Why is the recent ESSO fire investigation important for ergonomics ?

OVV report – Fire ExxonMobil in 2017

The Dutch Safety Board (OVV) recently published the results of an investigation into the fire at the ExxonMobil Refinery in Rotterdam. On August 21, 2017, after a chain of unplanned events, a fire started in a furnace of the Powerformer. The incident and the underlying causes are described in the OVV report. The general conclusion was, that "the design of the installation was not inherently safe".

One cause stands out: a flood of priority 1 and priority 2 alarms, up to a multiple of the number that is generally accepted in the process industry as a maximum for off-normal situations (see EEMUA publication 191 "Alarm systems"). Related to this, an inadequate overview of the process (process conditions) during the restart of the process units was also mentioned.

The goal of the Dutch Safety Board is "learning lessons from accidents". The Board did not consider "Human Factors" or "Ergonomics". However, for Human Factors Professionals in process industries, it will be clear that the analysis of this incident could teach us a lot about:

- Design of the process control system,
- Alarm management,
- Process information presentation
- Decision support systems.
- Human (operator) behavior.

This is a call to start learning lessons on the human factors of the 2017 ExxonMobil Rotterdam Refinery Fire Incident.

Background

As a Human Factors Engineer, I am well acquainted with the process industry, process control, and relevant standards and guidelines (ISO 11064, ISA.101.01, EEMUA 191 & 201). My first control room design project was at the Esso Refinery Rotterdam (Flexicoker project; 1985). I was "lucky" to observe operator actions during a fire. At the time, we learned a great deal from this incident. I am convinced that this is also possible in 2019 and should actually be following the fire at Esso. See my first attempt below.

Fire in furnace F1001 – Events

On 21 August 2017, a fire started in the F1001 furnace of the Powerformer factory (PWF) at 9.30 pm as a result of a split tube. About two hours earlier, a large compressor had failed, which subsequently led to a "trip" of all 6 PWF furnaces (automatic shutdown). The events are described minute by minute in the public ExxonMobil report on the fire. Summarizing:

1. A short circuit occurred in the power cable of compressor C5201B at 7.30 pm. Due to a voltage dip, the fan of the Waste Heat Boiler (WHB) also fails. This opens the automatic safety valves to the stack. Gas no longer passes through the steam generator, but through the stack.
   The operators could not find a probable cause for the safety valves to open.
2. Because the cause for the trip could not be identified immediately, the operator tried to close the safety valves and succeeds at 7.46 pm. However, as a result the pressure in the PWF's waste gas system increases, subsequently leading to an ESD (Emergency Shut Down or “Trip”) of all 6 PWF furnaces.
3. Now, the panel operator calls in the shift team lead (STL) and after consultation it is decided to restart the furnaces, to prevent the PWF from shutting down completely. The STL stays to assist at the console, taking care of other units.
4. 7.50 pm restart of 3 furnaces; 2 furnaces (including F1001) will follow at 8.09 and the 6th furnace at 8.18.
5. Apparently, so far everything goes well, until a warning (priority 2) for thermal overload occurred on feed pump P1003B of F1001 occurs (at 8.15 pm). The spare pump (P1003A) is under maintenance; however, the panel operator was not aware of this.
6. At 8.25 pm pump P1003B trips because of thermal overload. Then a priority 1 "low flow" alarm on the feed to the F1001 comes up, and F1001 trips. Nevertheless, the team wants to restart this furnace.
7. The restart of F1001 cannot proceed due to the activated low-flow protection. This protection is manually bypassed at 8.29 pm on the local control panel.
8. At 8.30 pm the restart succeeds. Alarms are acknowledged; and finally, the SG502 steam generator is running.

We did it! WHB is running again, the furnaces are running, etc. However, 50 minutes later, at 9.22 pm, a fire is detected. The furnace F1001, followed by the PWF are being shut down.

Alarms
ExxonMobil emphasizes in her report, that starting up the PWF furnaces is very complex and requires thorough preparation. Nevertheless, the operators have decided to restart the furnaces. From an human factors point of view, several comments can be made.

- During the restart period, on average there were 250 alarms per 10 minutes interval. Peaks of >60 Priority 1 alarms have occurred per 10 minutes interval. The failure of the feed pump P1003B has been overlooked (perhaps because it was a Priority 2 warning), or because the operator saw no problem here, assuming that pump P1003A would automatically take over.

- An overview of alarms prior to the incident, shows some remarkable information. It seems that Trips, as well as important alarms, are both labelled Priority 1. Also, there is a trip (pump P1003B), labelled a priority 2 alarm. This is evidence, that the refinery didn't have a clear alarm philosophy in place. A high priority alarm means, that the operator has limited time to take measures to avoid a serious problem ("limited time", "serious", to be specified in the philosophy). Once, a trip occurs, there is nothing for the operator to do to prevent this event from happening. It is only a message. Of course, the operator needs to take other actions, possibly guided by his process information graphics and an alarm/off-normal messaging system. Unfortunately, this topic is not addressed in the Dutch Safety Board report.

- According to the ExxonMobil report, the operators assumed that the flow meters were malfunctioning. The cause of the F1001 trip may not have been investigated by the shift team due to this assumption. This raises several human factors questions or issues:
  - Why was it assumed that the flow meters were unreliable? Had this alarm occurred incorrectly more often in the preceding weeks?
  - Was there nowhere visible that the P1003A pump was in maintenance?
  - The number of alarms are much larger than any standard or guideline in this area indicates as a maximum. It exceeded by far the ability of the operator to respond adequately. It is almost inevitable that something will be missed; a conclusion endorsed by the OVV. Could this alarm flood have been foreseeable, for example on the basis of systematic scenario analyses?
  - What does the alarms display look like? In practice ergonomists come across unclear and illegible presentation formats. Also, operators may have different sources for alarm information: for example a dedicated alarm display, or symbols in process graphics (like a red flashing pump symbol).
  - The OVV report emphasizes that the operators did not have a complete overview of the complexity of the restart of the furnaces. Could a good (improved) process information presentation have provided support in this case?
  - The Shift Team Lead starts assisting the panel operator at a certain moment in time. But, as the ExxonMobil report states, he was unable to keep an overview during the restart because he had to keep an eye on the other units at this console. But how can you lose the overview? A console is exactly the place where all process information is or should be clearly available and from which all communication can be followed. What about process overview displays?

Procedures
ExxonMobil writes critically about its procedures and the extent to which they have been followed. After all, the procedures immediately would have led to a PWF shut down. But the operators decided otherwise. How did that happen?
Operator behavior is an important human factor. A shut down has (major) economic consequences. From our own experience we know that operators usually are proud to be able to keep a plant running. Why did they restart? Was there an "overestimation of own capacities". It was impossible to apply procedures quickly enough. And why didn't the team trust a Priority 1 alarm of a flow measurement? Unfortunately, these human factors have not been considered in public reports and the OVV research.

Conclusion
Although we volunteered, we did not get an opportunity to participate in the 2017 fire investigation either at ExxonMobil or the OVV. Being familiar with process industries and with the ExxonMobil Refinery, we have made (presumably reasonable) assumptions on what happened, based on the public documents. The reports on this are clear and easy to read. We can learn a lot from them. Digging deeper may be considered, as a number of "human factors" apparently remain underexposed.

For example, alarm management is still a major challenge (worldwide). Anyone who deals with this topic must take notice of the ExxonMobil case. Unfortunately the OVV report was published in Dutch only.
The same applies to the topic of "process overview". Are current views on a good design of process information displays of complex processes (such as presented in the ISA101.01 standard, or Hollifields' High Performance HMI) good enough?
And finally "human behavior": did the procedures fit human behavior, i.e. or didn't automation support the operator sufficiently?

ErgoS Human Factors Engineering calls on ExxonMobil, the Dutch Safety Board, process industries, suppliers of process control systems and software, and others stakeholders to extend their considerations towards the field of ergonomics: the human factor. Any initiative in this area would be most welcome and can be send to the authors of this paper.

Ruud Pikaar Eur.Erg. & Niels de Groot
Senior Human Factors Engineers
e-mail: contact@ergos.nl

Public reports Esso fire

- Report Investigation fire stove F1001 (Public version, ExxonMobil reference 17-RBS-3060, December 2017).
- DCMR and Zuid-Holland Province Reports on the fire
- OVV report: Fire at Esso, August 21, 2017 (published July 2019).

Guidelines and standards

- EEMUA publication 191 (2013) – Alarm systems – a guide to design, management and procurement.
- EEMUA publication 201 (2019)- Process plant control desks utilising human-computer interfaces: a guide to design operational and human-computer interface issues.
- ISO 11064 – Ergonomic design of control centres (multi part standard)
- ISA 101.01 (2015) – Human Machine Interfaces for Process Automation Systems.

Literature

- Hollifield, B et.al (2008) – The High Performance HMI Handbook

- Pikaar, RN (2012) – HMI Conventions for process control graphics. In: IEA World Congress, Recife.
- Pikaar RN, De Groot N, Mulder E, Remijn SLM (2016) - Human Factors in Control Room Design & Effective Operator Participation. In: Proceedings SPE Intelligent Energy International Conference and Exhibition (2016) Aberdeen, Society of Petroleum Engineers.
- Pikaar RN, Thomassen PAJ, Degeling P, VanAndel H (1990) Ergonomics in control room design. Ergonomics 33, no 4, 589-600. (verslag van het ESSO Flexicoker project).