5

Smart Synergistic Security Sensory Network for Harsh Environments: Net4S

Igor Peshko
Department of Mechanical and Industrial Engineering, University of Toronto
Department of Physics and Computer Science, Wilfrid Laurier University
Canada

1. Introduction

This chapter discusses the basic requirements for the design and algorithms of operation of a multi-parametric, synergistic sensory network – Smart Synergistic Security Sensory Network or Net4S – specially adapted for operation at nuclear power plants or other potentially dangerous sites. This network contains sensors of different types and is capable of analyzing the dynamics of environmental processes and predicting the most probable events. The discussion includes analysis of: 1) the technical aspects of operability of the sensors, optical and electrical telecommunication channels, and computers in the presence of ionizing radiation; 2) the influence of environmental parameters on the sensors' accuracy and network operability; and 3) the development of simulators capable of advising safe solutions based on the analysis of the data acquired by the Net4S. Such a real-time operating network should monitor: (1) environmental and atmospheric conditions – chemical, biological, radiological, explosive, and weather hazards; (2) climate/man-induced catastrophes; (3) contamination of water, soil, food chains, and public health care delivery; and (4) large public/industrial/government/military areas. Military personnel, police officers, firefighters, miners, rescue teams, and nuclear power plant personnel may use the mobile terminals (man-operated vehicles or unmanned robots) as separate multi-sensor units for local and remote monitoring.

Among different types of sensors, only optical laser sensors can respond immediately and remotely. Such sensors can simultaneously monitor several gases, vapours, and ions with the help of single tunable laser; however, the use of several lasers operating at different, well separated wavelengths, dramatically improves accuracy and reliability, and increases the number of monitored substances. The Net4S, monitoring a number of parameters inside and outside a Nuclear Power Plant (NPP), can serve as the security, safety, and controlling system of the NPP.

Besides the technical issues, the chapter also discusses the social aspects of the Nuclear Power Plants' design, construction, and exploitation. Some power consumption-free technologies that significantly improve the reliability of the Nuclear Power Plant are discussed.

In principle, open access publishing is a purely commercial project. After submitting a paper to classical journals, the author should wait for a relatively long time and should fight with the reviewers – the "narrow specialists" are the author's competitors and usually state that

everything is known, that the subject of publication is not interesting, and that the author is of low qualification. The "wide specialists" do not understand what the paper is about and criticize in general – the current tendency in science and technology are out of the subject that the author discusses, that any laser now can be bought off the shelf, and so on. Because of this paradox, a lot of the papers that were later nominated for prestigious awards were initially rejected. In some sense, open access publishing is free from these disadvantages. However, since the publisher should generate maximum profits from this activity, the high requirements for the quality of publications are difficult to be completed.

The next argument is then why so critically select the papers if, anyway, no one can or wants to estimate the real value of new papers. At the same time, open access publications have one very serious advantage. Government experts mostly write in reports what their chiefs expect to hear from them, post-graduate students write to please their supervisors, and Professors write proposals on subjects that the funding agencies declare in calls, and so on. These are because, directly or indirectly, all these categories are payable from the "top publishers". So, once a funding agency declares a solicitation for the investigation of ozone hole, a lot of researchers demonstrate how dangerous the hole is. As soon as the funding ends, nobody remembers what the ozone hole is.

A somewhat different situation is present with open access publishing: the *author pays* for the publication, so he/she is almost free not to lie. However, other public requirements, such as generating more publications before a thesis defense, getting a Professorship position, or being awarded by a Government or private agency push people to publish something. Thus, they invest money in future benefits. No one is absolutely honest and those who believe that they are, very often have limited knowledge of the subject they discuss and analyze. The ways to develop a really safe and effective Nuclear Power plant are very twisted and long. The NPP is very big, complex, expensive to be built and proven in different variants. Drosophila flight is much more perfect in design and implementation since the generation time is several tens of hours, not tens of years as it is for NPPs. Until now, the problem of design and safe exploitation of a NPP is very challenging and uncertain.

The author of this chapter is a specialist in laser physics and optical sensors, not in atomic physics or its applications. However, Dr. I. Peshko was working in Kyiv, Ukraine at the moment of Chernobyl's "peaceful explosion" and watched the reaction and behavior of regular people, academics, government organizations, and researchers. These observations can be very useful for analytical specialists who develop general principles of design, exploitation, and control of the NPPs. In such a "twilling zone" as the NPP, the probabilistic estimation of a single independent person may sometimes be more valuable than official reports and opinions of specialists. The bottom line is that official reports are typically prepared by specialists and officials to protect themselves and to hide their past mistakes, not to protect the future of millions of people. Every time I think about Chernobyl's events, I remember my mother who spent all her life as a housekeeper in a small town in Northern Ukraine and understood nothing about atomic energy. One day, when a radio broadcast informed us about the government's decision to build Chernobyl's Nuclear Power Plant, my mother said, "My feelings are very bad. How is it possible to construct a nuclear station in a place that is a source of water for tens of millions of people?" As I laughed, I replied, "The Chief of the Atomic energy program promised to install his bed on the top of the reactor to demonstrate how safe a reactor is." Unfortunately, time has shown how wrong the best specialist was and how right a regular housekeeper was.

2. Synergistic sensory network

2.1 Threat classification

Nuclear Power Plants are strategically important objects that may be affected by internal and external threats. Consequently, a NPP is considered a potential source of danger to its surroundings and, in turn, environmental elements – natural, artificial, and human factors – are potential dangers for a NPP.

Five types of possible threats potentially affecting the NPP are:

1. Natural catastrophes;
2. Technological (internal and external) problems resulting in emergencies;
3. Terrorist threats;
4. Personnel and security staff sabotage;
5. Scientific uncertainty and scams.

The first and second threats in the list above were widely discussed and documented during the initial stages of the development of nuclear technologies. The third threat became extremely evident after the 9/11 attacks and until now, is a very popular topic of discussion at different public and government levels. The fourth threat may be linked with both internal and external country sources and may have criminal and political backgrounds. Finally, the fifth threat, to our knowledge, is discussed for the first time in this book. It is not an issue for detailed discussion here but this is a very serious problem of modern and future life. The falsification of scientific results; demonstrations of non-existing products or unachieved parameters on the Internet; publication of preliminary, "fast" materials in numerous journals; and awarding grants on the basis of relationships rather than merit result in unpredictable events with critical technologies.

I would like to present one example from my personal experiences. A very famous Canadian Professor, whom I was working with, proposed a thin diffractive grating filled with a biological material as a biosensor. The more specific substance the grating accumulates, the stronger the diffraction is. This works in some range of small changes in grating strength. However, the Bessel function that describes the diffraction process of the thin grating has multiple zero points (solutions); in other words, for several *different amounts* of measured substance, the output signal will be *the same*. I gently mentioned that this kind of technology cannot be used for sensor applications and two weeks later, was fired for some formal reasons. If a tenured Professor of a famous University does not know the properties of the Bessel functions, this is very bad. However, if the Professor knows this and hides it just to receive a grant for the "development" of critical technology, this is much worse.

In attempts to forecast the future, the principle question is: if we know that we don't know, how do we develop a probabilistic solution of the problem with minimal material losses? How can we estimate and forecast of "unpredictable" events? First of all, we need to collect maximal real-time flows of information. To control the situation inside and outside of a NPP, the Sensory Network should monitor several zones: a) core (reactor) area; b) plant building and surrounding territory; c) 30-km radius zone (the Chernobyl tragedy showed that the strongest radioactive poisoning happened within a 30-km zone); d) in North America: Mexico - USA - Canada region (depending on the specific plant location). Thus, a NPP is a duplex element of the global security network. It needs to accept information from near and far environmental areas, and information regarding what is going on inside the NPP should be retrievable from any control station in the country.

The safety zone classification depends on the reactor construction, type of emergency, population density, and the locations of other industrial plants. In the case of the recent Fucushima reactors catastrophe in Japan, the officials specified 5-km and 20-km evacuation zones.

2.2 Principles of 4SNet

The development of a Global Monitoring Security Network is the main task on route to several scientific, technological, business, military, and political directions of modern life. Such a real-time operating network should monitor: (1) environmental and atmospheric conditions: chemical, biological, radiological, explosive, and weather hazards; (2) climate/man-induced catastrophes; (3) contamination of water, soil, food chains, and public health care delivery; (4) large public/industrial/government/military areas. Such a system is expected to consist of mobile robotic and stationary platforms, equipped with a set of portable environmental sensors that are connected to the monitoring centers. Each sensor should be a self-registering, self-reporting, plug-and-play unit that uses unified electrical and/or optical connectors and operates with the IP communication protocol. Military personnel, police officers, firefighters, miners, rescue teams, and nuclear power plant personnel may use the mobile terminals (man-operated vehicles or unmanned robots) as separate multi-sensor units for local and remote monitoring. Some of the objects being monitored require special attention, such as nuclear and chemical plants, offshore oil platforms, mines, military ammunition production facilities, and so on. The Net4S components must operate at varying pressures and temperatures; at indoor and outdoor conditions; be immune to mechanical, thermal, electro-magnetic and radiological noise; and be able to operate in case of electrical blackouts.

In different areas of the reactor and surrounding territories, different types of sensors can be installed. This makes it possible to map temperature, ionizing radiation of different types, gas molecules and ion concentrations, vapors, and presence of dust particles. The overlapping of all these maps and reconstruction of their dynamics can predict what will happen in the close future. During several initial cycles of reactor operation in a "manual regime", the dynamics of all parameters should be recorded and analyzed. During the next routine operation, the total network should permanently measure the data, map them, and compare with previously averaged data. If even small changes of parameters are accumulated along time, this is a sign for alarm. It does not matter which parameter is out of the norm. A negligible event may initiate a catastrophe: a cup of coffee left by a personnel on the operational panel may flip over and cause damage to the electronics located under the desk. Of course, everyone can tell me that nobody is permitted to drink coffee on the command desk, and I absolutely agree, but I definitely know that real life is much richer with possibilities than any designer or programmer can imagine.

During the design stage, any chains of possible undesirable events should be simulated and analyzed. Let us continue the hypothetical "flipped coffee" example. Because of the short circuit in the desk electronics, several high power circuits in the power commutation station are simultaneously activated. This results in a fire and uncontrollable activation of the fuel reloading system that, in turn, results in the quick heating and destruction of the reactor. This example is naïve, very simplified, and may never be realized in practice due to specific reactor construction details and algorithms of operation; however, it helps to understand that to design a nuclear reactor, psychologists and specialists in the traditions of different cultures should be involved, not just specialists in nuclear physics. Previous background and

experience are very important as well. In case of a sudden earthquake, people who experience it for the first time will chaotically look around; those who have survived a strong earthquake may be in panic, but will run away as fast as possible. In both cases the reactor may be out of personnel control. So, it is better if the territory around the plant is supplied with sensors that can measure the amplitude of impact, activate the reactor shut down system, and sound alarms for the personnel. An even better solution is one where the Global Security Network can directly and automatically inform the NPP that a tsunami is approaching.

2.3 Reliability of an inhomogeneous network

In order to improve reliability, sensor redundancy (using multiple instances of a sensor) can be implemented; however, adequateness (ensuring the measured signal pertains only to specific parameters) is still not guaranteed. In real life, it is practically impossible to isolate a single process and be certain that the measurement is related to just one variable. A readable sensor signal may appear as a result of one "strong" interaction with an object, or several indirect interactions that affect the sensor in the same way as the "strong" one. Thus, the problem of reliability is apparent in these measurements, especially if we need to measure in unexpected, unpredictable, and unfriendly conditions. As a simple example: some house fire alarm sensors are typically activated every time someone takes a shower; both water and fire are interpreted as the same entity by the sensor. These sensors were tested for fire emergency events and definitely work well in corresponding conditions; however, nobody thought to test them in high humidity conditions, an absolutely "opposite" range of application. The result of this is that after several false alarms people typically turn off a fire alarm sensor. Thus, the adequateness of measurements is questioned every time.

A sensory network, where the sensors operate in different physical domains, should be used. This creates an inhomogeneous network with a variety of sensors capable to perform joint analyses and mapping of different datasets.

References (Peshko, 2007; Matharoo, 2010) discuss a concept of an "inhomogeneous network". This network combines a set of different types of sensors to measure different parameters (sub-networks), and different types of sensors that measure the same parameter but based on different physical phenomena. For example, temperature can be measured by a bi-metallic thermometer (mechanical thermo-deformation), by a thermocouple thermometer (a junction between two different metals that produces a voltage related to a temperature difference), and can be calculated from the gas optical absorption spectra (spectral line broadening is proportional to the temperature). Evidently, in this hierarchy, the simplest implementation (and one that does not require any power supply) is the bi-metallic thermometer. It may not give information very precisely, but it does "survive" in harsh conditions. In an inhomogeneous network, the sensors synergistically collect and analyze information that individual sensors cannot. This information may be used as a rough measurement for evaluation of more sophisticated multi-parametric processes. If one knows the local temperature of a gas even with relatively low accuracy, the gas concentration remote measurement based on spectroscopy principles may be many times more accurate than if the temperature is unknown.

The sensor network should be analyzed and tested very carefully for the possibility of very rare but theoretically possible scenarios: due to strong irradiation, signals may saturate the transmittance of the processing system that may be interpreted as no signal or a very weak signal.

The required ability to interface with different sensors poses a challenge in maintaining a high level of overall system reliability. Using duplicate sensors for the same task decreases the probability of failure. If different sensors are used, each type of sensor needs to be rigorously tested to identify its most appropriate ranges and conditions of operation. Once this data is available for all the different types of sensors, an algorithm will be deployed to choose the sensor that has the likelihood of providing the most accurate reading at those environmental conditions. This provides a base platform for synergistic reliability. The best way is if the same set of parameters, such as level of radiation, temperature in some specific places, humidity, and presence of some gases or ions, can be measured locally and remotely. A difference in data, being acquired by local and remote sensory networks, means that "something is wrong".

A typical situation in science and technology is one when different groups of scientists and engineers developing devices working in the same area of research or technology fight with each other, proving which technology is better, cheaper, more accurate, and so on. For such sites as a NPP, the “single best choice” is unacceptable as nobody can predict for sure which technology will survive longer and would be more accurate in some unexpected conditions.

The data acquired at a NPP should be accessible (monitored) at plant command station but the NPP's personnel should not have access and ability to modify these data. They should be transferred to the external command and processing center. Even in cases when the data seems incorrect or “stupid”, they should be transferred and analyzed together with data from surrounding areas. A meteorite can be registered by seismic, gaseous, and temperature sensors 5 km away from a NPP and this can be interpreted by the NPP’s security network and personnel as a nuclear bomb explosion. In any case, the reactor cannot be stopped immediately, so each minute is crucial when preparing for critical events.

2.4 Synergistic cross-data

In an inhomogeneous, multi-level security network, each sensor, first of all, is responsible for measuring some specific parameters; at the same time, it supplies other sensors with some additional information that serves for more accurate measurements, more precise description of the investigated multi-parametric phenomena, and for the development of some conclusions about the characteristics of monitored events. Typically, the smart sensory network uses a set of sensors that control some secondary phenomena but still help in evaluation of the main process. For example, the level of ionizing radiation around a reactor in a power plant can be monitored with a set of scintillators; however, the concentration of the ionized air over the reactor can be measured well remotely and the radiation level can be estimated. Of course, this is not a direct measurement and it strongly depends on the reactor construction and principles of operation. Though, in case of an emergency, such estimations can be done from hundreds or even thousands of meters away from danger zones. Being preliminarily calibrated, this technique can provide quite accurate measurements.

To introduce the concept of an “inhomogeneous network of synergistic sensors”, consider a simple example. If your home thermometer, barometer, and humidity meter show values of 28°C, 750 torr, and 70% respectively, considering these devices individually, one can conclude that the weather is beautiful. Now, a synergistic complex, which is actually a set of different sensors – humidity, temperature, pressure, oxygen, methane, carbon oxide/dioxide, etc. – tells you that during the last two hours, the pressure fell from 770 to 750 torr, the humidity increased from 45% to 70%, the temperature increased by 3°C, and

the concentration of methane in your kitchen increased from 0.0002% to 0.2%. The dynamics of pressure, humidity, and temperature readings tell you that a hurricane is approaching, while the methane reading tells you that there is a gas leak in the house. Each separate reading does not say something terrible, but the history of parameter changes may predict that the roof of your house (that you were going to repair), may be destroyed by a hurricane, and because of the methane explosion, your house will be on the news.

A very important feature of the synergistic sensory complex is its ability to predict events; thus, the complex can alert you that the current, "beautiful" environmental data is just the beginning of a critical event. As another example, all gasoline stations are supposed to be equipped with fire alarm sensors; however, no one has considered implementing detectors for the presence of explosive materials or checking the quality of the electrical ground of fuel tanks and electronic equipment at the station. Potential sources of sparks, burned cigarettes, or explosive materials should be monitored *before* the fire starts and is then detected. Thus, the fire alarm sensory network should be "inhomogeneous" – it must contain different types of sensors capable of synergistically analyzing different scenarios.

A combination of several sensors can provide an estimation of an environmental event or emergency. For example, in case of a fire, CO, CO_2, H_2O vapour, and other specific gases (C_xH_y, NO_x) are emitted. However, the temperature and relative concentrations of these gases are different in the case of burning gasoline, wood, or plastic. A smart, multi-gas, multi-functional sensor would be able to tell the difference between a well-done BBQ on the stove versus a stove on fire. The difference is in the corresponding gas concentrations and character of light. A flame is chaotically modulated whereas a lamp over the stove irradiates light with constant intensity.

By referencing the measured concentrations with a database and analyzing the deviations in environmental conditions, the sensory platform can immediately generate the most plausible reason for the emergency. Analysis of space-time event maps and weather conditions will help to remotely identify the event and predict its dynamics.

3. Natural inhomogeneous network

It is often said that nature is the best creator, and that after many years of evolution, we are all products of good design. Our bodies are complex systems comprising of sensors, a central processing unit, and actuation devices. The human sensory-network is an example of a "well-designed" system. Every day, we use our senses of smell, touch, taste, hearing, balance, and vision, and although different sensors located throughout the human body register these sensations, the information gathered is sent through the same neurons to the brain, where it is processed and interpreted. After the data is processed and a decision is made, the "CPU center" activates a movable platform – the body. The decision made is based on information extracted from sensors specializing in different domains, i.e. analysis of electromagnetic fields, mechanical vibrations, chemical reactions, etc. The design of new technology is often driven by efforts to mimic designs found in nature. The problem is how to develop a "smart" sensory network for a power plant and environment monitoring that operates in a similar fashion to its biological counterpart, yet is capable of performing tasks not possible by natural sensory-organs, in an effort to increase public and private security.

As an additional example, imagine that you say to your significant other that you love them. You then receive feedback signals from different information channels – verbal responses, facial expressions, body movement, breathing patterns, etc. Each separate channel may

generate a false signal or no signal, e.g. they may close their eyes, but is it because they are happy or afraid to say "no"?
If any sensor/channel of information fails, the total human ability drops down; however, because of synergistic inhomogeneity, a human still operates, i.e. visually impaired people.
Another very interesting capability of the human sensory network is that if one channel fails, the other ones increase sensitivity to compensate for the lost data set. This is why visually impaired people often have an "absolute musical" hearing and can easily recognize similar sources of sound belonging to different objects, i.e. the footsteps of different people. How to teach or train the 4SNet for these capabilities is not currently clear.

4. How and what to do?

From an initial glance, the market is full of different types of sensors; however, there are still some gaping holes. For example, there are many methane sensors on the market, but thousands of miners around the world still die each year due to methane asphyxia or explosions. Similar arguments can be made for carbon monoxide sensors. NASA still announces a competition for the development of O_2, CO, and CO_2 sensors for extra-terrestrial missions; military and recreational divers still lack compact, reliable, and long-lasting sensors for the control of breathing gases; soldiers still die from roadside bombs; and airport security systems still do not detect explosives well. Current tendencies in advanced technologies pertain to the development of simple, cheap hardware and sophisticated software. Each sensor measures something; the deficiency, however, is in the interpretation of the data, shifting the problem from the real to the virtual world – complicated software might be more unpredictable and unstable than complicated hardware. However, it is much cheaper to correct software and to reload processors than to repair or upgrade millions of sensors.
To summarize, we then pose the following question: What are the basic requirements for a "universal", portable alarm sensor capable of operating on a movable robotic platform or in a life-supporting system? Such a sensor should demonstrate:

1. Immediate response;
2. Reliability: several processes are used to measure one parameter;
3. Multi-functionality: one process is used to measure several parameters;
4. Operability in hard environmental conditions;
5. Cheap, effective, simple hardware;
6. Sophisticated, "smart" software;
7. Low power consumption;
8. Self-calibration ability;
9. Synergistic data processing;
10. No additional external devices: pumps, calibrator, power supplies;
11. Immune to thermal, radiation, and mechanical noise;
12. Compatible with other sensors, sensory networks, and scientific instruments.

5. Nuclear power plant operational conditions

A nuclear power plant is a very specific object where the requirements for the Net4S are especially high. There are some technical problems in the sense of network exploitation. The optical elements (fibers, lasers, optics) can be colored under ionizing radiation. The main

components of electronics (semiconductor materials) are affected by such radiation as well. The penetrating radiation can affect the computer and electronics operation without even physically destroying these elements, resulting in the generation of false signals through the system. So, the optical sensors have some troubles, operating in this area.

In space, nuclear power, and other scientific applications, optical glass may be exposed to high-energy radiation like gamma-, electron, proton, and neutron radiation. With the accumulation of higher doses, this radiation changes the transmittance of optical glass especially near the UV-visible edge of the spectrum. The investigations of resistance of glasses versus ionizing radiation were intensively provided in 50's; these investigations were connected with research on nuclear bomb action on optical devices and other techniques.

Generally speaking, a long history of space exploration and NPP exploitation has accumulated enough knowledge on safe operation of opto-electronic devices at regular reactor conditions. However, for emergency cases, the sensory network should be protected so as to survive in catastrophes similar to the one in Chernobyl. First of all, a circuit of well-protected sensors should be installed on the perimeter of the NPP to supply the "outside" world with information in case the internal system is down. As this chapter is oriented for a wide range of readers, let us consider very shortly the problems in design and construction of internal opto-electronic sensors.

Firstly, any glass components (fibers, objectives, prisms, filters, etc.) located in the reactor and surrounding zones can be affected by ionizing radiation. Ionization caused by photon and particle radiation, changes the transmittance of optical glasses (Friebele, 1974; Schott, 2007; Sigel, 1974; Smith, 1964). An absorbed radiation dose of 10 Gy (10J energy of absorbed ionizing radiation by 1 kg of matter) gamma radiation leads to recognizable loss in transmittance over the complete visible spectral range. The decrease of transmittance is most significant at the UV-edge of the spectrum. Most glasses become unusable for optical applications if the radiation is increased to 100 Gy. The intensity of the color change does not only depend on the type of radiation dose but also on the energy of the ionizing radiation and the radiation dose rate.

Optical glasses can be stabilized against transmittance loss caused by ionizing radiation by adding cerium to the composition. The extent of stabilization depends on the glass type. In general, the higher the cerium content, the more the glass is stabilized against higher total doses but the more the intrinsic transmittance is reduced. In addition, the impact to the color change by addition of cerium depends on the glass matrix.

Most of the modern technological and telecom lasers work within the 1-2 microns wavelength range. So, the ionizing irradiation affects the transparency of glasses mostly in the wavelength range where the typical lasers do not work.

It should be mentioned that most of the currently operating NPPs have been designed and built 20-40 years ago. During this time, a lot of new radiation-protected technologies have been developed. One techno-cluster that absorbs a lot of new, specially developed technologies is the Large Hadron Collider (which started to work in 2010). These technologies are extreme radiation-resisting plastics, micro-cables, and radiation detectors. These technologies were designed to survive the radiation levels that are equivalent to a 100-megaton nuclear bomb explosion. Now is definitely the time to use them on old and new NPPs.

Generally speaking, all semiconductor devices are very sensitive to ionizing radiation. The attempts to use robots on the Chernobyl NPP failed very fast. The fact that

semiconductor devices irradiated by nuclear bomb ionizing and radio pulses stop operating tens of kilometers around a bomb explosion is well known. However, old electronic bulb devices still survive despite being very close to the epicenter (if not destroyed mechanically). So, two variants are possible: 1) all robot controllers and other electronics units should be located in a protected cabin with a cable connected to the robot engines, or 2) the electronics should be designed with old-fashioned components that are very insensitive to ionizing radiation.

6. Located on-robot

A sensor system for a reconnaissance mobile robot must monitor many environmental parameters; however, in miniature systems, we cannot simply combine several different sensors because of weight, size, and power consumption limitations. Therefore, all available processes and information gathered from sensor-environment interactions should be used for monitoring these different parameters.

The current tendency in the development of technologies for dangerous sites is the application of mobile robots. Such systems are under intensive development in Japan, USA, Canada, China, and the EU. Robots, as "environmental" guards, have some advantages and disadvantages. From one side, having limited "intellectual" abilities, a robot cannot find probabilistic solutions for unexpected problems. On the other hand, a robot has no human characteristics such as panic, fatigue, or narcotic/alcohol dependency that can suppress normal human abilities. The most useful and current application for a robot is as a carrier of sensors with preprocessing of the data. Regular reconnaissance robots may be applied without limitation within a NPP zone. However, to increase the emergency protection of the robots within the core (reactor) and secondary (building and territory) zones, the robots should be designed with high radiation and temperature protection.

A mobile robot with multi-gas sensors and a multifunctional spectrometer on-board is capable of identifying more than a hundred gases, liquids, and solids, locally and remotely. Such a system can be additionally supplied with a non-linear microscope, cameras, rangefinders, a laser-ultrasound scanner, and other techniques for detailed scanning of the environment and atmospheric conditions. This system is under development at several industrial companies and Universities in Canada: 1) Engineering Services, Inc. (Toronto) (ESI, n.d.), University of Toronto (Department of Mechanical and Industrial Engineering) (RAL, n.d.), P&P Optica, Inc. (Waterloo) (P&P Optica, n.d.).

The end-goal is to develop a smart sensory network for environmental monitoring, which is capable of performing tasks not possible by natural sensory-organs, in an effort to increase public and private security (Peshko, 2007; Matharoo, 2010). As the first step in achieving this goal, the design of an integral part of the proposed smart sensor-network: an all-in-one, multi-gas, photonic sensor (for CO, CO_2, CH_4, N_2O, O_2, and H_2O vapor sensing) is provided. The sensory platform also houses independent total-pressure and temperature sensors, infrared, ultraviolet, and γ-ray radiation detectors.

7. Catastrophe simulator: Computer forecasting of processes and events

The problems of continuous reliability and adequateness are apparent in measurements, especially if we need to measure in some unexpected, unpredictable, and unfriendly conditions. Sometimes, occasional combinations of the sensor signals may be interpreted as

an alarm signal, and, sometimes, at really dangerous situations, the alarm system "is sleeping" because an unpredictable interference of the environmental parameters may mask the real event. Thus, modeling the environmental processes together with the reactor's operational processes is necessary. This includes mapping the internal temperature and pressure parameters (dependent on the external ones), radioactive background during the reload process of technological elements and normal standard operation, and other repair/maintenance operations. A simulator will help check a number of situations that may or may not have happened in real life over thousands of years. Additionally, analyzing space-time event-maps and weather conditions will help to remotely identify the event and predict its dynamics. The end-goal is to develop a smart sensor-network for monitoring a nuclear power plant and its surrounding areas to estimate the most probable means that are necessary to predict and prevent catastrophic events.
A full size simulator should include: 1) Modeling of meteorological conditions (in case of an emergency, the area located along the wind path should be alarmed first); 2) Temperature 3D map: the heating/cooling plant model (sun/wind action, reactor operation, air-conditioning operation) should be taken into account – is it an internal source of unexpected heating or are external current factors resulting in local internal heating; what are the amplitudes of possible construction stresses in case of catastrophes); 3) Map of the over-ground and underground rivers, big water reservoirs; 4) Possible action of earthquakes, hurricanes, and other natural phenomena; 5) Modeling of the security system and problems with its operation in case of a catastrophe, cyber or direct terrorist attacks, errors, and emergencies.

8. Reactor zone security monitoring

The general reason for an alarm in any type of the security system is, "something is wrong". This concept is not connected with any specific technology. It is based on pre-calibrated standard scenarios and logical chains of events that typically happen if "everything is right". For example, let us consider the monitoring of personnel motion inside some protected zone:

1. Someone inserts a card key into the (corridor) door (does not matter who as the key may be stolen);
2. The cameras monitoring the door space confirm a moving object (it does not matter who (what) is imaged on monitors, as the security system may be hacked and some recording transferred to the monitors);
3. The motion sensors confirm that something is moving along the corridor;
4. The sound analyzers confirm that the sound spectrum of steps belongs to a person who did open a door (codes of the key), the person is alone, and moves along the way he/she is authorized to walk.

Non-confirmation at any stage of the described chain results in the activation of an alarm. In this case, the most important thing is not the right signal at each stage that may be falsified or not mentioned by security personnel, but the right sequence of actions with some specific signs at each stage.
If no motion is detected by the cameras (comparing pixel information variations, not by motion sensors!) for 20-30 seconds in the security room, it means that the security guards are neutralized or sleeping; an alarm should be activated automatically. This algorithm can be applied in any protected zone: banks, treasures, military sites, and so on.

It is very important that the same logic and the same sensors can be used for NPP safety control.

9. After 9/11

After the events of 9/11, governments are paying more attention to the protection of NPPs. USA's Congressional Research Service published open documents that describe the main requirements for the newly designed plants and propose the means for protection of old operating units. These documents are focused on analyses of NPP vulnerability to terrorist attacks (Holt, 2007) and general problems of NPP security and vulnerability (Holt, 2010). I cite here some key paragraphs from these documents because of their high importance.

"Nuclear plant security measures are designed to protect three primary areas of vulnerability: controls on the nuclear chain reaction, cooling systems that prevent hot nuclear fuel from melting even after the chain reaction has stopped, and storage facilities for highly radioactive spent nuclear fuel. U.S. plants are designed and built to prevent dispersal of radioactivity, in the event of an accident, by surrounding the reactor in a steel-reinforced concrete containment structure.

The Nuclear Regulatory Commission (NRC) approved its final rule amending the design basis threat (DBT) (10 C.F.R. Part 73.1) on January 29, 2007, effective April 18, 2007. Although specific details of the revised DBT were not released to the public, in general the final rule

- clarifies that physical protection systems are required to protect against diversion and theft of fissile material;
- expands the assumed capabilities of adversaries to operate as one or more teams and attack from multiple entry points;
- assumes that adversaries are willing to kill or be killed and are knowledgeable about specific target selection;
- expands the scope of vehicles that licensees must defend against to include water vehicles and land vehicles beyond four-wheel-drive type;
- revises the threat posed by an insider to be more flexible in scope; and
- adds a new mode of attack from adversaries coordinating a vehicle bomb assault with another external assault.

In October 2006, NRC proposed to amend the security regulations and add new security requirements that would codify the series of orders issued after 9/11 and respond to requirements in the Energy Policy Act of 2005. The new security regulations were approved by the NRC Commissioners on December 17, 2008, and published March 27, 2009:

- Safety and Security Interface. Explicit requirements are established for nuclear plants to ensure that necessary security measures do not compromise plant safety.
- Mixed-Oxide Fuel. Enhanced physical security requirements are established to prevent theft or diversion of plutonium-bearing mixed-oxide (MOX) fuel.
- Cyber Security. Nuclear plants must submit security plans that describe how digital computer and communications systems and safety-related networks are protected from cyber attacks.

- Aircraft Attack Mitigative Strategies and Response. As discussed in the earlier section on vulnerability to aircraft crashes, nuclear plants must prepare strategies for responding to warnings of an aircraft attack and for mitigating the effects of large explosions and fires.
- Plant Access Authorization. Nuclear plants must implement more rigorous programs for authorizing access, including enhanced psychological assessments and behavioral observation.
- Security Personnel Training and Qualification. Modifications to security personnel requirements include additional physical fitness standards, increased minimum qualification scores for mandatory personnel tests, and requirements for on-the-job training.
- Physical Security Enhancements. New requirements are intended to ensure the availability of backup security command centers, uninterruptible power supplies to detection systems, enhanced video capability, and protection from waterborne vehicles."

From my point of view, these documents do not pay enough attention to the tendencies of modern weapons. It is much harder to protect a NPP from small, truck-launched weapons than from a big rocket sent from a plane or ship hundreds of kilometers away from the NNP.

It is interesting to note that the problems that took place at Fucushima's reactors (after earthquake) were listed in the NRC documents listed above. So, these documents and the NPP live their own independent life: corporate interests stand higher than the security of the entire country.

Technological monitoring of a power plant includes the control of radiation level (all types of ionizing radiation), temperature, humidity, and some ions and gases that may appear as a result of normal technological process or abnormal situations, for example, CO_2 or CO, C_xH_y, and NO_x in case of a fire. However, the gas monitoring system should also monitor explosive vapours, nerve/blister agents, and other substances that can be used in terrorist actions or during preparing for such actions.

10. Some simple ideas

The key issue is electrical consumption – feeding the security network and coolers for the reactors and burned fuel. The special attention zone is reserve electrical generators and pumps for cooling systems. The recent catastrophe (March 2011) in Japan definitely demonstrated that a reserve generator should be mounted on the damping pyramid with height two times higher than any tsunami or other floating debris potentially affecting the generator. It would be nice to introduce a technique where if the reserve generator is not checked once a year, the NPP should automatically slow down to a safe power minimum, and no NPP personnel, government official, or president of the NPP operating company can turn off the "shut down" option. The best way is to install a generator out of the NPP territory with several power lines going to the NPP by different ways. The cooling loops should be duplicated and triplicated (as much as engineers would decide). It is strongly recommended to have a lot of small pumps instead of fewer high power pumps.

The best option is to build a reservoir of alarm cooling liquid capable of autonomously operating the coolers until the NPP slows down to a safe level.
Every day, on my way to work, I see big tanks of water along the road in each municipality. A relatively low-power pump delivers water to the tank 25-m high and after that, the water runs to consumers without any pumping. So why this extremely simple technology, which was actually developed during the times of ancient Rome, is not used as an emergency reserve cooler that can work until the risk crew reconstructs a source of electricity to support the main pumps' operation?
Analysis of the recent cyber attacks around the world shows that from time to time, higher and higher protected entities, like banks, governments, and big corporations that put in extra efforts to protect their sites and databases, are successfully hacked. It is time to develop special interfaces that have no electrical (wire/wireless) contact between the inside-outside zones of the protected segments of the network.

11. Conclusions

This chapter discusses the principles of development of a Smart Synergistic Security Sensory Network for Harsh Environments: Net4S. It includes an analysis of:

- the technical aspects of operability of the sensors, optical, and electrical telecommunication channels, and computers in the presence of ionizing radiation;
- the influence of environmental parameters on the sensors' accuracy and network operability;
- the development of simulators capable of advising safe solutions based on the analysis of the data acquired by the Net4S; and
- social aspects of the Nuclear Power Plant design, construction, and exploitation.

In total, such a real-time operating network should monitor:

- environmental and atmospheric conditions: chemical, biological, radiological, explosive, and weather hazards;
- climate/man-induced catastrophes;
- contamination of water, soil, food chains, and public health care delivery; and
- large public/industrial/government/military areas.

The end terminals of the system consist of mobile robotic and stationary platforms, equipped with a set of portable environmental sensors that are connected to the monitoring centers. Each sensor should be a self-registering, self-reporting, plug-and-play unit that uses unified electrical and/or optical connectors and operates with the IP communication protocol.
To control the situation inside and outside a NPP, the Sensory Network should monitor several zones:

- core (reactor) area;
- plant building and surrounding territory;
- 10-30 km radius zone; and
- entire country and neighboring territories.

A concept of an "inhomogeneous network" is also introduced. This network combines a set of different types of sensors to measure different parameters (sub-networks), and different types of sensors that measure the same parameter but based on different physical phenomena. The Net4S aims to solve several problems simultaneously:

- the detection and estimation of critical events by a synergistic sensory-network,
- higher reliability of multi-substance sensors based on different operational principles; and
- prediction of critical events based on a history of monitored parameters.

The reactor area should be monitored by a network of local sensors and by the network of remote sensors, in case the core zone is in a state of emergency.

Among different types of sensors, only optical laser sensors can respond immediately and remotely. Such sensors can simultaneously monitor several gases, vapours, and ions with the help of one laser; however, the use of several lasers operating at different wavelengths, dramatically improves accuracy and reliability, and increases the number of monitored substances. A synergistic sensory network can monitor the background optical losses (scattering), environmental pressure, temperature, and humidity.

The Net4S, monitoring a number of parameters inside and outside a Nuclear Power Plant, can serve as the security, safety, and controlling system of the NPP.

The most critical parts of the cooling systems should be self-operable: the water should be delivered from the highly located tank by free running without any pumps.

In total, the security system should identify natural events (hurricane, earthquake, abnormally high or low temperatures and pressures), unauthorized access to the NPP (terrorist attack, hacker's attack) and wrong personnel actions.

12. References

Friebele, E.; Ginther, R.; Sigel Jr. G. (1974). Radiation protection of fiber optic materials: Effects of oxidation and reduction. Applied Physics Letters, Vol.24, No.9 1974 p.412 - 414.

ESI: Engineering Services, Inc. (n.d.). 01.03.2011, Available from www.est.com

RAL: Robotics & Automation Lab, University of Toronto, Department of Mechanical and Industrial Engineering (n.d.). 01.03.2011, Available from www.mie.utoronto.ca/labs/ral

Holt, M; Andrews A. (2007). Nuclear Power Plants: Vulnerability to Terrorist Attack. 01.03.2011, Available from http://www.fas.org/sgp/crs/terror/RS21131.pdf

Holt, M; Andrews, A. (2010). Nuclear Power Plant Security and Vulnerabilities, 01.03.2011, Available from http://www.fas.org/sgp/crs/homesec/RL34331.pdf

Matharoo, I.; Peshko, I.; and Goldenberg, A. (2010). Synergistically-reliable multi-gas photonic sensors for security networks *Proceedings of the Canadian Society for Mechanical Engineering Forum 2010.* Victoria, British Columbia, Canada, 7-9 June, 2010.

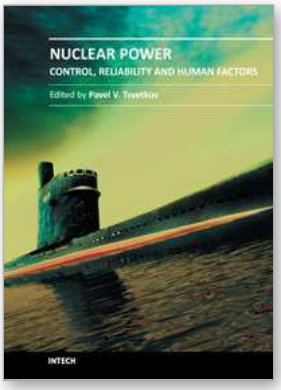
P&P Optica, (n.d.) .01.03.2011, Available from www.ppo.ca

Peshko, I. (2007). New-generation security network with synergistic IP-sensors *Proceedings of IEEE, Optics East: Advanced Environmental, Chemical, and Biological Sensing Technologies V* 6755 ed T Vo-Dinh, R A Lieberman and G Gauglitz. Boston, Massachusetts, USA, 9-12 Sep 2007.

SCHOTT Optical Glass Pocket Catalogue (2007). 01.03.2011, Available from http://www.schott.com/advanced_optics/english/download/tie-42_radiation_resistant_glasses.pdf

Sigel Jr, G.; and D. Evans, B. (1974). Effects of ionizing radiation on transmission of optical fibers. *Applied Physics Letters,* Vol. 24, No. 9, (1 May 1974), p.410-412.

Smith, H.; Cohen, A.. (1964). Color Centers in X-Irradiated Soda-Silica Glasses. *Journal of The American Ceramic Society* Vol. 47, No. 11, p.564-570.



Nuclear Power - Control, Reliability and Human Factors
Edited by Dr. Pavel Tsvetkov

ISBN 978-953-307-599-0
Hard cover, 428 pages
Publisher InTech
Published online 26, September, 2011
Published in print edition September, 2011

Advances in reactor designs, materials and human-machine interfaces guarantee safety and reliability of emerging reactor technologies, eliminating possibilities for high-consequence human errors as those which have occurred in the past. New instrumentation and control technologies based in digital systems, novel sensors and measurement approaches facilitate safety, reliability and economic competitiveness of nuclear power options. Autonomous operation scenarios are becoming increasingly popular to consider for small modular systems. This book belongs to a series of books on nuclear power published by InTech. It consists of four major sections and contains twenty-one chapters on topics from key subject areas pertinent to instrumentation and control, operation reliability, system aging and human-machine interfaces. The book targets a broad potential readership group - students, researchers and specialists in the field - who are interested in learning about nuclear power.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821