Application of STPA in the Development and Testing of an Automated Water Quality Management System

HEW CAMERON MERRETT¹, JAO JIA HORNG², ANDREW PIGGOT³, AMRO QANDOUR⁴ & CHEN WEI TONG⁵

¹GRADUATE SCHOOL OF ENGINEERING SCIENCE AND TECHNOLOGY, NATIONAL YUNLIN UNIVERSITY OF SCIENCE AND TECHNOLOGY, TAIWAN
²GRADUATE SCHOOL OF ENVIRONMENTAL, HEALTH AND SAFETY ENGINEERING, NATIONAL YUNLIN UNIVERSITY OF SCIENCE AND TECHNOLOGY, TAIWAN
³OAS, SWEDEN AB
⁴CENTRE FOR COMMUNICATIONS AND ELECTRONICS RESEARCH, EDITH COWEN UNIVERSITY, AUSTRALIA
⁵DEPARTMENT OF CIVIL AND CONSTRUCTION ENGINEERING, NATIONAL YUNLIN UNIVERSITY OF SCIENCE AND TECHNOLOGY, TAIWAN

CORRESPONDING AUTHOR: +886 972 504 960 AND HEW.MERRETT@GMAIL.COM
Introduction

A case study on the application of safety guided design for an Automated Water Quality Management System (AWQMS)

Automated systems are commonly used in water quality management where there are precise water quality requirements

The AWQMS is intended for use by operators with limited knowledge of water quality management operations

Two methods are compared – STPA and Bowtie Analysis

The focus is on the hazards from user interaction and operations with the AWQMS
wireless waterproof water sensing electrode modules for
- Oxidation Reduction Potential (ORP),
- pH,
- temperature, and
- electrical conductivity (EC).

Electrode modules are positioned in a rack attached to the base and receive power wirelessly.

The signal is then transmitted to the processing unit using an optical link method.

Outputs for controlling measured system parameters through auxiliary dosing, heating and cooling units

Web interface for viewing water quality data
Safety Guided Design

- Case study - Use in medium scale hydroponic/aquaponics systems
- The hazard assessment was commenced after the initial concept of the system was developed
- The hazard analysis outcomes were used to
  - Guide the equipment and software design process
  - Develop testing criteria
  - Provide assurance that safety is embedded into system operations
Hazard analysis methodology

- **System Theoretic Process Analysis (STPA)**
  - Based on STAMP
  - Views safety as an emergent property of the system

- **Bowtie Analysis**
  - Uses a barrier approach
  - Provides a visual representation of control over system hazard
System water quality not suitable for plant growth

Hydroponic system water quality operations

Generate user alerts if equipment not communicating correctly

Hardware design to prevent user from incorrectly installing components

Provide user with AWQMS installation procedures

Provide user with recommended specs for system components and performance

Installed incorrectly

Inefficient measurement errors

Ineficient dosing of chemicals

Incorrect thermal control

COR R7 installation from Web Interface

User generated errors

User friendly interface

Operational instructions

Maintenance and servicing

Ensure correct chemical is available when dosing is called

Accurate control of dosing by base unit

Dosing Alerts

Water Quality Alerts

Troubleshooting Guides

Loss of crop production

Loss of crop quality

Web notification of system errors

Periodic Calibration of probes

Calibration of probes

Generation of system errors

Detection of system errors

End of dosing by base unit

Base unit is calibrated prior to use

Unique identification for each user and gateway

Cloud storage service provider

Use of 3rd party cloud storage service provider

Post purchase user support

Provide user with operational instructions

User friendly interface

Purchase user support

Correct Installation of System components
Bowtie Results – preventative barrier

- System water quality not suitable for plant growth
- Hydroponic system water quality operations
- Generate user alerts if equipment not communicating correctly
- Hardware design to prevent user from incorrectly installing components
- Provide user with AWQMS installation procedures
- Provide user with recommended specs for system components and performance

- System is calibrated prior to use
- Calibration of system components
- Calibration of probes
- Maintenance and servicing
- Operation of system errors
- Operation of system errors

- Periodic maintenance and servicing
- Correct installation of system components
- Maintenance and servicing
- System calibrated prior to use
- Calibration of system components
- Calibration of probes
- Operation of system errors

- Accurate control of dosing by base unit
- Ensure correct chemical is available when dosing is called
- Periodic calibration of probes
- User-friendly interface
- Provide user with operational instructions

- Correct dosing of chemicals
- Periodic maintenance and servicing
- User-friendly interface
- Provide user with operational instructions

- Correct thermal control

- Use reliable 3rd party cloud storage service provider
- Unique identification for each user and gateway
- User-friendly interface
- Periodic maintenance and servicing

- Correct installation of system components
- Maintenance and servicing
- System calibrated prior to use
- Calibration of system components
- Calibration of probes
- Operation of system errors

- System calibrated prior to use
- Calibration of system components
- Calibration of probes
- Maintenance and servicing
- Operation of system errors
Bowtie Results – Recovery Barrier

- Quality not suitable for plant growth
- Water quality alerts
- Troubleshooting guides
- Loss of crop production
- Loss of crop quality

Dosing alerts

Water quality high & low

Troubleshooting guides
STPA Results

### Small to medium hydroponics installation (including crop, pumps, dosing equipment and water)

<table>
<thead>
<tr>
<th>Accident</th>
<th>Hazard ID</th>
<th>Hazard</th>
<th>Safety Constraint ID</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>system water quality violates criteria for supporting crop growth</td>
<td>SC1</td>
<td>system water quality must remain inside designated water quality parameters for crop growth</td>
<td></td>
</tr>
<tr>
<td>H2</td>
<td>control of physiochemical parameters and dosing chemicals causes out of spec WQ in the system</td>
<td>SC2</td>
<td>If WQ parameters are out of spec, then system must detect and correct WQ physiochemical parameters</td>
<td></td>
</tr>
<tr>
<td>H3</td>
<td>Production of crop is reduced when WQ is sub optimal</td>
<td>SC2</td>
<td>If WQ parameters are out of spec, then system must detect and correct WQ physiochemical parameters</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HCF ID</th>
<th>HCF</th>
<th>Countermeasure ID</th>
<th>Countermear</th>
<th>UCA</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCF11-D-1-3</td>
<td>The temp signal received from the base unit does not reflect actual system conditions</td>
<td>M10</td>
<td>label on sensor to indicate that it must be placed in the water to specified depth</td>
<td>(UCA11-D-1) the base unit ceases sending the heating/cooling command before the desired temp is achieved</td>
<td>Base unit, electrodes, wireless electrode interface</td>
</tr>
<tr>
<td>HCF16-T-3</td>
<td>The logic in the dosing levels allows for a low pH and high pH limits being set at the same level</td>
<td>M32</td>
<td>constraints in the software prevent the user being able to set the high and low pH set points being too close together</td>
<td>(UCA16-T-3) alkaline solution is dosed at the same time as acid solution</td>
<td>Base unit</td>
</tr>
</tbody>
</table>

### System Components

- **User/Operator**: Log into system, perform user calibration, position probes, configure alerts.
- **Base Unit**: Read wireless interface, send signal, power probe, send binary signal.
- **Electrodes**: Read water quality parameter, set baseline, configure alerts.
- **Temp Probe**: Optical transmission of value signal.

### Loss of Crop Production

- M10: Label on sensor to indicate that it must be placed in the water to specified depth.
- M32: Constraints in the software prevent the user being able to set the high and low pH set points being too close together.

### UCA Components

- UCA11-D-1: Base unit ceases sending the heating/cooling command before the desired temp is achieved.
- UCA16-T-3: Alkaline solution is dosed at the same time as acid solution.
The hazard analysis results from both methods provided useful information in the design and testing processes.

STPA results provide a higher level of detail which is valuable for developing design test requirements.

Bowtie Analysis provides a good visualisation of the causes, controls and consequences.

88 countermeasures developed based on STPA.

20 individual barriers from Bowtie Analysis.

<table>
<thead>
<tr>
<th>Bowtie Analysis Barriers (preventative and Recovery)</th>
<th>Number of times barrier is used in Bowtie</th>
<th>Number of STPA countermeasures matched with barrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate control of doing by base unit</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Correct Installation of System components</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Dosing Alerts</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>Ensure correct chemical is available when dosing is called</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Generate user alerts if equipment not communicating correctly</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Hardware design to prevent user from incorrectly installing components</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>High High &amp; Low Low water quality alerts</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Periodic Calibration of probes</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Periodic Maintenance and servicing</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Post purchase user support</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Provide user with AWQMS installation procedures</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Provide user with operational instructions</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Provide user with recommended specs for system components and performance</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>System is calibrated prior to use</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Troubleshooting Guides</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Unique identification for each user and gateway</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Use reliable 3rd party cloud storage service provider</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User friendly interface</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Water Quality Alerts</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Web Notification of system errors</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

No Matching Bowtie Barrier: 19
Input into the design process

- STPA results were preferred as the preferred input into the final AWQMS design
- 88 countermeasures were identified
- Software input
  - Develop user stories and functional criteria
  - Hardware design
- Develop functional design criteria
  - User information
  - User guides
  - System compatibility for auxiliary equipment
  - Trouble shooting guides

Key Hazard Causal Factor Groups

- Equipment: 37%
- User: 22%
- Multi: 6%
- Software: 35%
Input into the design process

- Example of safety input into the final design
  - The hazard analysis identified a series of HCFs associated with the loss of communication of the electrode module with the base unit
    - User incorrectly placing the module in the base unit rack
    - The module does not sit in the correct location when placed or after disturbance
    - The module does not sit close enough to transfer the required power level or support optical transmission of data
Input into the design process

- Design solutions to maintain compliance with system safety constraints
  - Design a unique shape and fit for each probe and corresponding location on rack
  - Use magnets to help hold in correct location
  - Display error messages on base unit
  - Provide a troubleshooting guide for the user
Conclusion

- Hazard analysis during the design process provides valuable insight into designing for safe operations by the user.
- The use of STPA early in the process can help reduce the time and resources required in the design and development. To realise this benefit requires a large investment of time in the development of scenarios and countermeasures.
- In this study the STPA process was able to identify several hazards which did not clearly relate to the Bowtie Analysis barriers.
- Challenge in prioritising the changes to system design based on the hazard analysis results. What countermeasures give the best value for money?
- Bowtie Analysis is relative quick and was helpful as tool in checking if anything had been missed during the STPA.
Thank you!

- Questions?