Case Study 2: PARCEL 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 PARCEL technique to analyse a computer-related failure. PARCEL consists of two different approaches. The first relies upon a simple flow-chart to identify causal factors. This is appropriate for relatively simple mishaps. The second approach relies on more formal modelling using the ECF techniques introduced in the presentation. You should feel free to use either technique. PARECL, like STAMP, is a relatively new approach. A secondary aim of this exercise is, therefore, to generate discussion about possible improvements to these techniques.

2. Case Study

The Case Study is based on a mishaps that was investigated by the US General Accounting Office (see http://161.203.16.4/t2pbat6/145960.pdf). For this exercise, a number of simplifying assumptions have been made. However, this incident is typical of many similar failures involving military systems.

2.1 Background

On February 25, 1991, a Patriot missile defence system operating at Dhahran, Saudi Arabia, during Operation Desert Storm failed to track an incoming Scud. This Scud subsequently hit an Army barracks, killing 28 people. The Patriot is an Army surface-to-air, mobile, air defense missile system. It was originally designed to operate in Europe against Soviet medium- to high-altitude aircraft and cruise missiles travelling at up to MACH 2 (1500 mph). To avoid detection it was designed to be mobile and operate for only a few hours at one location. The Patriot operates as part of a battalion usually composed of six batteries. Each battery is made up of one ground-based radar unit for surveillance and target detection, tracking, and engagement; an Engagement Control Station for manual or automated command and control of the missile interceptors; eight missile launchers; and a Communications Relay Group for communications support. An Information Coordination Center controls the batteries and coordinates their operation with other battalions and higher-level Command.

The Patriot’s weapons control computer performs the major functions for tracking and intercepting a target, as well as other battle management, command and control functions. The control computer used in Operation Desert Storm is based on a 1970s design with relatively limited capability to perform high precision calculations. To carry out its mission, the Patriot's weapons control computer obtains target information from the system's radar. The Patriot's radar sends out electronic pulses that scan the air space above it. When the pulses hit a target they are reflected back to the radar system and shown as an object (or plot) on the Patriot's display screens. Patriot operators use the software to instruct the system to intercept certain types of objects such as planes, cruise missiles, or tactical ballistic missiles (such as Scuds). During Desert Storm the Patriot was instructed to intercept tactical ballistic missiles. For the Patriot's computer to identify, track, and intercept these missiles, important information describing them was kept by

the system's range-gate algorithm. After the Patriot's radar detects an airborne object that has the characteristics of a Scud, the range gate--an electronic detection device within the radar system--calculates an area in the air space where the system should next look for it. The range gate filters out information about airborne objects outside its calculated area and only processes the information needed for tracking, targeting, and intercepting Scuds. Finding an object within the calculated range gate area confirms that it is a Scud missile.

The range gate's prediction of where the target will next appear is a function of the target's known velocity and the time of the last radar detection. Velocity is a real number that can be expressed as a whole number and a decimal (e.g., 3750.2563...miles per hour). Time is kept continuously by the system's internal clock in tenths of seconds but is expressed as an integer or whole number (e.g., 32, 33, 34...). The longer the system has been running, the larger the number representing time. To predict where the Scud will next appear, both time and velocity must be expressed as real numbers. Because of the way the Patriot computer performs its calculations and the fact that its registers are only 24 bits long, the conversion of time from an integer to a real number cannot be any more precise than 24 bits. This conversion results in a loss of precision causing a less accurate time calculation. The effect of this inaccuracy on the range gate's calculation is directly proportional to the target's velocity and the length of time the system has been running. Consequently, performing the conversion after the Patriot has been running continuously for extended periods causes the range gate to shift away from the center of the target, making it less likely that the target will be successfully intercepted.

2.2 Sequence of Events

During Desert Shield, Patriot battalions were deployed to Saudi Arabia and then to Israel to defend against Iraqi Scud missiles. This was the first time the Patriot had been used to defend against Scud missiles, which fly at approximately MACH 5 (3750 mph). To obtain Scud data, the Army relied on operational experience conveyed by Patriot users as well as other intelligence sources. With the launch of each Scud, the Army became more and more knowledgeable about the Scud's flight characteristics. Recorded data is another more useful tool that could have provided detailed data on the Patriot's actual performance. However, the Patriot was not equipped with an internal data recorder to retain system performance information. Although portable, external data recorders were available, U.S. commanders decided not to use them because they believed the recorders could cause an unanticipated system shutdown. However, Israeli commanders used data recorders on the Patriot systems they controlled and provided this data to the U.S. Army. As information from all sources became available, the Patriot Project Office in Huntsville, Alabama, made software changes from August 1990 to February 1991 to adapt the system to the Desert Storm environment. During the conflict, the Patriot's software was modified six times. Patriots had to be shut down for at least 1 to 2 hours to install each software modification.

On February 11, 1991, the Patriot Project Office received Israeli data identifying a 20 percent shift in the Patriot system's radar range gate after the system had been running for 8 consecutive hours. This shift is significant because it meant that the target (in this case, the Scud) was no longer in the center of the range gate. The target needs to be in the center of the range gate to ensure the highest probability of tracking the target. As previously mentioned, the range gate is calculated by an algorithm that determines if the detected target is a Scud, and if the Scud is in the Patriot's firing range. If these conditions are met, the Patriot fires its missiles.

Patriot Project Office officials said that the Patriot system will not track a Scud when there is a range gate shift of 50 percent or more. Because the shift is directly proportional to time, extrapolating the Israeli data (which indicated a 20 percent shift after 8 hours) determined that the

range gate would shift 50 percent after about 20 hours of continuous use. Specifically, after about 20 hours, the inaccurate time calculation becomes sufficiently large to cause the radar to look in the wrong place for the target. Consequently, the system fails to track and intercept the Scud. Significant shifts of the range gate away from the desired center of the target could be eliminated by rebooting the system-turning the system off and on--every few hours. Rebooting, which takes about 60 to 90 seconds, reinitializes the computer's clock, setting the time back to zero. Army officials said that they believed the Israeli experience was atypical--they assumed other Patriot users were not running their systems for 8 or more hours at a time. However, after analyzing the Israeli data and confirming some loss in targeting accuracy, the officials made a software change which compensated for the inaccurate time calculation. This change allowed for extended run times and was included in the modified software version that was released on February 16, 1991. However, Army officials did not use the Israeli data to determine how long the Patriot could operate before the inaccurate time calculation would render the system ineffective.

On February 21, 1991, the Patriot Project Office sent a message to Patriot users stating that very long run times could cause a shift in the range gate, resulting in the target being offset. The message also said a software change was being sent that would improve the system's targeting. However, the message did not specify what constitutes very long run times. According to Army officials, they presumed that the users would not continuously run the batteries for such extended periods of time that the Patriot would fail to track targets. Therefore, they did not think that more detailed guidance was required. Six Patriot batteries protected the airfields and seaports of Dhahran. Alpha Battery, the battery in question, was to protect the Dhahran Air Base. On February 25, Alpha Battery had been in operation for over 100 consecutive hours. Because the system had been on so long, the resulting inaccuracy in the time calculation caused the range gate to shift so much that the system could not track the incoming Scud. Consequently, Alpha Battery did not engage the Scud, which then struck an Army barracks and killed 28 American soldiers.

On February 26, the next day, the modified software, which compensated for the inaccurate time calculation, arrived in Dhahran. According to Army officials, the delay in distributing the software from the United States to all Patriot locations was due to the time it took to arrange for air and ground transportation in a wartime environment.

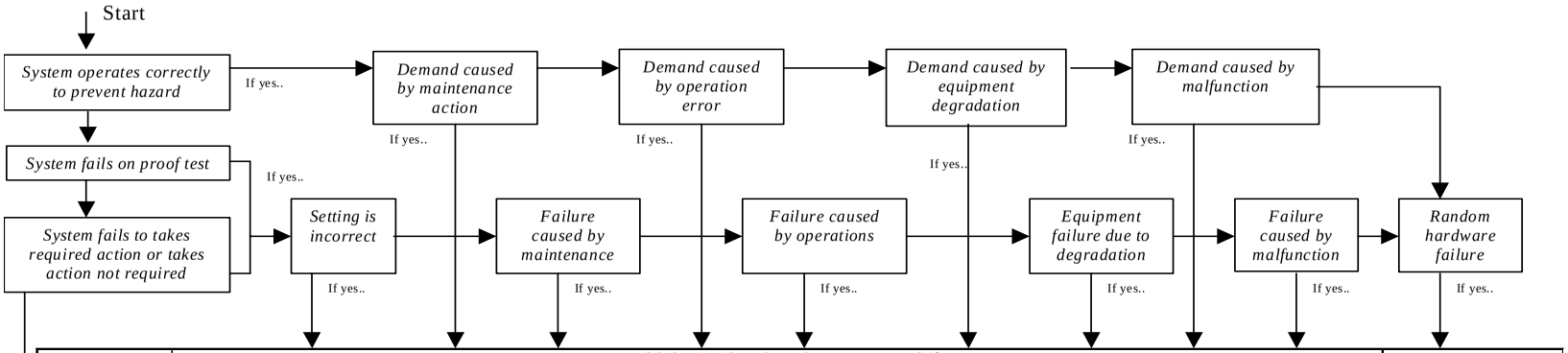
3. Your Task…

You should again work in groups. The aim of PARCEL analysis is to identify weaknesses in the lifecycle phases or common requirements that are described within the IEC61508 standard. These weaknesses are enumerate in the taxonomy that is shown in Table 1. There are two ways of doing this in PARCEL. You should agree as a group whether you will focus on the simplified flow-charting scheme or the more complex but flexible approach based around Events and Causal Factors Charting.

IEC 61508 Lifecycle phase	Detailed taxonomy	IEC 61508 ref
Concept	1. Hazard &Risk Assessment	7.2,7.3,7.4
Overall Scope		
Overall Safety Requirements	specification	7.2 (2)
	selection of equipment	7.4.2.2 (2)
Allocation	design and development	7.4 (2)
	installation design	7.4.4/5 (2)
Planning of I & C, V, and O&M	maintenance facilities	7.4.4.3 (2),
	operations facilities	7.4.5.2/3 (2)
Realization		7.4.5.1/3
Installation and commissioning	1. installation 2. commissioning	7.5 (2), 7.13.2.1/2, 7.13.2.3/4
Validation	1. function testing 2. discrepancies analysis 3. validation techniques	7.7.2.1/2/3 (2) 7.7.2.5 (2) 7.7.2.7 (2)
Operation and maintenance	1. maintenance procedures not applied 2. maintenance procedures need improvement 3. operation procedures not applied 4. operations procedures need improvement 5. permit/hand over procedures 6. test interval not sufficient 7. maintenance procedures not impact assessed 8. operation procedures not assessed 9. LTA procedures to monitor system performance 10. LTA procedures applied to initiate modification in the event of systematic failures or vendor notification of faults 11. tools incorrectly selected or not applied correctly	7.7.2.1 7.6.2.2.1/2/3 (2) 7.6.2.1 7.6.2.2 7.6.2.1 7.6.2.1 7.6.2.4 (2) 7.6.2.4 (2) 7.6.2.1 (2) 7.8.2.2 (2), 7.16.2.2 7.6.2.1 (2)
Modification	1. impact analysis incorrect 2. LTA manufacturers information 3. full lifecycle not implemented 4. LTA verification and validation	7.8.2.1 (2) 7.8.2.2 (2) 7.8.2.3 (2) 7.8.2.4 (2)
IEC 61508 common requirements		
Competency	1. LTA operations competency 2. LTA maintenance competency 3. LTA modification competency	6.2.1 h 6.2.1 h 6.2.1 h
Lifecycle	1. LTA definition of operations accountabilities 2. LTA definition of maintenance accountabilities 3. LTA definition of modification accountabilities	7.1.4 7.1.4 7.1.4
Verification	1. LTA verification of operations 2. LTA verification of maintenance 3. LTA verification of modification	7.18.2, 7.9 (2) 7.18.2, 7.9 (2) 7.18.2, 7.9 (2)
Safety management	1. LTA safety culture 2. LTA safety audits 3. LTA management of suppliers	6.2.1 6.2.1 6.2.5
Documentation	1. documentation unclear or ambiguous 2. documentation incomplete 3. documentation not up to date	5.2.6 5.2.3 5.2.11
Functional safety assessment	1. LTA O & M assessment 2. modification not assessed 3. assessment incomplete 4. insufficient skills or independence in assessment team	8.2 8.2 8.2.3 8.2.11/12/13/14

Key: LTA is Less Than Adequate, IEC 61508 references are to Part 1 except as indicated by parentheses e.g. (2)

Table 1: **Taxonomy for Analysing E/E/PES Related Failures Under IEC 61508.**

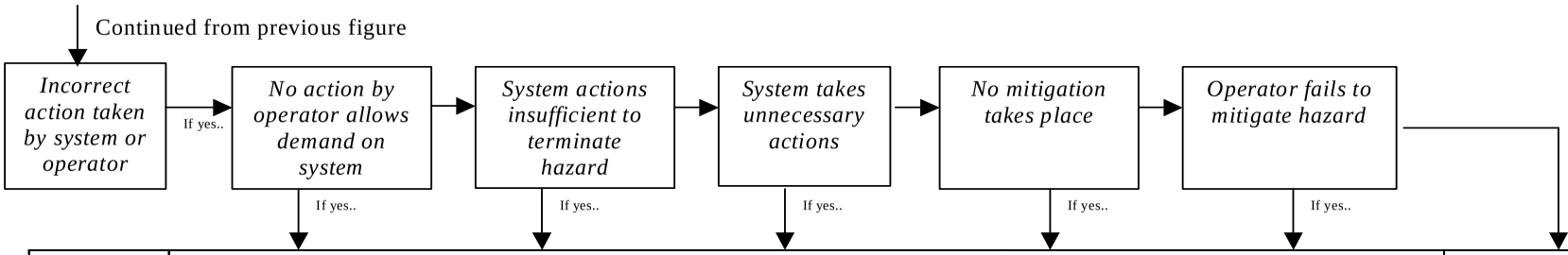


	Would the incident have been prevented if:					
Design	- different equipment selected? - installation design different? - configuration was correct	- maintenance facilities had been designed adequately	- operations facilities had been designed correctly	- different equipment selected? - installation design had been different?	- different equipment selected? - the installation design had been different? -configuration was correct	Log failure and check -if dangerous failure rate is in line with design assumptions -if all expected actions occurred and no unexpected actions occurred -if safe failure causes any unexpected actions Log demand and check if -demand rate is in line with design assumptions -demand cause was predicted in H & RA
Installation & Commission	- the equipment had been installed according to design	- the maintenance facilities had been installed according to design	- the operations facilities had been installed according to design	- the equipment had been installed according to design	- the equipment had been installed according to design	
Validation	- the setting had been checked during validation	- maintenance facilities had been fully checked	- operations facilities had been fully checked	- equipment condition had been fully checked	- equipment condition had been fully checked	
Operation & Maintenance	- maintenance procedures were applied - maintenance procedures were improved - maintenance tools better - test interval was reduced	- correct maintenance procedure had been used - maintenance procedure was improved - permit procedures better	- correct operation procedure was used - operation procedure was improved - permit procedures improved	- maintenance procedures applied - maintenance proc. better - test interval was reduced - additional protection provided	- maintenance procedures were improved - maintenance tools improved - test interval was reduced - additional protection provided	
Modification	- setting had been reviewed during impact analysis	- maintenance facilities or procedures had been reviewed during impact analysis	- operation facilities or procedures had been reviewed during impact analysis	- equipment used or installation design has been reviewed during impact analysis	- equipment used or installation design has been reviewed during impact analysis	

	Would the incident have been prevented if:					
	Competency	Lifecycle	Verification	Safety management	Documentation	Safety assessment
Operation & Maintenance	- operation or maintenance staff were more competent	- responsibilities were defined better	- a better verification scheme had been in place	- safety culture was improved - audits were more frequent	- documentation was clear and sufficient	- assessment had been carried out on O&M phase
Modification	- modification carried out by more competent staff	- modification lifecycle was better defined	- a better verification scheme had been in place	- accountabilities better defined - suppliers not reviewed	- documentation updated	- assessment carried out on modification

Continued …

Figure 1: High-Level PARCEL Flow Chart (Stage 1)



	Would the incident have been prevented if:					
Design	- operator facilities had been designed better - the installation design had been different?	- additional actions had been specified - actions had been faster - final actuation device were improved	- design requirements were better documented	- mitigation system had been specified - mitigation system had been better designed	- operator facilities had been designed better - the installation design had been different?	Log failure and check - if dangerous failure rate is in line with design assumptions - if all expected actions occurred and no unexpected actions occurred - if safe failure causes any unexpected actions Log demand and check if - demand rate is in line with design assumptions - demand cause was predicted in H & RA
Installation & Commissioning	- the equipment had been installed according to design	- the equipment had been installed according to design	- the equipment had been installed according to design	- mitigation system had been installed according to design	- the equipment had been installed according to design	
Validation	- operator facilities had been checked during validation	- operation facilities had been checked during validation	- operations facilities had been fully checked	- mitigation system had been fully checked	- operator facilities had been fully checked	
Operation & Maintenance	- operation procedures were applied - operation procedures were improved	- correct maintenance procedure had been used - maintenance procedure was improved - proof testing was more frequent	- correct operation procedure was used - operation procedure was improved - permit procedures were improved	- mitigation procedures were applied - mitigation procedures were improved - mitigation system was proof checked more frequently	- operation procedures had been applied - operation facilities or procedures were improved	
Modification	- operation facilities had been reviewed during impact analysis	- necessary system actions had been reviewed during impact analysis	- necessary system actions had been reviewed during impact analysis	- need for mitigation had been reviewed during impact analysis	- need for mitigation had been reviewed during impact analysis	
	Would the incident have been prevented if:					
	Competency	Lifecycle	Verification	Safety management	Documentation	Safety assessment
Operation & Maintenance	- operation or maintenance staff were more competent	- responsibilities were defined better	- a better verification scheme had been in place	- safety culture was improved - audits were more frequent	- documentation was clear and sufficient	- assessment had been carried out on O&M phase
Modification	- modification had been carried out by more competent staff	- modification lifecycle was better defined	- a better verification scheme had been in place	- accountabilities were better defined - suppliers not reviewed	- documentation had been updated	- assessment ad been carried out on modification

Figure 2: High-Level PARCEL Flow Chart (Stage 2)

3.1 Simplified Scheme: Flow Chart

This simpler of our two techniques relies on a form of flow-chart shown in Figures 1 and 2. Analysis begins by asking a series of high level questions about the nature of the E/E/PES related incident. For instance, investigators must determine whether or not the system correctly intervened to prevent a hazard, as might be the case in a near miss incident. If the answer is yes, then the analysis progresses by moving horizontally along the arrows to identify the nature of the failure. If the system intervened to address problems created by maintenance activities then the investigator would follow the arrow in Figure 1 down to the associated table entry. By reading each cell in the column of the table indicated by the arrow, investigators can identify potential causes in the simplified stages of the IEC 61508 lifecycle. Latent failures that might have been the source of an E/E/PES related incident can also be considered by examining the items listed under all six of the common requirements in the third row from the bottom. Investigators must continue along the top horizontal line repeating the classification against the cells in the table in the same manner described for maintenance related incidents. Analysis progresses by following the top-level questions down the flow chart. For some incidents, there will be failures identified by analysing several of these different questions. For instance, a system may operate correctly to prevent a hazard although in the process there may also be further subsystem failures or operator interventions that initially fail to rectify the situation. In this case, analysts would focus on the top line in Figure 1 and the further line of analysis continued on Figure 2. It is important to document the outcome of this flowchart analysis. This is done using the form illustrated in Table 2.

Causal Event	**IEC 61508 Lifecycle/ Common Requirement**	**Justification (Route through flow chart)**
Loss of electrical power and associated plant	Design	System fails to take required action-> Equipment failure caused by malfunction-> The incident would have been prevented if different equipment had been selected.

Table 2: Abridged IEC 61508 Flowchart Causal Summary for Case Study

3.2 Alternate Analysis Scheme: ECF Charting

The flowcharts cannot cover all possible causes of incidents in a broad range of industries. In contrast, the alternate causal analysis technique in PARCEL embodies a more complex but flexible approach based on Events and Causal Factors (ECF) diagrams. This technique was initially developed to support accident investigation by the US Department of Energy and a simplified form is illustrated in Figure 3. This diagram is based on an incident in which a floating production vessel lost all electrical and hydraulic power when 2 out of 2 voting was used on redundant PLC pipelines. The system could not resolve a disagreement between the redundant channels and caused a total shut-down that was exacerbated by the fact that ballast was being transferred to induce a list on the vessel. In the ECF diagram, the rectangles represent events. Ovals represent the conditions that make those events more likely. The diamond shape represents the outcome of the mishap. The development of a detailed ECF chart continues until all of the parties involved in an investigation agree that it provides a reasonable representation of the events that contributed to an adverse occurrence or near miss. This decision is influenced by the scope of the investigation and by pragmatics. As with the STAMP case study, it is important to balance the need to represent as many of the key events as possible and the limited amount of time available to complete this exercise.

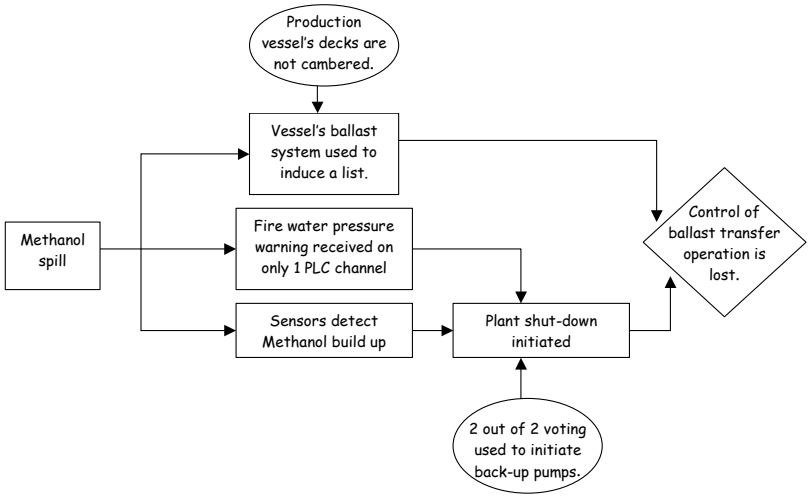


Figure 3: High-level ECF Chart

The ECF diagram reconstructs the events and conditions that contribute to a mishap. A further stage of analysis is required in order to distinguish potential causal factors from more contextual information. Analysis proceeds using what is known as counterfactual reasoning. The term 'counterfactual reasoning' denotes a common form of argument that is used informally in many different incident investigations. Starting at the outcome event, investigators must ask whether the incident would have occurred if that event had not taken place. If the incident would still have happened then the event cannot be considered as a casual factor. In Figure 3, the incident would not have happened if the plant-shut down had not been initiated hence this is a causal factor. However, the fact that the shut-down occurred during ballast transfer exacerbated the incident but was not a cause. Warning: counterfactual reasoning is non-trivial and is error prone.

The final stage is to link each causal factor back to potential problems in the development stages and common requirements of IEC 61508, illustrated in Table 1. The first task is to identify those conditions that contributed to each causal event using the ECF chart illustrated in Figure 3. In this case, the plant shut-down stemmed from the condition representing the decision to use a 2 out of 2 voting protocol. Table 2 might be used to relate this failure back to inadequate risk assessment prior to implementation. The key point is not to arrive at an unambiguous association of lifecycle phases with the conditions that contribute to causal events. The intention is to provide a focus for the analysis so that consensus can be achieved before recommendations are made. Table 3 illustrates one means of documenting the results of this more complex form of analysis.

Causal Event	**Associated Conditions**	**61508 Classification**	**Justification**
Plant shut-down	2 out of 2 voting used to initiate back-up pumps	Hazard and risk assessment 1: specification	Initial risk assessment failed to identify vulnerability if disagreement in the voting forced an unexpected system shut-down.

Table 3: Abridged IEC 61508 Causal Summary Chart for Case Study Incident

4. Wrap Up

As mentioned, both STAMP and PARCEL are under development. It would be very useful to know of your impressions from using these techniques.