An Integrated In-Situ Approach to Impacts from Natural Disasters on Critical Infrastructures

Sebastian Mittelstädt*, Xiaoyu Wang†, Todd Eaglin†, Dennis Thom‡, Daniel Keim*, William Tolone†, William Ribarsky†

*University of Konstanz, Email: firstname.lastname@uni-konstanz.de
†University of North Carolina at Charlotte, Email: firstname.lastname@uncc.edu
‡University of Stuttgart, Email: dennis.thom@vis.uni-stuttgart.de

Abstract—**Natural disasters can have a devastating effect on critical infrastructures, especially in case of cascading effects among multiple infrastructures such as the electric power grid, the communication network, and the road network. While there exist detailed models for individual types of infrastructures such as electric power grids, these do not encompass the various interconnections and interdependencies to other networks. Cascading effects are hard to discover and often the root causes of problems remain unclear. In order to enable real-time situational awareness for operational risk management one needs to be aware of the broader context of events. In this paper, we present a unique visual analytics control room system that integrates the separate visualizations of the different network infrastructures with social media analysis and mobile in-situ analysis to help to monitor the critical infrastructures, detecting cascading effects, performing root cause analyses, and managing the crisis response. Both the social media analysis and the mobile in-situ analysis are important components for an effective understanding of the crisis and an efficient crisis response. Our system provides a mechanism for conjoining the available information of different infrastructures and social media as well as mobile in-situ analysis in order to provide unified views and analytical tools for monitoring, planning, and decision support. A realistic use case scenario based on real critical infrastructures as well as our qualitative study with crisis managers shows the potential of our approach.**

I. INTRODUCTION

Responding to the destructive impact of a volatile hurricane to a network of critical infrastructure is the central challenge for emergency responders. After witnessing the devastating destruction from Hurricane Sandy during 2012 and the flood disaster in Germany 2013 decision makers are on high-alert for threats to their critical infrastructures such as power lines, food networks, shelters, etc., potentially caused by impact from natural catastrophes. Important backbones of our society are electrical power networks since the electricity supply has a strong impact on the fundamental societal structures such as life/health, environment, and economy. Especially, electric power systems are increasingly dependent on information and communication technology (ICT) systems as new monitoring, control, and protection functions, especially in the currently emerging Smart Grid installations. In order to deal with the increasing vulnerabilities of electric power systems, advanced ICTs, including network-based Supervisory Control and Data

Acquisition (SCADA) systems or Wide Area Monitoring Systems (WAMS) have been deployed by the power industry.

Analyzing the vast amount of information from different domains is a complex analytical issue. The monitoring of the interconnections between power grids and digital networks requires the integration of several data sources. With an overview the crisis manager is able to understand and explore the crisis allowing her/him to project the future development and to make decisions. Situational awareness is important on all levels of crisis response that range from central command centers to site-commanders and boots-on-the-ground. All levels have to access the information of a crisis. They need to communicate bottom-up or top-down since crisis managers typically rely on the information of the field and first responders lack context information.

Novel public communication platforms like social media services and other Web 2.0 sources have established a completely new information channel that can help to improve situational awareness for the decision makers. Citizens affected by critical events often report vital situation related information directly to messaging services like Twitter or Facebook. They use mobile and sometimes even GPS-enabled communication devices like smartphones or tablet computers. Gathering useful information pieces from the vast amounts of random unrelated chatter poses a completely new challenge for analysis and decision support systems.

Existing tools and systems do not support the integration of information over several critical infrastructures such as power grids and the ICT networks. The monitoring and understanding of the relationship of critical infrastructures and the coordinated management of their failures is therefore one of the biggest challenges in critical infrastructure protection and crisis response. In this paper, we present a system that supports all levels of command structures and enables situational awareness for crisis response. This system was developed within a nationwide interdisciplinary project [1] running for three years with an international research collaboration with a partner project [2].

Our contribution: We present a visual analytics system that: 1) supports all levels of crisis response with specialized equipment and visualizations for control rooms and mobile devices; 2) combines multiple critical infrastructures and
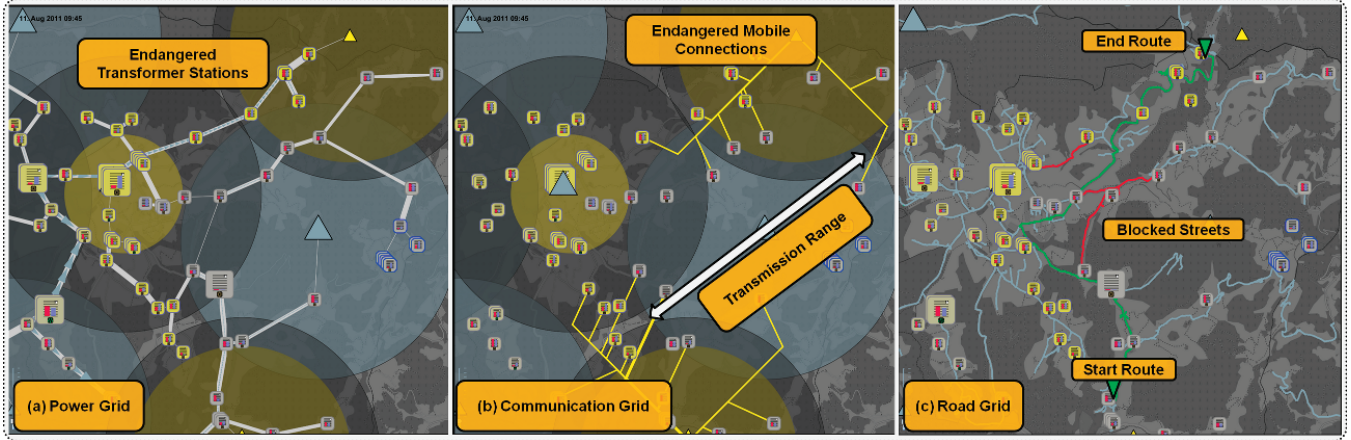
Figure 1. Overview of the power, mobile, and road grid. Transformer stations (rectangles) are connected via power lines and are also connected to the communication infrastructure (triangles), which transfers the information to the central control room. The transmission range of the mobile stations is visualized as concentric circles. While gray indicates normal operation mode, the yellow elements on the screen reveal a severe situation. High deviations in voltage cascaded from the energy grid into the mobile grid due to failures of the power supply. Now, the operator must intervene immediately. With malfunctions in the mobile grid, the crisis response commands from the control room won't reach the field, which then would result in a black out. Further, roads are blocked and hinder the response team to reach the target area, which is visible in the command center after the first responders update the street status. The dynamic routing adapts to these constraints and calculates a different route.

social media by information abstraction; 3) enables interactive simulation and visualization of the subsequent development of a crisis; 4) enables interdisciplinary and distributed teams to understand and react on crisis situations.

II. RELATED WORK

The advantage of visual analytics has been illustrated in an analysis of the 2005 outbreak of the avian flu by combining different analysis capabilities [3]. This scenario shows the power of an analytic setting that supports the analysis of complex, real-world scenarios. Also, first visual analytics tools in the area of crisis response were the result of SoKNOS [4]. This comprehensive environment requires integrated visual and traditional systematic analysis of massive data, including improved strategies for exploratory visual analysis, hypothesis testing and user-specific presentation of relevant information as a basis for actionable decision making. Furthermore, visual analytics tools for analyzing syndromic hotspots are presented by Maciejewski et al. [5] that allow the analyst to perform real-time hypothesis testing.

Much prior research has focused on using simulation and predictive modeling to anticipate hurricane movement and suggest possible landfall and impact locations [6], [7]. Campbell and Weaver [8] investigate situational awareness during emergencies using two different tools: RimSim Response! (RSR) and RimSim Visualization (RSV). The work of Kim et al. [9] focused on the use of mobile devices for situationally aware emergency response and training, and thus, their approach is similar to our work.

As part of the PSERC project, techniques are developed to visualize complex power systems and flows [10]. GreenGrid [11] was developed to explore the planning and monitoring of the North American Electricity Infrastructure. For the

interactive analysis of network related data sources such as server logs or BGP protocol data, Fischer et al. developed a visual analytics expert system in [12]. A detailed overview of cyber security and privacy issues in a smart grid context is presented in [13]. The control room is the central part of a system, where all information comes together. Notifications and alarms are collected and transferred to a central node. These events are typically evaluated by rule-based systems, where the rules are defined by domain experts. Rooney et al. gives an introduction to Root Cause Analysis (RCA) in [14]. There are also systems that use simpler fuzzy logic rules as a vehicle that allows engineers to incorporate human reasoning in the control algorithm [15]. Impacts on critical infrastructures are typically complex and involve several experts of different domains for crisis response. This demands for interactive workspaces but also for high-resolution environments that enable visualizing all elements of a crisis and their context. Approaches that utilize interactive workspaces combined with visualization devices were previously presented [16], [17].

Social media, such as Twitter and Facebook, contain time-critical information that can enhance situational awareness. First approaches for building and improving decision making systems in this domain were introduced by Tomaszewski et al. [18]. MacEachren et al. [19] developed a visual analytics tool that allows for querying social media sources and depicting aggregated results on a geographical map. Thom et al. [20] present a novel cluster analysis approach to detect spatiotemporal anomalies in Twitter messages.

The discussed approaches and systems focus on a specific domain and do not combine various external data sources. Integrate sensor data (electricity, weather, supply), social media and in-situ analysis is a challenging task. Furthermore, most of the current systems are intended for domain expert
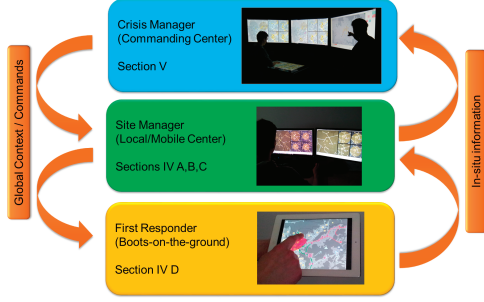
Figure 2. Overview of the Users that our system is designed to facilitate.

users, although crisis management teams may consist of interdisciplinary members. Enabling interdisciplinary teams to analyze and understand interdependent data leads to efficient crisis response.

III. DESIGN FRAMEWORK: TARGET USERS & REQUIREMENTS

Large scale emergency response has a command structure as illustrated in Figure 2, which was depicted by our crisis managers within the project. A large police or fire response, for example, will have a site commander who deploys first responders. If the emergency is larger and more wide-spread, there will be a command center with oversight over multiple site commanders. A similar structure applies to breakdown of the electrical grid or other critical infrastructures. The deeper one goes into the command structure, the more mobile the responders are; they are focused on the locales, tasks, and decisions at hand and traditionally don't have contextual understanding or situational awareness. Typically, site commanders also don't have situational awareness (in terms of the deployment of their personnel and what they are doing or seeing, for example) nor do they have the context to make the most effective decisions. To make decisions, the first responder will want to know what is happening in the locale, what is about to hit where and when. The site commander will want to know similar things over a wider locale and must in addition organize and manage a group of responders. Aspects of all this should flow up to the command center for overall decision-making.

Further, any feedback and updates they provide will be transmitted to the central system. Detailed location, movement, and action updates can be placed in the appropriate spatio-temporal context so that commanders can see, in unprecedented detail and without ambiguity, what is going on (and responders can see, minute-by-minute where there fellow responders are and what they are doing). Specifically, our system is designed to accommodate the three essential personnel in a crisis respond scenario:

Crisis Manger. Crisis Managers are a group of domain experts who oversees the entire emergence response process. This group is typically formed by interdisciplinary members from various analytical domains, such as grid operators from power companies, city-state officials, evacuation experts, and people from federal departments. Their objective is to understand and assess the severity of the crisis situation, select corresponding Site-Commanders with appropriate First Responders, and provide Just-In-Time decisions based on inputs from social media and in-field communications. The natural of the heterogeneous data inputs for the Crisis Managers determined that they will benefit from a control room setup, where they will be provided with a combined overview of the crisis situation. As detailed in section 5, our setup supports distributed as well as collaborative analysis, provides overviews of the development of the ongoing crisis, and it further enables the Crisis Managers to interactively deploy and arrange response effort, and receive the updates from site commanders in real-time.

Site Commanders. With the advanced mobile technology (e.g., mobile emergency response vehicles), site managers are the critical link between Crisis-Manager at control center and First Responders in the field. Based on our previous collaboration with local emergency responders, Site Commander (e.g., Police Chief) are often stationed near the crisis center where first responders were deployed to conduct on-site instructions and in-situ communications. At the mean time, they are relying on the mobility of the technologies to maintain an open communication channel with control center for further situation assessment and updates. Site Commanders act differently from Crisis Managers in a way that they have a more focused missions in a specific area that is assigned to them (e.g., a specific substation or a street blocks) and are in charge of provide real-time response as the crisis unfolds in the field.

First Responders. First Responders are the group that fights the diseases right in the center of where crisis occurs. These teams consist of various professionals, such as policeman, fire fighter, and power grid responders. These interdisciplinary group mainly conduct response effort in the field with instructions from Site Commanders. Their extreme needs of mobility determined that we need to provide them with a mobile-device based visual analytics system. Key functions in this system, as detailed in section 4.4, includes instructions that informs them about the areas that they need to focus their attentions, interactive methods to depict areas to prioritize their tasks, and finally communication methods to provide updates and situation reports to their Site Managers. All this information need to be shared through wireless networks that directly feedback to the Site Commanders and further to Crisis Managers.

IV. SYSTEM COMPONENTS

A. Simulation of Critical Infrastructures

Large scale natural disaster, a cyber-attack, or other wide spread crisis may affect multiple infrastructures. To capture these complex, multifarious, and dynamic effects, we utilize
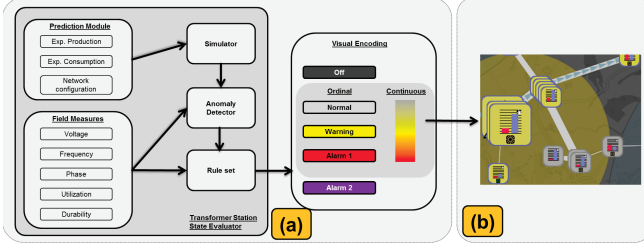
Figure 3. (a) Station state evaluators consider the incoming measurements and the comparison to the expected behavior, which reveals anomalies. A set of rules maps this input to color that expresses the status of the element. (b) Domain details are added to the symbols such as power consumption and production (red and blue bars), as well as producer types (photovoltaic or biogas) for transformer stations.

a simulation model that takes into account the interrelationships among critical infrastructures. The simulation is built within a rule-based framework for integrating multiple infrastructure components at a high level. The interlaced critical infrastructures are captures in a set of networks with each node having a set of properties according to its category and the edges providing a dependency rule according to the category and state of the two connected nodes. This results in a dependency/interdependency ontology (e.g., as illustrated in Figure 1(a) mobile transmitters are connected to transformer stations). Thus, for example, a breakdown of a power substation would immediately cascade to power loss at points on its distribution network.

In some natural catastrophes some roads may be affected and rescue or response teams, especially with heavy gear, are not able to pass them. This has to be considered in the evacuation and logistic management at all three levels: E.g., the crisis managers must plan the logistics of gear and troops; the site-commander sends in first responders on different routes to the crisis and first responders will update the status of streets if they are not passable. Our system supports dynamic routing with the state-of-the-art algorithms that consider the current status of streets.

B. Visualization of Interdependent Infrastructures

A smart grid (energy network) typically consists of power lines at different voltage levels connected by transformer stations. These stations distribute the power over regions and supply streets, households, and industrial facilities. In our scenario, a mobile communication grid transfers information and control commands from the central control room to the electrical grid. The mobile transmitters itself are power-supplied by common transformer stations and thus, the infrastructures are tightly interconnected.

1) Information Abstraction & Visual Encoding: Adapting and extending the visual abstraction presented in [21], the complex and vast amount of information of each infrastructure is reduced to the essentials, in order to enable the decision maker to understand the full crisis in its context and to detect potential cascading effects. Every infrastructure is abstracted
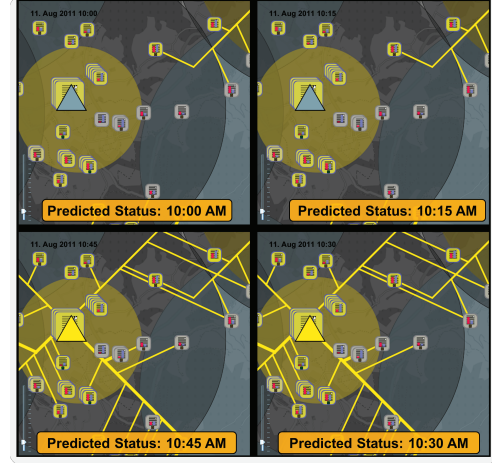

Figure 4. Subsequent Development: If there is any emerging problem in the future, the prediction view will show the future status of the network by small multiples, which shows the remaining time and the affected elements.

to an undirected graph. Its nodes are represented by symbols, such as rectangles for transformer stations and triangles for mobile transmission stations. The graph edges represent the domain dependent connection between infrastructure elements, such as power lines and mobile communication connections (see Figure 3(b) and Figure 1).

The status of each element is estimated by a state-evaluator model that is defined for each infrastructure. These models concern the actual information of the field, such as utilization and durability (see Figure 3(a)). We use a prediction module for our power grid that predicts the consumption and production at each transformer station according to weather forecasts and past data based on Monte Carlo simulation. This information is sent to the simulation server that simulates the subsequent development. This "expected" behavior is compared to the actual measurements. Thus, anomalies are detected, which may reveal damaged or harmed devices. The subsequent development can be visualized as small multiples (see Figure 4) in addition to the monitoring views.

A set of rules maps the input of the field and anomaly detector to color. Saturated and intense yellow, red, and violet represent warnings and alarms. Less saturated colors stand for less serious events, such as gray for normal (uninteresting) status. Some rules provide continues values in addition to ordinal signals. For these rules we use a continuous color scale that varies over saturation and lightness from gray to yellow and over hue from yellow to red. Thus, severe events are perceptually highlighted on the dark background whereas less important events do have less visual impact [22]. The size of elements represents the topological importance of infrastructure elements. We consider central elements (and their dependencies) more important, since their failures are more acute than failures of border elements. Thus, the size of important elements is increased, which also highlights dangers or failures of central elements. We also add domain
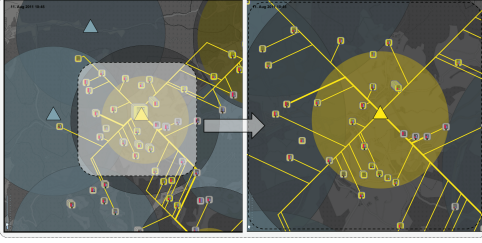
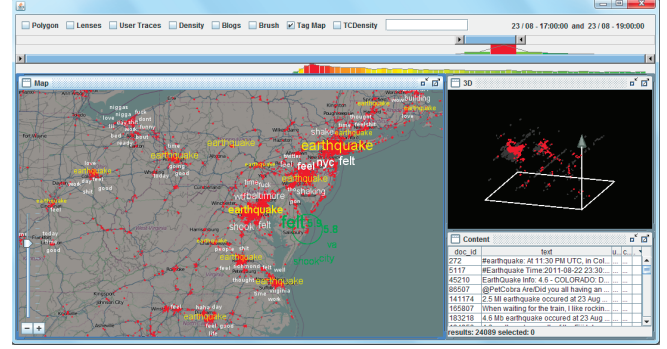Figure 5. Semantic zooming reveals more details on each zoom level as soon as enough space is available.

Figure 6. Overview visualization of crisis related topics based on automated anomaly identification. The image shows the social media component with activated anomaly visualization during a large earthquake that happened in August 2011 near Washington DC. The observation of earthquake related events lead to several "earthquake"-clusters in many cities along the coast.

details into the symbols such as the current power production and consumption as well as the producer type for transformer stations (see Figure 3(b)).

2) Zoom, Focus & Details on Demand: Two major problems arise when graphs are visualized: the over plotting of nodes and intersection of edges. The over plotting of nodes can be compensated by stacking the overlapping nodes and visualizing them at their average location. They are sorted by their current status. The domain details (e.g., power consumption and producer type) are aggregated and visualized in the foreground element. For the intersection of mobile communications, we omit the painting of connections that are working properly and use edge bundling in order to avoid intersections. These aggregation techniques enhance the readability of the visualization, however, at the cost of hiding or divert some information. The user is therefore able to zoom into areas of interest. If enough space is available, the system will visualize the elements in their normal layout and will provide additional information (see Figure 5).

The user can further interact with the field via control panels, e.g., disabling powerlines or deactivating producers at a transformer station. The user is further enabled to adjust the expected production and consumption for simulation and thus, can create alternatives for decision making.

C. Accessing Human Sensor Information

With the rise of community driven content services, such as Twitter and Facebook, a new information channel for situation awareness has been established in the Web. In contrast to more traditional data sources, like structured sensor data or detailed reports from emergency responders, these new information channels pose novel requirements for data filtering, ranking and aggregation. The relevant information has to be separated from general chatter and organized according to different topic categories. Large amounts of repetitive reports have to be integrated into a consistent and scalable situation overview. In our approach we propose novel methods to address these challenges in order to incorporate social media services as external community driven sensors within the command center environment.

1) Overview and exploration based on automated event identification: The complexity of events and the velocity of streaming data often hinders straightforward situation

awareness during critical situations. Means for automated detection and display of possibly relevant clues can be a key factor in successfully mastering crisis management. In case of social media data, it is particularly important to detect possible first-hand accounts (e.g. eyewitness information) of on-going situation between large quantities of irrelevant information and to provide visual representations of the discussed topics and observations.

As in [20], we rely on the presumption that messages addressing local events are often of related content and structure and that they are furthermore located in a spatial and temporal neighborhood. This ultimately leads to spatiotemporal clusters of messages reporting on the same situation related topics and keywords. Based on a cluster analysis approach, adapted to the specifics of real-time data, we automatically detect such spatiotemporal anomalies in the continuous data stream. Once a timeframe and geographic region is interactively selected by the analyst, the system generates a map of detected anomalies within that region and timeframe by finding frequent keywords in the message clusters and place them as labels at the corresponding cluster locations on the map. In order to avoid overlapping labels and at the same time show the analyst as much information as possible, we apply a collision avoidance technique that allows overlapping labels to move small distances from their designated locations. Ultimately, the label is not shown on the selected zoom level, if a certain maximum distance for that zoom level has been exceeded.

Our technique provides a broad overview of all events that occur in a given geographic region and, more importantly, an indication of keywords and topics that might be a good starting point for further investigations (see Figure 6). This is particularly helpful if the analyst does not know in advance what to search for or to initially inform him of an unknown ongoing situation. By zooming into the map, our layout technique automatically provides more labels for the given area, as more screen space becomes available for the given
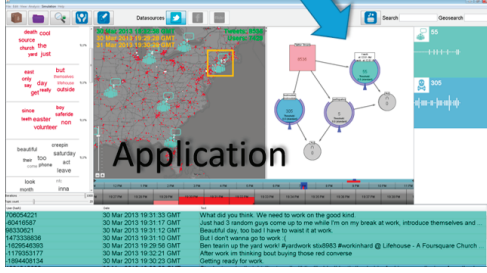
Figure 7. Classification and filtering of crisis related messages. Based on specific information of the past the analyst can load and combine modules from a library of the pre-trained classifiers using set operations. The occurrence of all new messages is shown in real-time. The analyst can associate the modules in the filter combination with specific labels, colors and symbols that are used to highlight messages detected in real time.

region. The analyst thus receives more details of possible sub-events connected to a larger event and can use this as a basis to extend his investigation with traditional textual search, content analysis and focus and context visualizations.

2) Detection of highly relevant information items based on user-steered classification: Besides the need to be informed about unknown or unexpected events, analysts usually also have a distinct domain and area of responsibility and are thus able to define information types that are clearly relevant to their tasks. For example, police officers will always be interested in information about the use of firearms or other acts of violence in their precinct. However, plain keyword-based approaches to find messages fitting to the given information need are often not powerful enough, as the complexity and specifics of language use in social media data can often not be properly reflected.

Especially in real-time analysis scenarios analysts need means to quickly build highly customized filters based on their information needs, their knowledge structure and the specifics of the situation. In our approach we propose a two-step process where a library of Support Vector Machine (SVM) classifiers customized to the specific information needs is trained first, which can then be adjusted and combined with each other and with more simple keyword-, spatial, temporal-, spam- and other filters based on interactive visual set operations (see Figure 7). This idea has already been introduced in [23].

3) Classifier Training: Based on historic data of previous, well understood events, an analyst can explore social media messages to label positive and negative examples for a given event type. This is supported by a range of exploration and analysis tools. Once the analyst has identified a sufficiently large set of example messages related (positive) and unrelated (negative) to the event type, the analyst can label them as such to iteratively progress the semi-automated training process. The training examples are especially useful if they are near the SVM-classifiers decision border, i.e. they have a high probability of being relevant to the topic in terms of keywords, and just the specific combination of terms renders them
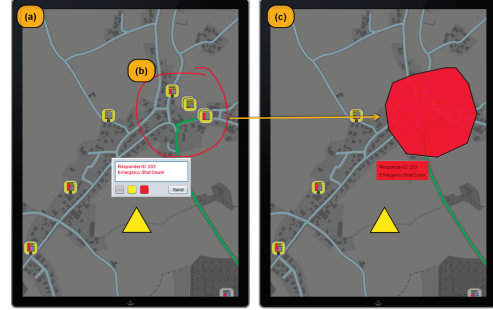

Figure 8. Overview Mobile Concept for First Responders.

related or unrelated (e.g. "This morning the power went down." vs. "I have no power to get out of bed").

4) Real-Time Monitoring: With repeated classifier training analysts can create a comprehensive library of annotated classifier modules for different event and message types relevant to their domain. In a real-time analysis scenario they would usually load and configure a range of classifiers and filters at the beginning of the monitoring period. The most relevant classifiers can be tagged with custom selected colors and symbols in order to highlight corresponding messages if they have been detected. This helps the crisis manager to detect messages related to topics of the current interest in real time, which help to relate human sensor information with events in abstract infrastructures such as smart grids.

D. High Mobility Visualizations & Visual Communication

Mobility for the First Responder is a crucial aspect in their field of work. Therefore, we designed a network visual analytics system that utilizes the advancement of mobile devices (e.g., iPad). Our mobile interface aims to provide an interactive environment where the First Responders would be able to receive detailed information in addition to commands from Site Commanders and Crisis Managers, examine the crisis scenario around them, conduct search and research with clear routine information, and finally provide feedback information to the managers. They have access to the visualizations and information of the command center, which can be focused to their particular location and interest. Section 5 discusses details of our implemented architecture to support these functions.

To help users quickly select and focus on a geospatial region, we developed probing gestures, as shown in Figure 8 (B). This is an extremely important analysis feature because it allows the user to drive the analysis and focus on what is important to their needs on the go. A First Responder can, with their touch enabled glove, directly draw onto the map with his or her finger by drawing a bounding area around a region or mark specific points. The system samples the gestures and computes the convex hull or straight line with linear regression, if demanded. Thus, rapid and noisy drawings are smoothed (see Figure 8(c)). They can further annotate in the selections with real-time updates, as shown
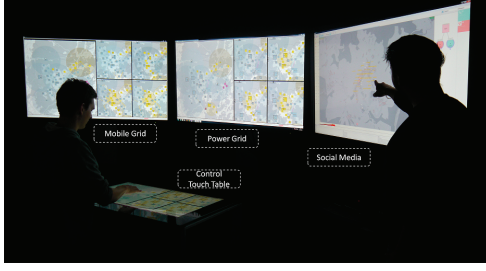
Figure 9. Our control room setup consists of three high resolution displays for the visualizations and a touch table for the steering of clients. At any time it is possible to add further clients.

in Figure 8 (c), and share the information back to their commanders and other responders, through a fast wireless or satellite connection.

V. Control Room

The different components are combined in a control room setup that synchronizes all views and clients on demand and allows the integration of mobile devices.

A. Concepts

Crisis management teams often consist of several experts from different domains. A common way to analyze crisis scenarios is the subsequent analysis of incidents. Typically infrastructures build large graphs and therefore, it is not possible to limit the analysis to a single screen. Hence, we setup a control room (see Figure 9) that supports a distributed and collaborative analysis among several experts. Our setup consists of three high-resolution displays (4xHD resolution per display) and one touch table (Samsung SUR 40). Each display can run and visualize a client that can be steered with the touch table. For example, in Figure 9 the left display shows the power grid and the middle display shows the mobile infrastructure. The user can synchronize the table with each display by pulling their current view/application and perform the application dependent interaction such as changing the viewport or select an infrastructure element. The viewport of the map is then synchronized throughout all clients. Further, the user can change the view or configuration and push the current view on the table to any display.

We see four advantages in this setup: First, single experts use this setup to explore and explain incidents with the aid of different views and visualizations on the crisis scenario as illustrated in Figure 1; these are displayed on the three high resolution displays. Second, the setup can be used to illustrate alternative solutions for decision making: Multiple alternatives and their subsequent development can be visualized simultaneously, which supports experts to draw decisions. Third, if several experts synchronously use this setup, the work can be partitioned on the three displays as well as on the touch table. Every expert receives his own interaction device, for instance a cordless air mouse, which is applied to his own workspace. In case an expert

needs to exchange information or enhance visualizations, we offer the possibility to synchronize the clients. Fourth, this setup easily enables a possible combination of the previously named social media component and critical infrastructures.

B. Architecture

In order to enable this vision of a distributed and collaborative environment, there is need for a supportive system architecture. In a collaborative working environment, multiple views and information have to be synchronized. We therefore set up a client-server architecture that supports synchronization across different clients. Our central server manages all connections to the clients and distributes information. Every interaction that needs to be synchronized is first sent to the server. However, the clients do not necessarily need to be synchronized and can also work independently if requested. In addition, the server also handles all connections to the external simulation servers and the local data sources (power grid, mobile grid, weather, and geography). The system requirements include hardware and system independence. In this distributed environment every client running a JAVA VM is able to connect to the server.

Hardware issues. We further support devices that are too weak to render our applications. Depending on their hardware, clients are classified into *complete* or *minimal* clients. *Complete clients* contain enough resources for standalone applications that render the components by themselves. Therefore, the server needs to transfer data and information, used for synchronization, to these clients. *Minimal clients* such as mobile devices do not have enough resources for the whole application and therefore, the server pre-renders the current view of the client according to the device, which is then send and visualized as image. Basic controls are also available such that the image contains the location and type of controls. Thus, *minimal clients* are not updated in real time, however, they have access to the full crisis scenario.

VI. Scenarios

Three scenarios were designed to highlight the need for such systems. Therefore, we designed multiple catastrophes that affect critical infrastructures, such as a mass disease, a cyber attack, as well as a flood-scenario that is presented here. The flood disaster is caused by heavy rain and thunderstorms in a region of Germany. The region is employed with a smart grid by one of the project partners and was flooded in 1987, from which the scenario is inspired.

The scenario starts with heavy rain and thunderstorms. Especially the high grounds of the scenario region are soaked and the soil already begins to become unstable. A thunderstorm in the early morning increased the danger for this area, which alarms the command center and site-commanders of the power grid domain. Due to the social media analysis, which detected messages about unusual water levels, the site-commander sends a power grid technician (first
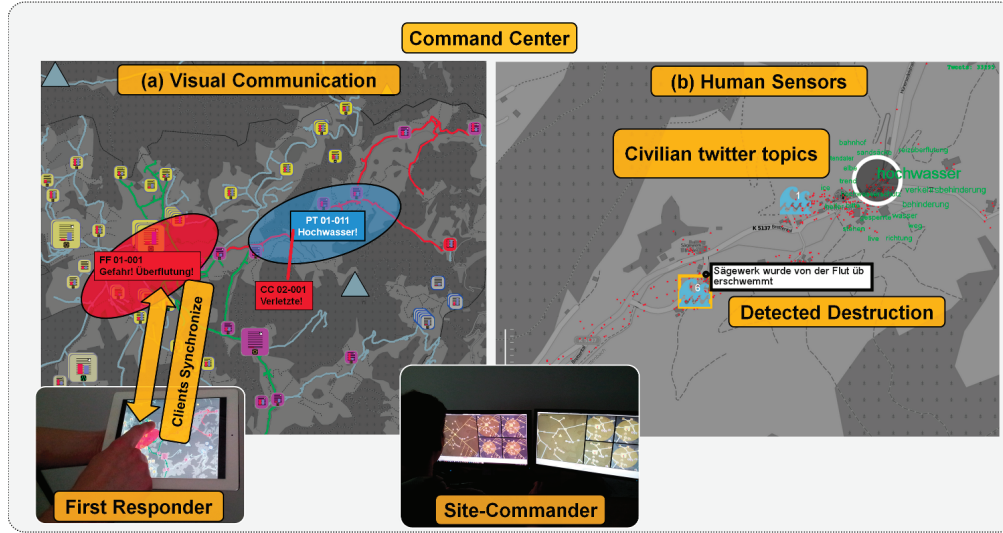
Figure 10. (a) The north-eastern part is flooded, which results in partial blackout (violet stations) and an endangered power grid. First responders update in-situ information about flooded areas and casualties ("Gefahr! Überflutung!", "Verletzte"). (b) The social media analysis early reveals messages about high water levels ("hochwasser") and detects destruction events in real time.

responder) to the region for on-site information. Figure 10 b) shows the detected messages of amblers about high water levels ("hochwasser"). Also, the command center reacts with alarming the regional response teams; in this case regional fire-fighters that are equipped with *mobile analysis devices*.

A debris avalanche hits a small village in the suburban region. Many homes are flooded and separated from the center of the region. The debris avalanche also hits a bridge and the flood is jammed. Transformer stations in the eastern parts are immediately destroyed and the blackout cascades from the east to the south (violet stations). The remaining power circuit in the west and north is suffering from this immediate loss of consumption, which raises the voltage levels (see yellow stations in Figure 10). The fire-fighters cannot reach the casualties since streets and fields are not passable. They update the flood-endangered areas and the status of streets and casualties (see Figure 10 (a): "Gefahr! Überflutung!", "Verletzte"). They request the context information, which is enriched by the technician who supports additional information from his location. Both teams update the information, which is synchronized between their clients and the central control room. The endangered areas and evacuation routes are coordinated by the command center and send to site-commanders and first responders. The fire-fighters begin to evacuate people to the south. The water level still raises and reaches over the bridge. The endangered area where one team of fire-fighters is located is flooded. The region is now suffering under a blackout since the central transformer station is hit. Evacuation routes and endangered areas are dynamically updated by first responders and command center.

After the situation stabilizes, the power grid site-commander and the technician coordinate how to ensure that most of the region can be power supplied. Therefore,

the technician updates the status of transformer stations and informs the site-commander, which station can be switched on. Further, the repair and response teams need to organize, which streets and transformer stations have to be repaired. Updating the on-site information to the command center and site-commanders enables their situational awareness and allows directing forces where they are needed. They can consider local incidents in their decision making, which is effective with our system.

VII. QUALITATIVE EVALUATION

Field studies for crisis management systems are hard to conduct. Realistic crisis data is often not available or classified. Therefore, the project partners decided to simulate realistic scenarios, which are then analyzed by target users with our system. We conducted a qualitative study based on expert feedback rounds and interviews.

A. Process

Evaluation Teams. We formed four teams within the nationwide interdisciplinary project: 1) *Data team* consists of two members of the Federal Office of Civil Protection and Disaster Assistance of Germany (henceforth, BBK), as well as four representatives of power suppliers, and further two simulation experts for smart grid technology and social media. They designed the scenarios mentioned above and provided the data. 2) The visual *design team* (represented by the authors) consists of eight visual analytics experts who designed the system based on the scenarios and data. 3) An *interview team* of two persons with backgrounds in visual design conducted the qualitative interviews with domain experts. 4) An external *experts team* consisting of two members of the BBK with experience in crisis response and ten power grid operators of different regional power grids

in Germany. We selected these different but related domains since they can be considered as the future target users. The crisis managers are part of the command center level, whereas the operators can be considered as site-commanders that are focusing on one particular affected region and domain.

Interviews. The *interview team* was involved in the creation of the scenarios but not in the design process and is therefore considered independent of the design decisions. However, this team was trained by the *design team* on the system components and supported with documentations. Further, they prepared questionnaires for the qualitative interviews. The *interview team* visited seven control rooms of regional power grid suppliers in Germany and also interviewed experienced crisis managers of the BBK. This *expert team* did not know the system and scenarios. The interviews were conducted in concrete steps: First, the *interview team* presented the single components of the system. After the experts were familiar with the system the interview team presented one scenario as a use case. The scenario was stopped at critical events and the experts were asked to analyze the crisis and to draw decisions with the help of the system. Then interviews according to the questionnaires were conducted. The *interview team* analyzed the results and summarized the findings, which were reported back to the *design team*, who carefully analyzed the findings and improved the system for a second iteration (future work).

B. Results & Discussion

1) Domain experts reported that such systems are needed for crisis response. The experts reported that there is an urge for information of the crisis site, because in most cases the command centers are blind and wait for phone calls: "The social media analysis is great. In most cases, first responders are too busy to update the crisis center. Direct access to Twitter messages that are linked to the crisis would give us a clearer and faster overview of the crisis.", "We want a direct visual communication with first responders". We found that they are not only interested in the information of first responders about the crisis but also how the affected civilians are describing their status: "Some people may just feel to be forgotten by the government and we could respond with sending in some teams to show our presence". Further, we found that first responders do have an urge for the context and development of the crisis, because they do not know what may hit them within the next minutes. They highlighted that in-situ and social media analysis can improve to narrow down root causes on-site and also to effectively steer first responders:"The control center does not even know, which transformer station can be reached by repair teams. We would need information about streets and areas around stations. If we could use these tools today, we could directly send the teams where they really could make a difference". The *interview team* found that the expert team efficiently understood the tools, however, they highlighted

that a target user of such systems would require a significant amount of training. They conclude that the concepts of our system are sound, however, will require further investigations to integrate this in future crisis response centers.

2) Crisis-Managers and Site-Commanders disagreed on the level of detail. All experts agreed that social media and linked communication with first responders is important and that our system could be used in crisis scenarios. We found that power grid operators and crisis managers disagreed on the level of details of such visualizations. The crisis managers wanted to perceive the crisis and simulate different alternatives in abstract manner. Thus, they were satisfied with our components. The power grid operators requested more domain details and domain standards in the overviews. They reported that the whole system is interesting; however, the visualizations do not meet the requirements of power grid monitoring. We conclude that our architecture must provide links to established domain systems. These interfaces must provide abstractions of domain details for the communication between the domain dependent site-commander and the crisis managers in order to adapt the level of detail.

C. Discussion, Limitations & Future Work

We found that our target users were convinced of the system and its applicability. However, we see that the system does not fulfill all requirements to be an operational system for power grid control. Research has evolved over decades to develop customized solutions for this particular infrastructure. Interestingly, the operators that were involved in the flood disaster that hit Germany in 2013 said that they were almost blind after the water destroyed the first transformer stations. Therefore, they highlighted an urge for on-site information and social media analysis. In the future scenario of interconnected infrastructures such as smart grid technology, we see a higher complexity as in today's power grids. Command centers must overlook and perceive the full context of a crisis. Therefore, abstract visualizations are needed, which was approved by our crisis managers. We argue that our system exemplifies a means for future central crisis managements to integrate different critical infrastructures, social media and in-situ analysis. It will be interesting to discover the correct level of detail to satisfy each role in the command structure. For this, we plan to conduct user assessments to improve our components to the needs of particular site-commanders. In addition, we will focus on interfaces to established domain solutions and to develop means for a seamless communication between the levels. Another issue is security. The architecture might be vulnerable although we encrypt the communication between clients and server. Further, the issue of in-feeding wrong information with, e.g., a stolen device or misleading Twitter messages was raised in our interviews. Therefore, we see an urge to include security protocols into this architecture.

VIII. Conclusions

In this paper, we present a visual analytics system that combines multiple critical infrastructures, social media and in-situ analysis to support the different levels of command structure in crisis response. We present specialized equipment and visualizations for control rooms and mobile devices. We discuss means for interactive simulation and visualization of the development of a crisis. This enables interdisciplinary and distributed teams to understand and respond to crisis situations. Our system was applied in realistic scenarios and presented to crisis managers, who conclude that there is an urge for such systems for crisis response.

References

[1] "VASA," 2011 – 2014, funded by the German Federal Ministry of Education and Research (BMBF) under the grant Visual Analytics for Security Applications.

[2] "VASA," funded by the U.S. Department of Homeland Security's VACCINE Center.

[3] P. Proulx, S. Tandon, A. Bodnar, D. Schroh, R. Harper, and W. Wright, "Avian flu case study with nspace and geotime," in *IEEE Symposium on Visual Analytics Science And Technology*. IEEE, 2006, pp. 27–34.

[4] J. Kohlhammer, T. May, and M. Hoffmann, "Visual analytics for the strategic decision making process," in *GeoSpatial Visual Analytics*. Springer, 2009, pp. 299–310.

[5] R. Maciejewski, S. Rudolph, R. Hafen, A. Abusalah, M. Yakout, M. Ouzzani, W. S. Cleveland, S. J. Grannis, M. Wade, and D. S. Ebert, "Understanding syndromic hotspots-a visual analytics approach," in *IEEE Symposium on Visual Analytics Science and Technology*. IEEE, 2008, pp. 35–42.

[6] V. Pascucci, D. E. Laney, R. Frank, G. Scorzelli, L. Linsen, B. Hamann, and F. Gygi, "Real-time monitoring of large scientific simulations," in *Proceedings of the 18-th annual ACM Symposium on Applied Computing*, Melbourne, Florida, March 2003, pp. 194–198.

[7] E. Santos, J. Freire, C. Silva, A. Khan, J. Tierny, B. Grimm, L. Lins, V. Pascucci, S. A. Klasky", R. D. Barreto, and N. Podhorszki, "Enabling advanced visualization tools in a simulation monitoring system," in *Proceedings of the 5th IEEE International Conference on e-Science*. IEEE, December 2009, pp. 358–365.

[8] B. Campbell and C. Weaver, "Rimsim response hospital evacuation: Improving situation awareness and insight through serious games play and analysis." *IJISCRAM*, no. 3, pp. 1–15.

[9] S. Kim, Y. Jang, A. Mellema, D. Ebert, and T. Collins, "Visual analytics on mobile devices for emergency response," in *IEEE Symposium on Visual Analytics Science and Technology.*, Oct 2007, pp. 35–42.

[10] T. J. Overbye and J. D. Weber, "New methods for the visualization of electric power system information," in *IEEE Symposium on Information Visualization*. IEEE, 2000, pp. 131–16c.

[11] P. C. Wong, K. Schneider, P. Mackey, H. Foote, G. Chin, R. Guttromson, and J. Thomas, "A novel visualization technique for electric power grid analytics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 3, pp. 410–423, 2009.

[12] F. Fischer, J. Fuchs, P.-A. Vervier, F. Mansmann, and O. Thonnard, "Vistracer: a visual analytics tool to investigate routing anomalies in traceroutes," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*. ACM, 2012, pp. 80–87.

[13] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[14] J. J. Rooney and L. N. V. Heuvel, "Root cause analysis for beginners," *Quality progress*, vol. 37, no. 7, pp. 45–56, 2004.

[15] A. B. Marques, G. N. Taranto, and D. M. Falco, "A knowledge-based system for supervision and control of regional voltage profile and security," *IEEE Transactions on Power Systems*, vol. 20, no. 1, pp. 400–407, 2005.

[16] D. Wigdor, H. Jiang, C. Forlines, M. Borkin, and C. Shen, "WeSpace: the design development and deployment of a walk-up and share multi-surface visual collaboration system," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009, pp. 1237–1246.

[17] H.-C. Jetter, M. Zöllner, J. Gerken, and H. Reiterer, "Design and implementation of post-WIMP distributed user interfaces with ZOIL," *International Journal of Human-Computer Interaction*, vol. 28, no. 11, pp. 737–747, 2012.

[18] B. M. Tomaszewski, A. C. Robinson, C. Weaver, M. Stryker, and A. M. MacEachren, "Geovisual analytics and crisis management," in *Proceedings of the 4th International ISCRAM Conference*. Delft, the Netherlands, 2007, pp. 173–179.

[19] A. M. MacEachren, A. Jaiswal, A. C. Robinson, S. Pezanowski, A. Savelyev, P. Mitra, X. Zhang, and J. Blanford, "Senseplace2: Geotwitter analytics support for situational awareness," in *IEEE Conference on Visual Analytics Science and Technology*. IEEE, 2011, pp. 181–190.

[20] D. Thom, H. Bosch, S. Koch, M. Worner, and T. Ertl, "Spatiotemporal anomaly detection through visual analysis of geolocated twitter messages," in *IEEE Pacific Visualization Symposium*. IEEE, 2012, pp. 41–48.

[21] S. Mittelstaedt, D. Spretke, D. Sacha, D. A. Keim, B. Heyder, and J. Kopp, "Visual analytics for critical infrastructures," in *Proceedings of International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*. VDE, 2013, pp. 1–8.

[22] L. Wang, J. Giesen, K. T. McDonnell, P. Zolliker, and K. Mueller, "Color design for illustrative visualization," *IEEE Transactions on Visualization and Computer Graphics*, vol. 14, no. 6, pp. 1739–1754, 2008.

[23] H. Bosch, D. Thom, F. Heimerl, E. Puttmann, S. Koch, R. Kruger, M. Worner, and T. Ertl, "ScatterBlogs2: real-time monitoring of microblog messages through user-guided filtering," *IEEE Transactions on Visualization and Computer Graphics*, vol. 19, no. 12, pp. 2022–2031, 2013.