
Volume 2

IDAACS’2017

The crossing point of Intelligent Data Acquisition & Advanced Computing Systems and East & West Scientists

September 21-23, 2017
Bucharest, Romania

ORGANIZED BY

IEEE Ukraine Section I&M / CI Joint Societies Chapter
Research Institute for Intelligent Computer Systems, Ternopil National Economic University and V.M. Glushkov Institute of Cybernetics, National Academy for Sciences of Ukraine
Faculty of Automatic Control and Computer Science, University “Politehnica” of Bucharest

SPONSORED BY
Reliability Issues for a Multi-Version Post-Severe NPP Accident Monitoring System

Vyacheslav Kharchenko 1, Herman Fesenko 2, Anatoliy Sachenko 3,4, Robert E. Hiromoto 5,6, Volodymyr Kochan 3
1 National Aerospace University KhAI, 17 Chkalov str., 61070, Kharkiv, Ukraine, v.kharchenko@csn.khai.edu
2 O. M. Beketov National University of Urban Economy in Kharkiv, 17 Marshal Bazhanyov str., 61002, Kharkiv, Ukraine, Herman.Fesenko@kname.edu.ua
3 Ternopil National Economic University, 46020, 11 Lvivska str., Ukraine, as@tneu.edu.ua
4 Silesian University of Technology, 44-100, 2A Akademicka str., Gliwice, Poland, as@tneu.edu.ua
5 University of Idaho, 709 S Deakin St, Moscow, ID 83844, USA, hiromoto@uidaho.edu
6 Center for Advanced Energy Studies, 995 University Blvd, Idaho Falls, ID 83401, USA, hiromoto@uidaho.edu

Abstract—The general structure and main principles of creating a multi-version post-severe NPP accident monitoring system, which consists of one wired and three drone-based wireless network subsystems, are proposed. Reliability block diagrams for the system are built. On the basis of the reliability block diagrams, reliability models of the system are developed. The dependence on probability of failure-free operation for different structures of the system on number of the redundant drones for the Wi-Fi drone-based communication section is obtained and analysed.

Keywords—drones; wired/wireless network subsystems; sensor- and drone-based communication networks; Wi-Fi; light fidelity; reliability block diagram; reliability models; redundancy

I. INTRODUCTION

In case of severe NPP accidents, a special highly resilient and survivable monitoring system is needed to measure critical parameters of the reactor’s safety subcomponents and provide mechanisms to physically assess critical accident levels. In addition, the monitoring system must also enhance the decision-making policies for NPP recovery and minimal start up sequences. In general, these issues can be mitigated by means of specialized equipment integrated into a post-accident monitoring system (PAMS). Such a system would typically consist of multiply redundant sensors and wired (cabled) networks connected to the Crisis Centre (CrS). However, the Fukushima NPP accident confirmed that such types of equipment are very vulnerable to both natural and man-made disasters. As a consequence, the design of a PAMS and similar systems must tolerate equipment failures, and maintain the ability to redirect critical information flows for proper decision making in real time.

The goal of the paper is to overview the principles, the design of scalable communications infrastructures and to present the analysis and conclusions on how to ensure reliability of post-severe NPP accident monitoring systems.

The paper begins with background information regarding NPP PAMS, and its integration and application of drones and other unmanned aerial vehicles (UAVs). In the main part we describe a multi-version post-severe accident monitoring system (MPSAMS) structure. A reliability model framework for different variants of MPSAMS is analysed.

II. STATE-OF-THE-ART

After the Fukushima accident, the implementation of a reliable and survivable PAMS has become a priority requirement within the national and international regulatory bodies. PAMS is also necessary for other critical infrastructures (e.g., chemical enterprises, oil-gas transport systems and so on). According to [1], such a system assures the functionality of accident and post-accident monitoring for any anticipated design-specific events. More importantly, the PAMS design must provide resilience under unforeseen and hazardous conditions such as earthquakes, severe fuel damage and full de-energization of an NPP unit.

The diversity (multiversity) principle [2] is applied to provide NPPs and other critical infrastructures with reliable and survivable PAMS. This principle incorporates the use of two or more options to perform the same functional operation. PAMS, based on this principle of version-functional redundancies, is called a multi-version system.

In [3] Kima et al. proposed the use of PAMS based on the multiversity principle. They argued that in coping with severe accidents, such as Fukushima, a fully independent monitoring system is required, which is separated (isolated) from the conventional instrumentation and control system. Recent development in data management as well as modern solutions in aviation technology makes possible the exploitation by UAVs for critical infrastructures monitoring. The work [4] is devoted to a modular multi-mission airborne sensor system capable of performing operations from reconnaissance to radiological and nuclear surveillance.
Towler et al. [5] present a remote sensing system for radiation detection and aerial imaging. Sanada and Torii [6] discuss a post-accident monitoring system, which includes UAVs, unmanned observation boat, radioactivity radio-sonde, manned helicopter and other devises needed for efficient monitoring such accident.

Schneider et al. [7] note that UAVs can be deployed in a short time frame to map large areas (on the order of square kilometres) with regards to dose rate, surface activity or radionuclide identification, they can collect vital data to be used by decision-makers.

The paper [8] proposes a drone-based solution to help on the search and rescue activities over disaster scenarios. The proposed architecture is composed of specialized drones to accomplish specific tasks and an internal modules organization to grant they will be able to accomplish their objectives.

Among the advantages UAVs may bring to an accident monitoring, in [9] authors highlight the gain in terms of time and human resources, as they can free rescue teams from time-consuming data collection tasks and assist research operations with more insightful and precise guidance thanks to advanced sensing capabilities.

Tina et al. [10] present a novel approach of using UAVs to establish a communication infrastructure in case of disasters. Authors explain the details of the system in three aspects: end-to-end communication, localization and navigation, and coordination.

An approach based on the extent of interaction between the UAV and terrestrially deployed wireless sensors is presented in [11].

The paper [12] deals with considering the possibility of the most efficient usage of a transmission channel capacity and receiving of a generalized image of a servicing object state as the entropy estimation of its sensors activities.

Hence, a problem of development and implementation of accident monitoring systems for NPPs and critical infrastructures as a whole using diverse means including UAVs is very challengeable in point of safety view.

Main principles of creating the PAMS:
- Diversity of sensors (three types of data sources (sensors) are applied: wired sensors; wireless sensors; light fidelity (Li-Fi) sensors based on a bidirectional wireless technology similar to Wi-Fi); diversity of transmission (wired, wireless drone-based and Li-Fi drone-based network); diversity of data (sensors, video).
- Mobility (drones).
- Dynamical reconfiguration and redundancy (drone fleet).

The drone fleet is divided into subsets: 1) repeaters (Slave) that work together on a principle of "one leader". If the “leading drone-repeater” (Master) is damaged then another drone-repeater takes over the previous Master’s functions; 2) observers (equipped with a TV camera), when enabled runs the continuous visual monitoring of the accident location; 3) additional sensors, that can be

III. STRUCTURE AND PRINCIPLES

Existing NPP PAMSs are based on wired networks that connect sensor areas with the crisis-control centre. Reliability and survivability of such systems are assured by redundancy of equipment, cable communications and other components. However, in the case of severe accidents, wired network-based PAMS can experience damaged sensors or broken cable connections. Under such conditions, the NPP PAMS is partially or totally rendered useless. To avoid such a problem, a multi-version approach is envisioned in which the wired network components and interfaces are expanded to include wireless communication components, which is more resilient to bridge physical failures.

To assure stability of a wireless network-based PAMS subsystem after an accident or a powerful jamming attack, a reliable transmission of data to support the possible failures of a wired network is deemed essential. Consequently, to improve the survivability of PAMS, the authors have introduced the use of a drone-fleet subsystem (Hiromoto et al. [13] and Kharchenko et al. [14]).

In the normal operational mode, data and command exchanges run through the wired network. If it is damaged during an accident, an auxiliary wireless network is created to support the activities of a fleet of communication drones. Drones are launched in the event of a wired network failure or the detection of a possible severe accident. The drones are designed to autonomously form a stable flight formation, which is configured in a Master/Slaves arrangement. In order to conserve battery power or in the case of node dropout, the Master node (which is given command responsibilities) can be reassigned to other Slave nodes when deemed appropriate. From this vantage point, the formation of drones will cooperate to maintain the following functions: to monitor and collect all data from sensor modules that are equipped with wireless connections; to form a reliable mesh network for optimal data streaming between point-to-point transmissions; to provide surveillance imaging for damage control, and search and rescue; to summarize areas of contamination; and provide an unmanned observation platform for exploratory surveillance.

Finally, in a severe accident, it will be very important to minimize the power consumption of both the measurement and control modules, since both the wired and wireless microcontrollers can be activated. As a consequence, the power demands required by the wireless interfaces that interact with the drones must be analyzed from a signal strength perspective.
carried by drones or placed in certain locations). Drones should be able to change their role by upgrading equipment at their base station.

Measurement and control modules are equipped with backup batteries, wireless communication modules; as well as, self-testing and self-diagnostic systems.

IV. RELIABILITY MODELS

The multi-version PAMS is a modified wired network that combines three wireless subsystems to support wireless data transmissions of a drone fleet with the integrated PAMS. The wireless network consists of three wireless network subsystems: Wi-Fi subsystem (SubW), Li-Fi subsystem (SubL) and Wi-Fi drone-based subsystem (SubD). In addition, the wired network is also regarded as subsystem (SubG). Using this designation of subsystems, Fig. 1 illustrates the version redundancy of sensors and communications for these components.

![Simplified structure of the MPSAMS](image)

In other words, the Wi-Fi subsystem, the Li-Fi subsystem, the Wi-Fi drone-based subsystem and the wired subsystem are all diverse among one another. Thus, such a multi-version PAMS can be considered as a MPSAMS. The communication section for the Wi-Fi subsystem and the communication section for the Li-Fi subsystem are drone-based. In addition, both sections for Wi-Fi drone-based subsystem are drones-based, and used to support reliable transmission of data if the wired subsystem section happens to fail.

The proposed MPSAMS (see Fig. 1) can be based on 2, 3 and 4 subsystems (Figs. 2–4).

Probability of failure-free operation (PFFO) is calculated according to (1)-(7).

Fig. 5 below is designed by simulation using (1)-(7), and they illustrate the ways of increasing the MPSAMS reliability.

![Reliability block diagrams for the MPSAMS based on: (a) the wired network subsystem (SubG) and the Wi-Fi subsystem (SubW), (b) the wired network subsystem (SubG) and the Li-Fi subsystem (SubL), and (c) the wired network subsystem (SubG) and the Wi-Fi drone-based subsystem (SubD)](image)

![Reliability block diagrams for the MPSAMS based on: (a) the wired network subsystem (SubG) and the Wi-Fi subsystem (SubW) and the Li-Fi subsystem (SubL), (b) the wired network subsystem (SubG) and the Wi-Fi drone-based subsystem (SubD), and (c) the wired network subsystem (SubG), the Li-Fi subsystem (SubL) and the Wi-Fi drone-based subsystem (SubD)](image)

![Reliability block diagram for the MPSAMS based on the wired network subsystem (SubG) and the Wi-Fi subsystem (SubW) and the Li-Fi subsystem (SubL) and the Wi-Fi drone-based subsystem (SubD)](image)
For example, all plots in Fig. 5 show that PFFO for the MPSAMS will increase if the number of the redundant drones grows from 0 to 3.

The second way is to use more reliable elements for subsystems of MPSAMS.

The third way is to increase the number of subsystems for MPSAMS. The MPSAMS based on SubG, SubW, SubL and SubD has the best PFFO among other structure modes.

V. DISCUSSION AND CONCLUSIONS

1. The use of diverse data transmitted from the measurement and control modules as well as additional modules (sensors), which can be placed in areas not accessible by human operators, allowing increase trustworthiness of information about the reactor and the station area as whole.

2. The use of wireless connections with specified modules (described in point 1) is a fail-safe mechanism to maintain critical operational monitoring for a severely damaged NPP wired network. It is understood that the deployment of wireless communication within an NPP is prohibited by current regulatory standard. However in the event of a major nuclear accident, all strategic technologies must be made available at that critical time.

3. Ensure an acceptable lifetime of accumulators for both operating measurement and control modules by relaying their signals. Thus, repeaters will be placed on the drones that reach NPP at the required time.

Authors propose the use of MPSAMS to mitigate the potential hazards arising from severe NPP accidents. The MPSAMS includes one wired network subsystem (traditional PAMS) and three wireless network subsystems that are more resilient to cope with wired communication failures. In particular:

- The number of MPSAMS’ wireless network subsystems can be reduced according to the NPPs characteristics.
- For example, all plots in Fig. 5 show that PFFO for the MPSAMS will increase if the number of the redundant drones grows from 0 to 3.
- The second way is to use more reliable elements for subsystems of MPSAMS.
- The third way is to increase the number of subsystems for MPSAMS. The MPSAMS based on SubG, SubW, SubL and SubD has the best PFFO among other structure modes.

V. DISCUSSION AND CONCLUSIONS

1. The use of diverse data transmitted from the measurement and control modules as well as additional modules (sensors), which can be placed in areas not accessible by human operators, allowing increase trustworthiness of information about the reactor and the station area as whole.

2. The use of wireless connections with specified modules (described in point 1) is a fail-safe mechanism to maintain critical operational monitoring for a severely damaged NPP wired network. It is understood that the deployment of wireless communication within an NPP is prohibited by current regulatory standard. However in the event of a major nuclear accident, all strategic technologies must be made available at that critical time.

3. Ensure an acceptable lifetime of accumulators for both operating measurement and control modules by relaying their signals. Thus, repeaters will be placed on the drones that reach NPP at the required time.

Authors propose the use of MPSAMS to mitigate the potential hazards arising from severe NPP accidents. The MPSAMS includes one wired network subsystem (traditional PAMS) and three wireless network subsystems that are more resilient to cope with wired communication failures. In particular:

- The number of MPSAMS’ wireless network subsystems can be reduced according to the NPPs characteristics.
- When all ground-based wired sensor sections are damaged, drone-sensors of Wi-Fi drone-based subsystem type can be deployed to bridge and replace lost services.
- When the wired network subsystem fails, then each of the wireless network subsystems are deployed by drone-based communication sections to support the reliable transmission of data.

To increase the MPSAMS’ survivability, both sensor and communication sections of wireless network subsystems are equipped with backup batteries and multiple blocks of wireless communication modules as well as self-testing and self-diagnostic systems.

To provide the increment of MPSAMS’ reliability a number of redundant elements (drones or sensors) of subsystems should be increased and more reliable subsystem components should be used.

Finally, the MPSAMS does not belong to widely used classes of systems. It is a system with the following properties:

- It is multifunctional because it performs many different tasks that are not homogeneous.
- It is extensible (scalable) because the number of components, including drones and measurement modules, can be changed dynamically.
- It is universal because it is invariant with respect to types of drones and modules employed, where these components can be defined by set of minimum requirements only.
- It is a complete system that can be deployed and operated in many different environments.

REFERENCES

[8] D. Camara, “Cavalry to the rescue: Drones fleet to help rescuers operations over disasters scenarios,” in Proceedings of the 2014


