CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331065

Situations Saved by the Human Operator when Automation Failed

Tomas O. Lackman*, Karl Söderlund

ÅF Infrastructure AB, Department of Risk Management, Frosundaleden 2, SE-169 99 Stockholm, Sweden
Tomas.Lackman@afconsult.com

In many systems an increased level of automation implies an altered role for the human operator. Behind the introduction of new automation lies different automation philosophies which stretches from trying to use as much automation as possible to adding automation only as a support to human tasks in specific situations.
The Swedish Radiation Safety Authority has assigned ÅF Infrastructure, Department of Risk Management to describe the current automation philosophies within the nuclear industry. The assignment also includes a survey of events in which human involvement was necessary in order to save situations in which the automation failed.
Much of the knowledge of human-machine interaction in process systems is derived by learning from incidents. These incidents, however, only represent a limited set of observations of real life human-machine interactions when the human in most cases did not have a positive effect on the sequence of events. Cases when the human operator did have a positive effect on the sequence of events are typically not reported as they in most cases do not lead to incidents. Thus, much of the available information on human-machine interactions is biased towards cases of human errors, and does not give a true picture of real-life. It is the hypothesis of this paper that the role of the human operator as a vital safety function is more significant than normally concluded by studying incident reports which claim human error as a contributing cause to accidents.
In this report two events are described in which human intervention was crucial for the successful outcome of the situation; Vandellos/Spain 1989 and Forsmark/Sweden 2006. These events show that the human operator is one of the most vital parts of the defence in depth at a power station, hence a strong focus should be given to looking after and maintaining the human abilities in order for her to be able to act safely in emergency situations.
The events also show the potential improvement of the defence in depth by making the most of the unique human abilities of intuitive and creative thinking and acting without access to external sources of power or prearranged procedures.
These abilities are, however, affected by the level of automation, e.g. a too high level of automation can lead to a lack in situation awareness whilst a too low level can lead to too high levels of mental workload for the operators. To avoid degradation in human abilities to safely intervene, changes in automation levels should always be preceded by an analysis of its long term effect on the human operators' skills and capabilities.
To gain more knowledge on the role of the human operator as a safety function in process systems, it is suggested that real-life human machine interaction is actively observed in order to also identify cases when human intervention prevents incidents at the very early stages of the sequence of events. These cases are normally impossible to retrieve from historical records, which mainly cover incident investigations of cases that lead to severe consequences.
Many of the theories on automation philosophy used in this paper originate from the aviation industry, but it is shown that they are equally applicable within other sectors as well, i.e. the process industry.

Please cite this article as: Lackman T. and Soderlund K., 2013, Situations saved by the human operator when automation failed, Chemical Engineering Transactions, 31, 385-390 DOI: 10.3303/CET1331065

1. Introduction

Since the beginning of the industrial revolution the level of automation has been continuously increasing. This implies an altered role for the human operator.
The selection of the functions to be performed by machine or the human operator can be made in different ways. Today cost, quality and time are strong drivers in most businesses. These three factors are also in many cases the underlying driving force behind the choice between automation and a human operator, e.g. by automating tasks previously performed by a human, it is possible to reduce personnel costs, increase quality and improve capacity.
In comparison with a computer, a human operator's ability to rapidly collect and process data is also limited. Muscle strength and speed of a human is limited in comparison with the machines. In addition to the incentives cost, time and quality, the choice of automation is also affected by factors such as health, safety and ergonomics.
Within businesses with a high risk, such as nuclear, aerospace and process industries, safety is superior to cost, time and quality. Thus, in these industries, the choice of whether a task should be performed by a human or machine also depends on which solution provides a minimal or at least acceptable risk.
The role of the human operator in functional safety has been studied by Fanelli (2010) and human control room actions in an emergency situation have been assessed by Nespoli and Ditali (2010). In this paper the current automation philosophies within the nuclear industry is described, and two events in which human involvement was necessary in order to save a situation when automation failed are presented. Which automation philosophy/level of automation that is most appropriate for obtaining a high level of safety is discussed.
The hypothesis of this paper is that the role of the human operator as a vital safety function is more significant than normally concluded by studying incident reports which claim human error as a contributing cause to accidents.

2. Current automation philosophies

In the nuclear industry the choice to automate a function rather to let a human operator do it is based on what is deemed to provide the highest safety. IAEA publishes requirements and general guidance on automation philosophy in IAEA (1999, 2000), which are mainly based on the findings in a Technical Document by IAEA (1992).
These requirements and guidelines are primarily focused on safety-critical functions. Operational functions, which are not significant to safety, are not regulated in the same manner.
The requirements can be summarized as follows:

- the plant must be user friendly, thus the consequences of possible human error must be limited.
- It also states that there should be a clear distinction between the functions to be performed by the human operator and the functions that must be handled by the automated system.
- People in the system have two roles: first, system manager, and second equipment operator. In the role of system manager, the human operator will get access to the information needed to supervise that automatic safety functions perform as expected. In the role of equipment operator, she will receive necessary information to initialize safety functions.
- A requirement on automatic safety systems is to handle foreseen scenarios on their own, without intervention from a human operator in the short term. The purpose of this is to create a respite for the human operator (30 min), and in this way avoid that the human operator jump to conclusion and make erroneous interventions.
- During the 30 min respite the operator shall nevertheless be able to follow actions and effects of the automatic safety functions.

The origins of the philosophy behind these requirements can be traced back to the incidents that have occurred in the industry, and the overall service experience from nuclear power plants worldwide. After the events at TMI and Chernobyl there has been a tendency to increase automation and to reduce the human operators' means to stop the automatic safety functions.
Another factor that has driven the automation is the development of technology. The original nuclear power plants were built with large safety margins and run with constant power (IAEA, 1999). These older plants have been modernized to deliver more power, and with greater opportunity to vary the power output. To achieve this, a greater degree of automation in control systems has been required.
Factors taken into account in allocating tasks to human or machine includes: existing procedures, experience feedback, requirements, feasibility, cost, technology, policy and social factors. One pitfall, noted by the authors of IAEA, in this allocation of tasks to human operators is that tasks could be allocated

to the human operators by convenience and economic reasons, where it is difficult to specify or automate a task.
Fitts list (Fitts, 1951) and the like indicate the strengths and weaknesses of human operators and machines.
The ability of the human operator is not static, however, but is influenced by the environment in which she operates and changes by experience and training. The choice of automation should therefore also consider how people's abilities are influenced by the chosen level of automation. Parasuraman et al (2000) has developed a system for describing the levels of automation in the division between man and machine. Whether a task is solved by a human or machine, any function is roughly divided into four steps:

1. Gathering information,
2. Analysis of the information;
3. Decisions and choices of action, and
4. Actuation

The level of automation in these tasks does not only influence man's ability to act independently, automation also affects the human operator's mental load, situational awareness, contentment and skills. Parasuraman mention some examples:

- In the first step of automation, information gathering, the human operators mental workload is positively affected by automation.
- Negative impact on mental load, for example, occurs if it is complicated to implement actions in the automated system, or if the automation requires that a human operator need to enter large amounts of data.
- The human situational awareness is adversely affected by highly automated systems.
- The degree of contentment is another human factor that is influenced by the degree of automation. If the human operator has over-confidence in automation, it may lead to that an error in the automatic system is missed.
- Finally, the human skills are adversely affected by a high level of automation. If tasks are automated the human capacity to perform these tasks slowly but surely erodes.

Most experiments performed to study the extent of how automation affects the human operator have been made in the aviation industry. However, a recently published article reports an experiment done in a nuclear simulators control room environment, Lin et al (2010).
The experiment involved 20 engineering students, who were divided into operator groups which then were assigned to perform a set of tasks at different levels of automation. A clear result from this experiment was that from a mental load-point-of-view, automation is beneficial to the human operators.
However, from a situational awareness-point-of-view the optimum level of automation is to force the operators to be involved in decision-making, as they in this way became more aware of what was going on and thus had a better situational awareness than if they were more passive - as in a fully automated system.
Sepp Moser, who is a flight specialist, supports the opinion that fully automated systems may have a negative impact on safety. In Swiss Engineering (2010) he describes the different automation philosophies at Boeing and Airbus, and how they affect the pilots. He presents a list of six serious incidents in aviation in 2009 where the control had a negative impact on the event, while the pilot tried to save the situation.
Reason (2008) have looked at the human's role as a saviour in dangerous situations from a broader perspective, not focusing on just automated systems. In his analysis, he has conducted a review of a large number of incidents where man has done what he calls a "heroic" rescue of a difficult situation. According to him, amongst others, situational awareness and decision making are of vital importance to our ability to rescue a situation.
Reason shows, that in some critical situations there is no time for rule-based and analytical thinking, but operators have to make rapid intuitive decisions, an ability which people has been equipped with from the evolution, and that "usually" is right. In cases where an operator is faced with an unprecedented situation, there might not be any rules available and the operator must rely on creative problem solving.
To study the automation philosophy in operation at Swedish nuclear power plants a study visit was conducted at a nuclear power plant in Sweden. Regarding safety features, most features, with few exceptions, are fully automated with no possibility for human operator intervention. For example, the safety function to isolate a reactor by closing valves is almost fully automated. The operator has some ability to intervene, but only if certain conditions in the measurements of the sensors are met.
Regarding the functions necessary for the operation of the plant, not safety critical, the approach towards automation has been conservative, and not to automate unnecessarily.

The philosophy behind this approach is to avoid the risk that the operators are too passive, and thus lose in situational awareness and put too much trust in automation. Some functions such as when a turbine is started, contains many tasks and large amounts of information, which gives an excessive mental load of the operators. In such cases, it was decided to automate simply because it works much better.

3. Situations saved by the human operator

Here follow two events from the nuclear industry where operators had opportunity to take control and save the situation when the automatic system failed. The choice of these two events was made as they describe human operator interventions that had a significant positive effect on the sequence of events.

3.1 Vandellos, Spain 1989

Vandellos 1 was a carbon dioxide cooled and graphite-moderated reactor of 545 MWe. The station was equipped with two turbine units with hydrogen-cooled generators. The following description of the event at Vandellos is a summary made from the training material for the simulator instructors at KSU Vattenfall (2010).

On the 19th of October 1989 the station produced 400 MWe, with stable operating parameters. At 21:39 indicators on the instrument monitors showed that turbine vibrations were off the scale. The moment after a massive explosion was heard and the floor of the control room shook. From the control room, the operators could see high flames sweep over the turbine unit.

The reactor stopped automatically. The explosion was a result of a turbine failure caused by vibrations. These vibrations sheared down the pipes to the turbine lubricating oil, which rapidly ignited. They also caused damage to the generator, which meant that hydrogen leaked out and exploded. The explosive fire melted the stations piping for compressed air and most of the valves had to be operated manually as they were air-driven. The fire also destroyed all the electrical cables in the affected areas. In addition, since a door had been left open large amounts of sea water from the turbine cooling system leaked into the reactor building, and caused a flood.

All in all the damaged air pipes, the damage to the electrical system and the flooding led to that

- Circulating fans stopped,
- Secondary water pumps were destroyed,
- Level control in the feed water tanks to the cooling system was not working,
- Internal communication system was destroyed,
- Lights around the turbines went out

Carbon dioxide pressure in the primary system rose to 0.4 bar below the value where a large loss of coolant could have occurred. The temperature rose simultaneously to only 5 °C below the value which when total loss of cooling could occur.

In the control room efforts concentrated on keep the two remaining main circulation fans operating. Since each pneumatic valve was fitted with a steering wheel for manual operation, there were several manual adjustments due to the failure of the automatic system. In doing so, next day the heat removal system was restored. Hence the core and block parameters stabilized to normal levels.

3.2 Forsmark, Sweden 2006

The incident at Forsmark, Sweden, 2006 is described in two reports from Forsmarks Kraftgrupp AB (2006a, b).

Forsmark 1 is a boiling water reactor with two turbine units, which at the time of the event delivered a full capacity of 990 MW. Tuesday, 25 July, at 13.20 there was a disturbance that originated in a short circuit in the 400 kV switch outside the Forsmark plant. This short circuit generated a strong current transient which caused major damage to the control system power supply, and thus the possibility of automation maintaining control over the reactor.

The first thing that happened at the disturbance was that a reactor shut-down system was initiated automatically. The sharp current transient had, however, knocked out several of the UPS (Un-Interrupted Power Supply) units which led to that two of the four diesel generator engines could not be started automatically. In addition, the power disruption also resulted in that signals from sensors on the reactor did not reach the operators in the control room, and among other things, they could not see the mode of the control rods.

This lack of information created an uncertainty about whether the automatic shut-down system would work as intended. After 22 min of disconnected power from the two disconnected diesel units, they were finally connected manually, and thus it was possible to regain power to the instruments, verify the control rod

position and continue the automatic shut-down sequence. In the investigation after the event it was concluded that:

- Both the power-up and other remedial measures were at the current situation dependent on operator intervention because the automatic system did not work.
- If all four sub-systems had been de-energized and no operator intervention made within eight hours, most likely a meltdown would have occurred.

4. Discussion

As the events above indicate, it is not yet possible to completely discount the humans. Events that are outside the scope of the control system have happened and will happen. In these cases, we will be dependent on the human operators' ability to save the situation. While we build as safe systems as possible, we need to keep in mind the ways in which these safe systems affect people's ability to rescue the situations that we do not anticipate or at least lie outside the scope of automation. The events at Vandellos and Forsmark show that man is one of the most vital safety functions in the defence in depth, and that it must be great emphasis on sustaining the ability of the human operator to rescue situations when the automatic system does not function.

According to Reason (2008), one of the success factors for a human to rescue a situation is situational awareness. In order to facilitate a high situational awareness it is important that the degree of automation is designed with this in mind. Lin et al (2010) have shown that situation awareness is adversely affected by automated decision making, especially if the operator is completely disconnected from both the analysis of the data and execution of the task. Lin's tests also showed that low level of automation can decrease the situational awareness because the operator in that case would probably be too busy with multiple tasks to have sufficient time to pause and reflect on the situation.

At an optimum level of automation operators are involved in decision making, while the actuation of tasks to a greater extent may be allocated to automation.

In the studied events there has also been an opportunity for the human to intervene when the automatic system did not function or was not available due to a failure of power supply such as electricity or compressed air. Thus, it should be pursued that man always has an opportunity to intervene in cases where the automatic system fails. The human operator should be equipped with flashlights, portable fire extinguishers, automatic valves with manual functions etc.

The level of automation in the industry has so far been decided by technology available and the experience from the serious incidents that has occurred in the past. This has resulted in that several systems today is fully automated for safety and operational reasons.

To avoid unnecessary erosion of human capacity to intervene in a situation when the automatic system does not work as intended, it is recommended that further changes in the level of automation shall be accompanied by an analysis of the long-term effect on the human operator's skills. In cases where a function must be fully automated, simulator training should be used to offset the negative impact that complete automation has on operator situational awareness and operator contentment.

Accidents consist of both latent and immediate causes, and follow a sequence of events where the human operator intervenes with the sequence of events at several stages.

The intervention of the human operators in the studied cases in this paper occur late in the sequence of events and could be considered as mitigating actions, rather than preventing actions. This is due to the fact, that it has been very difficult to retrieve documented historical records of human interventions that have prevented incidents – as these cases are not normally reported. Nevertheless, during the course of this project many "stories" from experienced people in the process industry has been told about human interventions which prevented incidents at a very start of a possible sequence of events.

To gain more knowledge on the role of the human operator as a safety function in process systems, it is suggested that real-life human machine interaction is actively observed in order to also identify cases when human intervention prevents incidents at the very early stages of the sequence of events, as in Skybrary (2010). These cases are normally impossible to retrieve from historical records, which mainly cover incident investigations of cases that lead to severe consequences.

By collecting less biased information on real-life human machine interaction the knowledge and recommendations regarding automation philosophy, hence safety, could be improved.

References

Fanelli P., 2010, Human Factor in Funcional Safety, Chemical Engineering Transactions, 19, 213-218, DOI: 10.3303/CET1019035

Fitts, P.M. (Ed), 1951, Human Engineering for an Effective Air Navigation and Control System, the Nuclear Regulatory Commission, Washington DC, USA

Forsmarks Kraftgrupp AB, 2006a, "Experience Report for the situation in the control room during the disturbance on 25/7 2006 "F1-2006-0703, Forsmark, Sweden

Forsmarks Kraftgrupp AB, 2006b, "Forsmark 1 - Noise Analysis - Loss of 400 kV and loss of diesel starter in the A-and B-sub 'F1 2006-0699, Forsmark, Sweden

Forsmarks Kraftgrupp AB, 2007, Analysis Background "Forsmark incident July 25, 2006" Issue 5, December 2006, year 19, Revised March (2007), Forsmark, Sweden

IAEA (International Atomic Energy Agency), 2000, IAEA Safety Standards Series, "Safety of Nuclear Power Plants: Design" Requirements No. NS-R 1

IAEA (International Atomic Energy Agency), 1999, IAEA Technical Reports Series No. 387, "Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook

IAEA (International Atomic Energy Agency), 1992, TECDOC-668, 1992, "The Role of automation and humans in Nuclear Power Plants "

KSU (Vattenfalls simulator training center), 2010, Description of Vandellos event in training material.

Lin, CJ, Yenn, TC, Yang, CW, 2010, "Design Automation in advanced control rooms of the modernized nuclear power plants ", Safety Science 48, pp 63-71

Moser, S., 2010, "Automatisierung für der oder Menschen gegen" in Swiss Engineering, http://www.sepp-moser.ch/docs/stz_automatisierung.pdf accessed 28.08.2012

Nespoli C., Ditali S., 2010, Human Error Probability Estimation for Process Risk Assessment with emphasis on Control Room Operations, Chemical Engineering Transactions, 19, 219-224, DOI: 10.3303/CET1019036

Parasuraman, R., Sheridan, T.B. and Wickens C.D., 2000, "A Model for Types and Levels of Human Interaction with Automation, "in IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems and Humans, Vol. 30, No. Third, pp. 286-297

Reason J., 2008, "The Human Contribution - Unsafe Acts, Accidents and Heroic recoveries ", Ashgate

SKYbrary, 2010, Article on Normal Operations Safety Survey (NOSS), www.skybrary.aero/index.php/Normal_Operations_Safety_Survey_(NOSS) accessed 01.01.2011