

DISCLOSING CYBER ATTACKS ON WATER DISTRIBUTION SYSTEMS. AN EXPERIMENTAL APPROACH TO THE SONIFICATION OF THREATS AND ANOMALOUS DATA.

Sara Lenzi

Density Design Lab, Design Department,
Politecnico di Milano
Via G. Candiani, 72
2058 Milano, Italy
sara.lenzi@polimi.it

Ginevra Terenghi

Density Design Lab, Design Department,
Politecnico di Milano
Via G. Candiani, 72
2058 Milano, Italy
ginevra.terenghi@mail.polimi.it

Riccardo Taormina

iTrust
Singapore University of Technology and Design,
8, Somapah Raod
487372 Singapore
riccardo_taormina@sutd.edu.sg

Stefano Galelli

Pillar of Engineering Systems and Design
Singapore University of Technology and Design,
8, Somapah Raod
487372 Singapore
stefano_galelli@sutd.edu.sg

Paolo Ciuccarelli

Art + Design Department
Northeastern University,
360 Huntington Ave.,
Boston, MA, 02115
p.ciuccarelli@northeastern.edu

ABSTRACT

Water distribution systems are undergoing a process of intensive digitalization, adopting networked devices for monitoring and control. While this transition improves efficiency and reliability, these infrastructures are increasingly exposed to cyber-attacks. Cyber-attacks engender anomalous system behaviors which can be detected by data-driven algorithms monitoring sensors readings to disclose the presence of potential threats. At the same time, the use of sonification in real time process monitoring has grown in importance as a valid alternative to avoid information overload and allowing peripheral monitoring.

Our project aims to design a sonification system allowing human operators to take better decisions on anomalous behavior while occupied in other (mainly visual) tasks. Using a state-of-the-art detection algorithm and data sets from the Battle of the Attack Detection Algorithms, a series of sonification prototypes were designed and tested in the real world. This paper illustrates the design process and the experimental data collected, as well results and plans for future steps.

1. INTRODUCTION

Water supply systems are experiencing a transition from physical to cyber-physical systems: networked devices (smart sensors, industrial computers, telemetry units...) are used for monitoring and control purposes in order to increase the reliability and controllability. At the same time, though, these devices expose water plants (a key infrastructure in any country) to cyber threats. Research has recently focused on understanding the potential impacts of cyber-attacks and designing appropriate countermeasures. [1]

1.1. The Anomaly Detection Algorithm

The sonification project presented in this paper is based on an algorithm specifically designed for detecting and localizing cyber-attacks against water distribution systems. The algorithm builds on a Deep Learning model that is able to replicate the patterns of all hydraulic processes observed within a distribution system. In particular, the model is first trained using data pertaining to normal operating conditions. When fed new data, the model is likely to poorly reproduce data containing anomalous patterns, such as those induced by cyber-attacks, resulting in higher reconstruction errors. These errors are then analyzed in real-time to identify the anomalies related to cyber-attacks.[2]

The current approach for representing data produced by algorithm for consumption by a final user typically relies on visual, analytical diagrams. These traditional representations,



This work is licensed under Creative Commons Attribution – Non Commercial 4.0 International License. The full terms of the License are available at <http://creativecommons.org/licenses/by-nc/4.0/>

displayed in real time on multiple screens and demanding continuous visual attention might be not suited to take an appropriate, informed response in a critical situation due to several reasons. Among these, the need for the operator to perform multiple visual tasks at a time and the visual channel overload caused by the introduction of a visual layer dedicated to cyber-threats as discussed in [3]. Thirdly, anomaly detection algorithms are still exposed to a certain degree of inaccuracy which results in the production of false alerts, with false positive alerts highly impacting on daily operations [2]. Furthermore, data compromised by an attack may differ very little from healthy data and therefore their visualization might be misleading.

1.2. Application of sonification to real-time process monitoring

Sonification [4] has been discussed in the past decades as a successful means of representing data in real-time process monitoring in the fields of medical applications [5]; financial [6]; security [3]; industrial production [7]. Specific characteristics of sound that make it a suitable candidate for the representation of real-time information have been extensively illustrated [8] and the specific area of process monitoring has also been extensively reviewed by recent literature. [9]

Cyber-security seems to be a promising field for the application of sonification to real-world situations. We already know that sound allows for peripheral monitoring [10] while leaving the center of our attention to visual tasks, also preventing information overload on the visual channel [11]. Additionally, human beings are very prompt at detecting changes in acoustic patterns [8], an added value of in anomaly detection tasks.

Despite promising results though, real-world applications are still far from being a recognized practice in academia, let alone in Industrial Control Systems. To the best of our knowledge, there is no offer of sonification tools available on the market to complement standard visualization dashboards. We believe that the main reason for this delay is the lack of prototype-based extensive experimental results involving real users in real settings. As repeatedly pointed out by the research community [12] [9] [13], the lack of applied and experimental results for sonification systems still represents one of the biggest weaknesses of a field that has shown and is showing a promising growth in public interest.

2. CYBER-ATTACKS TO WATER DISTRIBUTION SYSTEMS: DEFINING A USE-CASE FOR SONIFICATION

Artificial Intelligence is destined to gain predominance in the near future. In almost every aspect of our daily lives, we are immersed in an unprecedented mass of information we collect from the world around us: a continuous flow of data whose intricacies require an artificial intelligence able to work at a non-human scale to support humans in the task of collecting, organizing, and making-sense of it. On the other hand, hyper-reliance on automated systems and a *techno-chauvinistic* enthusiasm [14] tend to hide the fact that, in order to understand and make use of the information provided by AI systems, we still need to translate it into human – scaled knowledge.

Design is charged with the task of facilitating such translation. [15] Through design artefacts, final users are put in the condition to leverage their unique, sophisticated human experience in order to integrate machine systems and machine

thinking into everyday life. We understand the representation of data as a design process aiming to transform data into knowledge [16]. Through preliminary research, the designer delineates a narration where the specific means for representing data are not pre-determined but are the result of specific design constraints. In this sense, we do not see sonification as an independent means of data representation able to reach a universal validity. The use of sound intervenes in the continuum from data to knowledge in all those cases where, based on preliminary analysis, it adds a value to the data representation process.

The following paragraph illustrates the process we conducted to delineate a specific use case for sonification for anomaly detection in water distribution systems.

2.1. Design constraints

During preliminary analysis, a series of constraints for the design of the sonification were identified. A non-exhaustive list includes:

- We consider sound as an integration, and not as a substitute, for the visual display of information in control rooms;
- As such, we do not intend for sound to represent and report all the information currently reported by the embedded visualization tools;
- The user experience takes into account the current state of a real context of usage. Questions related to the type of sound diffusion system we could use will have to be answered. For example: will users be willing to use headphones? The answer will constraint the design, for example excluding the usage of sound spatialization;
- Data are represented in real-time. As the current data resolution is capped at one hour, a sound will be designed to play every hour. This will exclude, for the time being, the option of a continuous sonification, a choice that would imply other design considerations on exposing users to a continuous background sound; [17] [18]
- In the absence of solid evidence on the advantages of the use of tuned sounds (or music) versus non tuned sounds, we will produce different versions of the prototype in order to gather first hand results.

2.2. Defining the use-case

2.2.1. The Context

The sonification represents data on cyber-attacks to the digital components (e.g., sensors, PLCs) of a water distribution network causing anomalous hydraulic processes—for example, low water pressure at the consumers' nodes caused by the intentional malfunctioning of a digitally-controlled pumping station. Currently, there are not engineering practices specifically dedicated to understanding in real time when a water network is under cyber-attack. An attack would mainly be identified as such during a subsequent forensic investigation. In case of an attack, control room operators can only see that the plant is presenting anomalous or faulty behavior in one or more of its components (tanks, water pipes, pumps, valves).

The anomaly detection algorithm object of the present project was developed to be integrated into the daily operations of the water plant. The algorithm would run in real-

time in a computer hosted in the control room, and it would trigger an alert in case of an anomaly.

2.2.2. The User

Our user is typically an engineer expert in managing water-related infrastructures. At present day, the intervention of a security operator in the event of an alert is manual: he/she acknowledges the alarm and manually proceeds to further checkups of the system, for instance, opening the current software visual interface to access a detailed report on the behavior of a specific component; controlling other parts of the system that might be connected to the alarm; run a *in situ* manual check, and so on. A protocol is in place for the management of emergencies, as well as a detailed procedure provided by the developers of the system to help differentiating among types of alerts. During a normal operation day, the user would distribute his/her time among different tasks, ranging from reading historical data, compiling reports, receiving phone calls, talking to colleagues, monitoring the real time status of the system both in terms of quality and quantity of water. In a medium-sized water plant, a system of about nine screens will display to two operators all the necessary information, making most of their current tasks visual, thus requiring the focus on their attention.

2.2.3. The Objectives

Information is conveyed to the operator to allow him/her to gain awareness on the status of the system at all times. In this specific case, the anomaly detection algorithm for cyber-threats makes it possible for the operator to discriminate between anomalies generated by faults of the systems and anomalies generated by external, malicious intrusion. This second type of anomalies are extremely hard to identify due to their specific nature, notably, that cyber-attacks are able to interfere with existing monitoring systems to deliberately introduce false information to fool the operators. [2] Once information on a possible cyber-attack reaches the operator, he/she will use it to take action, be it cross check it against data from other software; run a manual check of the plant; analyze historical data; launch a full-scale alarm; dismiss it as non-relevant.

2.3. Preliminary hypothesis

As mentioned, at this stage of development, machine learning detection mechanisms, such as the one adopted in this study, are still subject to a considerable rate of false (mainly, false positive) alerts. As a consequence, they can lack reliability in a real context of usage. In a private communication, an operator of a water plant control room reported that as the rate of false positive alert reaches up to one per day, the only solution for maintaining an efficient work flow is to keep the alarm system off. As a participant to our experiment, and former operator, puts it, “*In a water plant we do not trust machines*”.

We hypothesize that this feeling of mistrust is essentially due to a design issue in the choice and implementation of the data-to-knowledge process. We consider our user a human operator with a thorough, sophisticated, long acquired knowledge of the system she/he manages. We therefore hypothesize that a well-designed relationship with the data should put the operator in the position to leverage his/her field experience to limit the impact of the algorithm’s errors on the decision-making process. Such

a well-designed relationship should grant a better understanding of causality between events (i.e. recognize and act in face of a real attack or dismiss alerts a false alarm), while taking advantage of an artificial intelligence-led system able to identify and make prediction on the specific nature of cyber-attacks.

2.4. The choice of sonification

We considered the following aspects as added values sonification could bring to the specific case:

- The sonification would keep at the periphery of attention while prompting the retrieval of analytical visual information when needed [10] [19]. Therefore, we won’t need to introduce a new visualization system dedicated to cyber-attacks on top of those already in use for routine operations;
- Current alarm systems act on an on/off, 1/0 principle. Acoustic or visual alarms in a control room will either communicate a full alarm or no alarm, which is a radical simplification of continuous data coming from the algorithm. We believe that communicating intermediate status of the system, even if uncertain, via sound [11] might help the operator leverage his/her experience to take further decisions;
- Finally, we hypothesize that the user will, over time, develop a knowledge on “how the system sounds” enabling him/her to make predictions, thus anticipating problems instead of merely reacting to emergencies when these have already occurred. [20]

3. SONIFICATION DESIGN: PROTOTYPING

We designed and implemented two series of prototypes. Description of choices of sounds, mapping strategies and implementation follows.

3.1. Data sets

Given the relevance of water distribution networks for national security, detailed information on cyber-attacks against water utilities are generally not available. Therefore, we adopted simulated, yet realistic, data produced by the numerical simulation software epanetCPA for the case of the C-Town water distribution system, a medium-sized network made of 429 pipes, 388 junctions, 7 storage tanks, 11 pumps and 1 distribution valve, distributed over five demand districts. The employed datasets featured a total of 43 synthetic variables including tank water levels, inlet and outlet pressure for the valve and the pumping stations, as well as their flow and status (on/off). In particular, the datasets were part of the BATtle of the Attack Detection ALgorithms (BATADAL), an international competition on cyber security of water distribution systems. The BATADAL features two training datasets and a test dataset which included a total of 14 different attack scenarios. [2]

Two sonification prototypes (Prototype 1 and 2) were designed based on data from the test data set.

3.2. First Prototype

A first prototype (Prototype 1) was designed based on the concept of embodied metaphors and embodied sonification. [21]

3.2.1. Mapping strategy

An analysis of the datasets led us to consider information related to the specific component of the system as the most relevant. We hypothesized that an early identification of the specific component under attack (i.e., tank, pump, valve) and of the variable under attack (i.e., pressure, status, flow) would allow the operator to more efficiently identify the issue and run further checks. Furthermore, we decided to add information on the geographical location in the network of the component under attack. Consequently, the focus of the first data-to-sound mapping was:

- To represent each network's component with a different sound content. For example, all tanks would have been represented by the same type of sound;
- To link the behavior of each sound to the behavior of each component's variable over time. For example, a specific behavior of the “tank sound” (an increase in volume, or a distortion of the original sound) would represent an anomalous behavior in the tank pressure;
- To play each component in a sequence representing a virtual spatial movement from left to right through the geographical map of the network, to easily locate the component while listening (for example, the first tank sound heard would be the first tank at the extreme left of the network map).

We so obtained a sort of score for a sonification whose duration was determined by user experience criteria. In a first round of sketches, we tried to balance between the need to understand the information with the efficiency of an excessively long duration of the sonification. In its last iteration, the typical duration of sonification for Prototype 1 was of about 2 minutes played every hour.

3.2.2. Sound Design

We assumed with [10] that a successful sound content for peripheral monitoring would be one that the operator would easily relate to real-world experience. Therefore, we designed sounds having in mind how a real tank, pump, or valve would sound. The main choice to represent the anomalous behavior of each component was to apply a distortion parameter to the above-mentioned sounds following experimental results by [11]. The use of other processing such as changing in pitch and volume was also explored. A demo of prototype 1 can be heard following [this link](#).¹

The prototype has been evaluated through experts' sessions with participants from the field of water management, cyber security, communication design and sound design. Following these sessions, the prototype has been dismissed due to various issues negatively impacting the user experience. To name a few:

- The overall duration of each instance of the sonification (two minutes every one hour) was deemed way too long to be efficiently sustained;
- There was an evident overload in the amount of information conveyed by sound, which included: the type of component; the type of variable for each component; the amount of anomaly for each component and variable; the geographical location of the component;

- Such an amount of information was not only extremely hard to understand in the current situation but made the prototype virtually impossible to scale up to larger networks with more than 7 tanks and 11 pumps.

Nonetheless, feedback from critique sessions helped us radically change strategy for the second series of prototypes. In particular:

- Duration had to radically shrunk in order to limit the impact of sonification with the routine of the control room;
- Information to be conveyed by sound had to be drastically reduced, too. In particular, while geographical information on the specific district under attack seemed very relevant, no added value seemed to resort from information on components and variables;
- In Prototype 1, an anomaly index was artificially introduced for the representation of anomalous behavior in order to normalize data. This index scaled the anomaly level on a 5-steps, scale from no anomaly to extremely serious anomaly. The scale was pre-determined by us, but it is not introduced by the algorithm per se. As we found no clear added value in pre-determining the anomaly level, we decided to leave it to the operator to decide, based on his/her own experience, on the gravity of the anomaly.

3.3. Second Prototype

In a radical pivoting, Prototype 2 followed a strict data – driven approach focusing on the direct communication to the operator of anomalous behavior as it comes from the algorithm. The reason for this shift was mainly a need to go back to a clear formulation of the problem to be solved by sonification in our specific context of application i.e., to allow the operator to quickly identify anomalies due to cyber-attacks for action-taking. As mentioned in 3.1, the numerical value corresponding to the reconstruction error identified by the algorithm, previously hidden to the final user, was introduced into the data set, and it was around this parameter that the second sonification was built.

Following the main feedback emerged from Prototype 1 (see Par. 3.2.2) we decided that only the anomalous behavior of each of the five districts (without reference to components or variables) would be conveyed by sound and that the duration of each sound representing each district would be limited to 3 seconds/sound.

3.3.1. Mapping strategy

In order to subsequently process data in form of sound, we used a Python script to convert our csv database to MIDI. So obtained MIDI files were imported into the commercial software Ableton Live™ for further processing. In particular, we used the open source script miditime 1.1.3² to convert data to MIDI format.

Four mapping strategies, later called *Scenarios*, were identified:

1. Scenario 1-Delay: every District is represented by a different sound. The duration of each sound is 3”. All sounds (five sounds for five districts) start at

¹ <https://sonifying.github.io/UNDERSTANDING-CYBER-ATTACKS-ON-WATER-SUPPLY-SYSTEMS/p1.html>

² MIDitime: <https://pypi.org/project/miditime/>

- Time 0 and in case of no anomaly, they stop playing after 3". In case of anomaly, the anomalous sound will start delayed by an amount of time directly proportional to the amount of the anomaly as taken from the reconstruction error's data.
2. Scenario 2-Length: starting from the same characteristics as Scenario 1, the duration of each sound increases proportionally to the increase in value of the anomaly level in data.
 3. Scenario 3-Repetition: the 3" sounds for each district will cycle over a 10" time span if anomalous. The frequency of cycling is determined by the level of the anomaly coming from data.
 4. Scenario 34-Pitch: the 3" sounds representing each district will increase their pitch proportionally to the level of anomaly.

After running a further critique session with experts, we narrowed down the options to the two prototypes which seemed to be more promising. For a series of reasons whose full account exceeds the scope of this paper, we focused our attention on Scenario 2-Length and Scenario 3-Repetition. A demo of all four prototypes as well as a map of the five districts can be found [at this link³](#).

4. EXPERIMENTAL DESIGN: TESTING WITH REAL USERS

Prototype 2 and 3 (from now on, Prototype 1 and 2) were produced in two versions (A and B, one with tuned one with non-tuned sounds) and were the object of a first experimental phase which included the collection of both quantitative and qualitative information. The experiment involved six expert users in cybersecurity and water management from five different countries (New Zealand, Italy, Singapore, Vietnam, Turkey). Over a two-weeks period, testers were asked to use the prototypes in a real context, during their daily work routine, for eight consecutive hours. One day was dedicated to each scenario/version, for a totality of four full days of testing. To limit biases and expectations we asked testers to keep a few days' break between one prototype and the following, thus obtaining a testing period of two weeks with only four full days dedicated to testing each prototype.

4.1. Experimental Protocol

The experiment included three phases: a preliminary questionnaire, a quantitative test to be completed during the four days of prototype testing, and a final, one hour long semi-structured interview for collection of qualitative feedback. The setup of the various phases was inspired by Research through Design practices [22] and in particular by experimental practices such as Annotated Portfolios [23], Technology Probes [24] and the more recent Design Probes [25].

The preliminary questionnaire gathered self-assessed information on the specific expertise and on the level of music/sound competence of the testers. The quantitative test had to be fulfilled after each sonification (every hour). Despite the very limited number of users not granting statistical relevance, we intend the test as a validation of the efficacy and effectiveness of each prototype in terms of user performance. Specifically, the test has been designed to answer the following questions:

- 1) can users recognize anomalous behaviors in the system through the sonification?
- 2) can users attribute a scale of severity to anomalies, identifying corresponding differences in the sound behavior?
- 3) can users identify in which district of the city is the anomaly occurring, through corresponding differences in sound content?

Interviews, on the other hand, had the goal of gathering a more nuanced series of insights from domain experts with the overall goal of identifying guidelines for the next prototype iteration. Specifically, the interview has been designed to gather feedback on the following:

- 1) the usage of sonification in a real-world context;
- 2) the different strategies used for the two scenarios;
- 3) the different sound content used in the different versions.

5. ANALYSIS OF RESULTS

Quantitative analysis, though not statistically relevant, helped us evaluate the potential of sonification in relationship with the tasks the experts have to carry out in our specific context of usage, i.e., firstly correctly identifying the information coming from the algorithm; secondly attributing a level of gravity to the anomaly and situating the anomaly in the correct district where it is occurring.

We remind the reader that we intend this sonification as an addition and preliminary step to the possibility of finding analytical, more granular information in the visualization system of the control room. We also remind that a pre-determined level of anomaly was not introduced "by design". As such, the interpretation of the level of anomaly in the quantitative testing presents a high degree of subjectivity, as highlighted by some testers. A second series of quantitative testing is planned in order to further investigate the relevance of attributing a level of gravity to the anomaly and of identifying the district, in order to determine their influence on the overall performance of the operator in taking further action. If a strong relevance should emerge, an objective level of anomaly gravity could be embedded in the sonification by design as well as a refined mapping strategy to scale district identification in case of larger networks.

Qualitative analysis helped us identify emerging patterns in the users' relationship with the sonification, in their strategy to learn from it and applying it to their real work context, as well as clustering reactions to the different versions of the prototype and suggestions for further developments.

5.1. Quantitative Analysis

All users showed a high level of performance in the identification of an anomalous status of the system. As Fig.1

³ <https://sonifying.github.io/UNDERSTANDING-CYBER-ATTACKS-ON-WATER-SUPPLY-SYSTEMS/p2.html>

illustrates, testers seemed to easily identify anomalous behavior through sound, while attributing an anomaly level and identifying the specific district seemed to be more challenging. In particular, and worth of further investigation, users tended to over-estimate the gravity of the anomaly while underestimating the number of districts involved. Over-estimation of anomaly level impacts more the sonification under Scenario 2 (and in particular, 2B) which might indicate a certain “anxiety effect” driven by the specific strategy and the specific sound contents used for Scenario 2B. Further investigation is needed to validate this hypothesis. On the other hand, the error in the quantification of the number of district involved in the anomaly is higher for Scenario 1, both A and B (based on length), which could be due to a sonification strategy that tends to superimpose, to an untrained ear, the sound of each district,

Relevance and direction analysis of error answers

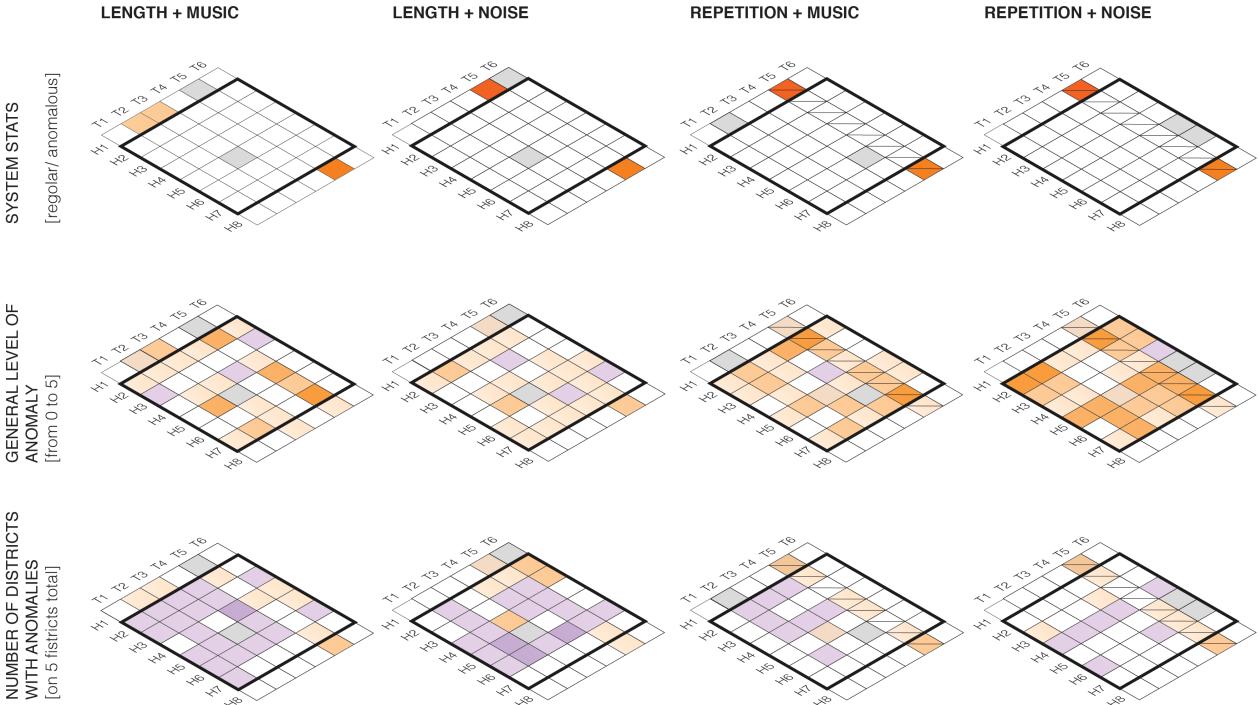
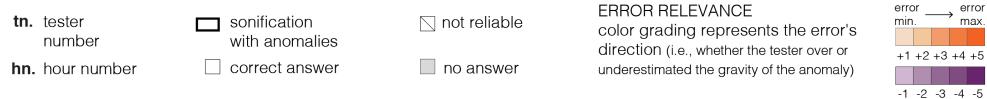
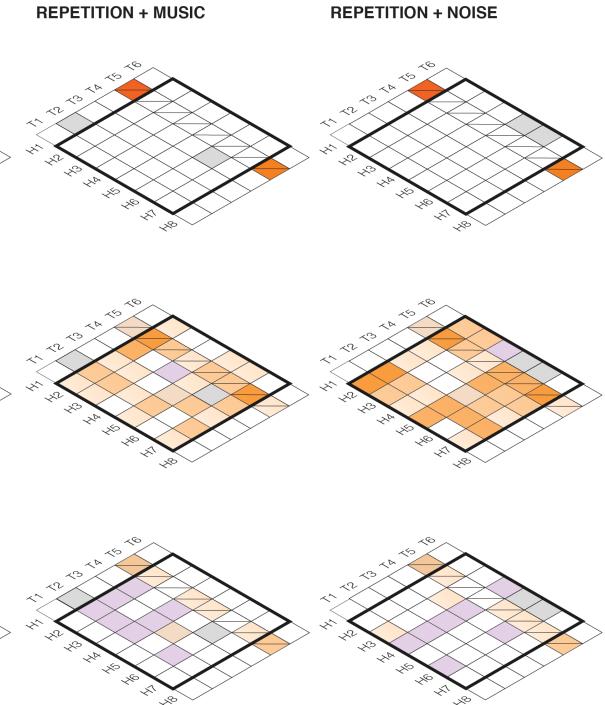
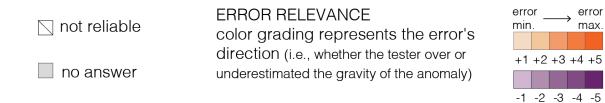


Figure 1. Excerpt from Quantitative Analysis Results.

5.2. Qualitative Analysis

The analysis of interviews highlighted a very positive attitude towards the integration of sonification in control rooms of water plants. Positive comments included: the possibility to hear sound at the periphery of attention while focusing on other (visual) tasks; the smoothness of integrating sonification in the daily routine of the work place; the low cognitive load required by the sonification to gather basic information that might be investigated further on visual tools. Some users highlighted the positive effect on performance of being able to discard an alert as non-dangerous dedicating only 3" of peripheral attention.

when more than one district presents anomaly. Both of these interpretations of the result will need further investigation. The majority of users reported improvements over time, from the starting of testing (at 10am) to its conclusion after 8 hours. We take it as a sign that the continuous usage of sonification in daily work operations can lead to a sophisticated capacity of understanding information through sound down to detailed nuances, as it does indeed happen in real life (for example in our relationship with natural soundscapes). Despite some initial mistakes in the understanding of instructions for the quantitative testing by some of the testers, all have been able to develop an individual, self-taught strategy to learn from their mistakes while using the prototypes.



All testers strongly highlighted the key role of sound design in their attitude towards the implementation of sonification in real life. One scenario (1B-Length) was clearly rejected as unpleasant, annoying and even scary while the others were all judged as pleasant to various degrees with a slight tendency towards tuned sounds. Some users tended to attribute significance to non-tuned sounds in Scenario 2B (Repetition) using metaphors coming from cartoons, video games or personal experience, opening up room for further investigation on the role of embodied metaphors. An interesting line of discussion emerged on the possibility of using unpleasant sounds for higher anomalies and pleasant sounds for non or little anomalous states, again re-introducing the possibility of embodied metaphors for further design of sounds.

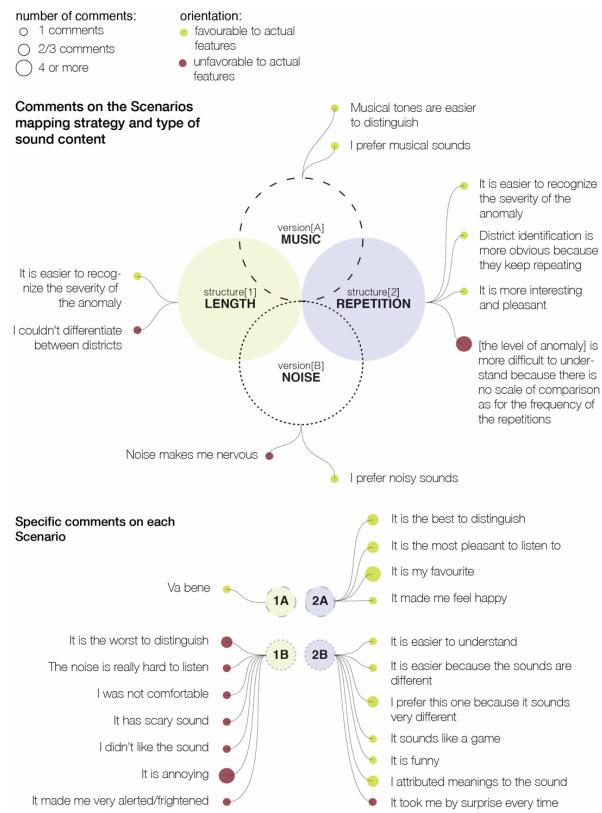


Figure 2. Excerpt from Qualitative Analysis Results.

As Figure 2 illustrates, no definitive judgement can be done on a preferred or “better” version of the sonification: there is no “winning” Scenario. If aesthetic and emotional inclinations seem, for the users, to be an added value for a better comprehension of the sonification itself, they do not seem to entail an improved performance and further testing with a statistically relevant numbers of users will have to be conducted.

6. CONCLUSIONS AND FUTURE DEVELOPMENTS

In general, a very positive, self-reflecting and self-learning attitude was shown by all testers in relation to the introduction of sonification in the daily routine of monitoring cyber-attacks in water plants. None of the testers had reported a particular training or passion for sound/music, leading us to think that, despite the general lack of preparation in reading information through sound, real-world applications can be effectively designed and introduced. All users were vocal in highlighting the need for preliminary training and real-time feedback to self-assess their performance while learning to use the sonification. The setup of the experiment purposely did not provide any such training or feedback. Only a website containing an introduction to sonification and all the instructions was provided and can be found at [this link](#)⁴.

Based on these encouraging results, a second phase of the project is envisaged. This phase will include testing the sonification along with the corresponding visualization, in a real setting; a new iteration of a single prototype ideally taking into account all the aspects emerged in this first phase,

including the possible re-introduction of embodied metaphors; an extended group of testers for a longer period of time in order to evaluate emerging concepts, such as subjectivity/objectivity of the anomaly level and the role of experience in making sense of additional information such as district identification. The final goal is the release of a real-world application, fully integrated with the anomaly detection algorithm which formed the basis of this project.

7. ACKNOWLEDGMENTS

First and foremost, we express our gratitude to the testers who took time to participate to the present research during their working time. We also wish to thank our colleagues at Density Design Lab for the precious advice and help with visualizing the results of the experimental phase. Dr. Taormina and Dr. Galelli were supported in part by the National Research Foundation (NRF), Prime Minister’s Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-40) and administered by the National Cybersecurity R&D Directorate.

8. REFERENCES

- [1] Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A., “Characterizing cyber-physical attacks on water distribution systems in *Journal of Water Resources Planning and Management*, 143(5), 04017009, 2017.
- [2] Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., Ostfeld, A., Eliades, D. G., ... Ohar, Z. “Battle of the Attack Detection Algorithms: Disclosing cyber-attacks on water distribution networks.” in *Journal of Water Resources Planning and Management*, 144(8), 2018.
- [3] Axon L, Creese S, Goldsmith M, Nurse JRC. "Reflecting on the Use of Sonification for Network Monitoring", In: *SECURWARE 2016: The Tenth International Conference on Emerging Security Information, Systems and Technologies*; 2016:254-261.
- [4] Hermann T, Hunt A, Neuhoff JG, Dombois F, Eckel G. "The Sonification Handbook". In: *The Sonification Handbook*, 2011:301-324.
- [5] Ballora M, Pennycook B, Ivanov PC, Glass L, Goldberger AL. "Heart Rate Sonification: A New Approach to Medical Diagnosis", *Leonardo*. 2004; 37(1):41-46
- [6] Nesbitt, Keith & Barrass, Stephen. (2004). "Finding Trading Patterns in Stock Market Data", IEEE computer graphics and applications. 24. 45-55. 10.1109/MCG.2004.28.
- [7] Hermann T, Hildebrandt T, Langeslag P, Rinderle-ma S, "Optimizing Aesthetics and PRrecision in Sonification for Peripheral Process-Monitoring" in *of the 21st International Conference on Auditory Display (ICAD 2015)* 2015:317-318
- [8] Vickers, Paul *Sonification for Process Monitoring*. In: The Sonification Handbook. Logos Verlag: Berlin, 2011 pp. 455-492.
- [9] Rinderle-Ma S, Hildebrandt T. "Server sounds and network noises", in: *6th IEEE Conference on Cognitive*

⁴ <https://ginevraterenghi.github.io/presentazione-prog/project.html>

Infocommunications, CogInfoCom 2015 - Proceedings. ; 2016:45-50.

- [10] Bakker S, van den Hoven E, Eggen B. "Knowing by ear: Leveraging human attention abilities in interaction design" *J Multimodal User Interfaces*. 2011, January 20.
- [11] Ballatore A, Gordon D, Boone AP. "Sonifying data uncertainty with sound dimensions". In: *Cartography and Geographic Information Science*, 2018.
- [12] Axon L, Nurse JRC, Goldsmith M, Creese S. A Formalised Approach to Designing Sonification Systems for Network-Security Monitoring. In: *International Journal on Advances in Security*. Vol 10. ; 2017:26-47.
- [13] Hermann T, Hunt A, Neuhoff JG. (eds.), *Theory of Sonification*, in "The Sonification Handbook", Logos Verlag: Berlin, 2011.
- [14] M. Broussard, *Artificial Unintelligence: how computers misunderstand the world*, Cambridge, MA: MIT Press, 2019.
- [15] D. A. Norman, *Things that Make Us Smart: Defending Human Attributes in the Age of the Machine*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1993.
- [16] Masud L, Valsecchi F, Ciuccarelli P, Ricci D, Caviglia G., "From data to knowledge: Visualizations as transformation processes within the data-information-knowledge continuum." in *Proc Int Conf Inf Vis*. 2010:445-449.
- [17] Hildebrandt T, Hermann T, Rinderle-Ma S. "Continuous sonification enhances adequacy of interactions in peripheral process monitoring.", in: *International Journal of Human Computer Studies*. Vol 95. Elsevier; 2016:54-65.
- [18] Deb S., Claudio D., "Alarm fatigue and its influence on staff performance", in *IIE Transactions on Healthcare Systems Engineering*, 5:3, pp. 183-196, 2015.
- [19] Rönnberg, Niklas & Lundberg, Jonas & Löwgren, Jonas, "Sonifying the periphery: Supporting the formation of Gestalt in air traffic control." in *ISon 2016, 5th Interactive Sonification Workshop*, CITEC, Bielefeld University, Germany, December 2016.
- [20] Hildebrandt, T., Hermann, T., Rinderle-Ma, S., "A sonification system for process monitoring as secondary task.", in: 2014 5th IEEE Conference on Cognitive Infocommunications (CogInfoCom), pp. 191–196 Nov. 2014.
- [21] Roddy S., Furlong D., "Sonification Listening: an empirical embodied approach", in *Proceedings of the 21st International Conference on Auditory Display (ICAD 2015)*.
- [22] Stappers, P. & Giaccardi, E. "Research through Design.", in Soegaard, M. & Friis-Dam, R. (eds.), *The Encyclopedia of Human-Computer Interaction, 2nd edition*, 2017.
- [23] Jonas Löwgren. 2013. Annotated portfolios and other forms of intermediate-level knowledge. *Interactions* 20, 1 (January 2013), 30-34.
- [24] Hutchinson H, Mackay W, Westerlund B, et al. Technology probes: Inspiring design for and with families. In: *CHI03 Poceedings of the Conference on Computer-Human Interaction*, 2003:17-24.
- [25] Hogan T, Hornecker E. Feel it! See it! Hear it! Probing Tangible Interaction and Data Representational Modality. *Des Res Soc*. 2016:1-13