Work 41 (2012) 4545-4551
DOI 10.3233/WOR-2012-0035-4545
IOS Press

Automations influence on nuclear power plants: a look at three accidents and how automation played a role

Kara Schmitt
Human Centered Design Institute (HCDi), Florida Institute of Technology, 150 W. University Blvd, Melbourne, Fl 32901, USA

Abstract. Nuclear power is one of the ways that we can design an efficient sustainable future. Automation is the primary system used to assist operators in the task of monitoring and controlling nuclear power plants (NPP). Automation performs tasks such as assessing the status of the plant's operations as well as making real time life critical situational specific decisions. While the advantages and disadvantages of automation are well studied in variety of domains, accidents remind us that there is still vulnerability to unknown variables. This paper will look at the effects of automation within three NPP accidents and incidents and will consider why automation failed in preventing these accidents from occurring. It will also review the accidents at the Three Mile Island, Chernobyl, and Fukushima Daiichi NPP's in order to determine where better use of automation could have resulted in a more desirable outcome.

Keywords: Automation, nuclear power, human-centered design, accidents

1. Introduction

Automation is something we all encounter every day. From spellcheck to cruise control, automation has assisted us in performing the menial tasks from life, allowing us to focus on more important things. In the context of this paper we will look at automation in the realm of nuclear power, and the specific roles it played in the three major accidents in the history of the nuclear industry. We will look at where improvements were, or recommended for future builds. Additionally we will report how the industry is setting and achieving the goals of greater safety within the new generation of nuclear power.

Automation has led to cost savings and increased comfort, safety, quality control, efficiency, magnification and scale of work within the NPP Industry. On the other hand, this can also lead to skill loss, less human involvement, rigidity, a lack of trust in the system, added initial cost and accident due to loss of situational awareness. Plan and conduct automation well; benefits must outweigh the cons in order for automation to be worthwhile.

2. Automation

Plant personnel and research professionals have performed large amounts of research in the realm of automation [2, 14, 19, and 22] and specifically within the nuclear power domain [8, 12]. Based on this research, we can quantify levels of automation onto a scale of 1 to 10, where 10 is highly automated with no human interaction, and 1 is not automated and has no computer interaction. The safety systems in a nuclear power plant are autonomous, and require no human interaction, thus they are at level 10. Other systems are manual, and these will be level 1, however most systems fall somewhere between the two.

The automation in the case of a nuclear power plant however, is very interesting. Though a human must initiate this system, once the system has been initiated, the following steps are almost entirely automated in order to ensure quality. This is supervisory control. Consider the question: Is the level of automation is the proper balance between human and computers. The general trend is to simply add software, thus add automation, however, if your system is overly automated, then it will not allow for the flexibility that may be required in a high risk system, in a high risk scenario. Consider Three Mile Island, where the misunderstanding of a control room light caused the event. "If the operators had not intervened in that accident at Three Mile Island and shut off the pumps, the plant would have saved itself. They [the designers] had thought of absolutely everything except what would happen if the operators intervened. So the operators thought they were saving the plant by cutting off the emergency water when, in fact, they had just sealed its fate [16]". The operators did not fully understand the automation, and this led to the first nuclear accident in the United States.

It is important to consider also that we generally think of automation in relation to machines or technology. While this is indeed a case of automation to be reviewed, we must also consider the automation of the human. This is done through the use of procedures and rules. Procedures, as opposed to guidelines, restrict the human operator to performing certain predetermined tasks or actions. When they are not allowed to deviate from the procedures at hand, we have essentially taken the responsibility for response off of the operator, and placed it on the procedures.

The United States Nuclear industry is extremely regulated and proceduralized, leaving little to no decision making to people. The industry also tends to be highly regulated in terms of software and technology; thus highly automated in terms of machine automation as well. This leads us to question if machines and technology have the proper flexibility required to deal with incidents and accidents as they occur.

The problem with this comes into play when a specific procedure is not written for the context that the operator is facing. The thought is that rules and procedures reduce risk by placing restrictions on people's behavior which in turn prevents them from making mistakes. When people are not properly trained to respond to new events, or they do not do so regularly, they will not be able to under pressure, such as the events of Chernobyl. A highly technical system such as that of a NPP has exposure to influences which may end in catastrophe are beyond the control of the operators, designers or engineers. Due to the non-linear complexity of the system, procedures cannot be planned for every context that may occur. Too many procedures and too many rules can lead to catastrophe just as much as too little. This is the challenge in creating automation without human interaction.

2.1. Evolution of Automation

The evolution of automation is important to understand. Without a doubt, automation has assisted us in numerous ways, taking the mediocre, redundant tasks from the human and placing it on the more physically resilient machine. Rasmussen's human performance model, or skill, rules, knowledge (SRK) model discusses the different levels of human interaction with a system.

The skill level is a direct cause and effect from the environment. Rasmussen was able to successfully model this in the 1960's. It was done through mechanical engineering, electrical engineering and control theory.

The rules based behavior portion, which has situational awareness, and can perform tasks and procedures, was then automated in the 1980's through the use of operational research, optimization and expert systems.

The highest level of function is the knowledge based function, fully conscious and very cognitive; one must identify the situation, make decisions, and appropriately plan based on the environment. This is essentially logic, and remains as a task that is primarily in the realm of humans although this is challenged unsuccessfully in the 1980s through an attempt with Artificial Intelligence [14, 17].

In order to achieve knowledge based behavior, agents (such as machines or people) must reduce uncertainty, and plan while being flexible, and have control while being held accountable. Reducing uncertainty requires understanding the complexity fully, and thus the interactions of the system. All this, while still operating within the proper context of the operation.

The functionality in a nuclear power plant can be characterized in the same way as the SRK model. For example, in regular situations, procedures are used to operate the plant, this is the rules level. In an emergency situation however, it automatically defaults to the knowledge level.

2.2. Methodologies

One of the methodologies put in place for achieving appropriate automation was established by the Nuclear Regulatory Commission (NRC). These guidelines for the identification and allocation of functions within a nuclear power plant are:

- Identification of functions,
- Specification of functional requirements,

- Analysis of Function Allocation,
- Determination of human, computer or shared control (Automation),
- Design development and modification,
- Function verification [12]

Early approaches to functional allocation, that is to assign the role of functions to man or machine, looked at who might be better suited to perform the task. In Fitt's approach, humans are better at perceiving patterns, using flexible and improvised procedures, inductive reasoning and exercising of judgment and decision making. Machines are better at performing repetitive tasks, responding quickly, multi-tasking and performing complex calculations [6]. Further research into this matter has led to an understanding that we must have cooperative agreement between humans and machines [20]. In addition, these relationships and interactions are influenced by environmental and situational parameters that can be difficult to predict.

Another methodology of assigning automation is the level of human authority that is able to intervene. If the automation of the people and hardware are built into the system, which is to say that the operational system is fully automated without human intervention, then the authority has been placed on the designer alone. However, in a large complex project, the designer may not be able to foresee all situations and circumstances an operator may encounter, thus in the case of a nuclear power plant, we must place some of the authority on the operators. In the end, humans create the system, so they have the authority over the automation. This makes it important for system operators to be involved in the design process for automation.

2.3. General Challenges of Automation

It is a difficult balance to determine what technical functionality to automated, and what needs to be primarily controlled by people. The benefit of people is the logical processing capability and adaptability to situations which cannot occur within the programing of a computer. If you program the automation to respond to blue or red, it does not know how to respond to purple. However, if a strong procedures based organization is in place without the proper training of each individual, they may not know how to respond to purple either.

The literature outlines some of the challenges of automation as follows:

1. Agents must understand each other.
2. Agents must be mutually predictable.
3. Agents must be directable.
4. Agents must be able to learn from one another.
5. Agents must be able to trust each other.
6. Agents must understand situational context.
7. Agents must be able to communicate well.
8. Agents must be able to negotiate.
9. Agents must be able to collaborate.
10. Agents must be able to monitor each other [1, 5, 10, and 24].

Do note that agents can refer to human or machines, and they must work together collaboratively in order to perform the task optimally.

We have established that one of the primary challenges of the nuclear industry is that of automation; we have also seen the methodologies put in place that allow for planning of that automation. The benefits of automation can include reduced schedule, risk, cost and an increase in safety. On the other hand, automation can lead to a catastrophe if not done correctly.

2.4. Issues of Operational Automation

Three of the primary issues of automation within the realm of nuclear power, or any complex system can also be labeled as a:

1. Misunderstanding of automation
2. Mistrust of automation
3. Lack of appropriate automation

These can also be closely related to problems of maturity, competence and complacency, respectively.

One of the other issues that faces the industry from an operational standpoint is that of standardization. All plants are different, and even those which were identical upon build have had forty years to develop their own personalities, and cultures that contribute to the socio-technical system of the plants themselves. Due to the lack of standard system in place, often times they have naturally developed methodologies, techniques and mindsets that are specific to one plant, even one unit reactor at that plant. This is an additional consideration that must be taken into account when working specifically with a site, as they are each specific in their own way.

Though significant time and effort goes into these procedures, software and methodologies, they do not always work as we expect. It is impossible to fully remove uncertainty from a system, and without the flexibility to handle that uncertainty, accidents can happen. We can see this in the history of the industry's most infamous accidents, Three Mile Island, Chernobyl and Fukushima Daiichi.

3. Three Mile Island – Misunderstanding of Automation

Three Mile Island was the first core meltdown at a United States power plant, and the first time the nuclear industry truly felt vulnerable. The incident, occurring in 1979, exposed many weaknesses not only in the hardware itself, but also in the organizational structure, the regulatory commission and the government oversight. The accident at Three Mile Island (TMI) occurred as a result of a series of human, institutional, and mechanical failures [9]. A hardware failure, organizational factors and human error are the reasons Three Mile Island became a household name and ammunition for champions against nuclear power.

The plant had been running at 97 percent of capacity producing nearly nine hundred megawatts of electricity [21] when the Pressurized Water Reactor (PWR) pumps in the condensate polishing system tripped. Though the automatic systems properly shut down the plant within eight seconds, it was necessary to remove decay heat from the system. Generally a simple and automatic process, it had become greatly over-complicated when a Pilot-Operated-Relief-Valve (PORV) became jammed open.

The automation was in place. Additionally, the automatic system did its job correctly, so well in fact, that had the operators not been present, the accident never would have occurred [16]. The operators had knowingly and intentionally turned off the safety systems that would have saved the plant. The operators were highly trained, with navy backgrounds, and had worked together for years. They scored above average on NRC testing, and knew plant operating procedures well [7], and they knew how the plant behaved [9]. The accident occurred when they turned off the safety systems that were in place. To do this seems unreasonable; however, they did not understand the automation involved and as a result, turned off the system that would have avoided significant damage.

The PORV leaked small amounts of radioactive waste which led the operators to believe that the plant was not acting as the gauges told them it should be - performing to standards. The control room light led operators to believe that the PORV closed; changed their entire mental model of how the plant should behave. In actuality the light in the control room was simply an indicator that the electrical signal to close the valve was sent. The electrical signal was not an indicator if the valve was actually closed, or open. A very small misunderstanding of the function of this light led to a misunderstanding of the automation. This caused the operators to have incorrect situational awareness. This situational awareness led them to make all the decisions leading up to the accident.

In simulated training, which operators are often given situations where the pressure and temperature are dropping. They are also faced with situations where the pressure and temperature are rising. Due to the open PORV, they were just placed into a situation where the pressure was dropping and the temperature was rising. This was an event they did not understand, and had not been trained to handle.

The primary concern, in the early hours of the accident, was not a loss of coolant accident, nor was the meltdown of the core was also not the expected outcome. The operators were faced with the pressurizer of the system "going solid." The pressurizer in a nuclear power plant is intended to keep a certain level of water and a steam cushion is used to maintain the primary loop pressure going into the reactor. "Going solid" refers to when the pressurizer fills with water and means to control the pressure in the primary coolant loop is lost. This can also cause water to blow out of relief valves. In all the training and manuals, it is hammered into operators that "going solid" is to be avoided at all costs. The safety systems which had automatically activated were causing the pressurizers to approach a solid point.

The actions of turning off safety systems were reasonable considering the assumption that their control room indicators were telling them that "Going Solid" was imminent. This event is the perfect example of how a very small misunderstanding had momentous results, not only in the plant, but in the industry as a whole.

The situation at Three Mile Island was rooted in a general misunderstanding of the system's automation. This is an issue of maturity. Maturity is a state of being fully developed, and in the early stages of any system unexpected issues can arise. Modeling and testing are one of the ways we can help to improve maturity before a system is operational.

This is part of the problem of non-linear, complex, large scale, technological systems. They are both tightly coupled and complexly interactive [14] causing rigidity in process and systems, and the ability for small issues to turn into extremely large events. This is similar to the concepts presented in chaos theory, which tends to govern complex systems on a mathematical level.

4. Chernobyl – Mistrust of Automation

The well-known event that occurred at Chernobyl also changed the climate of the nuclear industry for the worse. In 1986, the Chernobyl Nuclear Power Plant in the Ukraine faced catastrophe following a series of significant human error, flawed design, operational oversight, and general lack of safety culture.

The root cause of the accident can be traced back to operational engineers, and operators who did not have a good understanding of the physics of nuclear power [18], and a management chain that did not fully believe in the automation of the systems. In order to perform testing to see if they could draw emergency power out of a powered down turbine, they had to terminate the emergency core cooling pumps, the local automatic control system and the emergency power reduction system. They did this without the proper approval of regulators or design engineers.

A nuclear power plant utilizes a nuclear core which creates heat to turn a turbine to be converted to electricity. Beyond the heat source and safety systems, it can be easily compared to the design of a coal-burning power plant. In this situation, an experiment was planned to see if the turbine generators could power the emergency coolant pumps in the event of an emergency shutdown. In order to do this, the emergency core cooling system had to be turned off.

The High Power Channel Type Reactor (RMBK) already had instabilities built in technically in that the void coefficient is positive. If left alone, a positive and exponential chain reaction will occur and heat makes the reaction get hotter. This implies that this design of reactor is inherently unstable[1]. One of the parameters of the test that was to be run that day, was that the plant had to be running 700 MW (thermal); however they were only able to achieve 200 MW (thermal) which is dangerously low for an already flawed reactor. The operators and engineers decided to press forward with the test regardless. Due to this lower power output, and the instability of the reactor, control of the chain reaction was lost. The power spiked uncontrollably, and the operators were unable to maintain core cooling. Without the ability to remove decay heat from the system, the core reached outputs of an estimated 33GW (thermal), ten times the normal output of the plant. The core melted, and the catastrophe continued as workers and the community attempted to contain the radioactive gasses that were burning in the atmosphere.

Many causes of Chernobyl have been debated, from operator error to flawed reactor design, but in the end it is a mixture of flawed technology, organizational and regulatory structures, and human factors.

This situation is seen as an example of distrusting automation. The organizational structure in place had allowed the operators and engineers to become complacent about safety through the lack of proper training and insufficient knowledge of the hardware, physics and procedures involved with the plant. The management who ordered the test did not fully understand why the safety systems were in place, and thus decided without the proper approvals that it was acceptable to remove them from the equation in order to achieve faster test results. They had a perceived illusion of invincibility and did not fully understand the risks involved. This raises the question, should operators be able to turn off the safety systems? Should this flexibility be allowed? Automation as simple as cruise control has led to car accidents, yet some automation, such as the automatic airbags of a vehicle has saved lives. This is part of balancing automation.

In both of these instances, Three Mile Island and Chernobyl the operators made a conscious decision to terminate the safety systems, but the primary difference is the timing in which the operators suppressed the safety systems. In the event of Three Mile Island, the operators were already significantly progressing towards catastrophe when the system led them to the incorrect conclusion. In the event of Chernobyl, the management felt as though the test they were performing was valid, and without trust in the automation, they did not believe that it was critical enough. Both of these instances were process failures.

Mistrust of automation can cause a lack of situational awareness in two ways:

- In the instance of Chernobyl it leads to a sense of invincibility, that nothing could go wrong
- Mistrusting the automation can also cause operators and users to perform the incorrect task as well, such as not trusting a system due to its propensity for false alarms.

[1] Russia is the only country with operational RMBK reactors, but they have seen safety improvements and retrofits since the events of Chernobyl, including precautions against unauthorized access to emergency safety systems.

5. Fukushima Daiichi – Lack of Appropriate Automation

The most recent nuclear accident occurred at the Fukushima Daiichi power plant following a 9.0 magnitude earthquake on the Richter scale which triggered tsunami waves reaching upwards of 40 meters in March of 2011. The earthquake was recorded as one of the five most powerful earthquakes since 1900 when record-keeping began. The plant was designed to withstand earthquakes and did so properly. The design basis for tsunamis was 5.7 meters; the plant was struck at the site with waves reaching 10 meters [23]. This incident has brought the general safety of the nuclear industry back into the spotlight.

Though the designers planned for both of these instances to occur, they did not plan for them to happen in conjunction, and certainly not in the magnitude that they did.

The plant consists of six nuclear reactors, of which number 4 was shut down for de-fuelling, and 5 and 6 were in cold shutdown for planned maintenance. 1, 2 and 3 were online and running at the time of the earthquake.

The plant's safety systems relied on external power from the grid in order to function. These were active safety systems – that is to say that they required power in order to properly function. When the earthquake took the plant offline, the three online reactors shut down as expected, and the redundant diesel generators started, as expected. However, these generators were located in the basement of the plant, and the designers did not anticipate the following flooding that took place. Once the generators had become flooded, the backup batteries initiated as intended, but lasted only hours. This was not enough to cool the plant to a complete safe shutdown phase.

There were numerous attempts to cool the core of units including the injection of seawater into the cores, but the efforts were not able to prevent complete meltdown in cores 1 through 3. This situation was further compounded by fires in the spent fuel ponds, where emergency cooling was also unavailable, and explosions occurred due to extreme pressures and temperatures in the main coolant loops.

Restoring cooling to the cores took months, with the final restoration occurring on August 26th, 2011.

In addition, not all safety shutdown systems (such as the cooling system, control rod operators, pressure controls or the spent fuel rod pond water level controls) were automated, and operators did not have trust in the reliability of the systems that were present [11]. Had these systems been passive and fully automated, the outcome would have been significantly different than the catastrophe in Japan. The automation in this situation was insufficient for the events that occurred.

The events in Japan have had immense worldwide effects on the nuclear community. Re-evaluation of plants has been communicated by government agencies and nuclear working groups such as the International Atomic Energy Agency. The United States, Germany and most of the world have taken significant measure to inspect all current operational plants for levels of risk, and the full extent of the damage to the plant, area and industry are still being evaluated at this time.

6. Conclusion

Within the realm of the nuclear power plant, automation helps to ease some of the burden on the operator during normal operations, and to assist him/her in the event of an emergency. Automation in such a complex system is undoubtedly invaluable. Automation is a delicate balance however, as too much automation would cause the operators to lose their skill, too little and the workloads placed on the operator would be extremely difficult to manage. Remember:

1. Software or hardware is automation of technology.
2. Procedures are merely automation of people.

There is a significant amount of research that has been done, and it continues in order for us to achieve the proper cooperation between human and machine. As the systems grow and become more complex, and thus generally more automated, the role of the human operator is changing. What was once control of a system is now beginning to transfer into the cognitive tasks of monitoring the system instead. This requires that the operator have a full and complete sense of situational awareness, and that the hardware and operator have a very good understanding of one another in order to achieve higher levels of safety.

In applying this research to the major accidents of the nuclear industry's history, we were able to define that three of the primary issues of automation are:

1. Misunderstanding of automation
2. Mistrust of automation
3. Lack of appropriate automation

Each of these can be further described by understanding flawed design, training or organizational processes. Instances where these issues have caused accidents can be found in Three Mile Island where the automation was misunderstood, Chernobyl where the automation was mistrusted, and in Fukushima Daiichi when the automation was insufficient and inappropriate for the location.

The balance of automation has been studied for decades, and we still have not yet achieved an ideal solution for allocation, authority and cooperative sharing. This topic is currently being researched at the Florida Institute of Technology, amongst other organizations.

7. Acknowledgements

I would like to thank my PhD advisor Guy Boy for the assistance and guidance he has provided, and also Don Platt, Cindy Schmitt, Lucas Stephane, Robert Weirs, Carol Craig and Patrick Millot for their support and comments.

References

[1] Bainbridge L. (1987) Ironies of automation: increasing levels of automation can increase, rather than decrease, the problems of supporting the human operator. In: Rasmussen J, Duncan K, Leplat J, eds. New Technology and Human Error. Chichester, UK: Wiley: pp 276 - 283.

[2] Billings, C. (1996). *Aviation Automation: The Search for a Human-Centered Approach.* Hillsdale, NJ: Lawrence Erlbaum Associates.

[3] Boy, G. (1998). *Cognitive Function Analysis.* London: Ablex Publishing Group.

[4] Boy, G. (2011). *The Handbook of Human-Machine Interaction: A Human-Centered Design Approach.* Surrey, UK: Ashgate Pub Co.

[5] Clarke K, Hardstone G, Rouncefield M, Sommerville I, (2006) eds. Trust in Technology: A Socio-Technical Perspective. Dordrecht, NL: Springer; 221 pages.

[6] Fitts, P. E. (1951). *Human Engineering for an Effective Air Navigation and Traffic Control System.* Washington, D.C.: National Research Council.

[7] Grey, M. (2003). *The Warning.* New York: W. W. Norton & Company .

[8] International Atomic Energy Association (IAEA). (1992). *The role of automation and humans in nuclear power plants.* Vienna, Austria: International Atomic Energy Association (IAEA).

[9] Kemeny, J. G. (1979). *Report of The Preseidents Commission on The Accident at Three Mile Island: The Need for Change, The* Legacy of TMI. Washington DC: The Commission.

[10] Klein G, Woods DD, Bradshaw JM, Hoffman RR, Feltovich PJ. (2004) Ten challenges for making automation a 'team player' in joint human-agent activity. IEEE Intelligent Systems;19(6):91 - 95.

[11] Liptak, B. (2011, March 18). Automation Could Have Prevented the Nuclear Accident in Japan. Retrieved July 14, 2011, from Bela G. Liptak, P.E.: http://belaliptakpe.com/blogs/automation-could-have-prevented-the-nuclear-accident-in-japan/

[12] Nuclear Regulatory Commission. (2004). *Human Factors Engineering Program Review Model.* Washington, DC: Nuclear Regulatory Commission.

[13] O'Hara, J. M., & Higgins, J. C. (2010). Human-System interfaces to automatic systems: Review guidance and technical bases. *Human Factors of advanced reactors (NRC JCN Y-6529) BNL Tech Report No BNL91017-2010.*

[14] Parasuraman, R., & Mouloua, M. (1996). *Automation and human performance: theory and applications.* Mahwah, NJ: Psychology Press.

[15] Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A Model for Types and Levels of Human Interaction with Automation. *IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems and Humans, Vol 30, No 3*, 286-297.

[16] PBS. (1999). Meltdown at Three Mile Island. Arlington, VA.

[17] Rasmussen, J. (1983). Skills, rules, knowledge; signals, signs and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man and Cybernetics, 13*(257-266).

[18] Rhodes, R. (1993). *Nuclear Renewal: Common Sense About Energy.* New York City: Viking Press

[19] Sheridan, T. B., & Verplank, W. L. (1978). *Human and Computer Control of Undersea Teleoperators.* Cambridge, MA: MIT Man-Machine Systems Labratory.

[20] Vanderhaegen, F., Crevits, I., Debernard, S., & Millot, P. (1994). Human-machine cooperation: Toward an activity regulation assistance for different air traffic control levels. *International Journal of Human-Computer Interaction, Vol 6, Issue 1*(pp. 65-104).

[21] Walker, J. S. (2004). *Three Mile Island: A Nuclear Crisis in Historical Perspective.* Berkley: The University of California Press.

[22] Wickens, C. D., Mayor, A., Parasuraman, R., & McGee, J. (1998). *The Future of Air Traffic Control: Human Operators and Automation.* Washington, DC: National Academy Press.

[23] World Nuclear News. (2011, March 20). *Stabilization at Fukushima Daiichi.* Retrieved July 25, 2011, from World Nuclear News: http://www.world-nuclear-news.org/RS_ Zuboff S. In the Age of the Smart Machine: the Future of Work and Power. New York, NY: Basic Books; 1988, 468 pages.Stabilisation_at_Fukushima_Daiichi_2003111.html

[24] Zuboff S.(1998) In the Age of the Smart Machine: the Future of Work and Power. New York, NY: Basic Books;, 468 pages.