Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 1295 – 1300

Procedia
Computer Science

The 1st Workshop on Safety & Security Assurance for Critical Infrastructures Protection (S4CIP)

Experience Report: Constraint-based Modelling and Simulation of Railway Emergency Response Plans

Søren Debois[a], Thomas Hildebrandt[a,*], Lene Sandberg[b]

[a] *IT University of Copenhagen, Rued Langgaardsvej 7, 2300 Cph S, Denmark*
[b] *Metropolitan University College Copenhagen, Denmark*

Abstract

We report on experiences from a case study applying a constraint-based process-modelling and -simulation tool, `dcrgraphs.net`, to the modelling and rehearsal of railway emergency response plans with domain experts. The case study confirmed the approach as a viable means for domain experts to analyse and rehearse emergency response plans, through the activities of formally modelling the plan and subsequently rehearsing it by simulating that model collaboratively. In particular, the constraint-based modelling notation resulted in a flexible model giving rehearsal participants freedom to explore different ways to proceed, including ways not necessarily anticipated in the paper-based emergency response plans. The case study was undertaken as part of a short research, ProSec, project funded by the Danish Defence Agency, with the aim of applying and developing methods for collaborative mapping of emergency and security processes in the danish public transport sector and their dependency on ICT.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Emergency response plans; Railways; Simulation; Formal models; DCR Graphs;

1. Introduction

Safe and reliable public transport is a prerequisite for the Danish society. The sector has well established plans and processes for managing physical emergency and security threats. However, as also pointed out in[1], emergency handling is a multi-disciplinary concept, and the complexity and dynamic environment in which it is embedded makes it a serious coordination problem. Plans and processes are described in various paper documents that need to be continuously rehearsed and updated, and the knowledge of dependencies on ICT infrastructure and consequences of cyber-attacks is at best fragmented. Consequently, possible cascading effects of cyber-physical incidents are unknown.

The aim of the ProSec project running from June 2015 to March 2016 was to develop and demonstrate a general method for collaborative mapping and simulation of processes and plans for the safe operation of crucial functions in society and their dependencies on Information and Communication Technology (ICT). The project members combine expertise in process modelling, emergency and crisis management, and security and risk management. The *first key hypothesis* of the project is that the recently developed constraint based process modelling notation, Dynamic

[*] Corresponding author. Tel.: +45 7218 5279.
E-mail address: hilde@itu.dk

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.269

Condition Response (DCR) graphs[2,3,4] and the web-based modelling and simulation tool `dcrgraphs.net`[5] allow for capturing emergency plans jointly with domain experts in a way that allow for the collaborative simulation and exploration of expected paths and scenarios as well as non-expected paths not described in the existing paper-based plans and rehearsal processes. The *second key hypothesis* is that the models can be used to identify, model and evaluate the consequences of dependencies on Information and Communication Technology (ICT).

The present paper reports on a case study carried out to investigate the first hypothesis and lay the foundations for studying the second. Concretely, we applied DCR graphs to model a railway emergency response plan and rehearsal process jointly with domain experts at the danish national railways (DSB) and used the process and the `dcrgraphs.net` simulation tool for conducting two simulation-studies aimed at testing the applicability of the tool for rehearsals. The first simulation was carried out by 15 students at the emergency management study programme at the Metropol school, which were representative as domain experts in emergency management. The second was carried out with the main emergency responsible at DSB and a train-driver instructor.

On the positive side, the case study confirmed that the `dcrgraphs.net` tool provided good support for collaborative modelling and analysis of emergency plans jointly with domain experts. Also both the collaborative modelling and subsequent simulations unearthed unexpected paths and scenarios *not* described in the existing paper-based plans and rehearsal processes. On the negative side, the case study pin-pointed some needed improvements in the DCR graphs notation and simulation tool for the present application to emergency planning.

Below in Sec. 2 we briefly describe the existing source material describing the emergency response process. In Sec. 3 we then show excerpts of the DCR graph model, explaining the notation on the fly, and report on the simulations performed with students and the employees at DSB. Finally in Sec. 4 we conclude and outline the work to be carried out in the final phase of the project to test the second key hypothesis.

2. Emergency Response Plans and Rehearsals

For the case study, we modelled emergency response plans and procedures for an larger incident at the Great Belt Bridge. Together, the plans and procedures describe a process that contains aspects of both larger operational interruptions and crisis; it has a cross-organisational nature; and it is of critical importance for the danish society. Moreover, a larger exercise with the aim to rehearse the process in practice is planned to be carried out in the near future, which will make it possible to study the process also in practice.

The process is described in several documents serving different purposes: Firstly, *the emergency handbook*, describes the overall administrative and technical emergency management activities aimed at preventing, avoiding and managing crisis situations, including natural disasters, acts of terrorism, larger accidents and larger delays in the daily operation. Secondly, a more detailed description of the process is described in another document, describing the individual tasks and actors involved for in the management of a larger incident. Thirdly, there is a legal announcement (Bekendtgørelse, *BEK nr 1312 af 16/12/2008*) from the ministry of transportation, setting the legal requirements for the process. Finally, there is a description for the concrete case of an incident on the Great Belt Bridge. In addition to these documents, there are scripts produced prior to rehearsals describing a realistic emergency scenario, to be used for both paper simulations done off-location and real rehearsals on location. These documents are supplemented by *operational documents and artifacts*, such as information folders, used in practice and for rehearsals on location to implement and coordinate the procedures. Due to time limitations and the scheduling of the real rehearsal after the end of the research project, these artifacts are not part of the case study.

Clearly, the many information sources means that the same information is repeated in different forms within the many documents. This makes updating the information in a coherent way challenging. Moreover, the documents reveal almost no information about which IT systems the tasks depend on. This may be because such dependencies are not important for the process management, if the ITC systems work as intended. But it means that the processes do not document what may happen if the ITC systems do not work as intended, which would be the case if they were subject to a Cyber-attack. Finally, it is difficult to validate from the documents if the process is *sound*, *complete*, and *adaptable*. By sound we mean that the process only describes behaviours that are possible. By complete we mean that the process takes into account all known/predictable behaviours. By adaptable we mean that the process is prepared for adaptation and changes when unknown or unpredictable situations occur.

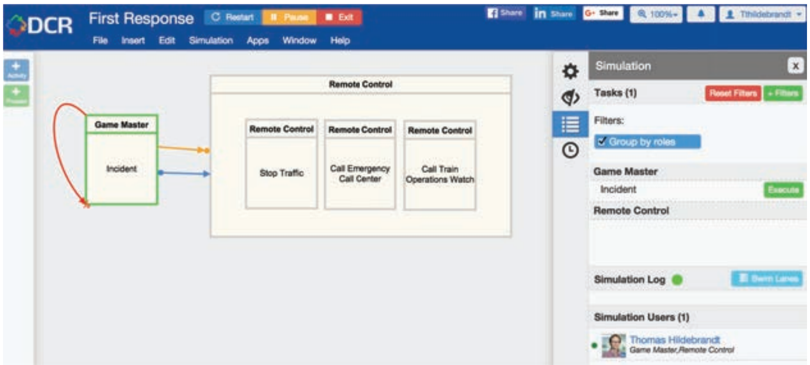
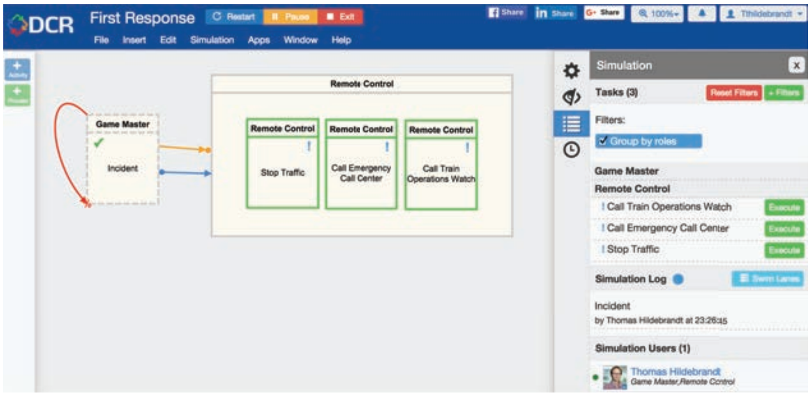


Fig. 1: The incident can only happen once and enables and triggers responses at the Remote Control Central.



Incident
by Thomas Hildebrandt at 23:26:45

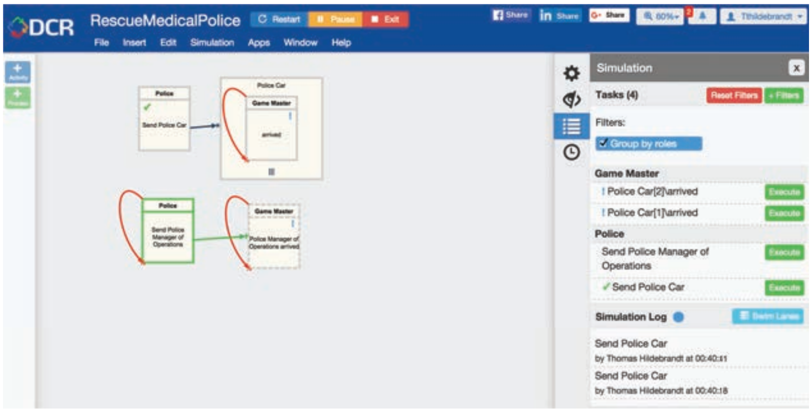
Fig. 2: After incident has happened it is excluded, and the three events at the Remote Control Central are required and enabled.

3. Modelling and Simulating the Emergency Response Process as a DCR Graph

Dynamic Condition Response (DCR) graphs are a particular constraint-based process modelling notation[6,2]. A DCR graph consists of a set of *events* (the nodes of the graph) and five different kinds of directed edges between events that declare respectively *condition*, *response*, *milestone* and dynamic *inclusion* and *exclusion* relations. Each event is labelled by an *activity name* and a set of *roles*. An event may be atomic or nesting. An atomic event represents an atomic activity that can be triggered by one of the roles assigned to the event. A nesting event is an event containing other events and faciliates grouping and shorthand notation: And edge to (from) a nesting event correspond to having the edge to (from) all the nested events. Finally, the state of a DCR Graph is given by a *marking*, which describes for each atomic event wether it has happened, wether it must happen again in the future and wether it is currently included. We will explain the meaning of the different relations now, while describing parts of the process.

The emergency response process covers 7 key organisational units: The Remote Control Central (central control of train traffic), the Train Service Operations Watch, the Emergency Call Center (112), the Bridge Control Central, the Police, the Local Rescue Team, and the Medical Emergency Staff. Within the latter three units we further have a Manager of Operations role and the Police unit in addition has a First Response role (first police car sent). Finally, we added for the rehearsal a Game Master role, controlling external events included in the script for the rehearsal (e.g. train leaking oil, passengers calling the alarm central, etc.).

To model what each role can do, we add events and constraint relations between them. The process is started by an *incident* event played by the Game Master role. The incident event should only happen once, and always as a response trigger three events performed by the Remote Control central: Stop the traffic, call the Emergency Call Center, call the train service operations watch. We model this as shown in Fig. 1. by adding an exclusion relation from the incident



Simulation

Tasks (4) Reset Filters + Filters

Filters:

☑ Group by roles

Game Master

! Police Car[2]\arrived Execute

! Police Car[1]\arrived Execute

Police

Send Police Manager of Operations Execute

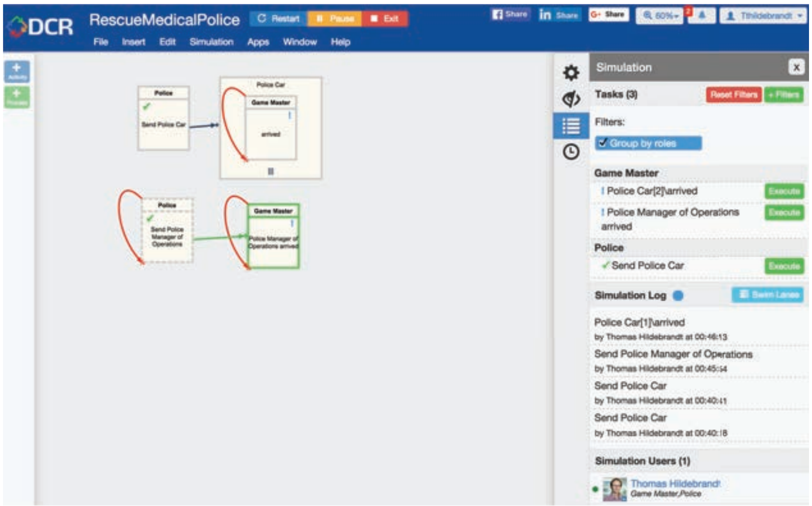
✓ Send Police Car Execute

Simulation Log ● Swim Lanes

Send Police Car
by Thomas Hildebrandt at 00:40:41

Send Police Car
by Thomas Hildebrandt at 00:40:18

Fig. 3: Two police cars sent.



Simulation

Tasks (3) Reset Filters + Filters

Filters:

☑ Group by roles

Game Master

! Police Car[2]\arrived Execute

! Police Manager of Operations arrived Execute

Police

✓ Send Police Car Execute

Simulation Log ● Swim Lanes

Police Car[1]\arrived
by Thomas Hildebrandt at 00:46:13

Send Police Manager of Operations
by Thomas Hildebrandt at 00:45:54

Send Police Car
by Thomas Hildebrandt at 00:40:41

Send Police Car
by Thomas Hildebrandt at 00:40:18

Simulation Users (1)

Thomas Hildebrandt
Game Master,Police

Fig. 4: First police car arrived and manager of operations sent.

event to itself (meaning that it gets excluded once it happens) and a response relation (shown in blue with a dot at the source) from the incident event to a nesting event containing the three events to be handled by the Remote Control Central (RCC), meaning that once the incident happens, the RCC must (eventually) stop the traffic, call the emergency call center and the train service operaitons watch. To limit the possible flows of the process (and rehearsals) we also add a condition relation (shown in orange with a dot at the end) which means that the incident is a condition for all three events at the RCC, and thus the events only get enabled after the event. Fig. 1 shows the result of starting the simulation: Only the incident event is enabled and Fig. 2 shows the result of executing the incident event, where the three events at the RCC is enabled. There is a recommended order of the activities, but in order to serve as a rehearsal testing if participants of the rehearsal know the order we did not model the order explicitly.

The Emergency Call Center is responsible for calling the Police, the Local Rescue Team, and the Medical Emergency Staff. These three units have similar reactions as shown in Fig. 3: They should all send response vehicles (e.g. police cars, rescue cars and ambulances respectively, and also send a Manager of Operations. We here also add events for the arrival of the response vehicle and Manager of Operations (played by the Game Master). We spawn a new arrival event using a multiple instance sub process for each response vehicle send, while we only need a single event for the arrival of the manager of operations, since only one such is send.

The constraint based modelling notation differs from traditional flow-based notations in that we do not specify a strict ordering of events, but rather specify the events of the system in question and the relations between them, e.g., which events enable and disable which other events, which events are required for other events to happen, and which event requires other events to happen in the future. The constraint-based approach proved particularly fruitful for emergency response planning. Emergencies tend to be highly fluid situations, and the appropriate response vary wildly with the actual circumstances of the emergency. The constraint-based approach encompasses all this fluidity and flexibility, both by allowing repetition of events (e.g., it is perfectly possible to decide to send additional police cars by simply invoking the "Send Police Car" event more than once. Similarly, because there is no strict sequencing, one may in simulation pretend to have a lax operator tardily send ambulances by simply waiting to take the corresponding action. The rest of the model is *not* blocked by this lack of actions, except of course for those specific actions that depend on the presence of ambulances.

We conclude from the modelling exercise that the formal modelling of emergency response plans has definite and very concrete benefits for practitioners; chiefly in identifying using simulation unfortunate hidden behaviour in the original paper plans.

Simulation study. We carried out two simulations of the final formalised plan with students from the Metropolitan University College. They are trained in Emergency and Risk Management, but they did not know the particular rehearsal script beforehand. At the first simulation, each student played a single role. The simulation had to be quickly aborted, since the actors lost overview of what had happened. The loss of overview was caused by several factors: (1) the tool suppressed detailed descriptions of past activities. (2) Each activity was visible to everyone in the log which meant that the actors got informed of events that they were not supposed to know about. A call to the Alarm Central (911), for instance, should only be visible to the caller and the Alarm Central. (3) It took several seconds to update the user-interface on every screen each time a user performed an action, and no other action could be carried out while waiting for the update. This meant that there was an unnatural race for being allowed to perform updates.

In the second simulation the students were divided into sectorial groups corresponding with the 6 key roles. Each group than had only one PC available. The students discussed their next action in advance and sought others groups inaction; this reduced the problem of the slow interface; however, the other two problems remained.

Besides simulation with the students we made a simulation with domain experts at the Danish Railways (DSB). It was carried out with the main emergency responsible person from DSB and a train-driver instructor. Each expert played several roles during the simulation. Again, the roles were assigned after the 6 key roles and the game-master role was also in use. There were few problems with the slow interface, yet it is not possible to perform more actions simultaneously. Actors should be aware of this during the simulation, because their activities often resulted in another series of activities and these activities may not be enabled if the previous action was not recorded. After the simulation the two experts came up with several recommendations: (1) Use pictures or small movie clips to support that the actors get the same operational overview of the incident. (2) Add the ability to read the emergency handbook and other emergency documents during the simulation. (3) Clarify the assigned roles and possible activities in the simulation. (4) Add the ability to associate text with event-export; they should be able to document their activities immediately.

In summary, the simulation studies showed that the tool can be used to collaboratively perform a process rehearsal trying out alternative paths, and thereby also reveal potential weaknesses or opportunities in the process. At the same time the simulation studies showed that the tool can be used for both teaching and exercises in various contexts. An important and recurrent evaluation point after major emergency incidents is the lack of communication and a common scenario understanding between actors and across sectors, e.g. see[7,8] for evaluations of emergencies in Denmark (in danish). Via the logging function the tool can document the time and order of the communication process. (1) It is for example possible to practice and control certain behaviour patterns in an emergency plan. (2) It is possible to make dialogue-based crisis management exercises, where the focus- and learning-points are the cooperation across sectors and coordination of the overview of operational activities of the incident.

However, the simulation studies also showed three needed improvements of the modelling formalism and simulation tool, which fortunately are not difficult to carry out: (1) It should be possible to get detailed information about events in the event log, e.g. by clicking on the entry in the event log. (2) It should be possible that events can also be annotated by the roles that can observe the execution and not only as it is now by the roles that are allowed to execute it. (3) The execution of an event should not block execution of independent events by other users. This can be remedied by the technique to infer independence of events given in[9].

4. Conclusion and Next Steps

We reported on the experiences from a case study during which the constraint based DCR graphs notation and simulation tool DCRGraphs.net was applied for the collaborative modelling and simulation of a railway emergency response plan and rehearsal process jointly with domain experts. The study confirmed the use of the approach to capture emergency plans jointly with domain experts, and that the constraint based approach and tools allow for the collaborative simulation and exploration of expected paths and scenarios as well as unexpected paths not described in the existing paper-based plans and rehearsal processes. It also helped identifying limitations in the DCR graphs modelling notation and simulation tool with respect to using it for collaborative real-time rehearsals, notably responsiveness of the user interface, the possibility to include additional information about past activities in the log and the possibility of hiding activities in the log depending on the role of the user.

The next step will be to investigate the use of the models as basis for eliciting dependencies on ITC following an approach similar to the one reported in[10]. In particular, we intend to present the emergency models for the key persons responsible for it services and security and involve them in the elicitation as suggested in[10]. In addition to that, we intend to research extensions to the DCRGraphs.net tool and DCR graph notation to eliminate the three observed problems. That is, to make it possible to read detailed descriptions of past events, allowing for limiting the visibility of events (such that they are not shown to everyone in the log) and implementing a better support for concurrent execution of independent events possibly exploiting results on inference of independence between events[9].

Acknowledgements. We gratefully acknowledge collaboration and support of DSB staff, especially from Brian Nygaard Jensen, the Metropol students participating in simulation, and the support of the Royal Danish Defence College.

References

1. Shen, S.Y., Shaw, M.J.. Managing coordination in emergency response systems with information technologies. In: *Tenth Americas Conference on Information Systems*. New York; 2004:2110–2120.
2. Mukkamala, R.R.. A formal model for declarative workflows - dynamic condition response graphs. Ph.D. thesis; IT University of Copenhagen; 2012.
3. Hildebrandt, T., Mukkamala, R.R.. Declarative event-based workflow as distr. dynamic condition response graphs. In: *PLACES*; vol. 69 of *EPTCS*. 2010:59–73.
4. Debois, S., Hildebrandt, T., Slaats, T.. Safety, liveness and run-time refinement for modular process-aware information systems with dynamic sub processes. In: *FM 2015*. No. 9109 in LNCS; Springer; 2015:143–160. doi:`10.1007/978-3-319-19249-9_10`.
5. Debois, S., Hildebrandt, T.T., Marquard, M., Slaats, T.. Hybrid process technologies in the financial sector. In: *BPM '15*. 2015:107–119. URL: `http://ceur-ws.org/Vol-1439/paper9.pdf`.
6. Pesic, M., van der Aalst, W.M.P.. A declarative approach for flexible business processes management. In: *Proc. of the 2006 international conference on Business Process Management Workshops*. BPM'06; Springer-Verlag. ISBN 3-540-38444-8, 978-3-540-38444-1; 2006:169–180. URL: `http://dx.doi.org/10.1007/11837862_18`. doi:`10.1007/11837862_18`.
7. Beredskabsstyrelsen, . Beredskabets indsats i forbindelse med orkanen 8. januar 2005 en tværgående erfaringsopsamling. 2005. `https://brs.dk/viden/publikationer/Documents/Orkanrapport_8januar2005.pdf`.
8. Brandvæsen, K.. Erfaringsopsamling og evaluering af københavns brandvæsens operative håndtering af skybrud 31. august. 2014. `http://www.brand.kk.dk/Aktuelt/Presse/Nyhedsoversigt/2014/~/media/Files/Publikationer/Evaluering_Skybrud31082014_24okt2014.ashx`.
9. Debois, S., Hildebrandt, T.T., Slaats, T.. Concurrency and asynchrony in declarative workflows. In: *BPM '15*; vol. 9253 of *LNCS*. Springer. ISBN 978-3-319-23062-7; 2015:72–89. URL: `http://dx.doi.org/10.1007/978-3-319-23063-4_5`. doi:`10.1007/978-3-319-23063-4_5`.
10. Sandkuhl, K., Matulevicius, R., Ahmed, N., Kirikova, M.. Refining security requirement elicitation from business processes using method engineering. In: *BIR '15*; vol. 1420 of *CEUR Workshop Proceedings*. CEUR-WS.org; 2015:98–109. URL: `http://ceur-ws.org/Vol-1420/scbp-paper1.pdf`.