Case Study 1: STAMP Analysis

Chris Johnson,
Dept. of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson

1. Introduction

This case study is intended to provide some first hand experience in using the STAMP technique to analyse a computer-related failure. The incident also involves a number of managerial and human factors issues. These aspects are addressed by the STAMP technique. However, there are some concerns about the adequacy of their representation. It should not, therefore, be surprising if you find some problems in applying the technique or if you feel that the approach fails to capture important elements of this incident. A secondary aim of this exercise is to generate discussion about possible improvements to the STAMP technique.

2. Case Study

The Case Study is based upon an accident that was reported to the US Dept. of Labor, Mine Safety and Health Administration (see http://www.msha.gov/fatals/2002/ftl02m34.htm). For this exercise, a number of simplifying assumptions have been made and identifying details have been removed. The level of detail is, however, consistent with that available to the investigators in the aftermath of the incident.

2.1 Sequence of Events

Limestone was being mined using bulldozers. The material was transported to a primary crusher, and then conveyed for processing into Portland cement. The finished product was sold for use in the construction industry. The processing relied on kilns that were powered by coal and natural gas, supplemented by liquid waste fuel. The waste fuel was a mixture of various organic solvents and other petroleum by-products. The company began utilizing liquid waste fuel in 1995 because of its high energy output and relatively low cost. This fuel was delivered to the plant in bulk via tanker trucks or railcars, and pumped into large storage tanks in the area of the plant near where the accident occurred.

On the day of the accident, the victim A reported for work at 7 a.m., his normal starting time. After a short meeting with his, supervisor, A was assigned to operate a front end loader. At about 12:45 p.m., the supervisor informed A of a decision to shut down the north waste fuel system due to elevated temperatures at the north pump seal. He directed A to switch the pumps delivering waste fuel to the kiln from the north system to the south system, which had been idle for 3 days due to a bad seal. At about 12:46 p.m., A went to the containment area where the pumps were located and began checking valves to see if they were positioned correctly to make the switch. He then shut down the north system pumps and started the south system pumps at about 12:48 p.m.

The kiln control operator, was located in the control room of the plant, monitoring the fuel system through fuel line sensors. She radioed the supervisor, who was in the containment area with A, and advised fuel was not getting to the kilns. Believing the cause of the problem was air in the system, the supervisor began bleeding air from valves installed in the waste fuel piping system

while A bled air at the pumps. A then radioed the kiln control operator to determine if fuel had begun flowing to the kilns and was told it had not. The supervisor left the area for a few moments to get a rubber drain hose. When the supervisor returned, he began bleeding the valve at the south pump while A was checking the other valves to see if they were in the open position.

At about 12:58 p.m., the supervisor observed that the pipe entering the south grinder began to vibrate. The grinder exploded and was propelled off its base. Fuel sprayed from the grinder base covering A and the supervisor. The fuel ignited and fire spread over the entire area. The supervisor's clothes caught fire. He ran outside where he extinguished himself. When A exited the containment area, the supervisor used a fire extinguisher on A's burning clothing. The kiln control operator saw the fire from the control room and radioed for help. The control room supervisor activated the manual emergency shut down on the pumps, and called 911 for assistance.

2.2 Additional Information

The switchover from the north to the south fuel system required air to be bled from the system on start-up. Air in the system caused low pressure in the fuel line in the kiln area. It was customary to bleed the air before starting the pumps. On one previous occasion, the fuel handlers bled air from the lines while the pumps were operating, as the victim and his supervisor did just prior to the accident. The pump manufacturer recommended strongly against bleeding air while the pumps operated because it could place undue strain on the components of the system. This procedure caused the fuel pipe, between the grinder and the pumps, to vibrate violently just prior to the explosion. The lack of flow in the fuel line following start-up was due to some type of blockage, either a clog or a closed valve. Just prior to the accident, the blockage was abruptly removed, and the pumps immediately elevated the pressure in the system. As the pumps reached their maximum speed, a "water hammer effect" caused an instantaneous over-pressurization to occur in the south pump system, converging at the grinder. Under this extreme pressure, the grinder was torn loose from its base. The 480-volt power cable was pulled loose from the grinder motor. The exposed electrical conductors sparking into the surrounding airborne fuel created the ignition source of the fuel fire and explosion.

The control room monitored the north and south fuel systems using sensors that activated alarms and displayed warnings on monitors when specific set points for temperature or pressure were exceeded. Three pressure sensors were installed on the fuel line: one in the kiln area of the plant, and one each on the north system and south system just prior to the point where the two system lines merged into a single line leading to the plant. No alarms were installed in the waste fuel containment area where valve adjustments on the systems were done manually when necessary. If an alarm sounded or a warning was displayed, the control room operator used two-way radios to communicate with personnel at other areas. Two independent but interconnected programmable systems monitored and controlled both the north and south fuel delivery systems. The Intelligent Automation, Distribution Control System (IADCS) was used to monitor and record normal operating parameters (temperatures, pressures, etc.) as well as audible and visual alarms. These could be viewed on displays at the plant control room. A PLC (Programmable Logic Controller) network performed the basic start-up/shutdown of the system and responded to electronic commands from the IADCS. The IADCS recorded information it sensed, but it did not record the PLC's actions.

One of the commands that the IADCS was programmed to send to the PLC was to de-energize all pumps in the fuel delivery system if a pressure of approximately 60 PSI was not sensed at the line in the kiln floor area within 3 minutes of system start-up. The 3-minute set point was based on a normal delay of 3 minutes for pressure to reach approximately 60 PSI at the kiln area from the

time the pumps were started. The accident occurred 10 minutes after the pumps started. When no pressure was detected in the line at the kiln area, the IADCS functioned properly in signalling the PLC to shut down the pumps 7 minutes before the accident, but the PLC did not respond. Three months prior to the accident, an older PLC system was replaced by a new PLC, and the IADCS connections to the older PLC system were never changed over to the new PLC. A test of the fuel pump automatic shutoff functions was scheduled 3 days prior to the accident, but was aborted when the south pump grinder motor failed, and the test was never rescheduled.

The victim had not received specific training regarding safe work procedures and the specific hazards associated with the task that he was assigned to perform. The victim and his supervisor had not been trained regarding the manufacturer's warning to not bleed the lines of air while the pumps were operating. Both had attended a training class on waste fuel system operation taught by Ash Grove Cement, but this procedure was not included in the training subject materials. Likewise, neither the supervisor nor any of the fuel handlers had been trained to recognize that the pumps should shut down automatically (as a result of the electronic sensor system) 3 minutes after they were started if insufficient pressure was detected in the line.

3. Your Task…

Your task is to work in groups of three or four to conduct a STAMP analysis of the incident described above. The first step is to construct a high-level control model. Figure 1 illustrates the initial template that is given in the STAMP papers. In practice, however, things are seldom this 'clean'. There will be multiple control relationships between operators and management.

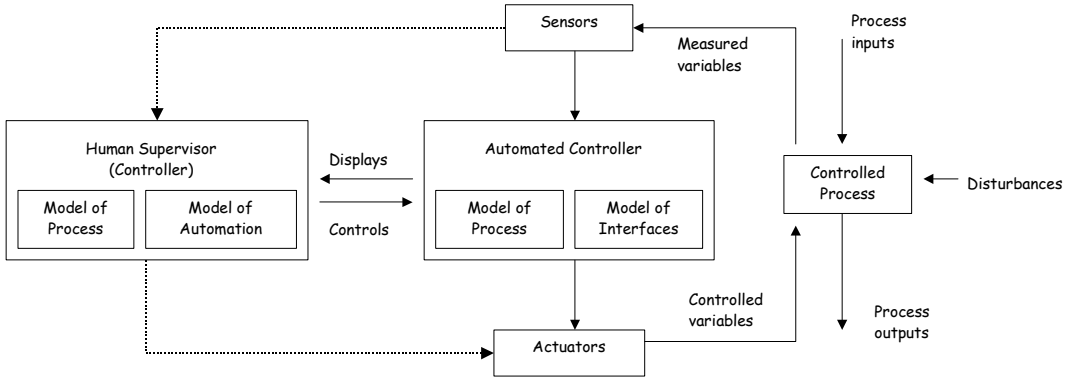

Figure 1: High-Level Model of Control

In this incident we know very little about the role of the State and Federal regulators. We are also told relatively little about the company management structure. If your group would like to include them in the analysis then they should be incorporated into the control model with a suitable annotation to indicate that further analysis is required. An important role of many causal analysis techniques is to help identify areas for further analysis and the elicitation of additional information.

There is not enough time to derive a perfect 'control model'. It can take 1-2 days to achieve consensus in a team on an incident of this complexity. I would develop an initial model that captures the relationship between the programmable systems, the fuel delivery application and the operators. I would also include management as indicated in the previous paragraph. The second stage of the analysis is then to identify flaws in the control relationships that led to the incident. Table 1 illustrates the control flaws that have initially been identified in the STAMP approach.

1. Inadequate Enforcements of Constraints (Control Actions)
- 1.1 Unidentified hazards
- 1.2 Inappropriate, ineffective or missing control actions for identified hazards
- 1.2.1 Design of control algorithm (process) does not enforce constraints
- Flaws in creation process
- Process changes without appropriate change in control algorithm (asynchronous evolution)
- Incorrect modification or adaptation.
- 1.2.2 Process models inconsistent, incomplete or incorrect (lack of linkup)
- Flaws in creation process
- Flaws in updating process (asynchronous evolution)
- Time lags and measurement inaccuracies not accounted for
- 1.2.3 Inadequate coordination among controllers and decision makers

2 Inadequate Execution of Control Action
- 2.1 Communication flaw
- 2.2 Inadequate actuator operation
- 2.3 Time lag

3. Inadequate or Missing Feedback
- 3.1 Not provided in system design
- 3.2 Communication flow
- 3.3 Time lag
- 3.4 Inadequate sensor operation (incorrect or no information provided)

Table 1: Control Flaws Leading to Hazards

As with the control model, there is insufficient time to perform an exhaustive analysis. I have never conducted an exhaustive analysis even in relatively serious commercial investigations. There is not enough time. Given such constraints, it is important that you identify what you consider to be key control relationships before conducting this analysis. After you have identified the key control relationships, you should try to develop a form similar to that illustrated in Table 2. This is intended to capture both the constraint violation and your potential recommendation for subsequent intervention. Each member of the team might complete their own form and compare them with those of their co-workers.

Control Relationship	Constraint violation	Justification	Recommendation
[Offsite managers-> Site managers-> Operators]	1.1 Process models inconsistent, incomplete or incorrect (lack of linkup)	Failure to realize that additional operator training and simulations would be required to prepare change over from reclamation configuration to initiation of high-capacity discharge pumps.	Need to review operational risk assessment for operator tasks following plant modification.

Table 2: STAMP Causal Analysis Summary

4. Wrap Up

This case study is intended to provide first-hand experience of the STAMP technique. You should see the strengths of the approach. It avoids focussing on immediate events and looks at control relationships. There are also limitations. For example, I think that the control flaws in Table 1 could and will be revised as greater experience is gained in the engineering application of the approach.