Comparison of STPA and Bow-tie Method Outcomes in the Development and Testing of an Automated Water Quality Management System

Hew Cameron Merrett[1,*], Jao Jia Horng[2], Andrew Piggot[3], Amro Qandour[4] and Chen Wei Tong[5]

[1]Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Taiwan
[2]Graduate School of Environmental, Health and Safety Engineering, National Yunlin University of Science and Technology, Taiwan
[3] OAS, Sweden AB
[4] Centre for Communications and Electronics Research, Edith Cowen University, Australia
[5]Department of Civil and Construction Engineering, National Yunlin University of Science and Technology, Taiwan

ABSTRACT

The technology available to water quality management applications needs to be advanced due to greater use of automation to increase ease of operation, support remote operation and reduce risks due to operator error. In this case study, a comparison is made between System-Theoretic Process Analysis (STPA) and the Bow-tie methodology for identifying process hazards and countermeasures which can be used to guide the design and testing of an automated water quality management system (AWQMS). For this study, the application considered is a small hydroponics installation where water quality management has been automated. The STPA methodology uses a system theory-based approach to identify hazards, which include operational failures, human errors, and component interactions. The Bow-tie diagram focuses on individual barriers for a given threat which can prevent the realisation of a hazardous event and unwanted consequences. Thus, the 22 preventative barriers and seven recovery barriers identified through the Bow-tie diagram provide the design process with broad requirements for reducing the risks of user error as well as the ones associated with ongoing operations. The STPA method identified many Causal Factors (CF) generated from the Unsafe Control Actions after considering all the feasible scenarios. For design input, the STPA provided the design process with 204 specific CFs which were used to create 94 countermeasures to be included in software and hardware design as well as user information material. Both methods identified useful measures to control the hazards associated with human interaction with the AWQMS. However, the measures differed in the level of detail and the involvement in the evolution in the final system losses. In this study, the STPA process was able to identify several hazards which did not visibly relate to the Bow-tie barriers. However, the Bow-tie diagram illustrates a distinction between preventative and recovery hazard controls.

Keywords: Water Quality Management; Hazard Analysis; System Theoretic Process Analysis; Bow-tie method; Product Design.

1. INTRODUCTION

The technology available to water quality management applications is becoming more and more advanced with greater use of automation to increase ease of operation, support remote

[*]Corresponding author: +886 972 504 960, hew.merrett@gmail.com

operation and reduce risks associated with operator error. As automated systems become more commonplace in water quality management, the precision in water quality control within these systems increases with the capacity to provide greater measurement and control (Olsson, 2007). Operating such complex systems manually relies heavily on the knowledge and expertise of the engineers and operators alone. However, introducing automation into water quality management processes for various applications often involve costly components and complex communication systems (Lee, 1995). These factors present some barriers in introducing automation in small to medium scale water quality control applications.

This study uses the case study of the development of a cost-effective mid-level automated water quality control system (AWQMS) which can be adapted for small to medium applications that require precise water quality conditions. As the system design allows for a variety of combinations of measured parameters depending on the intended use, this type of system has several operational applications including small-scale drinking water systems, wastewater treatment systems, irrigation systems etc. For this study the application considered is a small hydroponics installation where water quality management has been automated; the system considered can be readily scaled depending the produce being grown. For hydroponic and other controlled horticultural production systems to obtain the optimum growth rate there are precise requirements for parameters such as nutrients, dissolved oxygen and temperature. Out-of-specification water quality can result in loss of production and mortality of the crop.

Future developments in hydroponics are centred around increasing the automation of water quality parameters such as nutrient management (Savvas, 2003). The development of the AWQMS enables users to manage complex water quality requirements with only a basic knowledge of water quality and the needs of the system being managed. However, this heavy reliance on automation of a system to enforce safety requirements and associated system constraints introduces hazards associated with technical aspects of the system design and perhaps, more importantly, the user interaction and operation of the system. Therefore, a comprehensive analysis of the hazards of the socio-technical system is necessary during the product development process to provide reassurance that the system performance meets the user's requirements. This case study provides a qualitative comparison of the use of System Theoretic Process Analysis (STPA) and the Bow-tie method to identify hazards and associated control measures to improve usability and functionality in automated water quality control. The analysis results are used to develop suitable countermeasures to incorporate into product design and develop product testing criteria.

There are many factors to consider in selecting an appropriate risk and hazard analysis method to a given problem (Sulaman, Beer, Felder, & Host, 2017). Many methods have been developed and implemented to evaluate the hazards inherent in the operation of complex systems. Methods such as Hazard and Operability Analysis (HAZOP), Failure Modes Effect Analysis (FMEA) and Fault Tree Analysis (FTA) are widely used to identify hazards in complex systems, however these methods only consider the system as an "assembly" of individual components and can miss the hazards associated arising from the interactions among the components (Sulaman, Beer, Felder, & Host, 2017).

System-Theoretic Accident Model and Process (STAMP) is the accident causality model which STPA is based upon. The STAMP model views accident causality as more than component failures and chains of failure events (Leveson, 2015). The benefit of using STPA is that it is well suited to analyse complex socio-technical systems and that the method can be applied during early stages of system development of complex socio-technical systems while details about the system are still unknown (Leveson & Thomas, 2018). STPA has been applied to large complex systems with multiple systems where traditional methods have not provided the same level of detail on system interactions that STPA has provided (Fleming, Spencer, Thomas, Leveson, & Wilkinson, 2018).

In the context of water quality management systems, STAMP based models of the system control structure provide valuable information on safety-based system requirements for water quality control (Leveson, Daouk, Dulac, & Marais, 2003; Merrett, Horng, & Chen 2018). Water quality management systems are complex sociotechnical systems with multiple processes and rely partially on the user to ensure safe operations. The systematic nature of STPA is well suited to developing

systems and measures to understand and control the hazards in water quality management applications such as drinking water supply (Dokas, Feehan, & Imran, 2013).

The Bow-tie method as a risk management tool can be applied to identifying and displaying the barriers in place that aim to prevent the occurrence of unwanted losses in a system (McLoed & Bowie, 2018). The barrier approach to safety is well-known from the Swiss Cheese model (Reason, 2000). In this particular model, the holes in cheese represent the absence of barriers or scenarios or faults in barriers where the barrier is not effective in controlling the progression of the risk event. Bow-tie diagrams of hazard analysis outcomes are used widely in Australia and Europe in a wide range of applications where an organisation has identified significant risks to business objectives due to the ability of the diagram to illustrate how major hazards are identified and controlled (Saud et al., 2013). A multi-barrier approach is seen as good practice to reduce both the probability and consequence of a hazardous event in drinking water systems. For drinking water systems, Bow-tie diagrams provide the ability to both highlight the possible causes and consequences of hazardous events and the barriers required to prevent hazardous events or reduce the severity (Hokstad et al., 2009).

During the research and development stages of new products and systems in small enterprises, it is not uncommon to use a combination of previous experience, current design trends and brainstorming to identify system hazards and implement design solutions. However, without a structured approach, there is a limited assurance in the effectiveness of the design process in meeting the required objectives. As a result, faults can be easily overseen, and the redesign process can take up a significant amount of time and resources. To ensure the design and testing process occurred as efficiently as possible the conceptional design was used as the basis for the hazard assessment of the user interaction AWQMS. Findings from the hazard analysis of the conceptual design are used to enhance and assess final product design. The aim is to ensure that system performance matches user expectations and ensure there is confidence in the performance of the system to effectively manage the risks associated with water quality control.

2. METHODOLOGY

The following sections describe the design process for the AWQMS for use in the automated control of a hydroponics system and the role of hazard analysis in supporting this design process. Furthermore, an overview of the STPA and Bow-tie methodologies applied to the case study is also provided.

2.1. Case Study - Automated Water Quality Management System Design Process

This paper presents a case study in the application of hazard analysis to guide the design of the user interfaces, hardware and software of an automated water quality management system (AWQMS). In this case, the hazard analysis is performed after the initial concept, and functional requirements had been established. The AWQMS (Figure 1) consists of wireless waterproof water sensing electrode modules for the measurement of Oxidation Reduction Potential (ORP), acidity and basicity (pH), temperature, and electrical conductivity (EC). The water sensing electrode modules are positioned in a rack attached to the base processing unit and receive power from the processing unit using a wireless method. The signal is then transmitted to the processing unit using an optical link method. The unit also includes a digital water temperature sensor which is used for temperature compensation of sensor electrode modules when necessary.

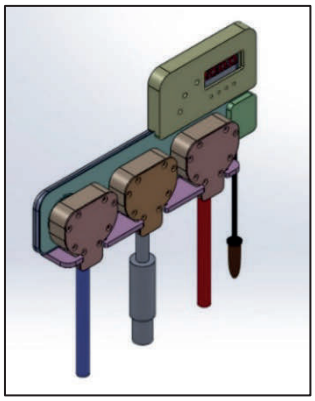

Figure 1: The base unit, wireless interface rack and probes of the AWQMS

The base unit includes outputs for controlling any of the measured system parameters through auxiliary dosing, heating and cooling units depending on the user requirements. Dosing commands are processed by algorithms within the processing unit to facilitate local feedback control mechanisms for any control parameter provided by the processing unit. Furthermore, the AWQMS can transfer sensor data to a web server to facilitate remote sensor data collection, analysis and monitoring complemented by higher level functions provided by a remote server. The higher-level functions processed remotely are not covered in the scope of this study. While there are many potential applications of the AWQMS, the application to hydroponics was selected for the case study, as the integration of the AWQMS into an existing installation provided a reliable testing platform. The hydroponic system in which the AWQMS was tested for the case study and the associated specifications are shown in Figure 2.

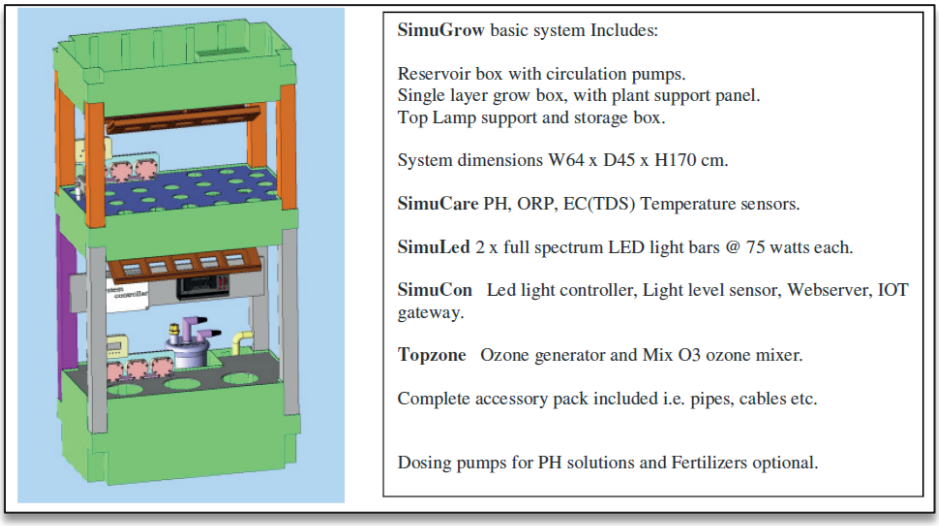

Figure 2: A drawing of the automated hydroponic system used for the development and testing of the AWQMS. The AQWMS is installed in the far-left corner of each tray
Note: The figure refers to the AWQMS as SimuCare

The product development and testing process were primarily based on the process engineering V Model shown in Figure 3. The process design started with a conceptional system operations design based on the requirements of target users for potential applications of the system. Several system subcomponents from other applications were integrated into the initial design to leverage off design work already completed.

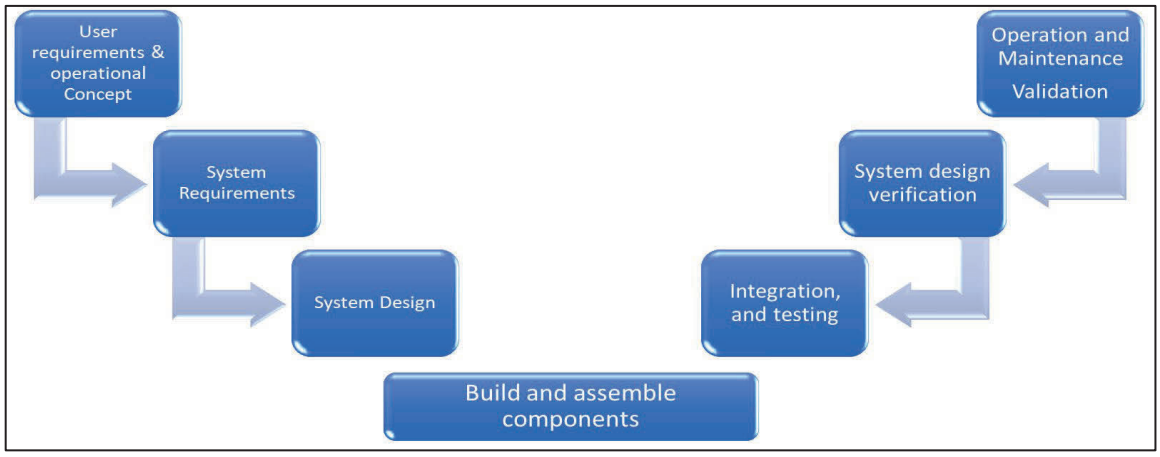

Figure 3: The process engineering V model applied to develop the AWQMS

The specific requirements for the AWQMS were developed based on monitoring and control of small to medium scale automated water quality control applications. Next, a hazard analysis was performed. From the hazard analysis output, safety-related requirements for the final system were generated. The integration of hazard analysis into the system design and testing process is shown in Figure 4. The resulting design requirements can be grouped into software requirements, design requirements and user information. Software requirements include all software programming solutions to address system hazards. Design requirements consist of the design of physical components to reduce the hazards generated from user interaction. Where the most appropriate countermeasure was to provide the user with detailed information to overcome the potential for hazard, a requirement for user information was generated — the safety-related requirements where then used together with all other product requirements as input for the prototype development and testing phase. After prototype development and testing, the design was verified against design criteria and functionality verified, then the final system design specifications were produced.

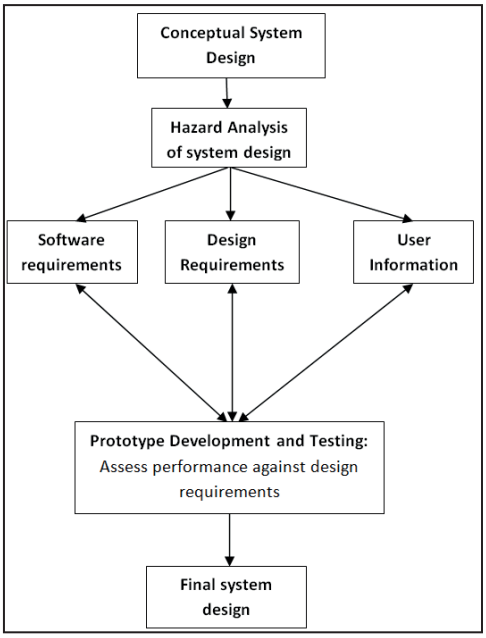

Figure 4: The design process for the AWQMS with the integration of the Hazard analysis to guide various system requirements for the prototype

2.2 STPA Method

The STPA methodology by taking system-wide approach identifies hazards which not only includes operational failures, but also considers aspects such as design error, human errors, and component interactions (Cameron et al., 2017). There is no need for a completed design before using STPA, and the design process can be guided through the STPA outputs (Leveson, 2011). As STPA focuses on the top down dynamic interaction of the various components of the system through a series of control loops, it is well suited to identifying the hazards associated with user interaction with a system such as the AWQMS. Hazard analysis using the STPA technique consists of four key steps (Leveson & Thomas, 2018):

- Define the purpose of analysis – identify losses, system level hazards and system-level safety constraints
- Model of the Control Structure – a system model consisting of feedback and control loops
- Identify unsafe control actions (UCAs) – are control actions in a worse case environment will lead to a hazard. The unsafe control actions can be grouped as unsafe when not provided, provided, provided to early or too late or in the wrong sequence, and provided too long or too short.
- Identify loss scenarios – Scenarios are the causal factors that lead to UCAs.

In this study, the associated causal factors (CFs) and related scenarios leading to a UCA were also identified during step 2 of the STPA process. CFs are the underlying factors which may lead to UCAs or scenarios where control actions are not executed as intended (Leveson & Thomas, 2018). Each UCA can be associated with one or more CF. Once the STPA results are obtained, the next step after the STPA hazard analysis process is the identification of countermeasures which can potentially prevent or reduce the impacts of the relevant CF for the scenarios considered. It's the countermeasures which will become the design and testing requirements for the development process. The STAMP Workbench V1.0.0/5c1123 by Apache Software Company was used to complete the analysis and capture the results.

3.3 Bow-tie Method

Bow-tie diagrams are well suited to providing a visual representation of operational risks and controls of complex systems and processes. The Bow-tie diagram is based upon the results of a supporting hazard analysis of the system followed by identifying suitable barriers to prevent the consequences of the hazards being realised. The term Bow-tie method is used to refer to the use of a hazard analysis process to identify relevant system hazards, threats and consequences in conjunction with a Bow-tie diagram to display the results with relevant barriers to prevent unacceptable losses. The Bow-tie method was chosen for a comparison with STPA as the outcomes of both are intended to provide qualitative information to guide measures for ensuring the safety of the AWQMS operations. In this case study, at the stage of hazard identification and analysis, a simple Hazard Identification (HAZID) process was used to identify the key threats and corresponding consequences associated with a loss of control over a hazard.

Once the initial HAZID step is completed the Bow-tie diagram can begin to be generated. There is no consensus for the exact methodology for developing Bow-tie diagrams. However the common components are the hazard, top event, threats, consequences and barriers (Chatzimichailidou, Ward, Horberry, & Clarkson, 2018). Typically for the Bow-tie diagram (Figure 5), the left side diagram represents a simplified FTA, which lists all the ways control can be lost over a hazard through a repeated process of asking what potential events can happen and what are the associated causes. The right side of the diagram is a simplified Event Tree Analysis (ETA) which describes how a loss of control over a hazard can lead to various outcomes and consequences. The

barriers between the threats and the top event are considered preventative measures to prevent the top event. The barriers to the right of the top event are considered recovery barriers.

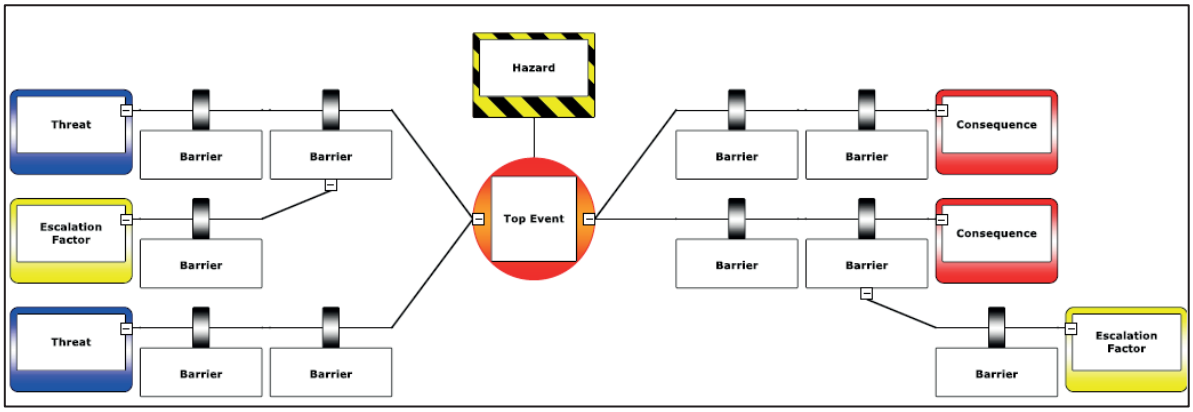

Figure 5: The basic layout and components of the Bow-tie method used in the Bowtie XP software package

This study used eight key steps in the development of the final Bow-tie diagram. These eight steps are as follows (CGE Risk, 2017):

1. Identify Hazard – the activity which can cause a risk
2. Identify top event – the way in which control is lost over the hazard
3. Identify Threats – the events that can cause the top event
4. Evaluate Consequences – The scenarios in which the top event is realised
5. Identify preventative barriers – barriers to the left of the top event; these barriers prevent the threats from causing the top event
6. Identify recovery barriers - barriers to the right of the top event; these barriers prevent the top event from causing a loss
7. Identify escalation factors – situations where specific barriers are not effective
8. Identify escalation factor barriers – barriers to prevent escalation factors from occurring

The initial HAZID process focused on identifying information required to support steps one to four. The process involved brainstorming to identify hazards, causes, and consequences associated with the user interface with the water quality system. To ensure that results from both the STPA and Bow-tie methodology could be compared effectively the same team of analysts were involved in both hazard studies. The background of the team included expertise in qualitative hazard analysis in water quality management, electronics design, software design and product manufacturing.

The brainstorming process for the HAZID was guided and recorded using a table containing the columns to capture potential threats, consequences likelihood and severity. The significance was based on inherent risk determined by the likelihood of the outcome occurring and the corresponding severity of loss in the system in a reasonable worst-case scenario. Using the information from the preliminary HAZID, the initial Bow-tie diagram was constructed containing hazard, top event, threat and consequences. From the basic Bow-tie diagram generated the team was able to work on stages five to eight of identifying barriers. Using the Bow-tie diagram for this stage allows the analysts to visualise better the barriers which can be used to prevent the progression of hazardous events towards unacceptable system losses. It's the barriers which will be used in guiding the development of design and testing criteria. The software package Bowtie XP version 9.2.3 by CGE Risk was used to develop and record the final Bow-tie diagram.

3. RESULTS

3.1. STPA Method

Define the purpose

The definition of the purpose of the analysis for the STPA analysis for the AWQMS is defined in Table 1. The key losses are a loss of crop production due to the unsuitable water quality; production refers to mortality of plants or sub-optimal production rates. The water quality can be unsuitable due to natural processes or due to incorrect control actions by the AWQMS.

Table 1 Definition of analysis purpose for the investigation of system hazards. The system level hazards and associated safety constraints

Accident	Hazard ID	Hazard	Safety Constraint ID	Safety Constraint
Loss of Crop production	H1	System water quality violates the criteria for supporting crop growth	SC1	System water quality must remain inside designated water quality parameters for crop growth

Model the Control Structure

A high-level model of the control structure for the hydroponics system is shown in Figure 6. The control structure is centred on the user's interaction with the AWQMS operations. As the AWQMS is a measuring and control system, there are several components in the wider hydroponic system which did not fall in the design scope. However, to capture the wider system interaction hazards, these hydroponic system components were included in the STPA hazard analysis. The components outside of the scope of the system are grouped as a single process. The dosing control loop identifies the dosing equipment (shown in grey in Fig 3) as actuators as there is no feedback provided from the dosing equipment to the base unit, this is a one-way flow of information. Being a closed control loop, information on the effectiveness of the dosing commands on the system is solely provided by the measurements of system water quality parameters. Also included in the control structure are the actions of the user in set up, operation and maintenance

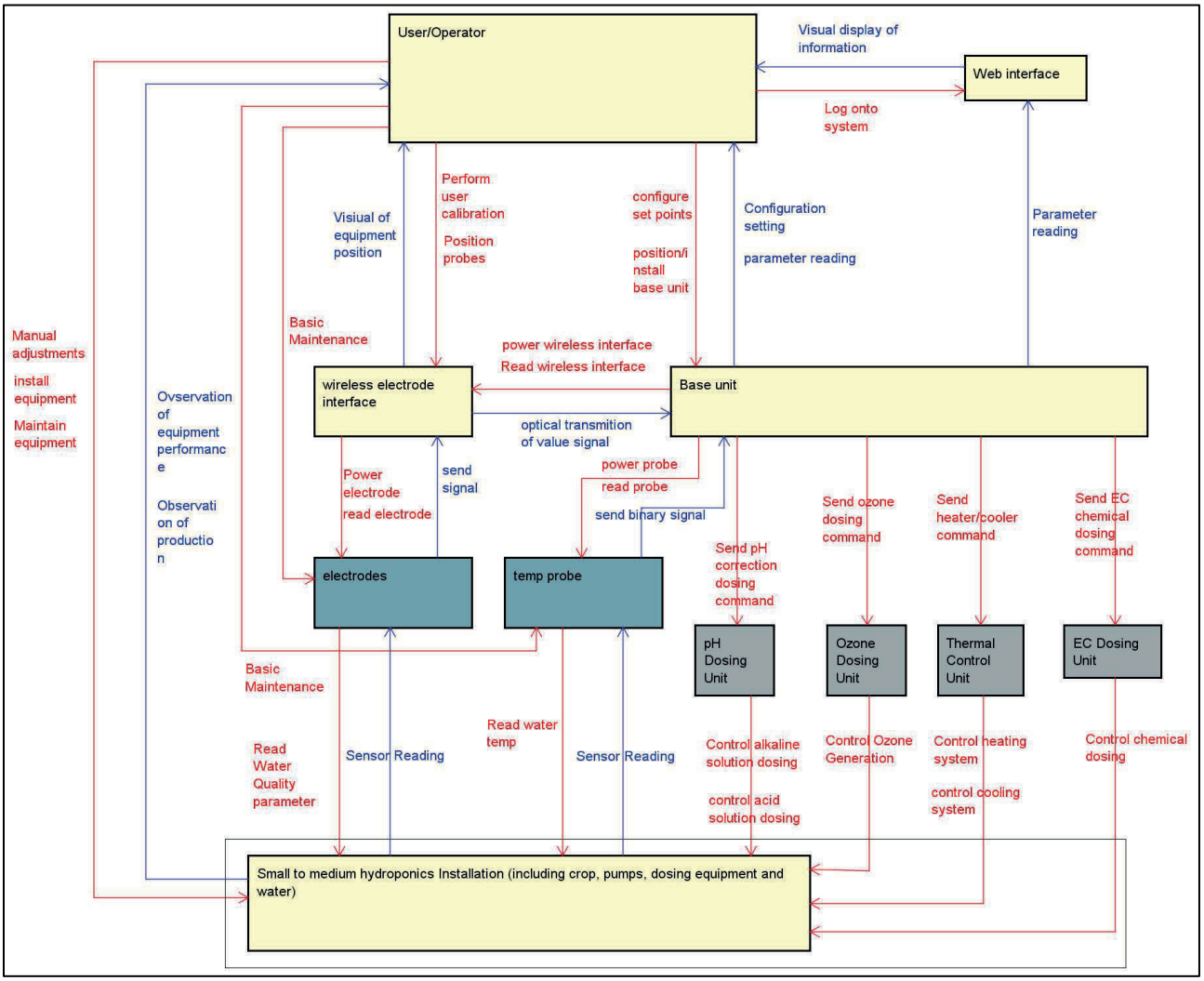

Figure 6: The high-level control structure for an automated water quality control system applied to hydroponics. Red arrows indicate control actions and blue arrows are feedback

Identify Unsafe Control Actions

The high-level control structure features a total of 27 control actions. Based on an assessment of these control actions a total of 123 unsafe control actions (UCA) were identified. UCAs were identified using both context tables and expert opinion of the analysis team. For control actions with less complex process models, UCAs were identified using expert opinion and the standard guidewords. For the control actions with more complicated process models with many variables and discrete values, context tables were used. Context tables proved to be a valuable tool where expert opinion may not identify all possible UCAs.

The control actions of '*perform user calibration'* is used as an example of the user providing a maintenance task and '*send ozone dosing command'* as an example of the control actions of the base unit. The process model with the variables and values for the control action '*send ozone dosing command'* by the base unit is as follows:

- Base unit ORP set point
  - Matches user defined ORP set point
  - Does not match user-defined ORP set point
- Measured ORP level
  - Equals user set point level

- Low level
- High level
- Critical Low level
- Critical high level

The process model with the variables and values for '*perform user calibration'* by the user is as follows:

- Calibration Schedule
  - Calibration due
  - Calibration not due
  - Calibration overdue
- Calibration Procedure
  - Correct calibration procedure followed
  - Incorrect calibration procedure followed

For each of the context tables, the combinations of variables and respective values were investigated for UCAs resulting either when providing or not providing the respective control actions. The resulting of the high-level context tables for both control actions used are provided in Tables 2 and 3.

Table 2 The context table for the control action '*send ozone dosing command'* by the base unit

Control Action	Base unit setpoint matches user-defined set point	ORP level	Hazardous if provided in this context	UCA
Base unit sends ozone dosing command when	No	*	yes	10-1
	yes	User-defined set point target range	Yes	10-2
	yes	Low-level ORP	no	
	yes	Critical Low-level ORP	no	
	yes	High-level ORP	yes	10-3
	yes	Critical high-level ORP	yes	
Base unit does not send ozone dosing command when	No	*	Yes	
	yes	User-defined set point target range	no	
	Yes	Low-Level ORP	yes	10-4
	yes	Critical Low-level ORP	yes	10-5
		High-Level ORP	no	
	yes	Critical high-level ORP	no	

* Indicates variable value not important in the respective context

Table 3 The context table for the control action for '*perform user probe calibration'*

Control Action	Calibration Schedule	Calibration procedure performed correctly	Hazardous if provided in this context	UCA
Perform User Calibration when	due	yes	No	
	not due	yes	No	
	overdue	yes	Yes	
	*	no	Yes	20-1
Doesn't Perform User	due	*	Yes	20-2
	not due	*	No	

Control Action	Calibration Schedule	Calibration procedure performed correctly	Hazardous if provided in this context	UCA
Calibration when	overdue	*	Yes	20-3

* Indicates variable value not important in the respective context

Using the information in the context tables for the given combinations of variables and values, UCAs were identified. The information obtained from the UCA column on the far right indicated if a given set of combination of values for the variables could result in a UCA. The UCA tables for the control action *send ozone dosing command* and *perform user calibration* are shown in Table 4.

Table 4 UCAs for the control actions identified using context tables

Control action	**Not providing**	**Providing**	**Providing too soon / too late**	**Stopping too soon / Applying too long**
send ozone dosing command	Dosing command not provided when below set point (UCA10 - 5)	The dosing command is provided for a set point not set by user (UCA10-1) Dosing command is provided when ozone is not required (UCA10-2)	The dosing command is delayed in being sent from base unit (UCA10 - 4)	The dosing command is still provided after the set point is achieved (UCA10-3)
perform user calibration	User does not perform user calibration (UCA 20-3)	User does not follow required procedure when performing a calibration (UCA20-1)	User calibrates probe after scheduled period (UCA20-3)	N/A

Identify Loss Scenarios

For each of the UCAs identified, the possible loss scenarios and associated CF were considered. The CF is the situation in which the UCA may occur, and the scenario provides the context of the situations. To guide the process of identifying possible scenarios and CFs the classification of control flaws leading to hazard presented in Leveson (2013) was used for each control loop in the system.

This second step in the STPA process identified a total of 204 CFs for UCAs in the user operation of the AQWMS, which provide insight into how UCAs may be realised during operation. However, 204 CFs proved to be a large amount to manage when developing the final countermeasures. A careful review of the scenarios by the analysis team revealed many of the CFs identified from the STPA scenarios could be addressed or removed through one or more countermeasures. For example, the CF of 'The user being unaware of how to place the probe unit in the rack correctly' and 'failure of probe components' both will result in no valid reading being available for the respective parameter. In both scenarios, the countermeasure of 'software will generate an error message when a parameter is called but no measurement is available' will inform the user of the potential for violation of the system safety constraint. Therefore, when developing countermeasures, the focus was on specifications that provide the development and testing requirements with the most coverage of potential CFs.

The final countermeasures developed by the analysis team based on the CFs identified in the STPA can be grouped into two main categories, requirements for design improvements and process logic requirements to minimise the opportunity for operator error. An example of the CF and

associated countermeasures which are used to test and refine design are provided in Table 5. Figure 6 shows the percentage of the CFs which can be attributed primarily to equipment design, user actions, software design and logic as well CFs which are a combination of one or more category.

Table 5 An example of the countermeasures for the product development

CF ID	CF	Counter measure ID	Countermeasure	UCA	Components
CF1-P-1-1	User is unaware of how to place the probe unit in the rack correctly	M1	Software will generate error "NP" on base unit display if no signal is received from wireless electrode interface	(UCA1-1) User doesn't place probe correctly when installing the system [SC4]	Base unit electrodes wireless electrode interface
CF16-T-3-1	The logic in the dosing levels allows for low pH and high pH limits being set at the same level	M32	Constraints in the software prevent the user being able to set the high and low pH set points being too close together	(UCA16-3) Alkaline solution is dosed at the same time as an acid solution [SC1] [SC2]	Base unit

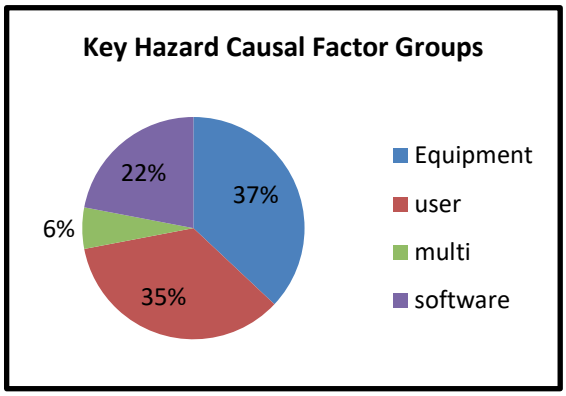

Figure 7: Hazard groups for the Hazard Causal Factors identified for the UCAs

Input into safety system

The STPA process identified 204 CFs related to the AWQMS design and user operations. From the CFs, 94 countermeasures were identified. These countermeasures were used to provide guidance in the final design of system functions, physical equipment and user information. To aid in the design and testing process, the countermeasures were grouped into the following categories:

- design solutions to remove the hazard from the system or prevent the hazard from occurring (e.g. hardware design forces the user to place equipment correctly).
- alert the user to unsafe system water quality (e.g. alarms and notification)
- provide information that guides the user in the operation of the AWQMS to avoid system hazards

For the software related CFs, the relevant countermeasures were translated into user stories to describe the required software solutions from the end-user perspective. The equipment related countermeasures were feedback to the equipment design process to ensure requirements were suitably addressed. Furthermore, the countermeasures serve as a guide for the development of testing criteria. As part of the testing phase, CFs serve as scenarios to assess the effectiveness of the design countermeasure in enforcing the required safety constraints.

3.2. Bow-tie Method

Taking a process approach, the hazard was identified as '*Hydroponic water quality operations*' as this is the key activity which can lead to a hazard in the system. The corresponding top event which can lead to an unwanted loss is identified as '*system water quality not suitable for plant growth*'. This was selected as it represented the event which could lead to the consequences identified but also aligned with the system level hazardous event identified in the STPA results. The items with a significant inherent risk identified in the HAZID are presented in table 6.

Table 6 The significant items identified in the HAZID process included in the bowtie diagram

Threats	**Consequences**	**Likelihood**	**Severity**
Equipment installed incorrectly	Loss of crop production or loss of crop quality	almost certain	full loss of crop
Water Quality measurement errors	Loss of crop production or loss of crop quality	possible	full loss of crop
Incorrect dosing of chemicals	Loss of crop production or loss of crop quality	very likely	considerable loss of crop production
Incorrect thermal control	Loss of crop production or loss of crop quality	possible	considerable loss of crop production
Errors in information from web interface	Loss of crop production or loss of crop quality	very likely	considerable loss of crop production
User-generated errors	Loss of crop production or loss of crop quality	almost certain	full loss of crop

The resulting Bow-tie diagram for the risk analysis of the AWQMS is shown in Appendix 1. Consequences of the top event occurring, and water quality not controlled within specification includes '*loss of crop production*' and '*loss of crop quality'*. The loss of crop production is the complete mortality of the crop due to incompatible water quality which will potentially require considerable effort to recover from, and loss of crop quality is the occurrence of sub-optimal production rates which can potentially be reversed much easier.

The six threats on the left-hand side of the diagram are the higher likelihood and severity hazards identified through the HAZID process. The threats Identified in the Bow-tie method include human interaction factors such as the activity of installing equipment and user-generated errors such as incorrectly assigning alert values for the intended application, as well as functional controls of the AWQMS components. The process identified a total of 23 preventative barriers and seven recovery barriers. To aid system development, each of the barriers has a short description which serves as an explanation of requirements for the system design. Requirements can be applied to the hardware design process, software design process and production of user information

Input into system design

The resulting Bow-tie diagram provides a visual representation of the path from the threats to the top event and from the top event to the consequences which represents losses due to unsafe actions of the AWQMS. The barriers provide guidance on the threats to plant growth that need to be considered in the development of the system. The barriers provide the developer with general requirements based on identified barriers rather than specific system design criteria. In the design process, an additional step is required for the design process to identify design solutions which meet the required functions of the barriers in place.

4. DISCUSSION

The outputs of STPA and the Bow-tie method are very different and provide information about the system hazards and risks in different ways. This difference means that a complete one-for-one comparison of the results of the results from the two different methods is not possible (Chatzimichailidou, Ward, Horberry, & Clarkson, 2018). Qualitatively, the key differences would be their possible contribution to the design of the AWQMS through the level of detail in the hazard identification and control requirements output by two methods. The Bow-tie method focuses on individual barriers for a given threat and barriers to potential escalation factors which can result in the reduced performance of a barrier. There are 22 preventative barriers and seven recovery barriers identified for inclusion in the design and testing process with broad requirements for reducing the risk of user error and the risks associated with ongoing testing and operations of the AWQMS. A key benefit is that the Bow-tie diagram provides a good visual representation of the risk progression from the threats to the top event and top event through to consequence as well as the role barriers have in halting this progression in risk.

During the process of developing design criteria based on hazard analysis results, additional judgement must be made on the priority for the design change based on resources and the contribution to the control of a hazard. The STPA process provides the design process with 204 specific CFs which were used to create 94 countermeasures for software, and hardware design needs as well as user information material. The biggest challenge for the STPA process is the large number of CFs which are generated from the UCAs and then ensuring all the feasible scenarios are considered. This step results in numerous countermeasures which need to be included, and many of the countermeasures can be applied to more than one CF. For the process, the countermeasures identified are used to develop design and testing requirements for consideration in the design and verification phases. With the large number of CFs, the challenge becomes identifying suitable countermeasures to ensure the risk is reduced to as low as reasonably practicable. The design process is constrained by many factors such as time, technology and cost which means that the requirements need to be prioritised. For the Bow-tie diagrams, a criticality level can be applied to the barrier based on the opinion of the analysts. However, the high-level nature means that different requirements may exist for the different design inputs to meet the intended function of the barrier.

Comparing the safety controls identified from both the Bow-tie method and STPA shows that many of the countermeasures from STPA can be mapped to the barriers in the Bow-tie diagram (Table 7). The larger number of STPA identified countermeasures resulted in mapping most of the Bow-tie method results with multiple countermeasures. During this process, 19 of the STPA identified countermeasures failed to align with any of the Bow-tie method barriers.

Table 7 Comparison of Bow-tie method barriers and STPA identified countermeasures

Bow-tie Method Barriers (preventative and Recovery)	Number of times barrier is used in Bow-tie	Number of STPA countermeasures matched with barrier
Accurate control of doing by base unit	1	10
Correct Installation of System components	1	1
Dosing Alerts	2	13
Ensure correct chemical is available when dosing is called	1	2
Generate user alerts if equipment not communicating correctly	1	2
hardware design to prevent user from incorrectly installing components	1	2
High High & Low Low water quality alerts	1	3
Periodic Calibration of probes	1	3

Bow-tie Method Barriers (preventative and Recovery)	Number of times barrier is used in Bow-tie	Number of STPA countermeasures matched with barrier
Periodic Maintenance and servicing	3	2
Post-purchase user support	1	2
Provide user with AWQMS installation procedures	1	7
Provide user with operational instructions	3	6
Provide user with recommended specs for system components and performance	1	2
system is calibrated prior to use	1	1
Troubleshooting Guides	2	7
Unique identification for each user and gateway	1	1
Use reliable 3rd party cloud storage service provider	1	1
User-friendly interface	3	2
Water Quality Alerts	2	4
Web Notification of system errors	1	2
No Matching Bow-tie Barrier		19

5. CONCLUSION

Incorporating hazard analysis early in the design process aids in assuring that the resulting design meets performance and user requirements. The hazard analysis process also supports expediting the prototyping and testing through developing criteria based on countermeasures identified to enforce safety in the system. To aid the design process, the countermeasures need to be practical and easily implemented without introducing further complications or disregard system hazards in the final design. This requires an iterative approach to testing and design.

As a hazard analysis tool, STPA provides a very effective analysis of the sociotechnical hazards associated with automated water quality management systems operations. The results, in turn, are used to further refine the system to improve usability, reduce the opportunity for both technical and operator error and even identify the needs for improvements in operator management. The output from the STPA is easily transformed into system requirements which can be used to reduce the chance of user error when operating the AWQMS. Bow-tie diagrams provide a visual representation of the system risk path from threat through to the final consequences. This visual representation is also beneficial in identifying which barriers are preventative and which barriers are recovery, this type of information is not readily visible in the STPA information. The biggest challenge is with the need to take the barriers and work further to ensure the system design meets the intent and performance of each of the barriers.

Both methods identified useful measures to control the hazards associated with human interaction with the AWQMS. However, the measures differed in the level of detail and the involvement in the evolution in the final system losses. In this study, the STPA process was able to identify some hazards which did not visibly relate to the Bow-tie barriers. However, the Bow-tie diagram includes a visible distinction between preventative and recovery hazard controls. Previous studies have proposed the complimentary use of the Bow-tie method and STPA, where a bow-tie diagram can provide the analyst with a prompt of the areas of concern before commencing the STPA process to provide a more robust outcome (Chatzimichailidou, Ward, Horberry, & Clarkson, 2018). In this case study, the STPA component required considerably more time than the Bow-tie method especially in the identification of factors which cause the hazards and the appropriate controls of the hazard. Measures that can improve the ease of the process of identifying system hazards and

reduce the time taken to complete analysis of the full system could prove beneficial in future technology design applications.

While this study considers the application the AWQMS to hydroponics, the hazard identification process can be applied to the same system when repurposing the design for other applications including drinking water management or recycled water applications where there is potential for public health impacts and also involve tight regulatory requirements. Such applications are often remote and or operated by staff with limited experience and training in all aspects of systems operations. In these scenarios, the automated systems and the operators must interact in a way which ensures ongoing safe operations.

ACKNOWLEDGEMENTS

The authors would like to thank the peer reviewers of this paper for their comments and suggestions. The feedback provided has significantly improved the content of this paper.

REFERENCES

Cameron, I., Mannan, S., N´emeth, E., Park, S., Pasman, H., Rogers, W., & Seligmann, B. (2017). Process Hazard Analysis, Hazard Identification and Scenario Definition: Are the conventional tools sufficient, or should and can we do much better? Process Safety and Environment Protection, http://dx.doi.org/10.1016/j.psep.2017.01.025.

CGE Risk. (2017). Bowtie Methodology Manual, Rev 17. CGE Risk Management Solutions.

Chatzimichailidou, M. M., Ward, J., Horberry, T., & Clarkson, J. P. (2018). A Comparison of the Bow-Tie and STAMP Approaches to Reduce the Risk of Surgical Instrument Retention. Safety Analysis, 38, pp. 978-990. https://doi.org/10.1111/risa.12897

Dokas, I. M., Feehan, J., & Imran, S. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. Safety Science, 58, 11-26. https://doi.org/10.1016/j.ssci.2013.03.013

Fleming, C. H., Spencer, M., Thomas, J., Leveson, N., & Wilkinson, C. (2018). Safety assurance in NextGen and complex transportation systems. Safety Science, 55, 173-187. https://doi.org/10.1016/j.ssci.2012.12.005

Hokstad, P., Røstum, J., Sklet, S., Rosén, L., Pettersson, T. J., Linde, A., . . . Niewersch, C. (2009). Methods for risk analysis of drinking water systems from source to tap - guidance report on Risk Analysis. TECHNEAU report.

Lee, P.G. (1995) A review of automated control systems for aquaculture and design criteria for their implementation. Aquacultural Engineering pp205-227, https://doi.org/10.1016/0144-8609(94)00002-I

Leveson, N. (2013). Engineering a Safer World: Systems Thinking Applied to Safety. Boston, Massachusetts: MIT Press. ISBN978-0-262-01662-9

Leveson, N. (2015). A systems approach to risk management through leading safety indicators. Reliability Engineering and System Safety, 136, 7–34. https://doi.org/10.1016/j.ress.2014.10.008

Leveson, N., & Thomas, J. (2018). STPA Handbook. Accessed: Apr., 2018. [Online]. Available: http://psas.scripts.mit.edu/ home/get_file.php?name=STPA_handbook.pdf.

Leveson, N., Daouk, M., Dulac, N., & Marais, K. (2003). Applying STAMP in Accident Analysis. Workshop on the Investigation and Reporting of Inicdents Accidents.

McLoed, R. W., & Bowie, P. (2018). Bowtie Analysis as a prospective risk assessment technique in primary healthcare. Policy and Practice in Health and Safety, 16, 177-193. https://doi.org/10.1080/14773996.2018.1466460.

Merrett, H. C., Horng, J. J., & Chen, W. T. (2018). Systems Analysis of the 1998 Sydney Water Crisis. Presentation at 2018 MIT STAMP Workshop.

Olsson, G., (2007) Automation Development in Water and Wastewater Systems. Environmental Engineering Research, 12, 197-200, https://doi.org/10.4491/eer.2007.12.5.197

Reason, J. (2000). Human error: models and management. British Medical Journal, 320, 768-770. https://doi.org/10.1136/bmj.320.7237.768

Saud, Y. E., Israni, K., & Goddard, J. (2014). Bow-Tie diagrams in downstream hazard identification and Risk Assessment Process. Safety Progress, 33, 26-35. https://doi.org/10.1002/prs.11576

Savvas, D. (2003). Hydroponics: A modern technology supporting the application of integrated crop management in greenhouse. Food, Agriculture & Environment, 1, 80-86.

Sulaman, S. M., Beer, A., Felder, M., & Host, M. (2017). Comparison of FMEA and STPA safety analysis methods: a case study. Software Quality Journal, 1-39. https://doi.org/10.1007/s11219-017-9396-0

APPENDIX 1: FULL BOW-TIE DIAGRAM FOR THE AWQMS