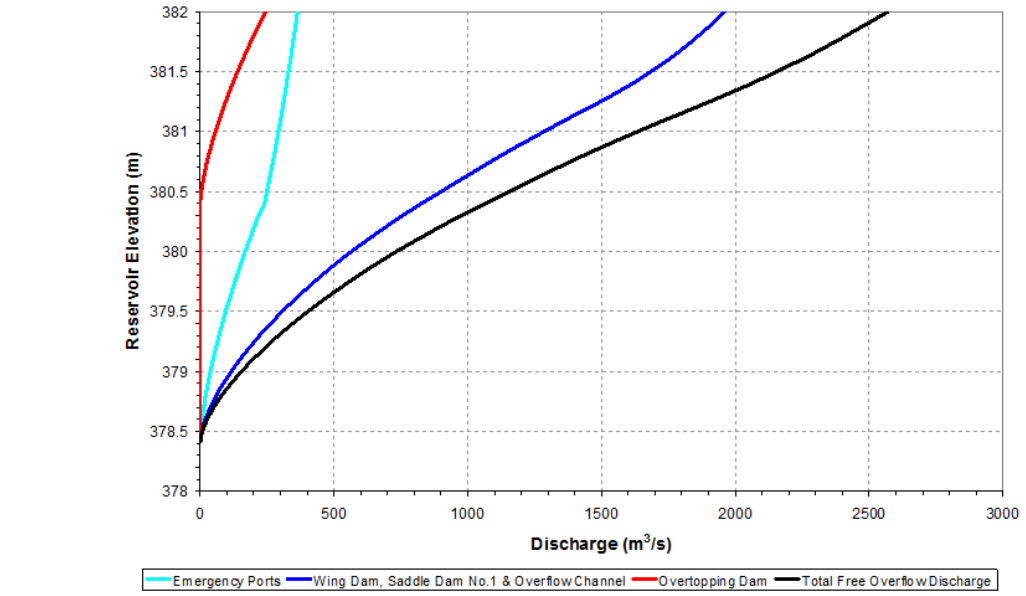

Figure 30. Discharge curves for overflow facilities – Cheakamus dam (after Kong, 2013)

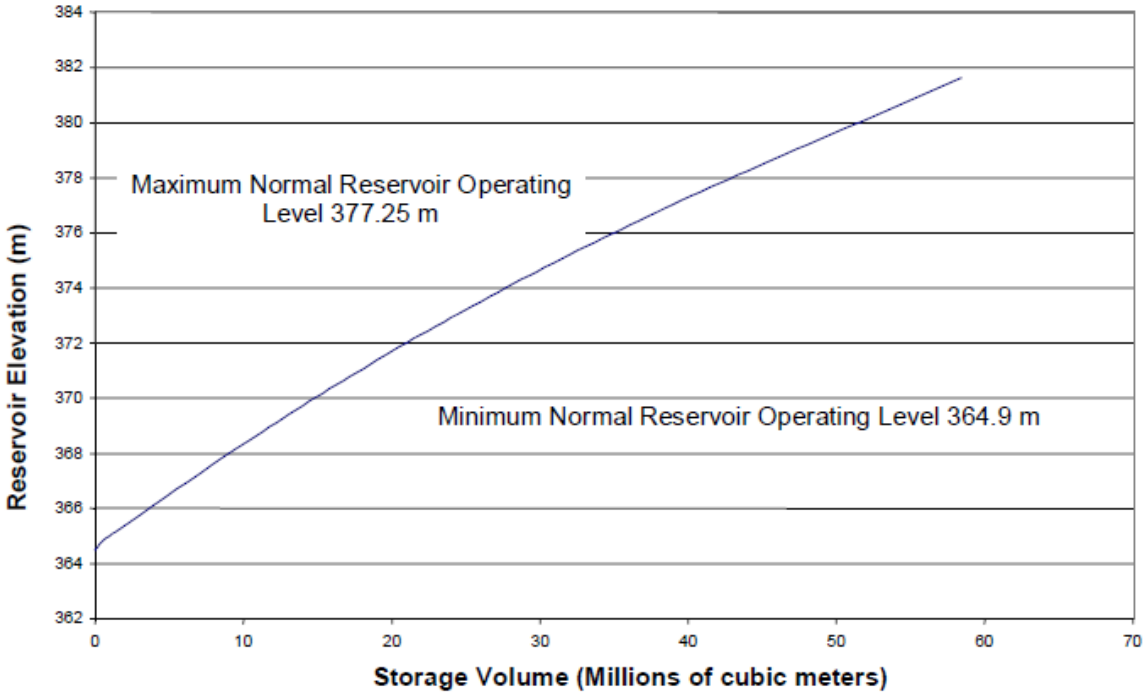

Figure 31. Stage – storage curve for the reservoir (after Matheson, 2005)

Variables and values used in Cheakamus Dam case study are shown in Tables 3 and 4.

Table 3: Input data for the Cheakamus Dam case study, part 1

Inflow(m^3/s)	Reservoir volume(m^3)	Gate Position	Sensor state	Debris(m)	Main grid	Diesel generator	Batteries
1	5000000	0	0	0	0	0	0
100	10000000	1	1	1	1	1	1
300	15000000	3	2	2			
500	20000000	5					
700	25000000	7					
900	30000000	9					
1000	35000000	10					
1500	40000000	11					
2000	45000000	12					
2500	50000000						
3000	55000000						
3500							
4000							

Table 4: Input data for the Cheakamus Dam case study, part 2

Hoist	Steel Cable	Gate structural condition	Sensor Relay	Stuff Presence	LLOG condition	Power Intake Gate condition
0	0	0	0	0	0	0
1	1	1	1	1	1	1
		2				

Water inflow (Table 3, column 1) is the only "input" to the reservoir. Direct precipitation and melting snow are included in the inflow values. Inflow range from a minimum of 1 m^3/s (can be changed to zero) to probable maximum flood (PMF) that is according to BC Hydro data 4,129 m^3/s. That number has since the year of 2003 been updated to a range between 2,300 and 2,900 m^3/s. PMF of 4,000 m^3/s is kept as the maximum flow in this case study. The reason for the update of PMF is not available. As seen in Table 3, column 1, inflow has 13 different values in the mentioned range. These values have been selected as representative and have smaller increments under 1000 m^3/s since historical daily maximum inflow value between years 1960 and 2000 was 648 m^3/s.

The lowest starting reservoir volume (storage) value used is 5,000,000 m^3 which corresponds to Cheakamus Dam water licence lower storage level (Wood, 2009) of 366.5 m. The highest starting reservoir volume used is 55,000,000 m^3 which corresponds to reservoir elevation of 380.7 m. This elevation is above overflow facilities but below Cheakamus Dam crest elevation. This starting condition is already a hazard since the overflow facilities are overtopped. This range of starting reservoir values was chosen to test whether the system can recover from H-2 hazard. Variables used for starting reservoir storage can be seen in Table 3 column 2.

Starting gate position is physically restricted to 12 meters, so the range is from 0 to 12 meters with increments of 1 to 2 meters. It is assumed that gate can be in any position at the start of the simulation. Starting gate position values are showed in Table 3 column 3.

Debris is assumed to create an impermeable block at the bottom of the spillway. If debris boom breaks, depending on the season, it is assumed that tree trunks and branches get stuck in the spillway and create an impermeable wall. According to the BC Hydro data, there have not been records of more than 1 meter of debris getting accumulated in the spillway, so 2 meters of maximum debris blockage is used to be on the safe side. Debris values are shown in Table 3 column 5.

Due to the lack of geologic and geomorphologic data, it is assumed that the landslide affects only the volume in the reservoir and that the whole land mass does not hit the surface of the water too fast (does not create big waves). Landslide volumes in the BC Hydro data are 300,000 m^3 (that happened in the 20^{th} century), 15,000,000 m^3 (half of the historical maximum), and 30,000,000 m^3 (the historical maximum which did hit the Cheakamus River area in the 19^{th} century). It has been found that these extreme values of landslide volume (compared to reservoir volume) skew the results, therefore landslide impact analysis is not present in the case study.

Availability of power source (Table 3, columns 6-8) and mechanical equipment (Table 4 columns 1 and 2) is implemented in a binary form, 0 or 1, not available or available. It is assumed that staff (Table 4, column 5) can arrive at the site in less than an hour or approximately one hour if the need arises (for example, if the sensor relay is not working). It is also assumed that in an additional hour

staff can determine the rate of rise (of reservoir level) and start controlling the gates manually (from the control station on site).

More information is needed on how sensors (Table 3, columns 4) work and how exactly software for monitoring sensor output is working to improve the system dynamics simulation model. Reservoir elevation sensors can have three states: (a) 1, the sensors are functioning properly and displaying correct elevation, (b) 0, the sensors are not working and (c) 2, the sensors are malfunctioning and are displaying elevation lower for 1 meter than the real reservoir elevation, therefore negatively influence controller's decision – making. Sensor relay (Table 4, column 4) transmits the reservoir elevation data to a remote controller. The relay can either function properly (1) or malfunction (0) and not transmit any data to the remote operator. It is assumed that system is controlled remotely. Therefore, if the relay is not functioning properly, and the local operator is not on site, no control action can be taken.

Reservoir management and planning is not part of the model, and there is insufficient data on the operation of low – level outlet gate. Low – level outlet gate (LLOG, Table 4, column 6) and power intake gate(Table 4, column 7) operation have been simplified in the presented study. LLOG is used if the spillway gates malfunction or if the inflow is greater than the spillway discharge capacity. LLOG is fully open in both cases. The power intake gate has the smallest flow capacity and is also used only if the spillway gates malfunction or if the inflow is greater than the spillway discharge capacity.

For some variables, value increment might be significant. The increment value should be selected to provide accurate results i.e. to cover all of the possible conditions. For now, one of the

limitations is the physical computer memory, simply because of the size of the input data that has to be stored and accessed during simulation. Another important point is that there are simply too many iterations to go through depending on the size of the context.

4.1. Computer implementation

A simplified flowchart of the computational procedure applied to the Cheakamus Dam case study is shown in Figure 30.

Figure 32. Programming flowchart

Variables and values are stored in a spreadsheet. From these variables and their values, using context generator (described in the Python code – Appendix B), the full context for STPA is generated. Simulation is done using MATLAB software (Mathworks, 2015) and code is presented in Appendix C. Since the product of the number of variable values is 17,791,488 (13*11*9*3*3*2*2*2*2*2*3*2*2*2*2), that is the number of rows of the context. Therefore, 1-hour time step, 3-hour time horizon simulations have been repeated 17,791,488 times, each time with different starting conditions. Time horizon of 3 hours has been selected because of the long duration of the computing time. Part of the generated context is shown in Table 5. The notation used in Table 5 includes:

Table 5: Part of the Cheakamus case study context (the first nine rows)

IN	RV	GP	Sens	Debris	MG	DG	BAT	Hoist	Cable	GSC	SR	SP	LLOG	PG
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	0	0	0
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	0	0	1
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	0	1	0
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	0	1	1
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	1	0	0
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	1	0	1
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	1	1	0
1	$5*10^6$	0	0	0	0	0	0	0	0	0	0	1	1	1
1	$5*10^6$	0	0	0	0	0	0	0	0	0	1	0	0	0

IN as the inflow (same in each time step), RV as the starting reservoir volume, GP as the starting spillway gate position, Sens as the reservoir elevation sensor condition, Debris as the amount of debris accumulated in the spillway, MG as the availability of the main grid, DG as the availability of the diesel generator, and BAT as the availability of backup batteries. Hoist and Cable represent the state of the hoist – cable mechanism. GSC is the spillway gate structural condition. SR is the condition of the sensor relay system. SP is the staff presence. LLOG is the condition of the low - level outlet gate. PG is the condition of the power intake gate.

Results of the procedure are recorded in two separate spreadsheets. One spreadsheet records each starting combination of variable values and controller's decision throughout the simulation that resulted in a hazard (both H-1 and H-2, discussed at the beginning of Chapter 4). Another spreadsheet records the hourly changes of the reservoir storage in each of the 17,791,488 simulations.

4.2. Justification for the use of fuzzy rules

An experiment was conducted to compare spillway gate operation and reservoir elevation changes when fuzzy rules and crisp rules are used for control actions. Two simple system dynamics simulation models based on the Cheakamus dam are developed and used for the experiment. Historical hourly inflow data is used as input to the both models. Inflow data was provided by BC Hydro from one of the events recorded at Cheakamus Dam. Inflow hydrograph of the event is shown in Figure 33.

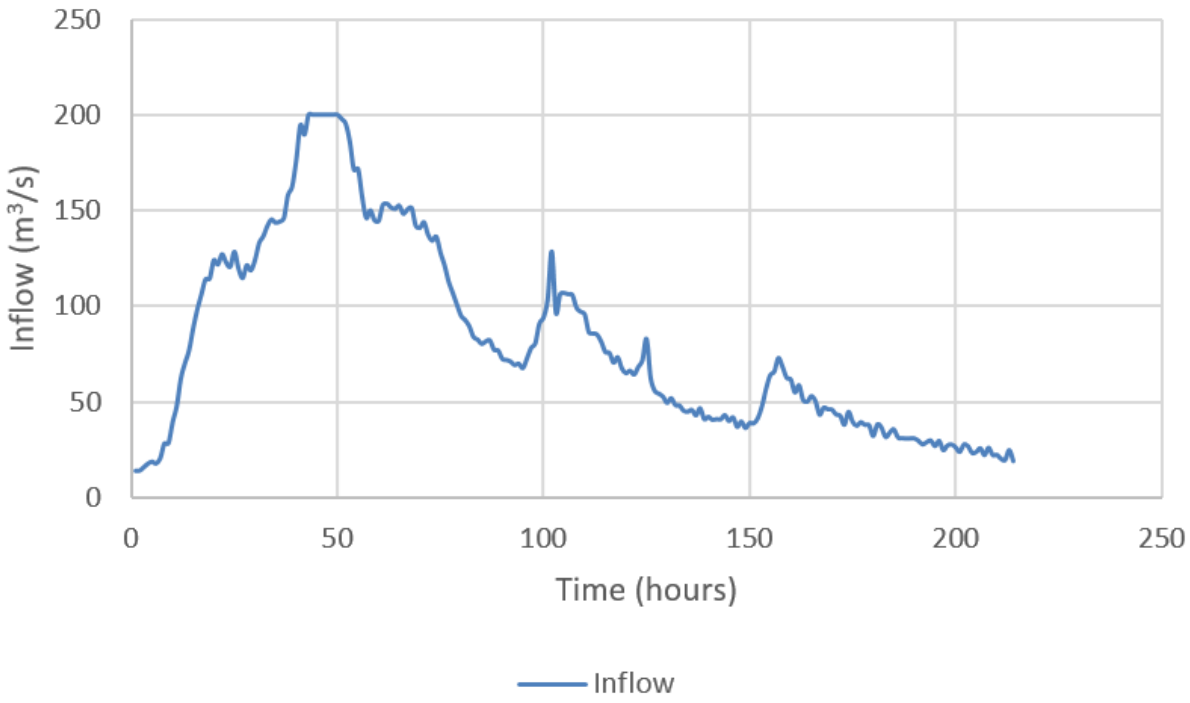

Figure 33. Cheakamus Dam historical inflow hydrograph

4.2.1. Fuzzy rules (FIS) example

System dynamics simulation model structure is shown in Figure 34.

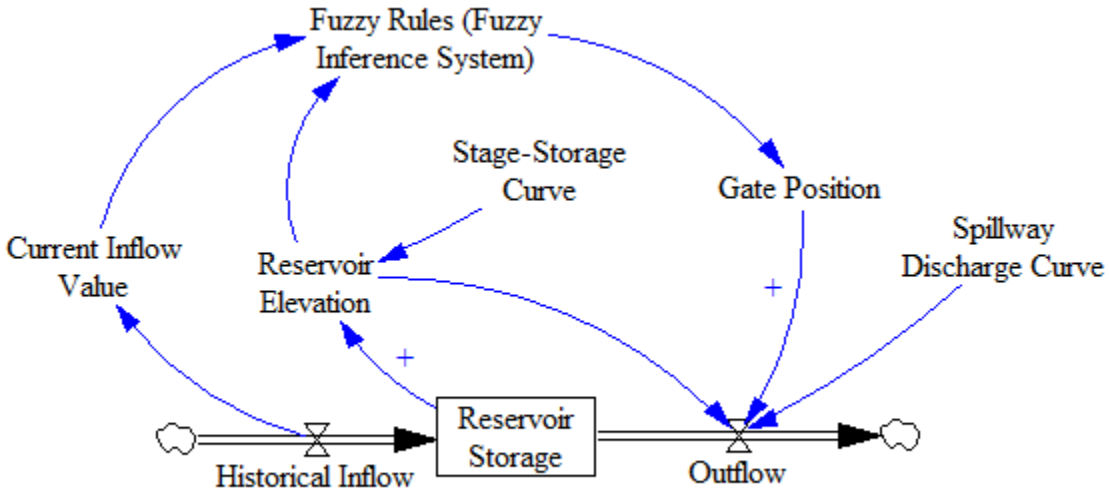

Figure 34. Stock and flow diagram of the Cheakamus Dam System with fuzzy rules

Reservoir storage (volume of water in the reservoir) accumulates or integrates the flows:

$$RS(t) = \int_{t_0}^{t} [Historical\ inflow(s) - Outflow(s)]ds + RS(t_0) \quad (4.1)$$

where *RS(t)* is the reservoir storage in current time *t* in m^3, *Historical inflow(s)* is the value of the inflow at any time *s* between the initial time t_0 and the current time *t* in m^3/s, *Outflow(s)* is the value of the outflow at any time *s* between the initial time t_0 and current time *t* in m^3/s, and $RS(t_0)$ is the reservoir storage at initial time t_0 in m^3. The net rate of reservoir storage change can be presented by its derivative:

$$\frac{d(RS)}{dt} = Historical\ Inflow(t) - Outflow(t) \quad (4.2)$$

The ordinary differential equation (4.2) is the basis of the system dynamics simulation. The Euler method is used for the numerical integration:

$$RS_{t+1} = RS_t + \Delta t \times (Historical\ inflow_t - Outflow_t) \quad (4.3)$$

where RS_{t+1} is the reservoir storage in the next time step, RS_t is the reservoir storage in the current time step t, Δt is the time step of 1 hour, $Historical\ inflow_t$ is the value of the inflow in the current time step, and $Outflow_t$ is the value of the outflow in the current time step t. Outflow is a function of reservoir elevation and spillway gate position:

$$Outflow_t = f(Gate\ position_t, Reservoir\ elevation_t) \quad (4.4)$$

where $Gate\ position_t$ is the position of the spillway gate in the current time step t and $Reservoir\ elevation_t$ is the elevation of the reservoir water surface in the current time step t in meters above sea level. Outflow is evaluated from the spillway discharge curve shown in Figure 35.

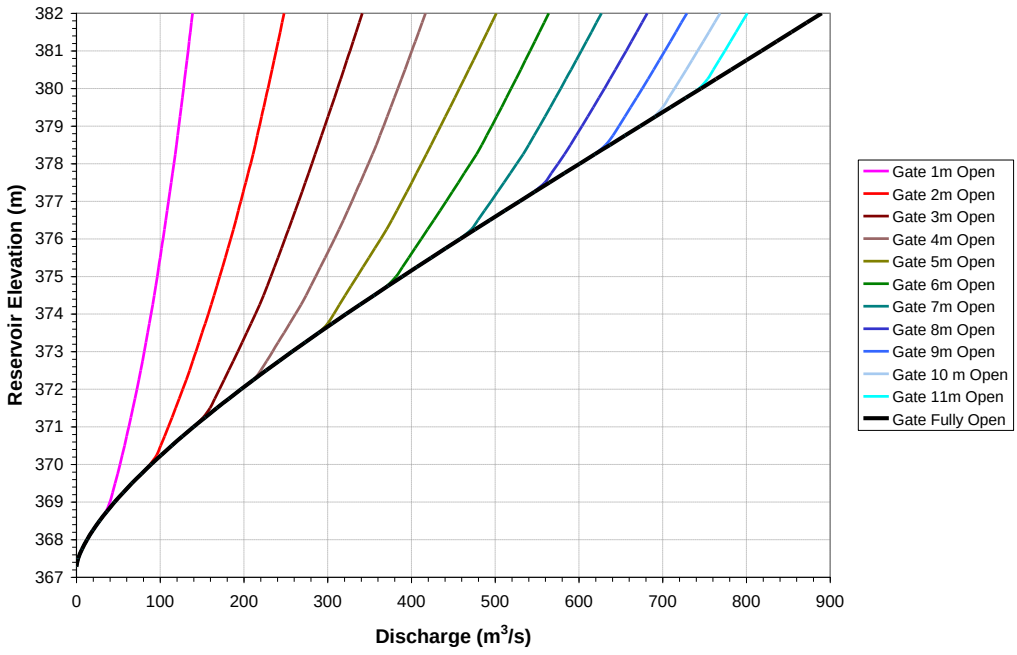

Figure 35. Spillway discharge curve for spillway gate #1 – Cheakamus dam (after Kong, 2013)

Reservoir elevation is evaluated from the stage – storage curve (see Figure 31 for Cheakamus Dam reservoir stage – storage curve).

Gate position in each time step is determined using control action rules. The proposed FIS belongs to the class Mamdani fuzzy inference systems. The goal of the fuzzy rules is to keep the reservoir at the same elevation as starting elevation, without discharging more than the inflow. Therefore, the goal of the FIS is to match the outflow value to the inflow value. The FIS achieves that goal by control of the gate position. The FIS has two inputs, inflow and reservoir elevation, and one output, gate position, as shown in Figure 36.

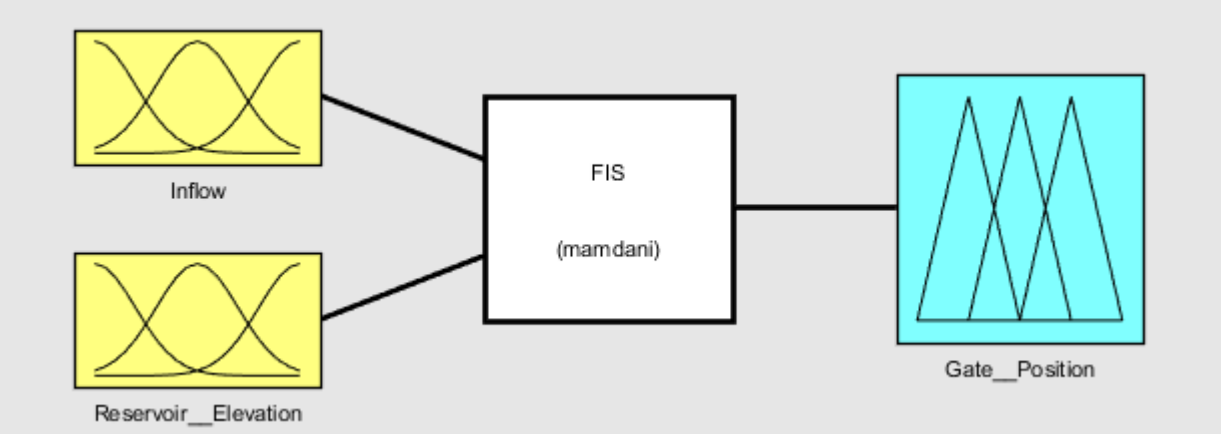

Figure 36. Fuzzy inference system inputs and outputs

The inputs and output fuzzy sets and membership functions were created on the basis of hydraulic capability of the spillway, similarly to Cheakamus Dam case study. Membership functions of the inflow fuzzy sets are shown in Figure 37.

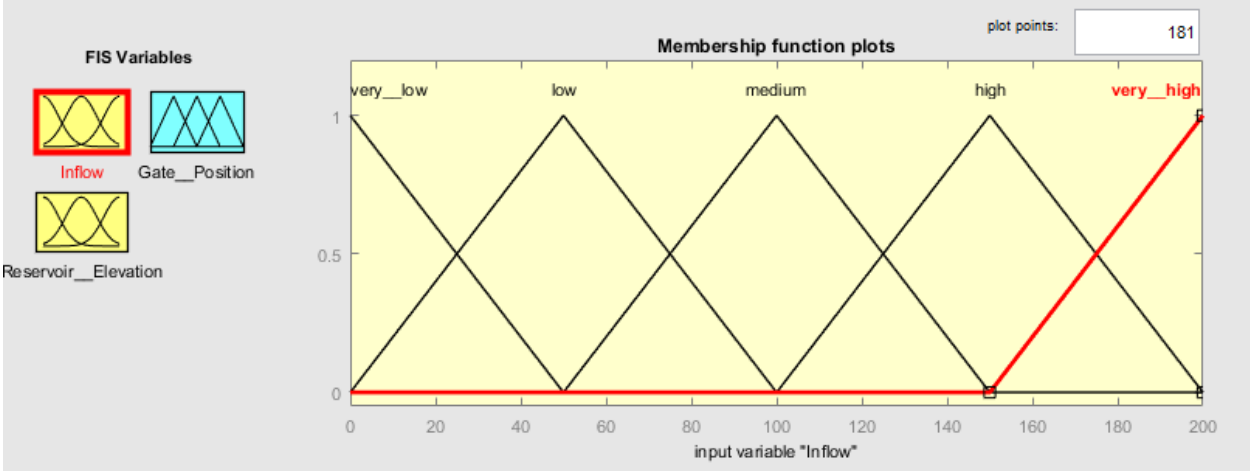

Figure 37. Membership functions of inflow fuzzy sets for the FIS. The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the inflow in m3/s.

Membership functions of the reservoir elevation fuzzy sets are shown in Figure 38.

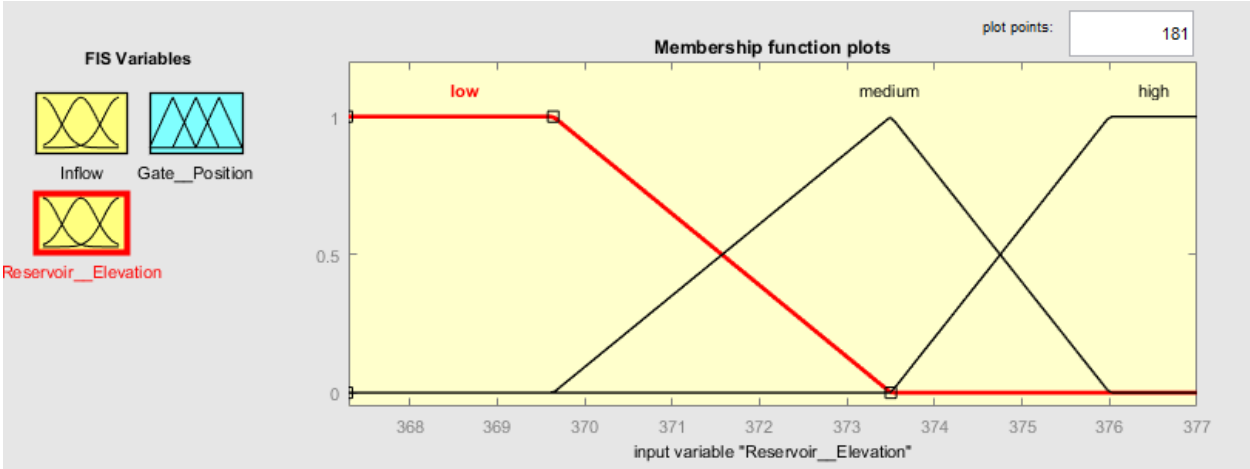

Figure 38. Membership functions of reservoir elevation fuzzy sets for the FIS. The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the reservoir elevation in meters above sea level.

Membership functions of gate position fuzzy sets are shown in Figure 39.

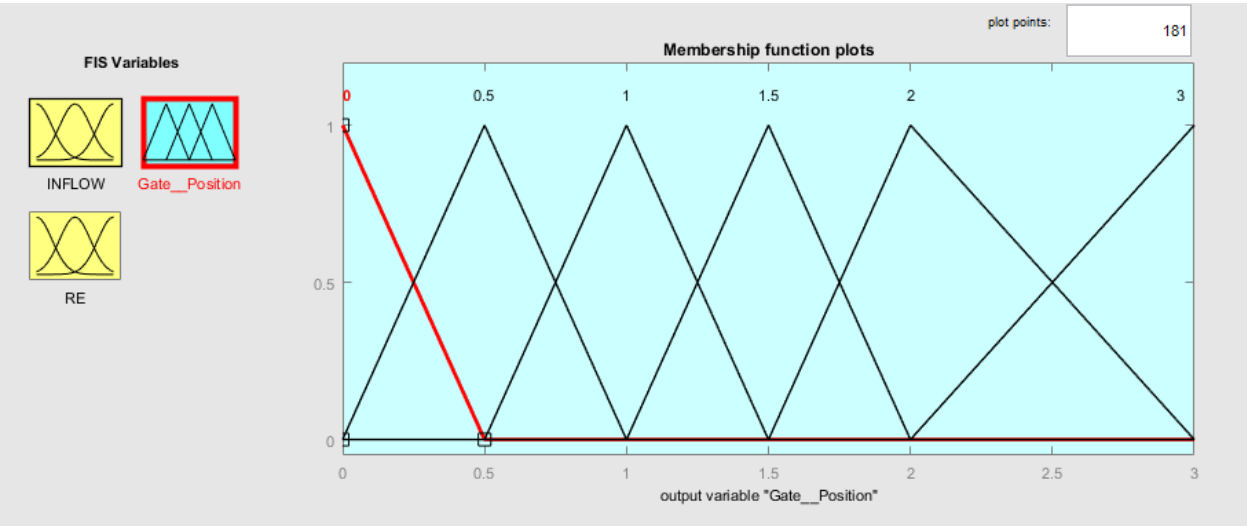

Figure 39. Membership functions of gate output fuzzy sets for the FIS. The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the gate opening in meters.

FIS has following fuzzy rule base:

IF *inflow* is **very low** AND *RE* is **low** THEN *gate position* is **0** (4.5)

OR IF *inflow* is **very low** AND *RE* is **medium** THEN *gate position* is **0** (4.6)

OR IF *inflow* is **very low** AND *RE* is **high** THEN *gate position* is **0** (4.7)

OR IF *inflow* is **low** AND *RE* is **low** THEN *gate position* is **1** (4.8)

OR IF *inflow* is **low** AND *RE* is **medium** THEN *gate position* is **0.5** (4.9)

OR IF *inflow* is **low** AND *RE* is **high** THEN *gate position* is **0.5** (4.10)

OR IF *inflow* is **medium** AND *RE* is **low** THEN *gate position* is **2** (4.11)

OR IF *inflow* is **medium** AND *RE* is **medium** THEN *gate position* is **1.5** (4.12)

OR IF *inflow* is **medium** AND *RE* is **high** THEN *gate position* is **1** (4.13)

OR IF *inflow* is **high** AND *RE* is **low** THEN *gate position* is **3** (4.14)

OR IF *inflow* is **high** AND *RE* is **medium** THEN *gate position* is **2** (4.15)

OR IF *inflow* is **high** AND *RE* is **high** THEN *gate position* is **1.5** (4.16)

OR IF *inflow* is **very high** AND *RE* is **low** THEN *gate position* is **3** (4.17)

OR IF *inflow* is **very high** AND *RE* is **medium** THEN *gate position* is **3** (4.18)

OR IF *inflow* is **very high** AND *RE* is **high** THEN *gate position* is **2** (4.19)

Historical info provided was for an event that lasted 214 hours. Therefore, simulation time horizon is 214 hours and simulation time step is 1 hour. Starting reservoir storage is 14,798,916 m^3 corresponding to reservoir elevation of 370 meters above sea level. Simulation is done using MATLAB® software, and the code is included in Appendix D.

4.2.2. Crisp rules example

System dynamics simulation model structure is shown in Figure 40.

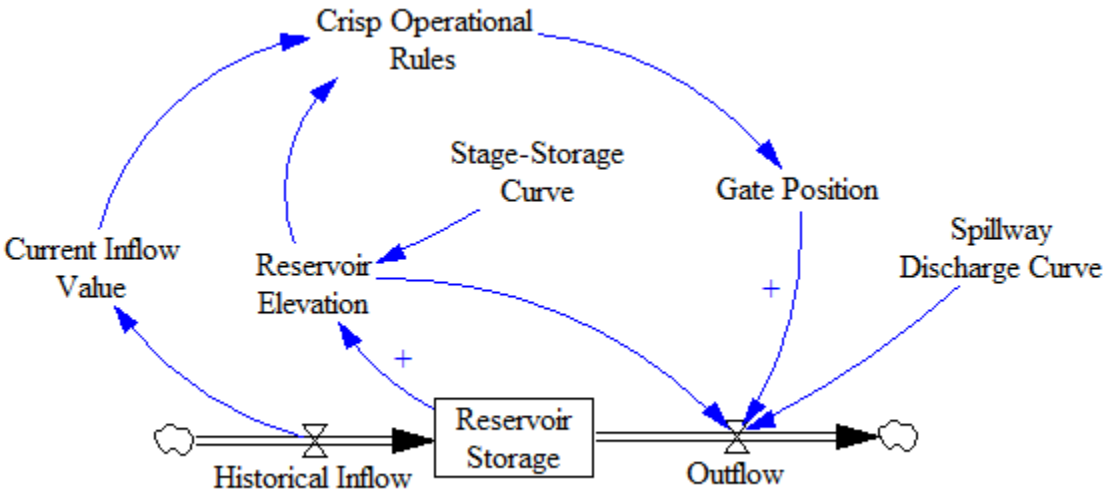

Figure 40. Stock and flow diagram of the Cheakamus Dam system with crisp operational rules.

This structure is similar to the structure used in the previous example and equations (4.1) to (4.4) are also used in this model. Outflow is evaluated from the spillway discharge curve (see Figure 35 for Cheakamus Dam spillway discharge curve). Reservoir elevation is evaluated from the stage – storage curve (see Figure 31 for Cheakamus Dam reservoir stage – storage curve).

Gate position in each time step is determined using crisp control action rules. The goal of the crisp rules is to match the outflow value to the inflow value. This is achieved by control of the gate position. The crisp rules have two inputs, inflow and reservoir elevation, and one output, gate position. The input inflow value can be a member of one of following sets:

$$"0" = \{inflow \in HI | 0 \leq inflow \leq 25\} \quad (4.20)$$

$$"50" = \{inflow \in HI | 25 < inflow \leq 75\} \quad (4.21)$$

$$"100" = \{inflow \in HI | 75 < inflow \leq 125\} \quad (4.22)$$

$$"150" = \{inflow \in HI | 125 < inflow \leq 175\} \quad (4.23)$$

$$"200" = \{inflow \in HI | 175 < inflow \leq 200\} \quad (4.24)$$

where “0”, “50”, “100”, “150”, and “200” are the inflow sets and *HI* is the set of all inflow values from the historical data. Since these are crisp sets, degree of membership of each element of these sets is always 1. Membership functions of inflow sets are shown in Figure 41.

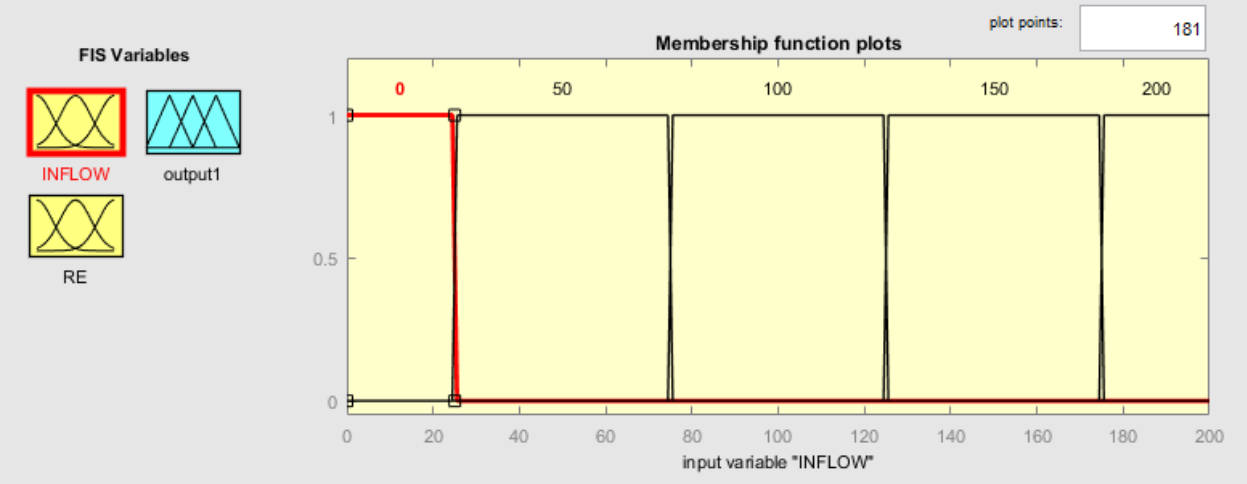

Figure 41. Membership functions of inflow sets for the crisp rules. The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the inflow in m3/s.

The reservoir elevation value can be a member of one of following sets:

$$Range\ 1 = \{reservoir\ elevation \in RER | 367.28 < reservoir\ elevation < 372\} \quad (4.25)$$

$$Range\ 2 = \{reservoir\ elevation \in RER | 372 \leq reservoir\ elevation < 375\} \quad (4.26)$$

$$Range\ 3 = \{reservoir\ elevation \in RER | 375 \leq reservoir\ elevation \leq 377\} \quad (4.27)$$

where, *Range 1*, *Range 2*, and *Range 3* are the reservoir elevation sets and *RER* is the set of all reservoir elevations between 367.28 meters above sea level and 377 meters above sea level. Membership functions of these sets are shown in Figure 42.

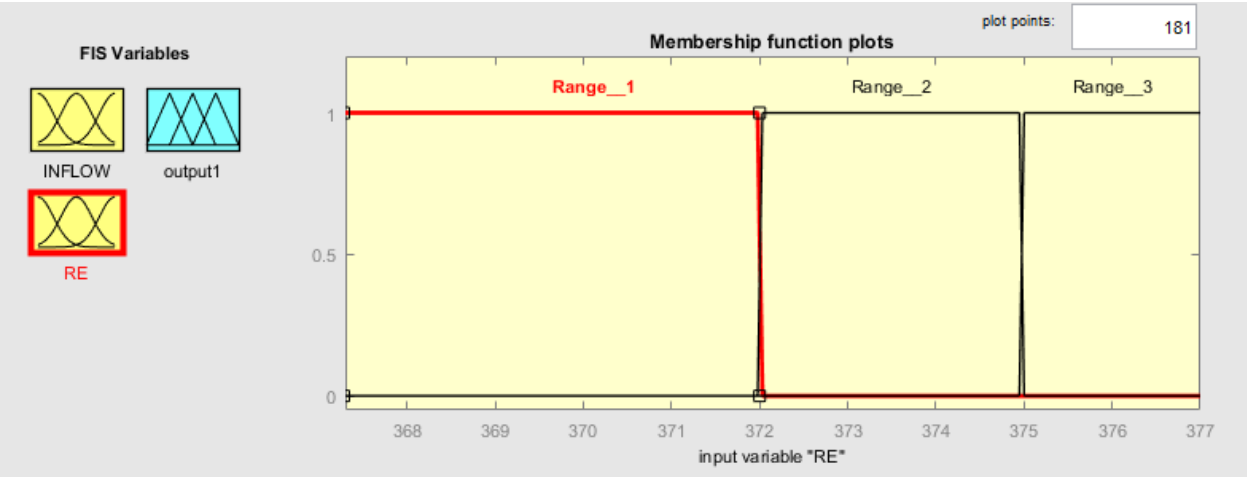

Figure 42. Membership functions of reservoir elevation sets for the crisp rules. The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the reservoir elevation in meters above sea level.

The output of the crisp rules are singletons, sets with exactly one element. Gate position output can be one of the following sets:

$$"0.5" = \{0.5\} \quad (4.28)$$

$$"1" = \{1\} \tag{4.29}$$

$$"1.5" = \{1.5\} \tag{4.30}$$

$$"2" = \{2\} \tag{4.31}$$

$$"3" = \{3\} \tag{4.32}$$

Membership functions of these sets are shown in Figure 43.

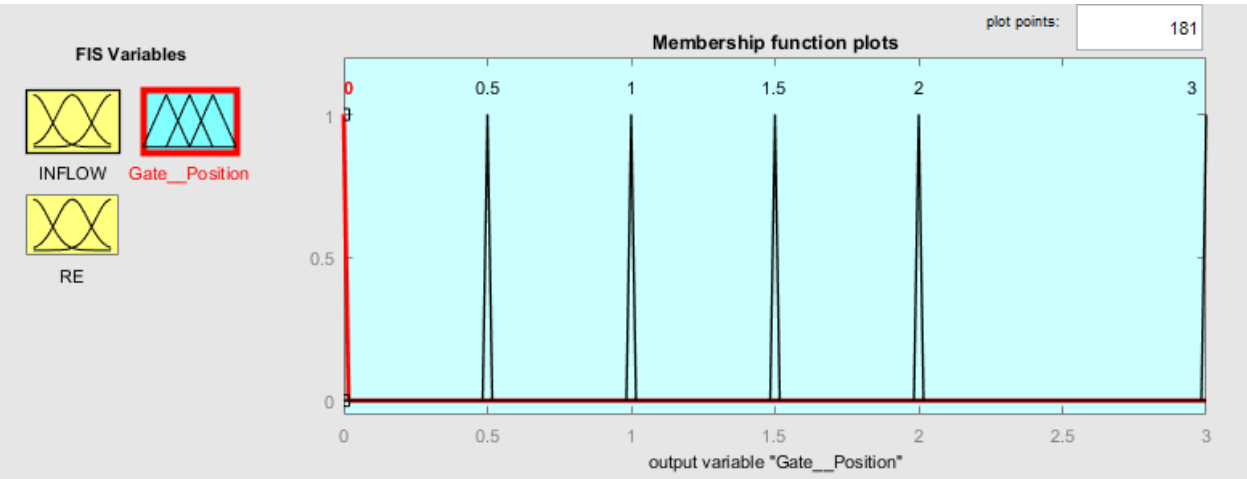

Figure 43. Membership functions of gate position sets for the crisp rules. The vertical axis is the degree of membership (from 0 to 1), and the horizontal axis is the gate position in meters.

Following crisp control action rules are used:

$$\text{IF } \textit{inflow} \in \textbf{“0”} \text{ AND } \textit{RE} \in \textbf{Range 1} \text{ THEN } \textit{gate position} = \textbf{0} \tag{4.33}$$

$$\text{ELSE IF } \textit{inflow} \in \textbf{“0”} \text{ AND } \textit{RE} \in \textbf{Range 2} \text{ THEN } \textit{gate position} = \textbf{0} \tag{4.34}$$

ELSE IF *inflow* ∈ **"0"** AND *RE* ∈ **Range 3** THEN *gate position* = **0** (4.35)

ELSE IF *inflow* ∈ **"50"** AND *RE* ∈ **Range 1** THEN *gate position* = **1** (4.36)

ELSE IF *inflow* ∈ **"50"** AND *RE* ∈ **Range 2** THEN *gate position* = **0.5** (4.37)

ELSE IF *inflow* ∈ **"50"** AND *RE* ∈ **Range 3** THEN *gate position* = **0.5** (4.38)

ELSE IF *inflow* ∈ **"100"** AND *RE* ∈ **Range 1** THEN *gate position* = **2** (4.39)

ELSE IF *inflow* ∈ **"100"** AND *RE* ∈ **Range 2** THEN *gate position* = **1.5** (4.40)

ELSE IF *inflow* ∈ **"100"** AND *RE* ∈ **Range 3** THEN *gate position* = **1** (4.41)

ELSE IF *inflow* ∈ **"150"** AND *RE* ∈ **Range 1** THEN *gate position* = **3** (4.42)

ELSE IF *inflow* ∈ **"150"** AND *RE* ∈ **Range 2** THEN *gate position* = **2** (4.43)

ELSE IF *inflow* ∈ **"150"** AND *RE* ∈ **Range 3** THEN *gate position* = **1.5** (4.44)

ELSE IF *inflow* ∈ **"200"** AND *RE* ∈ **Range 1** THEN *gate position* = **3** (4.45)

ELSE IF *inflow* ∈ **"200"** AND *RE* ∈ **Range 2** THEN *gate position* = **3** (4.46)

ELSE IF *inflow* ∈ **"200"** AND *RE* ∈ **Range 3** THEN *gate position* = **2** (4.47)

The structure of the crisp rules is similar to the fuzzy rules, but different sets are used in the two examples. The simulation time horizon is 214 hours and simulation time step is 1 hour. Starting

reservoir storage is 14,798,916 m^3 corresponding to reservoir elevation of 370 meters above sea level. Simulation is done using MATLAB® software, and the code is included in Appendix E.

4.2.3. Comparative analysis of the results

Depending on control action rules, the gate position will change in each time step. Gate position changes from both systems are shown in Figure 44.

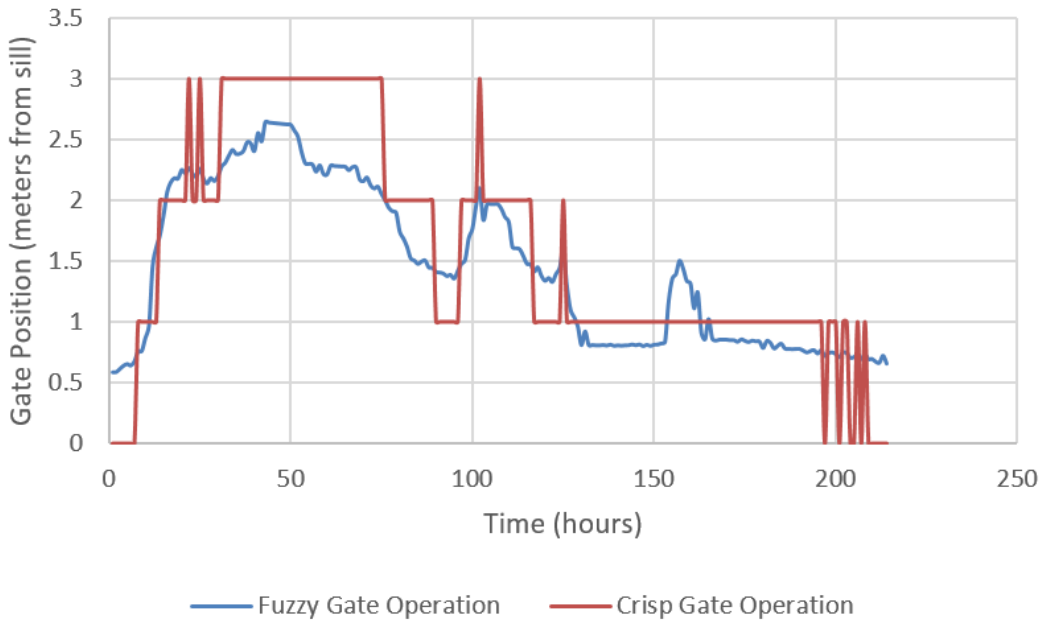

Figure 44. Cheakamus Dam spillway gate operation (blue – simulated using fuzzy control action rules; red – simulated using crisp control action rules)

Fuzzy control action rules result in a much smoother gate operation. Gate position is changed every time step, but in small increments, usually several centimeters. In contrast to that, gate operation using crisp control action rules results in a "choppy" gate operation. The gate alternates between two positions several times in a matter of hours. This kind of gate operation is highly impractical, unsafe, and impossible depending on the rate of gate movement. Additionally, sudden changes in

gate position of this range may wear down the mechanical equipment and lead to the failure of the gate actuator systems. The rate of the Cheakamus Dam spillway gate movement is not available. Shorter time step cannot be used with the hourly historical inflow data. Gate operation using crisp rules might be even more erratic with shorter time step. From gate operation point of view, the use of fuzzy rules results in better control actions.

Simulated reservoir storage is transformed to reservoir elevation (using stage – storage curve), and the results from both examples are shown in Figure 45.

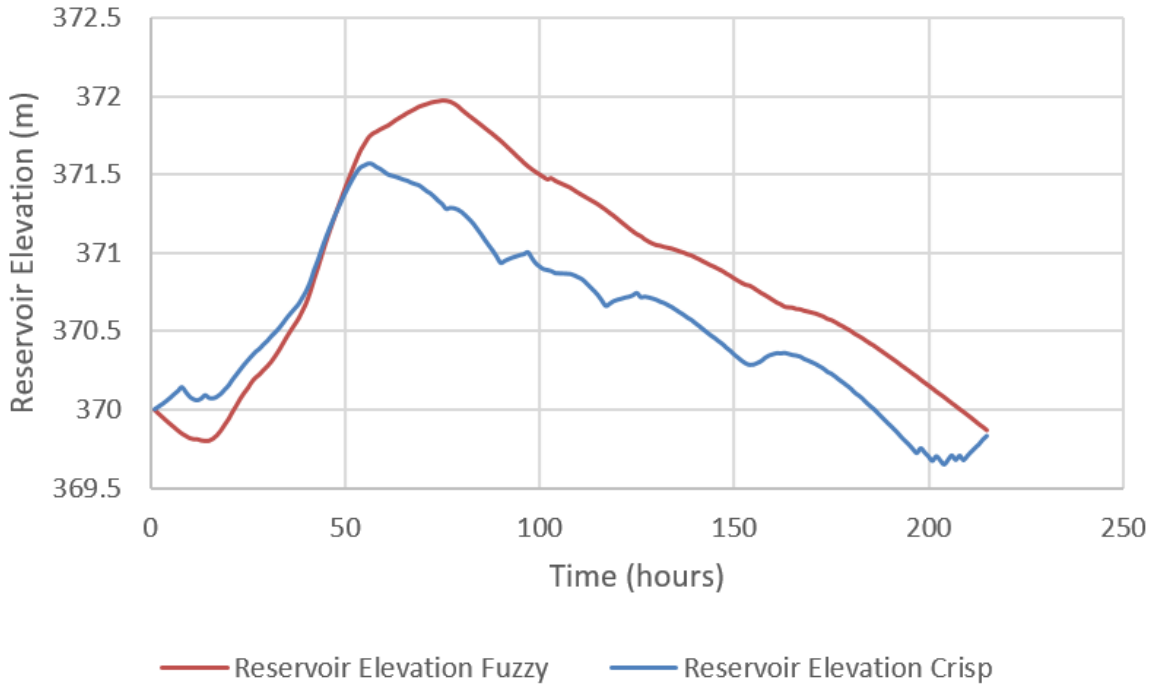

Figure 45. Cheakamus reservoir elevation changes (blue – simulated using crisp control action rules; red – simulated using fuzzy control action rules)

Reservoir elevation levels are similar in both examples. Both sets of control action rules satisfy the goal of keeping the reservoir elevation close to the starting reservoir elevation at the end of the

event. Fuzzy control action rules result in smoother reservoir elevation changes. Example using the crisp control action rules shows lower reservoir elevations, which from the dam safety point of view is a better result. However, the lower reservoir elevations in the second example are achieved with impractical and unsafe gate operation, thus invalidating the result.

4.3. Results and the discussion

The results of the system dynamics simulations are automatically saved in a spreadsheet and are ready to be analyzed. Result include hourly reservoir storage values. The reservoir volume is of main concern, together with its change through time and its relationship with the state of other system components and control actions. The Cheakamus Dam model presented in this thesis can show how components interact and how the lack of safe control action might not always result in a hazardous state for the reservoir. Sometimes, external disturbance may be too large for the system as it is designed. Millions of combinations of variable values or context "rows" provide an answer to an important question: what happens if something changes during the simulation time. The answer is in the robustness of the presented methodology. If the state of a system component changes in a short period of time, that state of the system is described in another combination of variable values ("row" of context). Therefore, no potential hazardous state is omitted from the final results. All of the physically possible values of the 15 variables are already in the context.

Results were analyzed and several scenarios are selected for visual presentation in the following subsections.

Following scenarios are presented:

- Scenario 1: Spillway gates closed and cannot be opened
- Scenario 2: Spillway gates open and stuck 1 meter above the spillway sill
- Scenario 3: Spillway gates open and stuck 3 meters above the spillway sill
- Scenario 4: Spillway gates open and stuck 5 meters above the spillway sill
- Scenario 5: LLOG closed and not functioning
- Scenario 6: Power intake gate closed and not functioning

Scenarios obviously do not cover the whole context, but just some of the combinations of variable values. The goal of these scenarios is to determine if a certain failure will lead to a hazardous state, depending on the context in which the failure happened. These six scenarios were selected as the spillway gates, LLOG and power intake gate are the critical components of the hydropower dam system. Without them, outflow control and reservoir operation are not possible. Failure of the outflow gates poses a serious risk for the dam system.

Frequency histograms of the reservoir volumes for each scenario are created throughout simulation time horizon in order to have a clear understanding of the reservoir volume changes with time. Since simulation time step is 1 hour, hourly histograms are presented.

In each scenario starting reservoir conditions (0 hours) are distributed into bins of the same width of 5,000,000 m^3, starting with 5,000,000 m^3 and ending with 65,000,000 m^3. 5,000,000 m^3 to 65,000,000 m^3 is the range of the Cheakamus Dam reservoir storage. An example of the 0-hour histogram with 10 bins is shown in Figure 46.

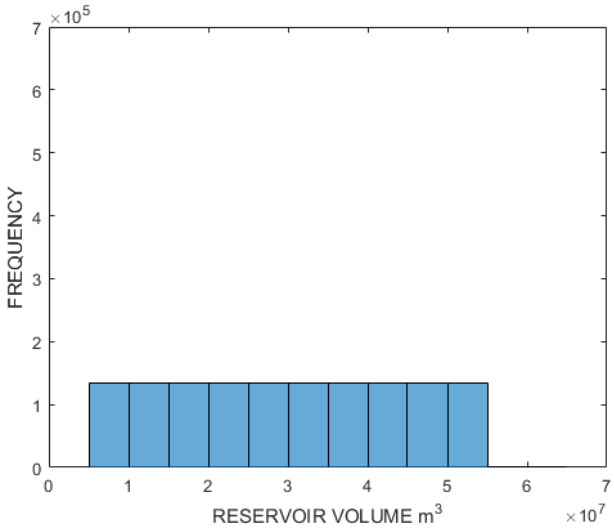

Figure 46. An example of starting reservoir volume histogram

Reservoir volume histograms after one, two, and three hours of simulation time have two different bins. An example of the histogram for later stages of the simulation is shown in Figure 39.

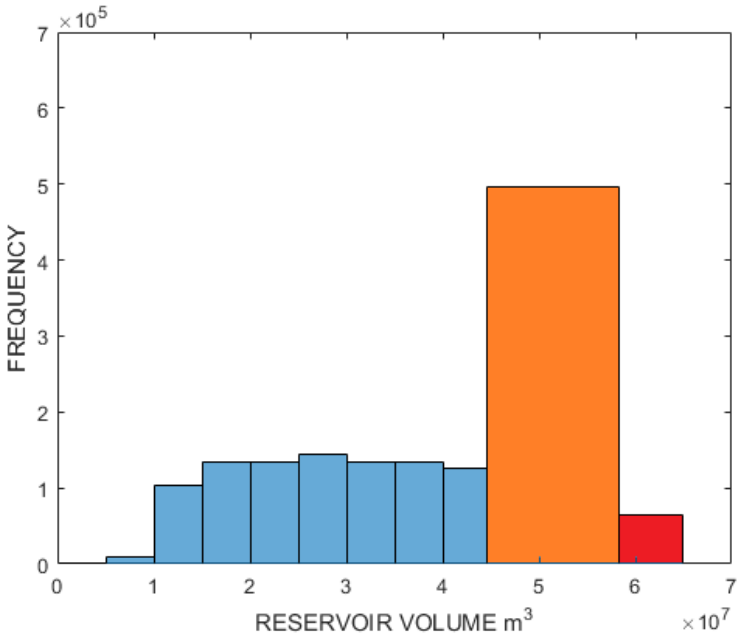

Figure 47. An example of reservoir volume histogram after 1, 2 or 3 hours of simulation time

The ninth bin from the 0-hour histogram has different width. New ninth bin ranges from 44,654,877 m^3 to 58,254,767 m^3. Those volume values correspond to free crest weirs (overflowing facilities) elevation and elevation of the top of the dam. This bin is in orange color. Therefore, the frequency of the reservoir volumes in the orange bin is equal to the number of simulations in which uncontrolled spilling occurred over the free crest weirs. This is the number of times H-2 hazard occurs in the selected scenario.

The tenth bin also has different width in later stages. The tenth bin is colored red and ranges from 58,254,767 m^3 to 65,000,000 m^3. Lower volume value corresponds to the elevation of the top of the dam. Therefore, the frequency of the reservoir volumes in the red bin is equal to the number of simulations in which the dam is overtopped, which is the H-1 hazard.

4.3.1. Scenario 1: Spillway operating gates (SPOG) closed

In this Scenario, SPOGs are malfunctioning and the spillways are completely closed. SPOGs were completely closed 1,482,624 times out of 17,791,488 combinations. This means that combinations of system variables resulted in SPOG being closed in 1,482,624 context rows. Figures 48 to 51 show changes in the reservoir volume through time.

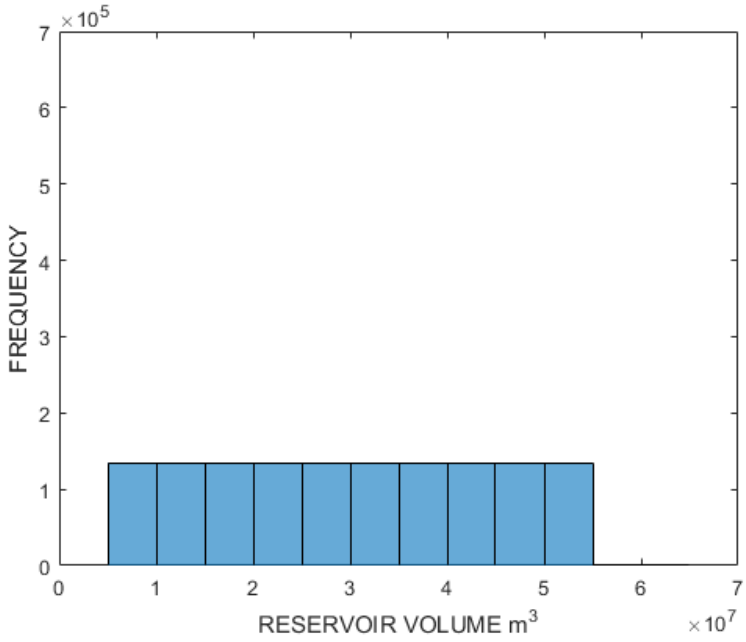

Figure 48. Cheakamus Dam case study Scenario 1: frequency histogram of the reservoir volume at the beginning of the simulation

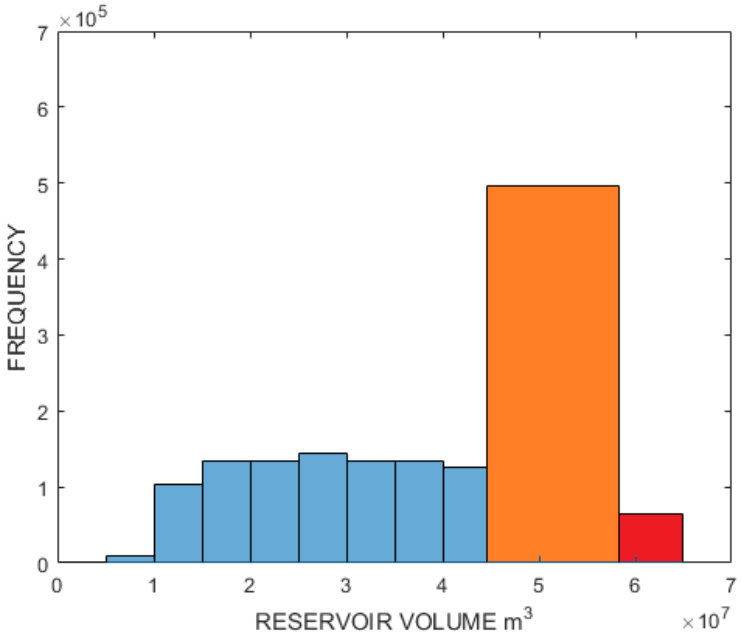

Figure 49. Cheakamus Dam case study Scenario 1: frequency histogram of the reservoir volume after 1 hour of the simulation

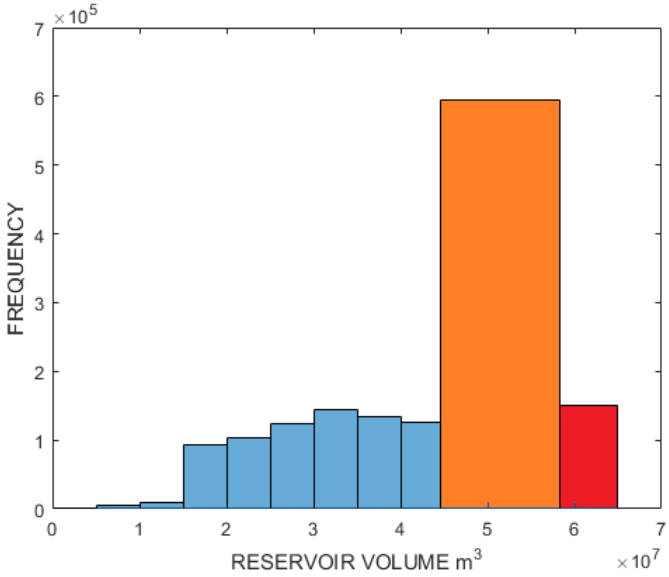

Figure 50. Cheakamus Dam case study Scenario 1: frequency histogram of the reservoir volume after 2 hours of the simulation

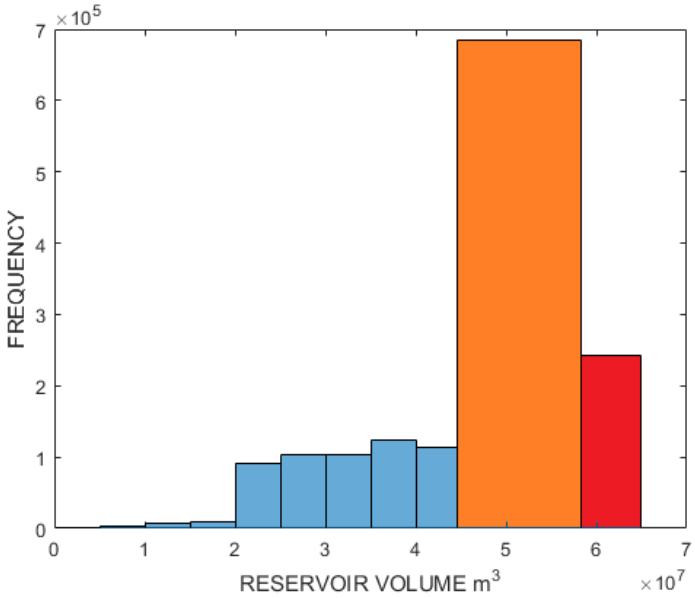

Figure 51. Cheakamus Dam case study Scenario 1: frequency histogram of the reservoir volume after 3 hours of the simulation

It is evident that this is a very dangerous scenario for dam safety. The spillway can release a large amount of water (when completely opened approximately 1600 m^3/s, according to spillway discharge curve). Uncontrolled spill over free crest weirs and through emergency ports, after 3 hours, is happening in approximately 700,000 cases (variable combinations, context "rows") out of 1,482,624 combinations analyzed. Additionally, the dam overtopping frequencies are substantial. Without the main discharge facilities, most of the water will spill over overflow facilities and will overtop the dam. The situation is only getting worse as the simulation progresses with more reservoir volume values ending in the orange and red bins.

4.3.2. Scenario 2: SPOGs open and stuck at 1 meter

In this SThcenario, SPOGs are malfunctioning and the spillways are partially open and stuck at 1 meter from the spillway sill. SPOGs were stuck at 1 meter 164,736 times out of 17,791,488 combinations. This means that combinations of system variables resulted in SPOG being stuck at 1 meter in 164,736 context rows. Figures 52-55 show changes in the reservoir volume through time.

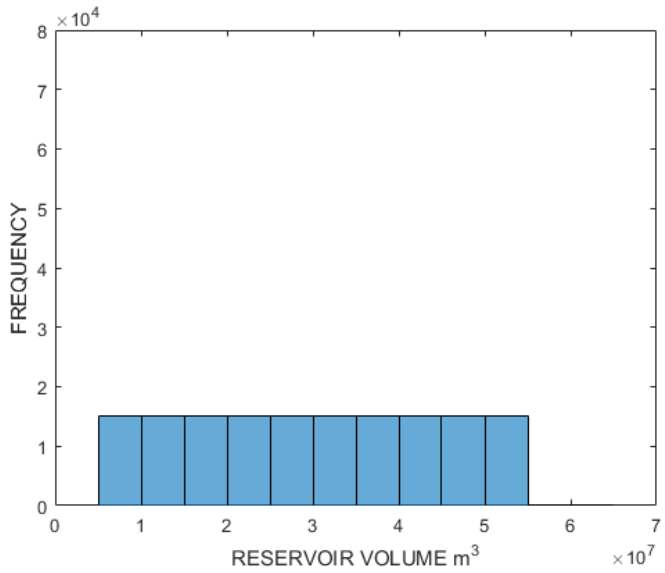

Figure 52. Cheakamus dam case study Scenario 2: frequency histogram of the reservoir volume at the beginning of the simulation

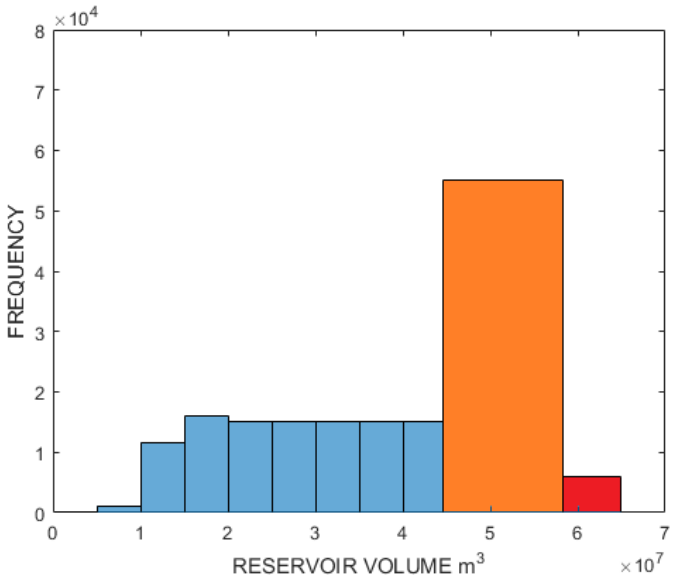

Figure 53. Cheakamus dam case study Scenario 2: frequency histogram of the reservoir volume after 1 hour of the simulation

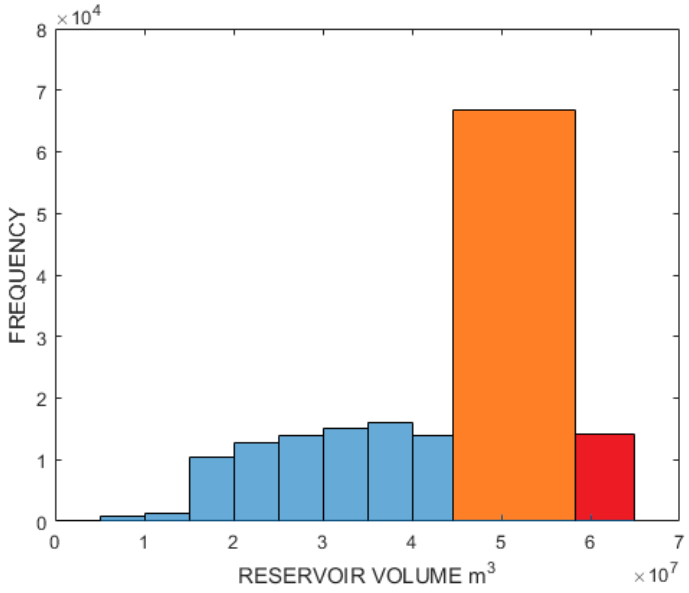

Figure 54. Cheakamus dam case study Scenario 2: frequency histogram of the reservoir volume after 2 hours of the simulation

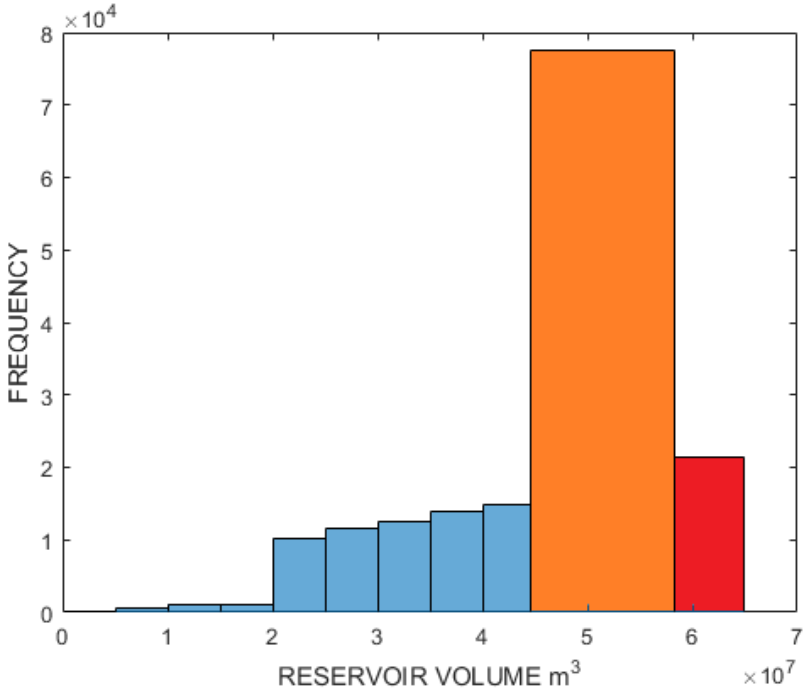

Figure 55. Cheakamus dam case study Scenario 2: frequency histogram of the reservoir volume after 3 hours of the simulation

Not as bad as Scenario 1, but uncontrolled spills and overtopping are still occurring. Uncontrolled spill over free crest weirs and through emergency ports, after 3 hours, is happening in approximately 78,000 cases (variable combinations, context “rows”) out of 164,736 combinations analyzed. Additionally, the dam overtopping frequencies are still substantial. Slightly raised spillway gates do not mitigate the overtopping and uncontrolled spills. The frequency of reservoir volume values ending in the “orange” and “red” ranges is increasing after each hour.

4.3.3. Scenario 3: SPOGs open and stuck at 3 meters

In this scenario, SPOGs are malfunctioning and the spillways are partially open and stuck at 3 meters from the spillway sill. SPOGs were stuck at 3 meters 164,736 times out of 17,791,488 combinations. Figures 56 to 59 show changes in the reservoir volume through time.

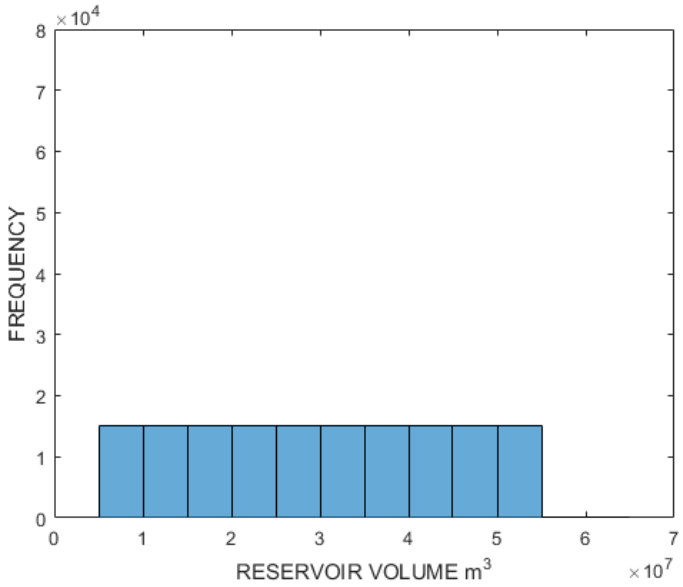

Figure 56. Cheakamus dam case study Scenario 3: frequency histogram of the reservoir volume at the beginning of the simulation

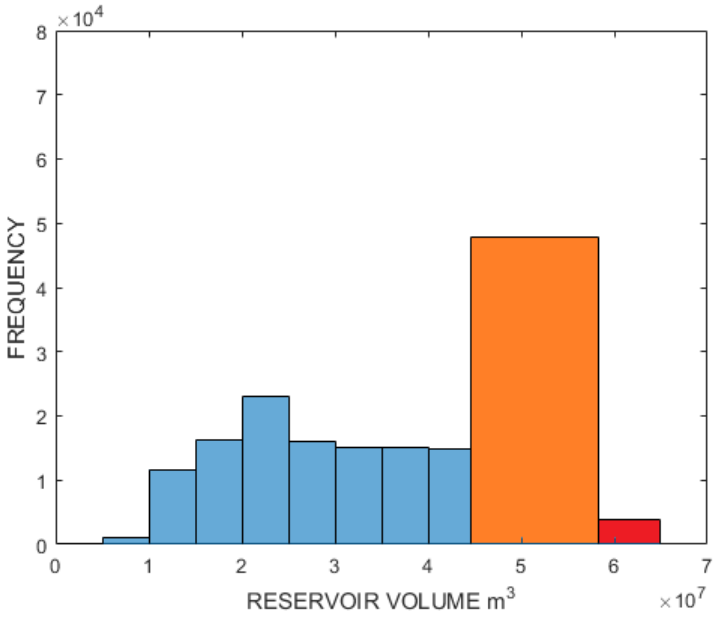

Figure 57. Cheakamus dam case study Scenario 3: frequency histogram of the reservoir volume after 1 hour of the simulation

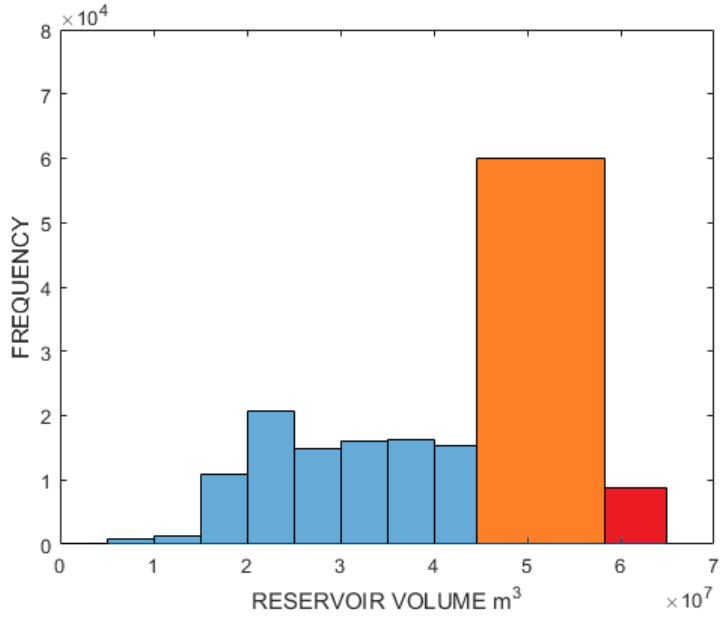

Figure 58. Cheakamus dam case study Scenario 3: frequency histogram of the reservoir volume after 2 hours of the simulation

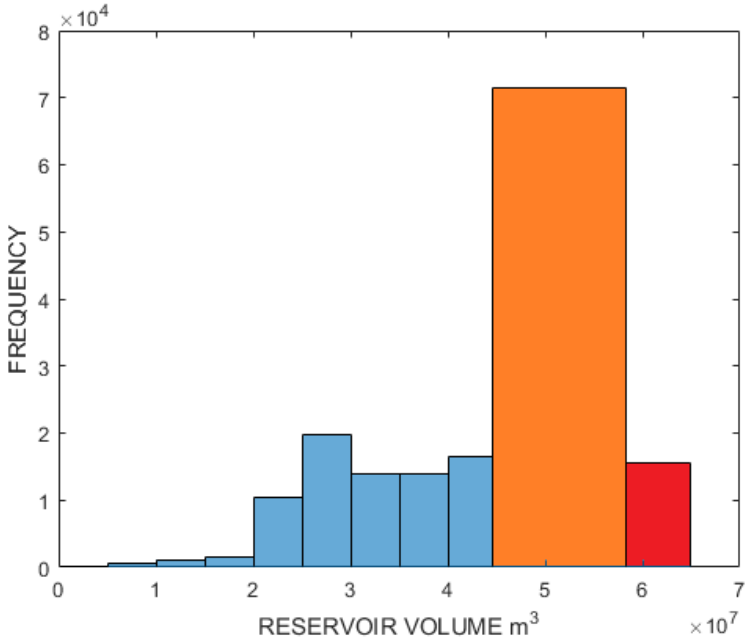

Figure 59. Cheakamus dam case study Scenario 3: frequency histogram of the reservoir volume after 3 hours of the simulation

Uncontrolled spills and overtopping are still occurring. Uncontrolled spill over free crest weirs and through emergency ports, after 3 hours, is occurring in approximately 71,000 cases (variable combinations, context “rows”) out of 164,736 combinations analyzed. Additionally, the dam overtopping frequencies are still substantial, but less than in Scenario 2. Additionally, a slow shift of the reservoir volumes to the lower ranges is noticeable.

4.3.4. Scenario 4: SPOGs open and stuck at 5 meters

In this Scenario, SPOGs are malfunctioning and the spillways are partially open and stuck at 5 meters from the spillway sill. SPOGs were stuck at 5 meters 164,736 times out of 17,791,488 combinations. Figures 60 to 64 show changes in the reservoir volume through time.

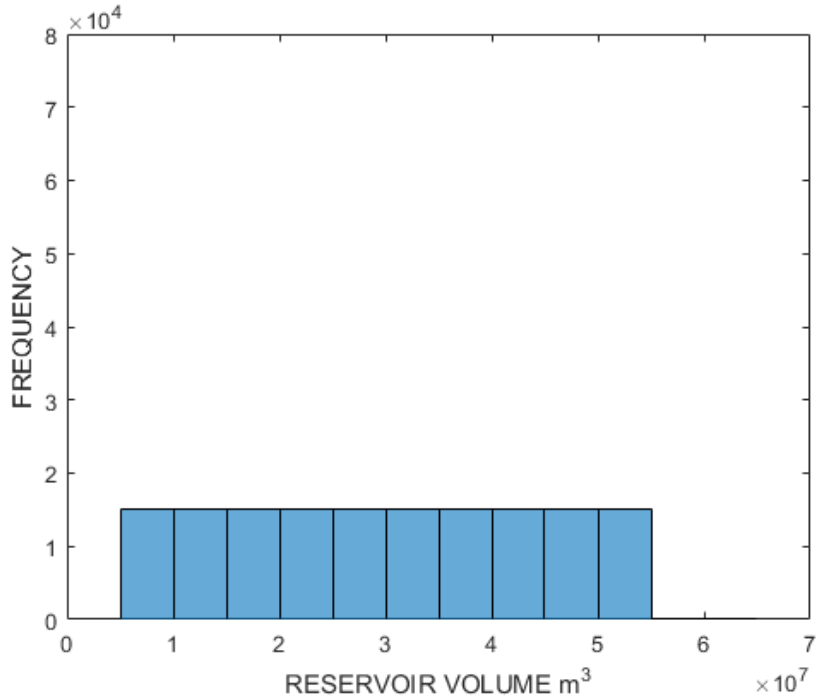

Figure 60. Cheakamus dam case study Scenario 4: frequency histogram of the reservoir volume at the beginning of the simulation

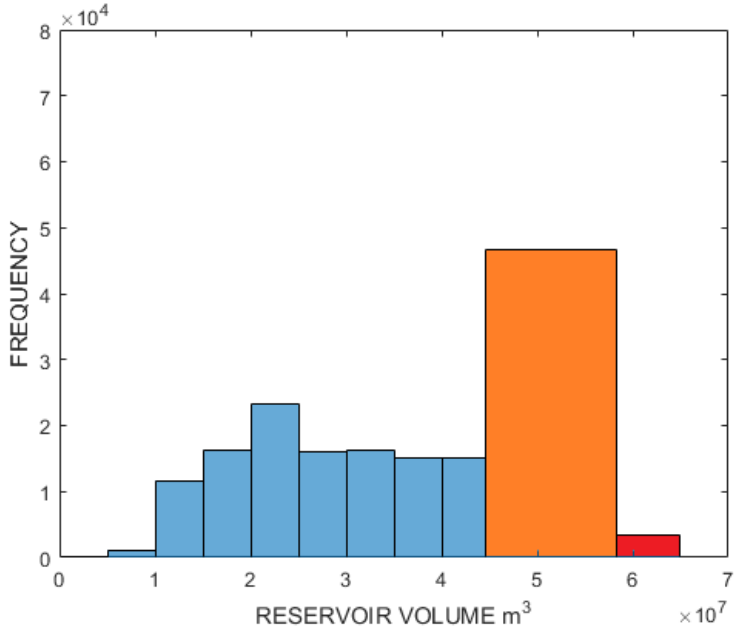

Figure 61. Cheakamus dam case study Scenario 4: frequency histogram of the reservoir volume after 1 hour of the simulation

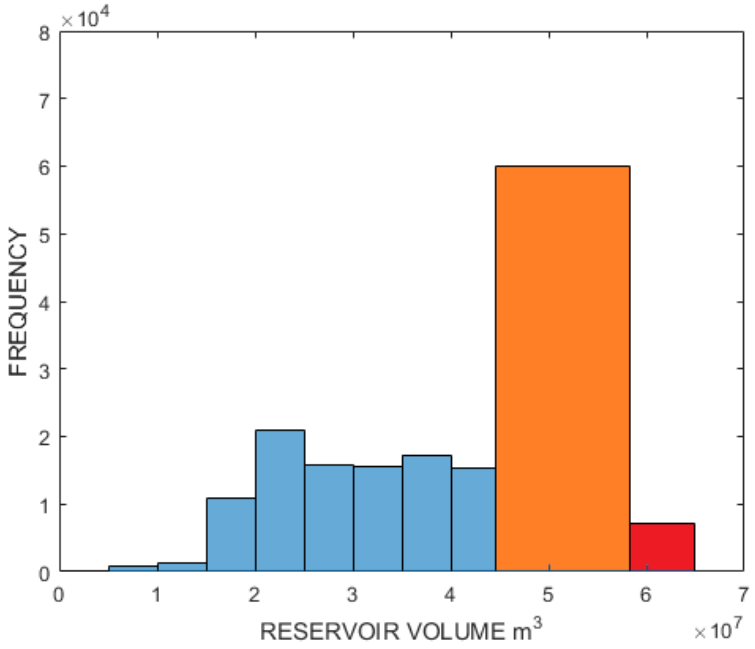

Figure 62. Cheakamus dam case study Scenario 4: frequency histogram of the reservoir volume after 2 hours of the simulation

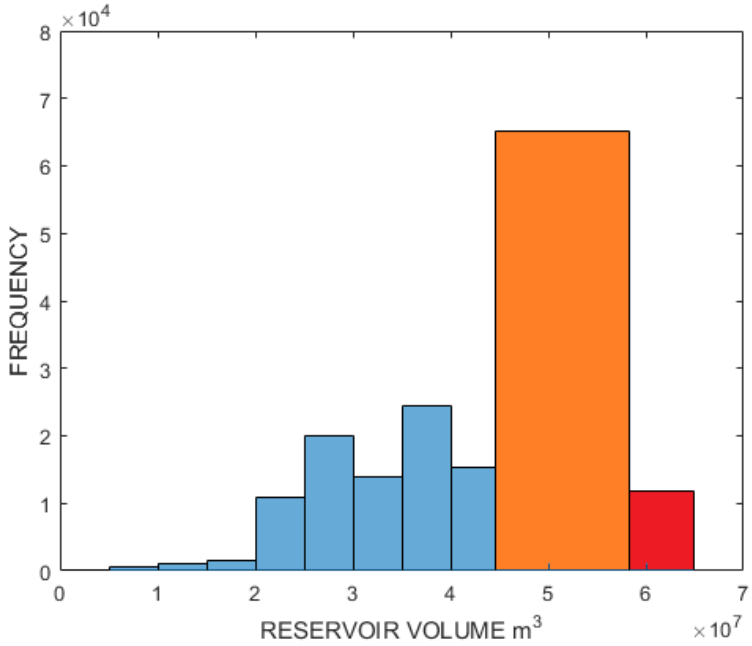

Figure 63. Cheakamus dam case study Scenario 4: frequency histogram of the reservoir volume after 3 hours of the simulation

Improvements compared to two previous scenarios are noticeable, but uncontrolled spills and overtopping are still occurring. Uncontrolled spill over free crest weirs and through emergency ports, after 3 hours, is occurring in approximately 67,000 cases out of 164,736 combinations analyzed. Additionally, the dam overtopping frequencies are still substantial, but less than in Scenario 3. Additionally, the slow shift of the reservoir volumes to the lower ranges is noticeable.

4.3.5. Scenario 5: Low-level outlet gate (LLOG) not functioning

In this Scenario, LLOG is malfunctioning and is completely closed. LLOG was completely closed 1,482,624 times out of 17,791,488 combinations. Figures 64 to 68 show changes in the reservoir volume through time.

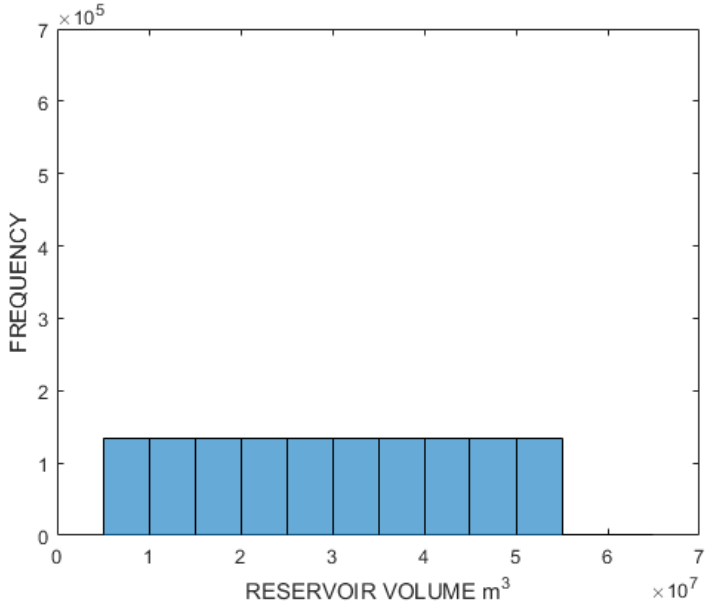

Figure 64. Cheakamus dam case study Scenario 5: frequency histogram of the reservoir volume at the beginning of the simulation

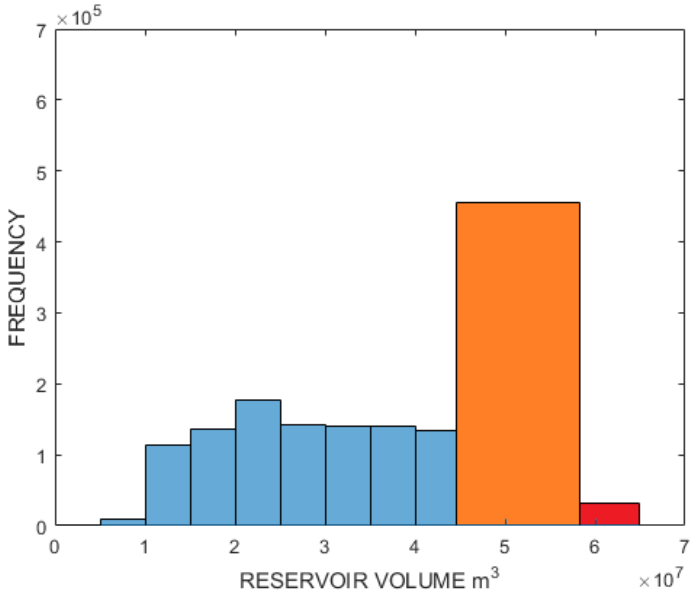

Figure 65. Cheakamus dam case study Scenario 5: frequency histogram of the reservoir volume after 1 hour of the simulation

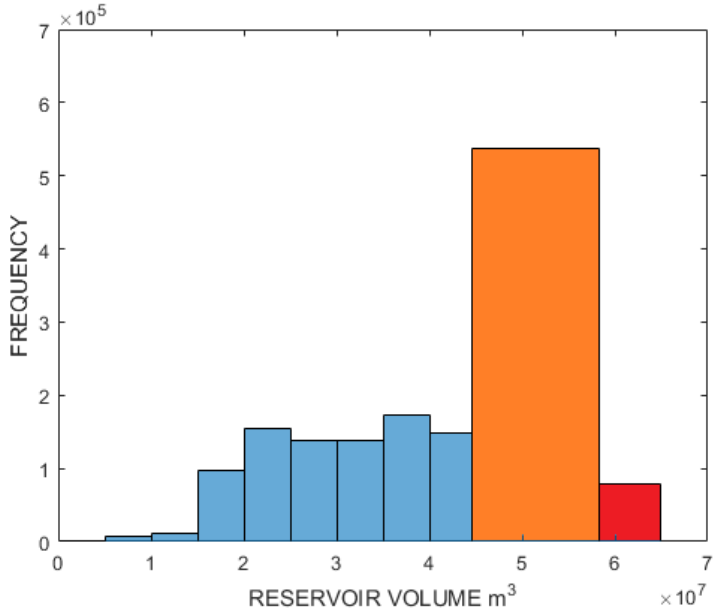

Figure 66. Cheakamus dam case study Scenario 5: frequency histogram of the reservoir volume after 2 hours of the simulation

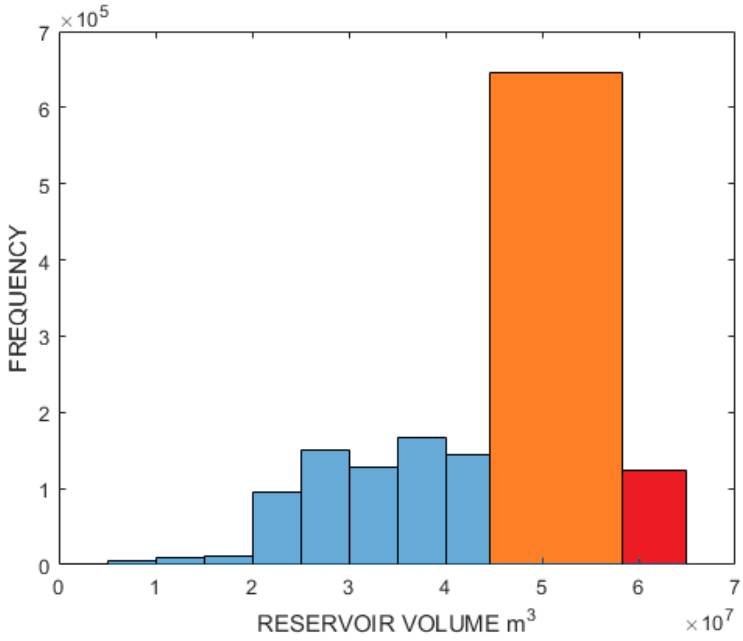

Figure 67. Cheakamus dam case study Scenario 5: frequency histogram of the reservoir volume after 3 hours of the simulation

The results are relatively close to Scenario 1 and there are two reasons for it: (1) four out of thirteen inflow values are over the updated probable maximum flood value, and (2) in order to investigate all of the possible system states, three out of eleven starting reservoir volume (5,000,000-65,000,000 m^3) values are over the value that corresponds to the elevation of the overflow facilities. Spillway gates cannot be controlled and used when they are overtopped, which explains the results. Uncontrolled spill over free crest weirs and through emergency ports, after 3 hours, is happening in approximately 650,000 cases (variable combinations, context "rows") out of 1,482,624 combinations analyzed. Additionally, the dam overtopping frequencies are substantial.

4.3.6. Scenario 6: Power intake gate (PG) is not functioning

In this Scenario, PG is malfunctioning and is completely closed. PG was completely closed 1,482,624 times out of 17,791,488 combinations. Figures 68 to 71 show changes in the reservoir volume through time.

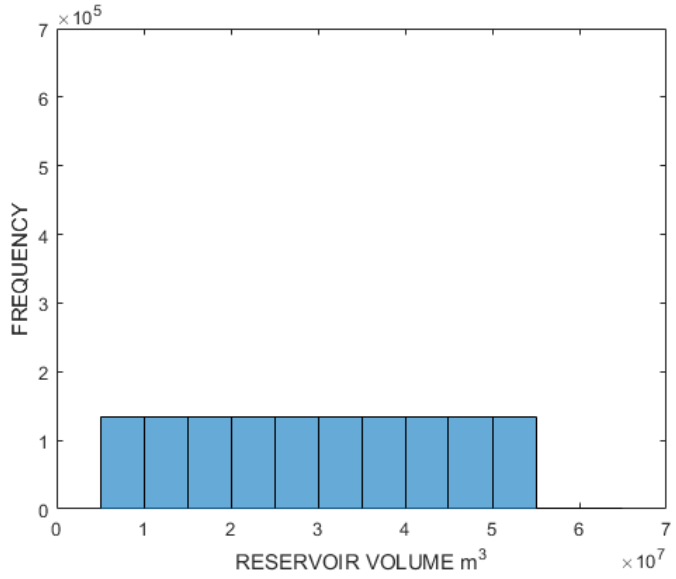

Figure 68. Cheakamus dam case study Scenario 6: frequency histogram of the reservoir volume at the beginning of the simulation

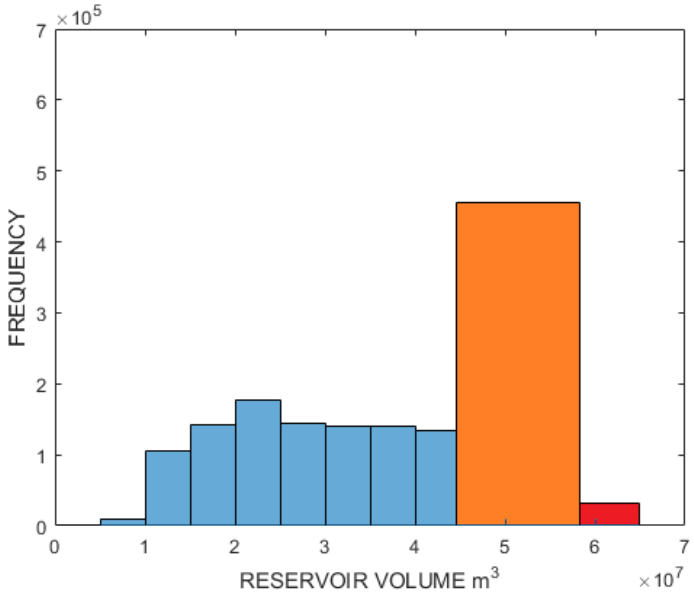

Figure 69. Cheakamus dam case study Scenario 6: frequency histogram of the reservoir volume after 1 hour of the simulation

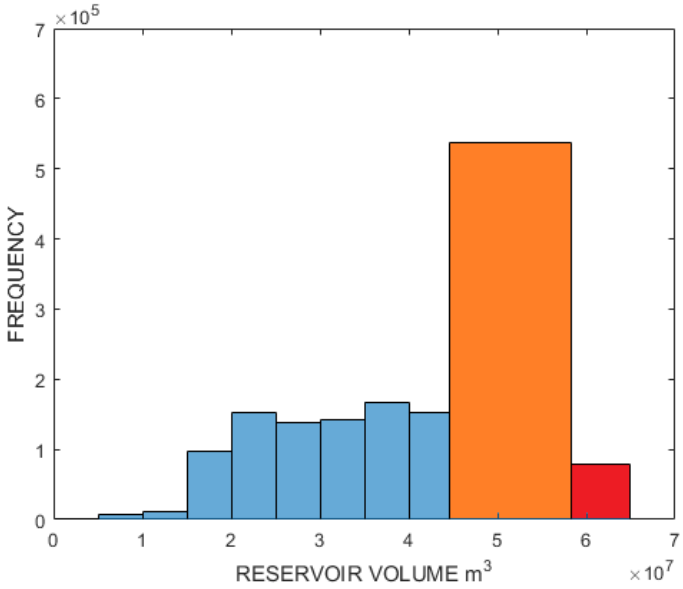

Figure 70. Cheakamus dam case study Scenario 6: frequency histogram of the reservoir volume after 2 hours of the simulation

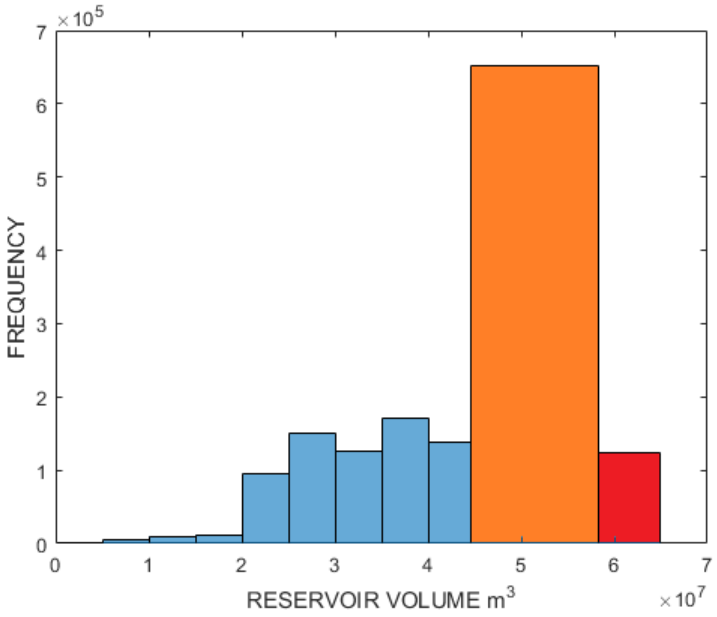

Figure 71. Cheakamus dam case study Scenario 6: frequency histogram of the reservoir volume after 3 hours of the simulation

The results are similar to Scenario 6 since the difference between power intake and maximum LLOG discharge (65 m^3/s and approximately 200 m^3/s) is not that relevant compared to the probable maximum flood. Uncontrolled spill over free crest weirs and through emergency ports, after 3 hours, is happening in approximately 660,000 cases out of 1,482,624 combinations analyzed. Additionally, the dam overtopping frequencies are substantial.

4.3.7. Probability distribution of failure states

Frequency histograms are transformed into probability distribution graphs of failure states. The probability of each bin is calculated by dividing each bin frequency value by the total number of combinations covered by each scenario. In order to better assess the changes through time, a 3D surface is created from hourly histogram data for each scenario. Figures 72 to 77 show probability distribution graphs of reservoir volume for each scenario. Notice that Y and X axis scale are not the same for each graph.

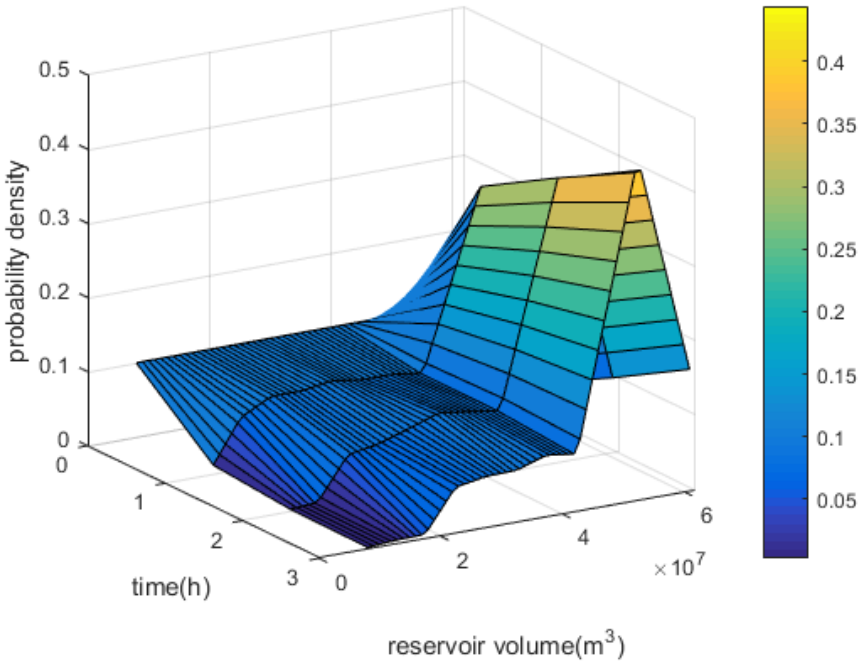

Figure 72. Cheakamus Dam case study Scenario 1 probability distribution through time

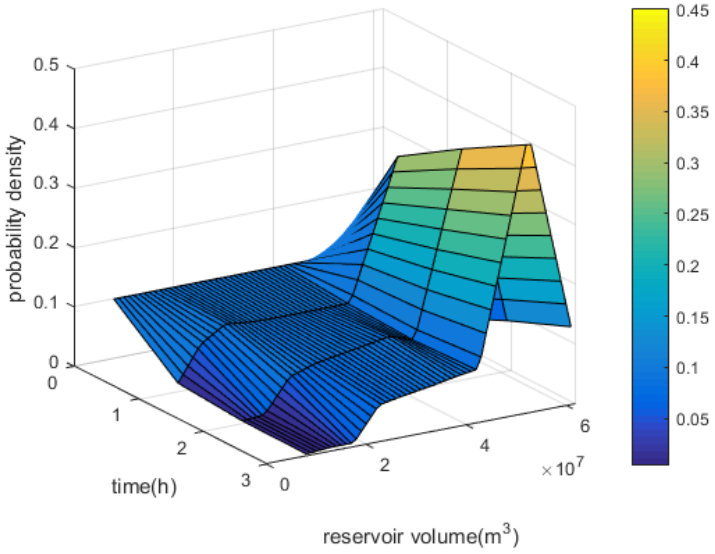

Figure 73. Cheakamus Dam case study Scenario 2 probability distribution through time

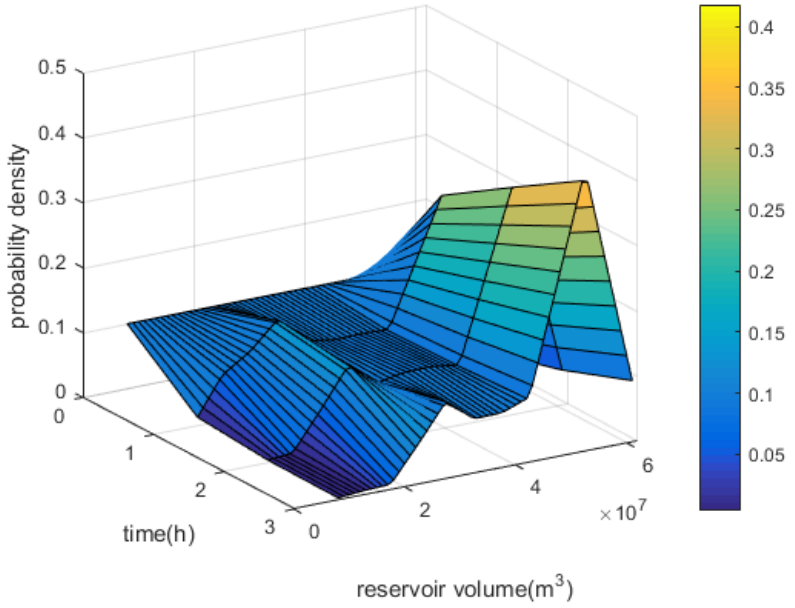

Figure 74. Cheakamus Dam case study Scenario 3 probability distribution through time

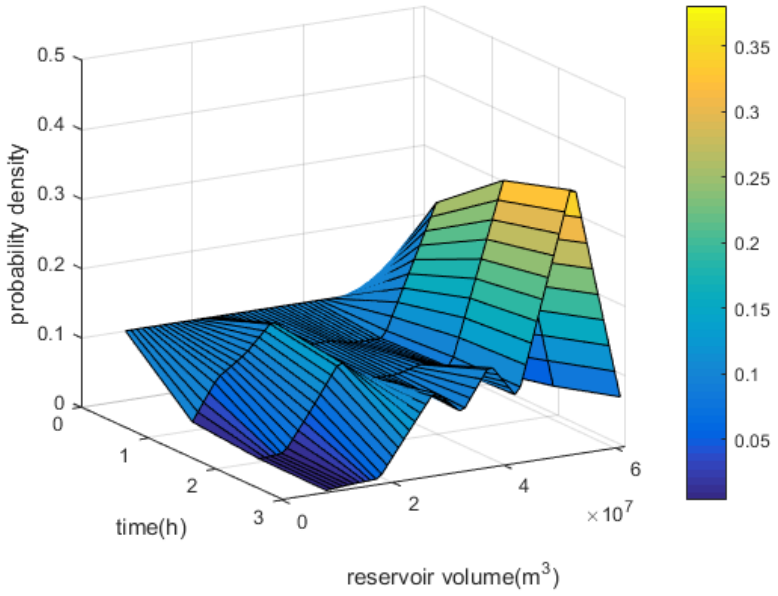

Figure 75. Cheakamus Dam case study Scenario 4 probability distribution through time

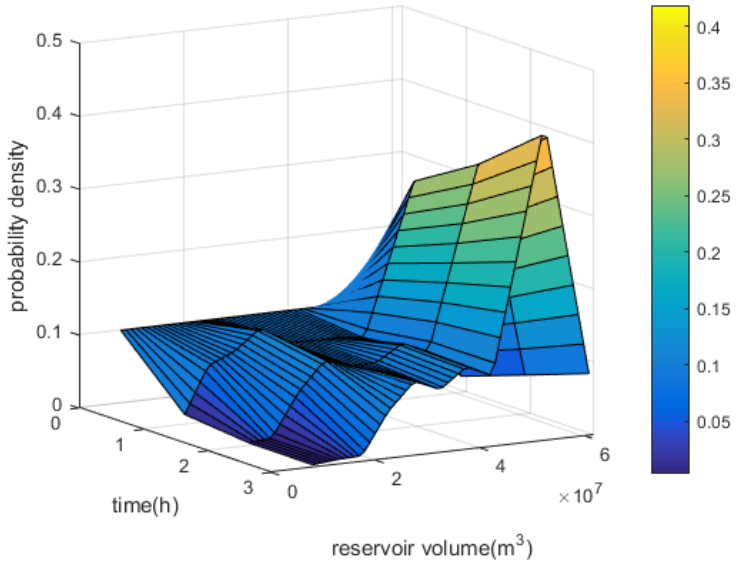

Figure 76. Cheakamus Dam case study Scenario 5 probability distribution through time

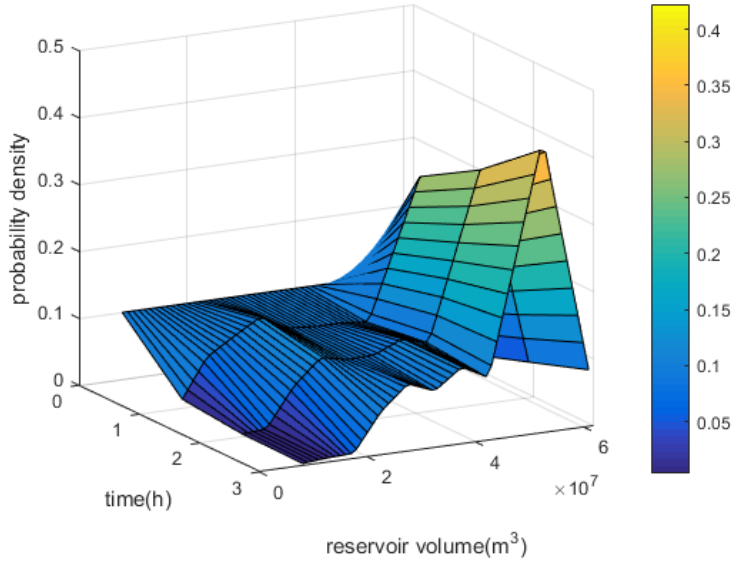

Figure 77. Cheakamus Dam case study Scenario 6 probability distribution through time

These surfaces should be considered with the previous histograms. These surfaces are created from mesh points. Mesh point M have x, y and z coordinates, where x coordinate represents the time passed since the beginning of the simulation, y represents the reservoir volume value, and z is the probability of reservoir being between two values, or belonging to one bin. Or in mathematical form:

$$M=(x,y,z) \tag{4.48}$$

where,

$$x \in X = \{0,1,2,3\} \tag{4.49}$$

$$y \in Y = \{7.5, 12.5, 17.5, 22.5, 27.5, 32.5, 37.5, 42.5, 52.5, 61\} * 10^6 \tag{4.50}$$

$$z \in Z = [0, 1] \tag{4.51}$$

Notice that y coordinates are bin midpoints. This way if we pinpoint a mesh point on the surface, we can determine the probability of reservoir being in a particular state after a certain amount of time. This is just an alternative way of presenting the hourly histogram, with a probability of reservoir volume belonging to each bin. The surface "temperature" (shown in different colors) represents the probability, with dark blue being zero and yellow approximately 0.42.

5. Conclusions and Future Work

This research addressed the main issues and disadvantages of traditional dam systems risk analysis methods. Traditional analysis methods place emphasis on failures opposed to control flaws and assume linear progression of events. Traditional methods cannot account for the multiple feedback

loops in the systems and disregard interdependencies of system components. In the traditional analysis, human behaviour is usually oversimplified.

Cheakamus dam case study illustrates the need for a systems approach to reservoir infrastructure risk analysis. Many hazardous states are the product of unusual combinations of usual events. The results illustrate that extreme events are not the only source of the hazardous states. System structure, description using identified system components and their interdependencies, together with the identification of the control flaws is of primary importance for the analysis of system safety.

Traditional analysis methods' issues were approached with a systems approach to dam systems. System dynamics simulation is used as a method to implement System Theoretic Process Analysis (STPA). STPA is a hazard analysis method that investigates the control actions impact on the system. Fuzzy inference system is used to model the controller's decision – making and drive the STPA process.

Component interdependencies, system feedbacks, the nonlinear progression of events, and event dependencies are addressed using system dynamics simulation. Complex human behaviour and decision making are addressed using fuzzy inference systems. Control actions and control flaws are addressed using STPA. Dam systems are complex systems with many components and implementing all of them in a system dynamics model is a challenge. Uncertain hydrologic and hydraulic data, lack of dam system data, or clear connections between the system components can negatively influence systems approach to risk analysis. The scope and the size of the modelled system are another issue. For example, a road that is the only way to reach the dam might be

unusable, preventing the controller from reaching the dam and performing the control action. Looking at the Sayano – Shushenskaya accident, many social and economic factors must be taken into consideration, such as the company privatization, focus on financial profit, and shady maintenance contracts. These aspects are also hard to cover and implement while designing the system model.

The developed methodology is applied to a case study system based on the BC Hydro's Cheakamus Dam in British Columbia. Hydrologic, hydraulic, mechanical and structural data provided by BC Hydro is used in the study. Hydraulic capabilities of the spillway and hydrologic data is used to develop the fuzzy inference system. Python programming language and MATLAB software are used for automating the development of the control flaws and hazardous system states. Control decisions were implemented in any context of the investigated system. Hazardous combinations of control actions and system states are separated. Additionally, several failure scenarios are used to illustrate the results of methodology implementation.

Future work will consist of adding more starting values for the system variables, implementing more components, improving the fuzzy inference system, and developing fuzzy inference system for control of all the outflow gates. Implementation of more variables will create even more interdependencies and therefore describe each system in the control loop more accurately.

One of the future goals is the development of a generalized dam system model that can be applied to various dam types, dam purposes, and all possible dam components.

The research results illustrate clearly how complex the reservoir infrastructure systems are and what is the utility of the proposed analysis method. It is important to note that in spite our best

efforts, there will always be an unforeseen external disturbance that cannot be easily incorporated into the model. The results of the case study illustrate how sensitive dam systems are to losing the ability to operate main spillway gates. Control actions can have dire consequences based on the context in which they are issued.

6. References

Åström, K. J., & Murray, R. M. (2008). *Feedback Systems: An Introduction for Scientists and Engineers*. *Control And Cybernetics* (Vol. 36). Princeton, NJ: Princeton University Press. http://doi.org/10.1086/596297

Bagis, A., & Karaboga, D. (2004). Artificial neural networks and fuzzy logic based control of spillway gates of dams. *Hydrological Processes*, *18*, 2485–2501. http://doi.org/10.1002/hyp.1477

Baecher, G., Ascila, R., and Hartford, D. N. D. (2013). "Hydropower and dam safety." *STAMP/STPA Workshop*, Cambridge: 1-25

De Dianous, V., Fiévez, C. (2006). ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials*. http://doi.org/10.1016/j.jhazmat.2005.07.010

Dulac, N. (2007). "A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems." *PhD Thesis*, Massachusetts Institute of Technology, Cambridge. pp 5-10

Ericson, C. (1999). "Fault Tree Analysis – A History". *Proceedings of the 17th International Systems Safety Conference.* (from

http://www.relken.com/sites/default/files/Seminal%20Documents/ericson-fta-history.pdf, accessed last time on 28/08/2016.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., & Veitch, B. (2013). Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. *Process Safety and Environmental Protection*. http://doi.org/10.1016/j.psep.2011.08.010

Hakobyan, A., Aldemir, T., Denning, R., Dunagan, S., Kunsman, D., Rutt, B., & Catalyurek, U. (2008). Dynamic generation of accident progression event trees. *Nuclear Engineering and Design*. http://doi.org/10.1016/j.nucengdes.2008.08.005

Hartford, D. N. D., and Baecher, G. B. (2004). *Risk and Uncertainty in Dam Safety*. Thomas Telford, London, 5-100.

Karanki, D. R., Kim, T. W., & Dang, V. N. (2015). A dynamic event tree informed approach to probabilistic accident sequence modeling: Dynamics and variabilities in medium LOCA. *Reliability Engineering and System Safety*. http://doi.org/10.1016/j.ress.2015.04.011

Komey, A., Deng, Q., Baecher, G. B., Zielinski, P. A., & Atkinson, T. (2015). Systems Reliability of Flow Control in Dam Safety. In *12th International Conference on Application of Statistics and Probability in Civil Engineering, ICASP12* (pp. 1–8). Vancouver, Canada.

Kong, G. (2013). *Generation Operating Order*. (Cheakamus Project Report CMS 4G-25 v.2.2) Vancouver, British Columbia: BC Hydro

Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. *Vasa, The MIT PRESS*, Cambridge, Massachusetts, 211-251

Mamdani, E. (1974). "Application of Fuzzy Algorithms for Control of Simple Dynamic Plant." *IEEE 212*, 1585–1588.

Markowski, A. S., & Kotynia, A. (2011). "Bow-tie" model in layer of protection analysis. *Process Safety and Environmental Protection*, (89), 205–213. http://doi.org/10.1016/j.psep.2011.04.005

Matheson, C.D. (2005). *Cheakamus Project Water Use Plan*. BC Hydro, Vancouver, British Columbia.

Mathworks®, (2015). *Fuzzy Logic Toolbox™: User's Guide (R2015b).* Retrieved February 8, 2016, from http://www.mathworks.com/help/pdf_doc/fuzzy/fuzzy.pdf accessed last time on 28/08/2016.

Mathworks®, (2015) MATLAB® R2015b. http://www.mathworks.com/downloads/ accessed last time on 28/08/2016.

Mathworks®, (2015). *MATLAB® Primer (R2015b).* Retrieved February 8, 2016, from http://www.mathworks.com/help/pdf_doc/matlab/getstart.pdf

Oswell, M. T. (2009). *Operation, Maintenance and Surveillance Manual for Dam Safety* (Report No. OMSCMS), Vancouver, British Columbia: BC Hydro.

Python.org. (2015) Python 3.4.4 Release https://www.python.org/downloads/release/python-

344/ (accessed last time on 21/07/2016)

Python.org. (2015) History and Licence 3.4.4 Release https://docs.python.org/3.4/license.html (accessed last time on 21/07/2016)

Regan, P. J. (2010). "Dams as systems - A holistic approach to dam safety." *USSD Annual Meeting and Conference*, Sacramento, California, 1307–1340.

Ross, T. J. (2010). *Fuzzy logic with engineering applications*. John Wiley & Sons, Ltd., Chichester, West Sussex, United Kingdom, pp. 1-21

Simonovic, S. P. (2009). *Managing Water Resources: Methods and Tools for a Systems Approach*. Earthscan, London, UK, http://www.vodoprivreda.net/wp-content/uploads/2014/08/managing.pdf (last accessed on 21/7/2016)

Simonovic, S. P. (2009). *Managing Water Resources*. London: UNESCO, pp 297-421

Simonovic, S. P., and Peck, A. (2013). "Dynamic Resilience to Climate Change Caused Natural Disasters in Coastal Megacities Quantification Framework." *British Journal of Environment and Climate Change*, 3(3), 378–401.

Teodorović, D., and Šelmić, M. (2012). *Računarska inteligencija u saobraćaju* [Transportation Computational Intelligence], University of Belgrade, Faculty of Transport and Traffic Engineering, Belgrade, Serbia.

Thomas, J. (2012). *Extending and Automating a Systems- Theoretic Hazard Analysis for Requirements Generation and Analysis* (Sandia Report, Report No SAND2012-4080).

Albuquerque, New Mexico.

UNISDR. (2009). "UNISDR Terminology on Disaster Risk Reduction." *International Strategy for Disaster Reduction (ISDR),* DOI: 978-600-6937-11-3 1–30. http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf , last accessed on 21/7/2016

Vucetic, D., and Simonovic, S. P. (2011). *Water resources decision making under uncertainty (Report No: 073).* London, Ontario, Canada. http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1035&context=wrrr (last accessed on 21/7/2016)

Wood, S. (2009). *Lower Mainland Generation,* (Coastal Operations, Report No LOO 3G-CMS-06) ,Vancouver, British Columbia: BC Hydro

Zadeh, L. A. (1973). "Outline of a new approach to the analysis of complex systems and decision processes." *IEEE Trans. Systems, Man and Cybernetics*, 3: 28–44.

Zimmerman, H. J. (2001). *Fuzzy set theory and its applications - Fourth Edition*. Kluwer, Boston, 2nd ed., 1993, pp 1-23

Appendix A: Cheakamus Dam Case Study FIS Rule Base

CWL is the current water level or the reservoir elevation. GP is the gate position.

Complete list of the fuzzy rules:

1. If (CWL is 367) and (INFLOW is 100) then (GP is 1) (1)
2. If (CWL is 367) and (INFLOW is 200) then (GP is 1) (1)
3. If (CWL is 367) and (INFLOW is 300) then (GP is 1) (1)
4. If (CWL is 367) and (INFLOW is 400) then (GP is 1) (1)
5. If (CWL is 367) and (INFLOW is 500) then (GP is 1) (1)
6. If (CWL is 367) and (INFLOW is 600) then (GP is 1) (1)
7. If (CWL is 367) and (INFLOW is 700) then (GP is 1) (1)
8. If (CWL is 367) and (INFLOW is 800) then (GP is 1) (1)
9. If (CWL is 367) and (INFLOW is 900) then (GP is 1) (1)
10. If (CWL is 367) and (INFLOW is 1000) then (GP is 1) (1)
11. If (CWL is 367) and (INFLOW is 1100) then (GP is 1) (1)
12. If (CWL is 367) and (INFLOW is 1200) then (GP is 1) (1)
13. If (CWL is 367) and (INFLOW is 1300) then (GP is 1) (1)
14. If (CWL is 367) and (INFLOW is 1400) then (GP is 1) (1)
15. If (CWL is 367) and (INFLOW is 1500) then (GP is 1) (1)
16. If (CWL is 367) and (INFLOW is 1600) then (GP is 1) (1)
17. If (CWL is 371) and (INFLOW is 100) then (GP is 1) (1)
18. If (CWL is 371) and (INFLOW is 200) then (GP is 1) (1)
19. If (CWL is 371) and (INFLOW is 300) then (GP is 2) (1)
20. If (CWL is 371) and (INFLOW is 400) then (GP is 2) (1)
21. If (CWL is 371) and (INFLOW is 500) then (GP is 2) (1)
22. If (CWL is 371) and (INFLOW is 600) then (GP is 2) (1)
23. If (CWL is 371) and (INFLOW is 700) then (GP is 2) (1)
24. If (CWL is 371) and (INFLOW is 800) then (GP is 2) (1)

25. If (CWL is 371) and (INFLOW is 900) then (GP is 2) (1)
26. If (CWL is 371) and (INFLOW is 1000) then (GP is 2) (1)
27. If (CWL is 371) and (INFLOW is 1100) then (GP is 2) (1)
28. If (CWL is 371) and (INFLOW is 1200) then (GP is 2) (1)
29. If (CWL is 371) and (INFLOW is 1300) then (GP is 2) (1)
30. If (CWL is 371) and (INFLOW is 1400) then (GP is 2) (1)
31. If (CWL is 371) and (INFLOW is 1500) then (GP is 2) (1)
32. If (CWL is 371) and (INFLOW is 1600) then (GP is 2) (1)
33. If (CWL is 372) and (INFLOW is 100) then (GP is 1) (1)
34. If (CWL is 372) and (INFLOW is 200) then (GP is 1) (1)
35. If (CWL is 372) and (INFLOW is 300) then (GP is 2) (1)
36. If (CWL is 372) and (INFLOW is 400) then (GP is 3) (1)
37. If (CWL is 372) and (INFLOW is 500) then (GP is 3) (1)
38. If (CWL is 372) and (INFLOW is 600) then (GP is 3) (1)
39. If (CWL is 372) and (INFLOW is 700) then (GP is 3) (1)
40. If (CWL is 372) and (INFLOW is 800) then (GP is 3) (1)
41. If (CWL is 372) and (INFLOW is 900) then (GP is 3) (1)
42. If (CWL is 372) and (INFLOW is 1000) then (GP is 3) (1)
43. If (CWL is 372) and (INFLOW is 1100) then (GP is 3) (1)
44. If (CWL is 372) and (INFLOW is 1200) then (GP is 3) (1)
45. If (CWL is 372) and (INFLOW is 1300) then (GP is 3) (1)
46. If (CWL is 372) and (INFLOW is 1400) then (GP is 3) (1)
47. If (CWL is 372) and (INFLOW is 1500) then (GP is 3) (1)
48. If (CWL is 372) and (INFLOW is 1600) then (GP is 3) (1)
49. If (CWL is 373) and (INFLOW is 100) then (GP is 1) (1)
50. If (CWL is 373) and (INFLOW is 200) then (GP is 1) (1)
51. If (CWL is 373) and (INFLOW is 300) then (GP is 2) (1)
52. If (CWL is 373) and (INFLOW is 400) then (GP is 3) (1)
53. If (CWL is 373) and (INFLOW is 500) then (GP is 4) (1)
54. If (CWL is 373) and (INFLOW is 600) then (GP is 4) (1)
55. If (CWL is 373) and (INFLOW is 700) then (GP is 4) (1)
56. If (CWL is 373) and (INFLOW is 800) then (GP is 4) (1)
57. If (CWL is 373) and (INFLOW is 900) then (GP is 4) (1)
58. If (CWL is 373) and (INFLOW is 1000) then (GP is 4) (1)
59. If (CWL is 373) and (INFLOW is 1100) then (GP is 4) (1)
60. If (CWL is 373) and (INFLOW is 1200) then (GP is 4) (1)
61. If (CWL is 373) and (INFLOW is 1300) then (GP is 4) (1)
62. If (CWL is 373) and (INFLOW is 1400) then (GP is 4) (1)
63. If (CWL is 373) and (INFLOW is 1500) then (GP is 4) (1)
64. If (CWL is 373) and (INFLOW is 1600) then (GP is 4) (1)
65. If (CWL is 374) and (INFLOW is 100) then (GP is 1) (1)
66. If (CWL is 374) and (INFLOW is 200) then (GP is 1) (1)
67. If (CWL is 374) and (INFLOW is 300) then (GP is 1) (1)
68. If (CWL is 374) and (INFLOW is 400) then (GP is 2) (1)
69. If (CWL is 374) and (INFLOW is 500) then (GP is 3) (1)
70. If (CWL is 374) and (INFLOW is 600) then (GP is 5) (1)
71. If (CWL is 374) and (INFLOW is 700) then (GP is 5) (1)
72. If (CWL is 374) and (INFLOW is 800) then (GP is 5) (1)

73. If (CWL is 374) and (INFLOW is 900) then (GP is 5) (1)
74. If (CWL is 374) and (INFLOW is 1000) then (GP is 5) (1)
75. If (CWL is 374) and (INFLOW is 1100) then (GP is 5) (1)
76. If (CWL is 374) and (INFLOW is 1200) then (GP is 5) (1)
77. If (CWL is 374) and (INFLOW is 1300) then (GP is 5) (1)
78. If (CWL is 374) and (INFLOW is 1400) then (GP is 5) (1)
79. If (CWL is 374) and (INFLOW is 1500) then (GP is 5) (1)
80. If (CWL is 374) and (INFLOW is 1600) then (GP is 5) (1)
81. If (CWL is 375) and (INFLOW is 100) then (GP is 1) (1)
82. If (CWL is 375) and (INFLOW is 200) then (GP is 1) (1)
83. If (CWL is 375) and (INFLOW is 300) then (GP is 1) (1)
84. If (CWL is 375) and (INFLOW is 400) then (GP is 2) (1)
85. If (CWL is 375) and (INFLOW is 500) then (GP is 3) (1)
86. If (CWL is 375) and (INFLOW is 600) then (GP is 4) (1)
87. If (CWL is 375) and (INFLOW is 700) then (GP is 5) (1)
88. If (CWL is 375) and (INFLOW is 800) then (GP is 6) (1)
89. If (CWL is 375) and (INFLOW is 900) then (GP is 6) (1)
90. If (CWL is 375) and (INFLOW is 1000) then (GP is 6) (1)
91. If (CWL is 375) and (INFLOW is 1100) then (GP is 6) (1)
92. If (CWL is 375) and (INFLOW is 1200) then (GP is 6) (1)
93. If (CWL is 375) and (INFLOW is 1300) then (GP is 6) (1)
94. If (CWL is 375) and (INFLOW is 1400) then (GP is 6) (1)
95. If (CWL is 375) and (INFLOW is 1500) then (GP is 6) (1)
96. If (CWL is 375) and (INFLOW is 1600) then (GP is 6) (1)

97. If (CWL is 376) and (INFLOW is 100) then (GP is 1) (1)
98. If (CWL is 376) and (INFLOW is 200) then (GP is 1) (1)
99. If (CWL is 376) and (INFLOW is 300) then (GP is 1) (1)
100. If (CWL is 376) and (INFLOW is 400) then (GP is 2) (1)
101. If (CWL is 376) and (INFLOW is 500) then (GP is 3) (1)
102. If (CWL is 376) and (INFLOW is 600) then (GP is 4) (1)
103. If (CWL is 376) and (INFLOW is 700) then (GP is 5) (1)
104. If (CWL is 376) and (INFLOW is 800) then (GP is 6) (1)
105. If (CWL is 376) and (INFLOW is 900) then (GP is 7) (1)
106. If (CWL is 376) and (INFLOW is 1000) then (GP is 7) (1)
107. If (CWL is 376) and (INFLOW is 1100) then (GP is 7) (1)
108. If (CWL is 376) and (INFLOW is 1200) then (GP is 7) (1)
109. If (CWL is 376) and (INFLOW is 1300) then (GP is 7) (1)
110. If (CWL is 376) and (INFLOW is 1400) then (GP is 7) (1)
111. If (CWL is 376) and (INFLOW is 1500) then (GP is 7) (1)
112. If (CWL is 376) and (INFLOW is 1600) then (GP is 7) (1)
113. If (CWL is 377) and (INFLOW is 100) then (GP is 1) (1)
114. If (CWL is 377) and (INFLOW is 200) then (GP is 1) (1)
115. If (CWL is 377) and (INFLOW is 300) then (GP is 1) (1)
116. If (CWL is 377) and (INFLOW is 400) then (GP is 2) (1)
117. If (CWL is 377) and (INFLOW is 500) then (GP is 2) (1)
118. If (CWL is 377) and (INFLOW is 600) then (GP is 3) (1)
119. If (CWL is 377) and (INFLOW is 700) then (GP is 4) (1)
120. If (CWL is 377) and (INFLOW is 800) then (GP is 5) (1)

121. If (CWL is 377) and (INFLOW is 900) then (GP is 6) (1)
122. If (CWL is 377) and (INFLOW is 1000) then (GP is 7) (1)
123. If (CWL is 377) and (INFLOW is 1100) then (GP is 7) (1)
124. If (CWL is 377) and (INFLOW is 1200) then (GP is 7) (1)
125. If (CWL is 377) and (INFLOW is 1300) then (GP is 7) (1)
126. If (CWL is 377) and (INFLOW is 1400) then (GP is 7) (1)
127. If (CWL is 377) and (INFLOW is 1500) then (GP is 7) (1)
128. If (CWL is 377) and (INFLOW is 1600) then (GP is 7) (1)
129. If (CWL is 378) and (INFLOW is 100) then (GP is 1) (1)
130. If (CWL is 378) and (INFLOW is 200) then (GP is 1) (1)
131. If (CWL is 378) and (INFLOW is 300) then (GP is 1) (1)
132. If (CWL is 378) and (INFLOW is 400) then (GP is 2) (1)
133. If (CWL is 378) and (INFLOW is 500) then (GP is 2) (1)
134. If (CWL is 378) and (INFLOW is 600) then (GP is 3) (1)
135. If (CWL is 378) and (INFLOW is 700) then (GP is 4) (1)
136. If (CWL is 378) and (INFLOW is 800) then (GP is 5) (1)
137. If (CWL is 378) and (INFLOW is 900) then (GP is 6) (1)
138. If (CWL is 378) and (INFLOW is 1000) then (GP is 7) (1)
139. If (CWL is 378) and (INFLOW is 1100) then (GP is 8) (1)
140. If (CWL is 378) and (INFLOW is 1200) then (GP is 8) (1)
141. If (CWL is 378) and (INFLOW is 1300) then (GP is 8) (1)
142. If (CWL is 378) and (INFLOW is 1400) then (GP is 8) (1)
143. If (CWL is 378) and (INFLOW is 1500) then (GP is 8) (1)
144. If (CWL is 378) and (INFLOW is 1600) then (GP is 8) (1)

145. If (CWL is 379) and (INFLOW is 100) then (GP is 1) (1)
146. If (CWL is 379) and (INFLOW is 200) then (GP is 1) (1)
147. If (CWL is 379) and (INFLOW is 300) then (GP is 1) (1)
148. If (CWL is 379) and (INFLOW is 400) then (GP is 1) (1)
149. If (CWL is 379) and (INFLOW is 500) then (GP is 2) (1)
150. If (CWL is 379) and (INFLOW is 600) then (GP is 3) (1)
151. If (CWL is 379) and (INFLOW is 700) then (GP is 4) (1)
152. If (CWL is 379) and (INFLOW is 800) then (GP is 4) (1)
153. If (CWL is 379) and (INFLOW is 900) then (GP is 5) (1)
154. If (CWL is 379) and (INFLOW is 1000) then (GP is 6) (1)
155. If (CWL is 379) and (INFLOW is 1100) then (GP is 7) (1)
156. If (CWL is 379) and (INFLOW is 1200) then (GP is 9) (1)
157. If (CWL is 379) and (INFLOW is 1300) then (GP is 11) (1)
158. If (CWL is 379) and (INFLOW is 1400) then (GP is 11) (1)
159. If (CWL is 379) and (INFLOW is 1500) then (GP is 11) (1)
160. If (CWL is 379) and (INFLOW is 1600) then (GP is 11) (1)
161. If (CWL is 380) and (INFLOW is 100) then (GP is 1) (1)
162. If (CWL is 380) and (INFLOW is 200) then (GP is 1) (1)
163. If (CWL is 380) and (INFLOW is 300) then (GP is 1) (1)
164. If (CWL is 380) and (INFLOW is 400) then (GP is 1) (1)
165. If (CWL is 380) and (INFLOW is 500) then (GP is 2) (1)
166. If (CWL is 380) and (INFLOW is 600) then (GP is 3) (1)
167. If (CWL is 380) and (INFLOW is 700) then (GP is 3) (1)
168. If (CWL is 380) and (INFLOW is 800) then (GP is 4) (1)

169. If (CWL is 380) and (INFLOW is 900) then (GP is 5) (1)
170. If (CWL is 380) and (INFLOW is 1000) then (GP is 6) (1)
171. If (CWL is 380) and (INFLOW is 1100) then (GP is 7) (1)
172. If (CWL is 380) and (INFLOW is 1200) then (GP is 8) (1)
173. If (CWL is 380) and (INFLOW is 1300) then (GP is 9) (1)
174. If (CWL is 380) and (INFLOW is 1400) then (GP is 12) (1)
175. If (CWL is 380) and (INFLOW is 1500) then (GP is 12) (1)
176. If (CWL is 380) and (INFLOW is 1600) then (GP is 12) (1)
177. If (CWL is 381) and (INFLOW is 100) then (GP is 1) (1)
178. If (CWL is 381) and (INFLOW is 200) then (GP is 1) (1)
179. If (CWL is 381) and (INFLOW is 300) then (GP is 1) (1)
180. If (CWL is 381) and (INFLOW is 400) then (GP is 1) (1)
181. If (CWL is 381) and (INFLOW is 500) then (GP is 2) (1)
182. If (CWL is 381) and (INFLOW is 600) then (GP is 2) (1)
183. If (CWL is 381) and (INFLOW is 700) then (GP is 3) (1)
184. If (CWL is 381) and (INFLOW is 800) then (GP is 4) (1)
185. If (CWL is 381) and (INFLOW is 900) then (GP is 4) (1)
186. If (CWL is 381) and (INFLOW is 1000) then (GP is 5) (1)
187. If (CWL is 381) and (INFLOW is 1100) then (GP is 6) (1)
188. If (CWL is 381) and (INFLOW is 1200) then (GP is 7) (1)
189. If (CWL is 381) and (INFLOW is 1300) then (GP is 9) (1)
190. If (CWL is 381) and (INFLOW is 1400) then (GP is 10) (1)
191. If (CWL is 381) and (INFLOW is 1500) then (GP is 11) (1)
192. If (CWL is 381) and (INFLOW is 1600) then (GP is 12) (1)

193. If (CWL is 382) and (INFLOW is 100) then (GP is 1) (1)
194. If (CWL is 382) and (INFLOW is 200) then (GP is 1) (1)
195. If (CWL is 382) and (INFLOW is 300) then (GP is 1) (1)
196. If (CWL is 382) and (INFLOW is 400) then (GP is 1) (1)
197. If (CWL is 382) and (INFLOW is 500) then (GP is 2) (1)
198. If (CWL is 382) and (INFLOW is 600) then (GP is 2) (1)
199. If (CWL is 382) and (INFLOW is 700) then (GP is 2) (1)
200. If (CWL is 382) and (INFLOW is 800) then (GP is 4) (1)
201. If (CWL is 382) and (INFLOW is 900) then (GP is 4) (1)
202. If (CWL is 382) and (INFLOW is 1000) then (GP is 5) (1)
203. If (CWL is 382) and (INFLOW is 1100) then (GP is 6) (1)
204. If (CWL is 382) and (INFLOW is 1200) then (GP is 7) (1)
205. If (CWL is 382) and (INFLOW is 1300) then (GP is 8) (1)
206. If (CWL is 382) and (INFLOW is 1400) then (GP is 9) (1)
207. If (CWL is 382) and (INFLOW is 1500) then (GP is 11) (1)
208. If (CWL is 382) and (INFLOW is 1600) then (GP is 12) (1)
209. If (CWL is 367) and (INFLOW is 1) then (GP is 0) (1)
210. If (CWL is 371) and (INFLOW is 1) then (GP is 0) (1)
211. If (CWL is 372) and (INFLOW is 1) then (GP is 0) (1)
212. If (CWL is 373) and (INFLOW is 1) then (GP is 0) (1)
213. If (CWL is 374) and (INFLOW is 1) then (GP is 0) (1)
214. If (CWL is 375) and (INFLOW is 1) then (GP is 0) (1)
215. If (CWL is 376) and (INFLOW is 1) then (GP is 0) (1)
216. If (CWL is 377) and (INFLOW is 1) then (GP is 0) (1)

217. If (CWL is 378) and (INFLOW is 1) then (GP is 0) (1)
218. If (CWL is 379) and (INFLOW is 1) then (GP is 0) (1)
219. If (CWL is 380) and (INFLOW is 1) then (GP is 0) (1)
220. If (CWL is 381) and (INFLOW is 1) then (GP is 0) (1)
221. If (CWL is 382) and (INFLOW is 1) then (GP is 0) (1)

Appendix B: Python Code for Automatic Context Generation

Python code for creating combinations of variables:

```
"""
Created on Tue Jul 14 12:33:26 2015
"""
from itertools import product
import csv


#Read in csv file
criteria = []
with open("Failure Modes.csv", 'rb') as f:
    for i,row in enumerate(csv.reader(f)):
        if i == 0:
            header = row
        else:
            criteria.append(row)
#Filter spaces and separate columns
criteria = [filter(lambda x: x != '', row) for row in zip(*criteria)]
#Unpack criteria and take cartesian product
combos = product(*criteria)
#Write out combos iterator and retain original column names
with open("Failure Combos.csv", 'wb') as f:
```

```
writer = csv.writer(f)
writer.writerow(header)
for c in combos:
    writer.writerow(c)
```

Appendix C: Cheakamus Dam Case Study MATLAB Simulation Code

```
function [V1,V2,V3] = STPAcomb8( GO, V, IN, gate_opening,
discharge, reservoir_elevation, storage,
storagelvl,fcrl,fcd,t,sensors, debris, MG, DG, BAT, Hoist, Rope,
FuzzyGP,gate_str, sr, presence,HR,PG, llogdis,llogwl)
F=scatteredInterpolant(gate_opening, reservoir_elevation,
discharge);
filename='output13.csv';
maxit=17791488;
iter=1;
V1=zeros(17791488,1);
V2=zeros(17791488,1);
V3=zeros(17791488,1);
for i=1:maxit
    cwv=V(iter);
    for c=1:t
        cwl=interp1(storage,storagelvl,cwv);
        if (MG(iter)==0) && (DG(iter)==0) && (BAT(iter)==0)
            GP=GO(iter);
            GP2=min(GP, 12-debris(iter));
        else
        if sr(iter)==1
        if sensors(iter)==1
                if (cwl>367.28) && (cwl<=382) &&
(IN(iter)<=1600)
                    GP=evalfis([cwl IN(iter)], FuzzyGP);
                    GP2=min(GP, 12-debris(iter));
                elseif (cwl>367.28) && (IN(iter)>1600)
                    GP2=12-debris(iter);
                end
        elseif (sensors(iter)==0) && (presence(iter)==1) &&
(c>=2)
               if (cwl>367.28) && (cwl<=382) && (IN(iter)<=1600)
                    GP=evalfis([cwl IN(iter)], FuzzyGP);
                    GP2=min(GP, 12-debris(iter));
               elseif (cwl>367.28) && (IN(iter)>1600)
                    GP2=12-debris(iter);
               end
        elseif (sensors(iter)==0) && (presence(iter)==0) &&
(c<=2)
            GP=GO(iter);
```

```
            GP2=min(GP, 12-debris(iter));
        elseif (sensors(iter)==0) && (presence(iter)==0) &&
(c>=3)
            if (cwl>367.28) && (cwl<=382) && (IN(iter)<=1600)
                    GP=evalfis([cwl IN(iter)], FuzzyGP);
                    GP2=min(GP, 12-debris(iter));
                elseif (cwl>367.28) && (IN(iter)>1600)
                    GP2=12-debris(iter);
            end
        elseif (sensors(iter)==0) && presence(iter)==1 && (c==1)
            GP=GO(iter);
            GP2=min(GP, 12-debris(iter));
        elseif (sensors(iter)==2) && (c==1)
                if (cwl>367.28) && (cwl<=368.28)
                    GP2=0;
                elseif (cwl>368.28) && (cwl<=382) &&
(IN(iter)<1600)
                    k=cwl-1;
                    GP=evalfis([k IN(iter)], FuzzyGP);
                    GP2=min(GP, 12-debris(iter));
                elseif (cwl>368.28) && (IN(iter)>1600)
                    GP2=12-debris(iter);
                end
        elseif (sensors(iter)==2) && (c>=2)
               if (cwl>367.28) && (cwl<=382) && (IN(iter)<=1600)
                    GP=evalfis([cwl IN(iter)], FuzzyGP);
                    GP2=min(GP, 12-debris(iter));
                elseif (cwl>367.28) && (IN(iter)>1600)
                    GP2=12-debris(iter);
               end
        end
        elseif sr(iter)==0
            if presence(iter)==1
                if sensors(iter)==1
                    if (cwl>367.28) && (cwl<=382) &&
(IN(iter)<=1600)
                        GP=evalfis([cwl IN(iter)], FuzzyGP);
                        GP2=min(GP, 12-debris(iter));
                    elseif (cwl>367.28) && (IN(iter)>1600)
                        GP2=12-debris(iter);
                    end
                elseif (sensors(iter)==0) && (c==1)
                    GP=GO(iter);
                    GP2=min(GP, 12-debris(iter));
                elseif (sensors(iter)==0) && (c>=2)
```

```
                    if (cwl>367.28) && (cwl<=382) &&
(IN(iter)<=1600)
                        GP=evalfis([cwl IN(iter)], FuzzyGP);
                        GP2=min(GP, 12-debris(iter));
                    elseif (cwl>367.28) && (IN(iter)>1600)
                        GP2=12-debris(iter);
                    end
                elseif (sensors(iter)==2) && (c==1)
                     if (cwl>367.28) && (cwl<=368.28)
                        GP2=0;
                     elseif (cwl>368.28) && (cwl<=382) &&
(IN(iter)<1600)
                        k=cwl-1;
                        GP=evalfis([k IN(iter)], FuzzyGP);
                        GP2=min(GP, 12-debris(iter));
                elseif (cwl>368.28) && (IN(iter)>1600)
                        GP2=12-debris(iter);
                     end
                elseif (sensors(iter)==2) && (c>=2)
                    if (cwl>367.28) && (cwl<=382) &&
(IN(iter)<=1600)
                        GP=evalfis([cwl IN(iter)], FuzzyGP);
                        GP2=min(GP, 12-debris(iter));
                    elseif (cwl>367.28) && (IN(iter)>1600)
                        GP2=12-debris(iter);
                    end
                end
                elseif presence(iter)==0
                    if c<=2
                        GP=GO(iter);
                        GP2=min(GP, 12-debris(iter));
                    end
                    if c>=3
                        if (cwl>367.28) && (cwl<=382) &&
(IN(iter)<=1600)
                            GP=evalfis([cwl IN(iter)], FuzzyGP);
                            GP2=min(GP, 12-debris(iter));
                        elseif (cwl>367.28) && (IN(iter)>1600)
                            GP2=12-debris(iter);
                        end
                    end
            end
        end
        end
                if cwl<378.41
```

```
                    overflow=0;
                 else
                    overflow=interp1(fcrl, fcd, cwl);
                end
                 if cwl<367.28
                     outflow=0;
                 else
                     if gate_str(iter)==1
                        if ((MG(iter)==0) && (DG(iter)==0) &&
(BAT(iter)==0)) || (Hoist(iter)==0)
                            outflow=F(GO(iter), cwl);
                        elseif (Rope(iter)==0)
                            outflow=0;
                        else
                            outflow=F(GP2, cwl);
                        end
                     elseif gate_str(iter)==0
                         outflow=0;
                     elseif gate_str(iter)==2
                         outflow=F(GO(iter), cwl);
                     end
                 end
                 if ((IN(iter)>1600) && HR(iter)==1) ||
((gate_str(iter)==0) && HR(iter)==0)
                     LLD=interp1(llogwl,llogdis, cwl);
                 else
                     LLD=0;
                 end
                 if ((IN(iter)>1600+LLD) && PG(iter)==1) ||
((gate_str(iter)==0) && PG(iter)==1)
                     PD=min(65, IN(iter)-1600-LLD);
                 else
                     PD=0;
                 end
                 if ((MG(iter)==0) && (DG(iter)==0) &&
(BAT(iter)==0))
                     LLD=0;
                     PD=0;
                 end
                    newwv=min((cwv+3600*(IN(iter)-outflow-
overflow-LLD-PD)), 58254767);
                    cwv=newwv;
                    if c==1
                        V1(iter,1)=newwv;
                    elseif c==2
```

```
                        V2(iter,1)=newwv;
                    elseif c==3
                        V3(iter,1)=newwv;
                    end
                c=c+1;
    end
    iter=iter+1;
end
CO1=[V1 V2 V3];
csvwrite(filename, CO1);
end
```

Appendix D: MATLAB Code for The Simulation Using Fuzzy Control Action Rules

```
function [RE2] = EXP2(
gate_opening,discharge,reservoir_elevation,inflow,storage,storagelvl,
swl,FIS)
F=scatteredInterpolant(gate_opening, reservoir_elevation, discharge);
filename='output12.xlsx';
maxit=32;
iter=1;
RE2=zeros(32,1);
GPE2=zeros(32,1);
cwl=swl;
for i=1:maxit
    if cwl<=367.28
        GP=0;
    elseif cwl>367.28
        GP=evalfis([inflow(iter) cwl], FIS);
    end
    if cwl<=367.28
        outflow=0;
    elseif cwl>367.28
        outflow=F(GP, cwl);
    end
    cwv=interp1(storagelvl, storage, cwl);
    newwv=min(38859746, (cwv+3600*inflow(iter)-3600*outflow));
    newwl=interp1(storage,storagelvl, newwv);
    cwl=newwl;
    iter=iter+1;
    RE2(i,1)=cwl;
    GPE2(i,1)=GP;
end
CO=[RE2 GPE2];
xlswrite(filename, CO);
end
```

Appendix E: MATLAB Code for The Simulation Using Crisp Control Action Rules

```
function [RE2] = EXP22(
gate_opening,discharge,reservoir_elevation,inflow,storage,storagelvl, swl)
F=scatteredInterpolant(gate_opening, reservoir_elevation, discharge);
filename='output12.xlsx';
maxit=214;
iter=1;
RE2=zeros(214,1);
GPE2=zeros(214,1);
cwl=swl;
for i=1:maxit
    if cwl<=367.28
        GP=0;
    elseif (cwl>367.28 && cwl<372) && (inflow(iter)>0 && inflow(iter)<=25)
        GP=0;
    elseif (cwl>=372 && cwl<375) && (inflow(iter)>0 && inflow(iter)<=25)
        GP=0;
    elseif (cwl>=375 && cwl<=377) && (inflow(iter)>0 && inflow(iter)<=25)
        GP=0;
    elseif (cwl>367.28 && cwl<372) && (inflow(iter)>25 && inflow(iter)<=75)
        GP=1;
    elseif (cwl>=372 && cwl<375) && (inflow(iter)>25 && inflow(iter)<=75)
        GP=0.5;
    elseif (cwl>=375 && cwl<=377) && (inflow(iter)>25 && inflow(iter)<=75)
        GP=0.5;
    elseif (cwl>367.28 && cwl<372) && (inflow(iter)>75 && inflow(iter)<=125)
        GP=2;
    elseif (cwl>=372 && cwl<375) && (inflow(iter)>75 && inflow(iter)<=125)
        GP=1.5;
    elseif (cwl>=375 && cwl<=377) && (inflow(iter)>75 && inflow(iter)<=125)
        GP=1;
     elseif (cwl>367.28 && cwl<372) && (inflow(iter)>125 &&
inflow(iter)<=175)
        GP=3;
    elseif (cwl>=372 && cwl<375) && (inflow(iter)>125 && inflow(iter)<=175)
        GP=2;
    elseif (cwl>=375 && cwl<=377) && (inflow(iter)>125 && inflow(iter)<=175)
        GP=1.5;
    elseif (cwl>367.28 && cwl<372) && (inflow(iter)>175 && inflow(iter)<=200)
        GP=3;
    elseif (cwl>=372 && cwl<375) && (inflow(iter)>175 && inflow(iter)<=200)
        GP=3;
    elseif (cwl>=375 && cwl<=377) && (inflow(iter)>175 && inflow(iter)<=200)
        GP=2;
    end
    if cwl<=367.28
        outflow=0;
    elseif cwl>367.28
        outflow=F(GP, cwl);
```

```
    end
    cwv=interp1(storagelvl, storage, cwl);
    newwv=min(38859746, (cwv+3600*inflow(iter)-3600*outflow));
    newwl=interp1(storage,storagelvl, newwv);
    cwl=newwl;
    iter=iter+1;
    RE2(i,1)=cwl;
    GPE2(i,1)=GP;
end
CO=[RE2 GPE2];
xlswrite(filename, CO);
end
```

CURRICULUM VITAE

Name:	Bogdan Pavlovic
Post-secondary Education and Degrees:	The University of Belgrade Belgrade, Serbia 2009-2014 B. Sc.
Related Work Experience:	Graduate Research Assistant The University of Western Ontario 2014-2016 Teaching Assistant The University of Western Ontario 2015-2016

Publications:

Pavlovic, B., Simonovic, S. P. (2016). Automated Control Flaw Generation Procedure: Cheakamus Dam Case Study. Water Resources Research Report no. 093, Facility for Intelligent Decision Support, Department of Civil and Environmental Engineering, London, Ontario, Canada, 78 pages. ISBN: (print) 978-0-7714-3113-5; (online) 978-0-7714-3114-2.