Applying Generic AcciMap to a DDOS Attack on a Western-European Telecom Operator

Hans C.A. Wienen
University of Twente
h.c.a.wienen@utwente.nl

Faiza A. Bukhsh
University of Twente
f.a.bukhsh@utwente.nl

Eelco Vriezekolk
Radiocommunications Agency Netherlands
eelco.vriezekolk@agentschaptelecom.nl

Roel J. Wieringa
University of Twente
r.j.wieringa@utwente.nl

ABSTRACT

After a large incident on a telecommunications network, the operator typically executes an incident analysis to prevent future incidents. Research suggests that these analyses are done ad hoc, without a structured approach. In this paper, we conduct an investigation of a large incident according to the AcciMap method. We find that this method can be applied to telecommunications networks with a few small changes; we find that such a structured approach yields many more actionable recommendations than a more focused approach and we find that both the onset of an incident and the resolution phase merit their own analysis. We also find that such an analysis costs a lot of effort and we propose a more efficient approach to using this method. An unexpected outcome was that AcciMap may also be very useful for analyzing crisis organizations.

Keywords

Telecommunications, AcciMap, accident analysis, incident analysis

INTRODUCTION

Telecommunications networks are part of vital and critical infrastructure that needs to be in place for society to run smoothly. Unavailability of telecommunications services can lead to unreachability of emergency services, severe traffic jams and impossibility to inform the populace. In order to make telecommunications networks more robust, we have started the LINC project with the Dutch telecom regulator. Purpose is to analyze incidents on these networks in order to learn from those incidents and share those lessons with the practitioners. These lessons may result in better risk management: impact and probability of risks may be better assessed as result of the lessons and the insights gained may result in better mitigation.

Previously, we conducted a literature review of Accident Analysis Models and Methods (Wienen *et al.* 2019). We identified three families of accident analysis methods and we also identified the methods that had seen the most scrutiny from academia. In this paper, we take the most discussed methods in academia and apply them to a real-life telecommunications incident that severely hindered the email and interactive TV services of the provider.

Please note, that in contrast to the practice in other industries, Telecommunications use the term *incident* as opposed to *accident*. In this paper, we follow this practice and hence with "incident" we mean an undesired and unplanned event that results in a loss, damage or injury.

This paper is organized as follows: first, we will share some theoretical background regarding incident analysis methods; then we pose our research questions. We will describe the research design and then the incident itself, after which we will describe the execution of the research. We then report our results, which we will then discuss and finally we will draw some conclusions, while answering our research questions.

Theoretical Background

Accident Analysis Methods can be divided into three families: sequential, epidemiological and systemic. They differ on the extent in which the socio-technical context and control loops and feedback mechanisms are addressed. As mentioned in (Wienen *et al.* 2019), the families can be described as follows. Note that we talk about incidents where in other domains the term "accident" would be used.:

Sequential incident models describe the accident as the end point of a sequence of causes.

Epidemiological models describe the incident as the product of the interaction among a set of entities and actors, some of which may be visible, and others invisible. In effect, it is a sequence of causes that are inhibited or enabled by environmental factors that also have a place in the model. This model is similar to models of how diseases develop, hence the name. A key factor in epidemiological types of analysis is the description of latent factors that contribute to the development of an unsafe act into an incident.

Systemic incident models describe the incident as the result of the interaction within a tightly coupled system and between the system and its context. Feedback loops may play an important role in these models.

We have applied both FTA (Fault Tree Analysis), the most discussed sequential method as measured in our previous research (Wienen *et al.* 2019), and AcciMap, the most discussed epidemiological method as measured in the same research. However, this paper focusses mainly on the application of AcciMap.

Research question

The telecommunications community does not have a standardized incident analysis model and method, making it hard for authorities to compare incidents and to draw lessons from those incidents. One of the goals of the LINC project is to find or create an incident analysis model and method that can be used to draw lessons from those incidents that can then be shared with the telecommunications operators. Furthermore, in reading existing incident reports, the majority of methods used was of a sequential nature – even though no real formal methods were used. This leads us to ask the following research questions:

1. Do epidemiological methods add more value to the incident analysis in Telecommunications services?
2. Is the Generic AcciMap method a viable method for analyzing Telecommunications incidents?

Research Design

In order to compare the two results, we have co-operated with two Western-European Telecommunications operators. The operators have each selected an interesting case and have provided access to sensitive information. They also provided employees who were involved with the incidents to participate in our incident analysis workshops. This article reports the results of one of the two cases: a DDOS attack.

One researcher conducted the workshops, using Branford's approach (Branford *et al.* 2009) to AcciMap, the *Generic AcciMap Approach*. The other created an FTA according to the definition in the Fault Tree Handbook (Vesely *et al.* 1981). As the incident analysis reveals sensitive information about the company involved, the details of the research have to remain confidential. The company will be called Alpha in the remainder of this article.

Short description of the Incident

According to an internal report drawn up by Alpha as part of the post mortem of the incident,

> *A distributed denial of service attack was staged against Alpha's DNS servers, using several different attacks (DNS reflection, UDP flooding, ICMP flooding). This attack caused Alpha's firewalls to collapse. As a consequence, all services behind the firewall were impacted and the customers experienced outage on DNS, mail, internet and telephony (VoIP). The attack took place in 4 waves which eventually were stopped by applying ACLs, bypassing the firewalls for DNS resolution and redirecting traffic [...] to take advantage of the [...] scrubber.*

In other words: due to an overload of requests, Alpha's firewall collapsed. This caused outage of several services for customers. To resolve the incident, the company had to redirect traffic outside their own network and to clean the traffic to their network from malicious requests.

This description implies two stages to the incident: the stage in which the incident develops and causes its harm (the *onset*) and the stage during which Alpha worked hard to resolve the incident (the *resolution*). Both stages have their own characteristics and we decided during the analysis to treat them separately, resulting in individual

AcciMaps for both stages.

EXECUTION

The execution of the analysis took place over several sessions, as indicated in the timeline below:

Table 1: timeline of the analysis

Date	Activity	Parties
16-06-2017	Preparation of 1st DDOS workshop	BCM, UT
06-07-2017	1st DDOS workshop	Alpha, UT
14-07-2017	2nd DDOS workshop	Alpha, UT
15-09-2017	Preparation of 3rd DDOS workshop	BCM, UT
03-11-2017	Formulation of recommendations onset	BCM, UT
17-11-2017	3rd DDOS workshop: Establish AcciMap of response phase	BCM, R&C, UT
24-11-2017	Formulation of recommendations response phase	BCM, UT
08-12-2017	Compare recommendations with earlier analyses	BCM, UT

Note: BCM: Business Continuity Manager – the person who is responsible for enabling the organization to continue business critical activities during the most challenging circumstances; UT: Researchers from University of Twente; R&C: representative from Risk & Compliance – the department responsible for corporate risk management and for follow up on defined risk mitigation plans.

Introduction to AcciMap

AcciMap has been thoroughly described in the literature (Branford *et al.* 2009; Salmon *et al.* 2014; Svedung and Rasmussen 2002; Underwood and Waterson 2013; Underwood and Waterson 2014). As a short introduction, AcciMap is an epidemiological incident analysis method that takes the complete socio-technical system into consideration. Part of the method is a diagram that links all causal factors to their causes, stopping only at causes for which further analysis is not useful given the incident. The Generic AcciMap Method we apply, contains three levels of causal factors: the physical / actor level, in which actions and malfunctioning equipment play a role; the organizational level, in which organizational errors and malfunctions play a role, and an external layer, subdivided into regulatory, government and society. Each causal factor is part of one layer and the causal factors that are part of the physical/actor level and the organizational level are considered in formulating recommendations for the organization suffering from the incident.

Workshops

The workshops consisted of an introduction to AcciMap including an example and subsequently performing steps 1 – 8 of the *Generic AcciMap Method.* (*See* Sidebar 1). We made a slight change to steps 2-4: we had the participants write out the causal factors on sticky notes directly and we discussed the level on which they had to be attached in the group as we put the notes on the overall AcciMap paper. The group identified 64 causal factors, and we did not finish all steps in one workshop. The factors were identified using two methods: first, we let the participants individually formulate causal factors without any other input than the introduction of AcciMap. We then presented the participants with the table with *categories of cause* as listed in Branford's article. These are listed in Sidebar 2. This helped in formulating additional causal factors.

1. (Create a blank AcciMap format on which to arrange the causes)
2. Identify the outcome(s)
3. Identify the causal factors
4. Identify the appropriate AcciMap level for each cause
5. Insert the causes
6. Insert the causal links
7. Fill in the gaps
8. Check the causal logic
9. Formulate Safety Recommendations

Sidebar 1: the 9 steps in the Generic Accimap Method

During the discussions in the first workshop, we observed that the participants not only included the causal factors leading to the incident, but also factors that impacted the resolution of the incident. We decided to make two groups of causal factors and two different AcciMaps: one for the onset of the accident and one for the resolution or response phase. We then concentrated on the onset of the accident and the completion of steps 5-8.

The onset of the accident

During the first workshops we were able to identify some of the causal links. These were recorded and modelled in a preliminary AcciMap which we completed in the second workshop. We then decided to review the final AcciMap for the onset in a smaller committee (the researchers and the representative of the company for Business Continuity). In that meeting, we also formulated the safety recommendations.

The resolution of the accident

As the workshops take quite some effort, we decided to do steps 2-9 for the response phase in a smaller committee: the two researchers and two representatives of the company: one from Risk & Compliance, and one from Business Continuity. This resulted in a second set of recommendations.

1. Financial, such as (s/a) cost cutting
2. Equipment and Design, s/a poor quality equipment
3. Defences, s/a missing alarms
4. Communication and Information, s/a inadequate knowledge
5. Auditing and Rule Enforcement, s/a missing internal auditing
6. Organizational Culture, s/a incompatible goals
7. Risk Management, s/a inadequate security
8. Manuals and Procedures, s/a missing manuals
9. Human Resources, s/a insufficient staff
10. Training, s/a inadequate exercises

Sidebar 2: Branford's Categories of Cause

Formulating the safety recommendations

We formulated safety recommendations in a manner analogous to Branford, with a few changes:

- We formulated safety recommendations per causal factor. This way, we had a structured approach to go through the different causal factors, and we made sure that we covered all three types of recommendation per causal factor.
- Branford has a heuristic to formulate recommendations: she uses the terms *Change, Control* and *Compensate* to describe different types of recommendations. *Change* means what can be rectified directly, *Control* means what can you do to control the outcome of an incident and *Compensate* means what can you do to compensate for the consequences. This heuristic we reused, but as our audience had trouble applying those terms, we chose to use the terms *Prevent, Mitigate* and *Compensate*. These terms had the same meaning in our applications, but they were more easily understood by our audience

RESULT

Table 2: Identified causal factors and recommendations per stage and AcciMap level

Stage	Number of Causal Factors			Number of Recommendations		
	External	Organizational	Physical /Actor	External	Organizational	Physical/Actor
Onset	11	17	4	0	54	6
Resolution	4	16	12	0	50	26

From previous research (Bukhsh *et al*. 2019) we found that Telecommunications operators do not use structured methods. Their analysis mostly concentrates on the physical parts of an incident, and the activities of the different actors in the incident. Applying AcciMap clearly adds more levels to the picture, as can be seen from Table 2. This was also the feedback we got from the professionals in company Alpha.

After analyzing all causal factors, we noticed that both the onset of the incident (the causal chain leading up to the incident) and the resolution of the incident (the causal chain leading up to the resolution of the incident, or back to "business as usual") were of interest to Alpha. This makes sense: from a prevention perspective, the chain of events leading to the accident is relevant to prevent a similar incident from occurring again, or at least to make the socio-technical system more robust against future attacks (as this was an incident caused by an attack, and attacks will happen). But given the fact that attacks will happen, and Telecommunications operators are always vulnerable to attacks, while hackers are resourceful, an operator will always have to plan for situations in which they could not prevent a successful attack. This means that resolution of the incident is paramount in that case: the quicker the operator is back in business, the lower the damage in terms of costs, lost revenue and damage to corporate image.

Table 3: Identified recommendations per Category of Cause and AcciMap level

Stage	Category of Cause	Organizational	Physical/Actor
Onset	Risk Management	17	
	Finance	7	
	Equipment & Design	12	6
	Defenses	5	
	Communication & Information	3	
	Auditing & Rules Enforcement	10	
Resolution	Information Sharing	6	
	Technical issues extending crisis period		6
	Crisis Management	17	4
	Staff	8	
	Training	2	
	Company Culture	5	
	Crisis Facilities & Tools	12	16

For the onset, we have grouped the recommendations according to the different categories of cause as discussed by Branford. When analyzing the recommendations for the resolution phase, these categories did not add to the understanding and we grouped the recommendations differently, as indicated in Table 3. This is not entirely unexpected: the onset can be covered by generic strategic, tactical and operational processes. All recommendations are meant to improve those processes or – if missing – define and implement them. The processes around the resolution phase are more crisis oriented: the resolution stage is one of crisis management: getting business back to normal as soon as possible in a situation in which not all information is available and the cause of the crisis is still there. In this phase, more recommendations have been formulated on the physical and actors level. This can be understood as follows: crisis facilities can be planned and prepared beforehand, but actions during the crisis (usually a situation with at least some characteristics that cannot be predicted) require a certain amount of improvisation – a feature of the actor layer.

Table 4: Comparing recommendations between investigations

Category of Cause	AcciMap	Alpha's investigation	Accountancy Firm
Risk Management	17	0	0
Finance	7	4	0
Equipment & Design	18	6	0
Defenses	5	0	0
Communication & Information	3	0	1
Auditing & Rules Enforcement	10	0	0
Information Sharing	6	0	1
Technical issues extending crisis period	6	0	1
Crisis Management	21	6	10
Staff	8	0	0
Training	2	0	2
Company Culture	5	0	0
Crisis Facilities & Tools	28	4	0
Total	136	20	15

Feedback from telecommunications operator

After applying the method to the incident, Alpha found that

- AcciMap really helps to get more insights in the context of an incident
- AcciMap is a structured method to find recommendations for the organization as a whole
- It is very time consuming
- It is not appropriate for the resolution of the incident itself, only as post mortem after the incident has been resolved
- Alpha intends to use this method in the future for the post mortem of larger incidents. We are currently preparing a second case study with Alpha, using a less-time-consuming version of AcciMap.

DISCUSSION AND CONCLUSION

Answers to the research questions

Do epidemiological methods add more value to the incident analysis in Telecommunications services?

According to Alpha, AcciMap adds more value than the ad hoc, sequential methods they used before. This is also reflected by the number of actionable recommendations when compared to the method employed by Alpha (136 vs 20). The number of recommendations from the accountancy firm is less relevant as a comparison number, as their recommendations were based on comparing Alpha's crisis organization to the firm's ideal model of a crisis organization.

Is the Generic AcciMap method a viable method for analyzing Telecommunications incidents?

According to Alpha, the method is viable for large incidents, given the investment in time and effort. For quick resolution, an epidemiological method is less apt: during the resolution phase, time is of the essence and a sequential method is more appropriate. This is also confirmed by our experience in applying FTA as part of this analysis – which took far less time. As far as we could determine from discussions with Alpha's staff, this is also in accordance with their mental model for quick incident resolution.

Other findings supporting AcciMap as a method for incident analysis in Telecommunications

The case study yielded more results than just the answers to our research question.

Difference between onset and resolution

During the analysis of the incident, we found that the experts in Alpha listed causal factors that lead to the incident as well as causal factors that prolonged the incident. To keep things manageable, we decided to create two different AcciMaps (onset and resolution) in order to give some structure to the discussion. This proved helpful and as a result, we have been able to also generate recommendations for crisis management (the brunt of the resolution phase in this case).

For Alpha, the resolution phase was as interesting as the onset to the accident. Although Alpha is keen on preventing the next incident, they do realize that incidents will happen and that quick resolution is also important.

Applicability to crisis organizations

The resolution phase is of further interest, as it is actually applying AcciMap not to an incident, but to a crisis organization: how did Alpha respond to the crisis and what lessons can be learned from that? Of the 76 recommendations for the resolution phase, at least 49 where directly related to crisis management and crisis facilities. This means that AcciMap may also be a very interesting method to analyze crisis resolution and by its extension, crisis organizations.

Difference between strict focused investigation and broad investigation

The large difference in recommendations from the AcciMap method and from the two other investigations can partially be explained by the stricter focus of the latter: both Alpha's investigation and the accountancy firm's restricted themselves (consciously or unconsciously) to only a part of the problem: Alpha's to the technical and security aspects of the incident, the accountancy firm's to the crisis management aspects. This may be an added benefit of AcciMap or indeed of any epidemiological method: it forces you to look at the incident from all angles, yielding recommendations in areas where you would beforehand not expect them, simply because you

did not consider them.

Other findings suggesting opportunities for improvement of AcciMap when applied to incident analysis in Telecommunications

Large number of actionable recommendations due to structured approach of formulating recommendations

The structured approach of formulating recommendations lead to a large number of actionable recommendations: as each causal factor was considered individually, each factor could give rise to a large number of recommendations. In our case, the average number of recommendation per causal factor in the organizational and physical/actor level was 2.5 for the resolution phase and even 2.9 for the onset. Such a large number of recommendations calls for central co-ordination of follow up and prioritization of the recommendations. We did not go into the way how to prioritize them, although several methods spring to mind (based on cost / benefit, or risk based for example).

Time consumption

As can be seen from the timetable in Table 1, the method is time consuming. It took three workshops with multiple staff, which is costly. This means that the method – in this version – is only feasible when dealing with incidents that have a severe impact on the business. This also signals an opportunity for improvement: if this effort can be reduced, the method will be easier to apply and the cost-benefit relation will improve.

Furthermore, much discussion centered around the assignment of blame: it was hard to keep the discussion away from the blame game. This may be an aspect of the organization itself, but we think we may be able to avoid these discussions by first concentrating on the physical layer of the incident – something that can be done relatively neutral and factual. After the core mechanism of the incident has been established, this small success may set a better atmosphere for the organizational discussions.

Alpha's Business Continuity Manager suggested to have a short video message from the CEO before starting an incident analysis to emphasize that the analysis should uncover *all* sources of failure with the express purpose of preventing future incidents, while also admitting that not all measures may be implemented for reasons of time or due to monetary constraints.

Lack of IT systems in the levels for AcciMap

We noticed that the AcciMap when applied to telecommunications may benefit from adding a sublevel to the physical/actor and the organizational level: Systems and Software are as important as actors and organizational aspects. We did not consider this division in this analysis, but it may be beneficial to do so in further research.

Changes to AcciMap

Changes to the model

In order to give software or digital issues a more prominent place in the AcciMap (which we feel is necessary to adequately describe phenomena in technical environments), we propose the following:

- Describe the external and the organizational layer each from the point of view of three aspects: social, physical and digital.
- Describe the outcomes in terms of operational and technical aspects
- Describe the organization in terms of its components (organizational units) and the causal factors as relating to an aspect of those components (financial, communication, information flow, et cetera).

Changes to the method

For efficiency reasons, and to get everyone on board and avoid spending too much time on avoiding blame assignment, we propose a new approach for the method. Note that it may be hard to impossible to convince the experts that non-events do not exist, or to prevent non-events from cropping up. This is why we added step 2 in the approach below. These are the proposed steps:

1. Establish the physical core mechanism of the accident including the causal flow.

2. Find mitigations. This may be in terms of failure or absence of barriers, norms and entities.
3. Find how the mitigations would have influenced the causal flow and model this.
4. Use a heuristic to find recommendations (we follow Branford in her approach to look at three aspects: prevention of an event, controlling an event and compensating for the outcome of an event).
5. Prioritize the recommendations –many methods have been described in the literature.

Future Work

We are currently applying the adapted method in a case study with another telecom operator, and will use it also in a second case study at Alpha. These studies will test the changes to model and method we propose and supply more evidence to test the claim of usefulness. Enhancing efficiency and applicability to telecommunications will in our opinion greatly improve the value of this method to operators. Greater value may lead to widespread use, giving more opportunity to learn from these incidents.

REFERENCES

Branford, K., N. Naikar and A. Hopkins (2009). "Guidelines for AcciMap Analysis". Learning from High Reliability Organisations, CCH Australia Ltd.

Bukhsh, F.A., E. Vriezekolk, H. Wienen and R. Wieringa (2019). "Availability Incidents in the Telecom Domain: A Literature Review", Cybersecurity and Safety Group, University of Twente, The Netherlands (pre-print)

Salmon, P. M., N. Goode, F. Archer, C. Spencer, D. McArdle and R. J. McClure (2014). "A systems approach to examining disaster response: Using AcciMap to describe the factors influencing bushfire response." Safety Science **70**: 114-122.

Svedung, I. and J. Rasmussen (2002). "Graphic representation of accident scenarios: mapping system structure and the causation of accidents." Safety Science **40**(5): 397-417.

Underwood, P. and P. Waterson (2013). "Accident analysis models and methods: guidance for safety professionals."

Underwood, P. and P. Waterson (2014). "Systems thinking, the Swiss Cheese Model and accident analysis: a comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models." Accid Anal Prev **68**: 75-94.

Vesely, W. E., F. F. Goldberg, N. H. Roberts and D. F. Haasl (1981). "Fault tree handbook."

Wienen, H.C.A., F.A. Bukhsh, E. Vriezekolk and R.J. Wieringa (2019). "Learning from accidents: a systematic review of accident analysis methods and models." IJISCRAM 2019 (In Press)