Local Success, Global Failure: Challenges Facing the Recovery Operations of Critical Infrastructure Breakdowns

A. Cedergren
Division of Risk Management and Societal Safety, Lund University, Sweden

J. Johansson
Division of Industrial Electrical Engineering and Automation, Lund University, Sweden

L. Svegrup
Division of Risk Management and Societal Safety, Lund University, Sweden

H. Hassel
Division of Risk Management and Societal Safety, Lund University, Sweden

ABSTRACT: Many of society's critical infrastructures have become increasingly interconnected. At the same time they have also faced a substantial institutional fragmentation. These trends are clearly visible in the Swedish railway system. While previous research has shown that many critical infrastructures, despite significant re-organisations, operate at a remarkable high reliability, this paper highlights the negative effects of increased institutional fragmentation once these types of critical infrastructures do break down. More specifically, the paper shows that the strive towards increased efficiency and cost-effectiveness within each organisation involved in the recovery operations following infrastructure breakdowns in the Swedish railway system also creates an overall more complex and time-consuming recovery of the functioning of the system as a whole. In this sense, each organisation achieves local success in terms of increased efficiency, but also contributes to global failure in the terms of problems of sustaining and quickly restoring railway operations.

1 INTRODUCTION

Many of society's vital functions and services (such as power supply, telecommunications, and transportation) have become increasingly interconnected (Amin, 2001). While this gives rise to increased efficiency, tighter connections also invites increased vulnerability and the risks of cascading failures (Ansell, Boin, & Keller, 2010; Rinaldi, Peerenboom, & Kelly, 2001). Moreover, at the same time as many of these vital systems have become increasingly interdependent, they have also faced a substantial institutional fragmentation (de Bruijne, 2006). Despite significant re-organisations, previous research has shown that many critical infrastructures operate at a remarkable high reliability (de Bruijne & van Eeten, 2007). However, limited attention has been placed on the effects of infrastructure re-organisations once these types of critical infrastructures do break down, which is the objective of this paper. More specifically, the empirical basis of the paper consists of a case study of the recovery operations following two types of breakdowns of railway transport in Sweden, which are used as a basis to discuss the impact of deregulation and dispersion of responsibility with respect to the recovery of infrastructure systems.

1.1 *Dispersed responsibility in a deregulated market*

The trends involving increased interdependencies as well as institutional fragmentation are clearly visible in the Swedish railway system. As a result of substantial deregulations of the Swedish railway market during the last decades, responsibility for different activities has become dispersed among a variety of stakeholders (Alexandersson, Hultén, Nilsson, & Pyddoke, 2012), which to some extent has given rise to challenges to managing risk and safety (see e.g. Cedergren, 2013a, 2013b). What used to be a state-owned sector has become an institutionally fragmented arena. While responsibility for infrastructure provision in Sweden mainly lies with the Transport Administration, many other activities are open for competition on the free market. These activities include train operation (passenger trains as well as freight trains) and maintenance of trains and rail infrastructure. These contracts are rewarded on lowest price, which naturally means that each bidder has a strong incentive to keep costs as low as possible, while still fulfilling the obligations stipulated in the contract. This commoditization of work related to infrastructure operation (Almklov & Antonsen, 2010) clearly has some unintended side-effects once the infrastructure system breaks down, which we illustrate in this paper with the two case studies as the point of departure. The method used and the empirical data underpinning the case studies are further outlined in the next section.

2 METHOD AND MATERIALS

The data presented in this paper is collected from an analysis of two rather frequently occurring types of accidents and disturbances in the Swedish railway system; breakdown of traction power lines and unauthorised persons on railway premises (which often are related to suicides). In both types of events, a number of stakeholders are involved in the response and recovery operations. Data collection has been conducted by interviews involving the most relevant stakeholders, including representatives from the Transport Administration (people representing three different organisational branches, including safety department, operations coordinator, and maintenance manager), three of the main passenger train operators, rescue service, maintenance contractor, and the regional public transport provider. In total, 8 persons have been included in the study, and some of these persons have been contacted several times (several meetings, or follow-up conversations by telephone or email).

The interviews were conducted by a semi-structured approach, where respondents initially were asked to describe their organisation's role in the two types of disturbances, as well as their view on other organisations' roles during these types of events. As a complement to this description, the respondents were asked to draw a process chart of the actions and events occurring during the two types of disturbances of interest. Although the individual respondents naturally drew on their own experiences from specific accidents and disturbances, focus during the interviews were placed on a general description of these types of incidents, rather than on a detailed account of one specific event. Interviews lasted between 1 h and 30 min to approximately 2 h 15 min. Based on the findings from the interviews, a generic illustration of the normal practice for managing each type of disturbance is outlined in the following section. In addition to the data collected from interviews, media coverage as well as incident investigations conducted by the Transport Administration following these types of events have also been studied.

3 A CASE OF SUCCESS AND FAILURE

3.1 *Unauthorised persons on railway premises*

The first type of event relates to unauthorised persons on railway premises. Sadly enough, this type of event often turns out to be suicides, which unfortunately is a large problem to railways throughout Europe (European Railway Agency, 2013). While acknowledging the fact that this is a terrible tragedy to all parties involved, focus of this paper will be placed on the way this type of event is managed by the professional actors involved in response and recovery activities. In particular, the case is used to highlight the way that local adaptation of these actors affects the resilient performance of the system on the global level.

When a train driver reports an unauthorised person on the railway premises, or that the train has hit someone, first responders (rescue service, police, and ambulance) are called to the site. In addition, an operational manager appointed by the Transport Administration (called the accident site commander) is called to the site. Initially, the event is typically defined as a rescue operation, and the rescue service is responsible for leading the operation. If a person is confirmed deceased (which is judged by the police), the police are responsible for the operation until it has been confirmed that no crime is suspected. When the event no longer is seen as either a rescue operation (no life to rescue), or a criminal investigation (no crime suspected), the accident site commander appointed by the Transport Administration is responsible to lead the recovery operation (although the interviews revealed that responsibility in practice is sometimes unclear). Consequently, whether the event is seen as a rescue operation, a criminal investigation, or a railway disturbance determines who is in charge and what actions are considered most important. This framing of the event is therefore crucial for the overall response, which will be further described in subsequent paragraphs.

At the same time as first responders are heading to the site, the Transport Administration sets up a telephone meeting with the train operators and the regional public transport provider, where information is updated on a regular basis and communicated to passengers on the trains and on the stations as well as on homepages. The train company provides replacement staff to the train in question, and sends a debriefing team to support the train driver. Due to the tight connections characterising railway transportation, this type of event gives rise to significant disturbances in the railway system and therefore leads to substantial re-scheduling work for all affected train operators in the region. In particular, trains that were supposed to operate a specific railway line end up in the wrong location, and can therefore not be used as planned. The same happens to the staff on board these trains, which means that they may need to work extended hours. In this way, they are not allowed to begin their next shift (due to work hour regulations), which calls for further re-planning.

Following a confirmed causality, the body needs to be removed and the track needs to be cleaned before the tracks are taken into use. The police have appointed funeral agencies to move the deceased, and consequently, until this actor has arrived, no operation of the tracks is possible. After moving the deceased, the rescue service is normally appointed by the Transport Administration to provide assistance in cleaning the train and the tracks, until the tracks are finally taken into use. The main stakeholders involved are illustrated in Figure 1, which also gives a brief description of the main activities carried out by each of these actors.

1. Train driver reports unauthorised person on railway premises, or that a person has been hit by the train.
2. Rescue service, police and ambulance are called. An accident site commander appointed by the Transport Administration often arrives to the site, although usually later than the other actors.
3. Replacement staff (train driver and conductors) is sent to the site.
4. Police confirms that the person is deceased, and whether a crime is suspected or not. Police calls funeral agency to remove the deceased.
5. Funeral agency removes the deceased.
6. Rescue service cleans the train and tracks (and in some cases, passengers are evacuated and further transported by bus).
7. Train taken to service.
8. Train operation is resumed.

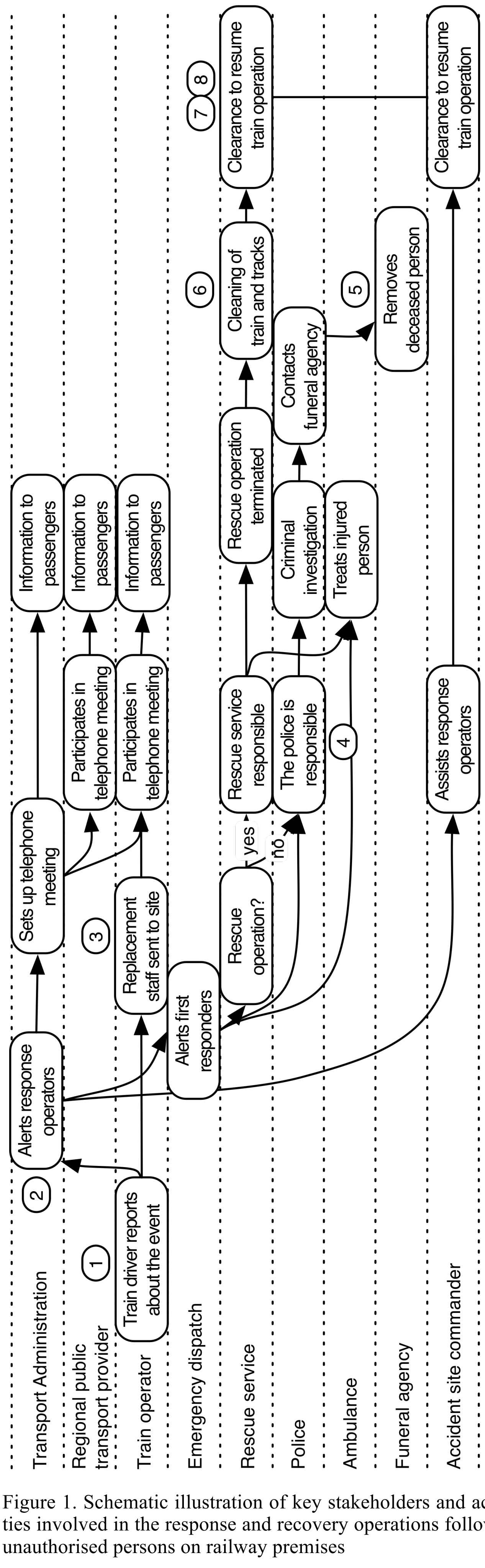

Figure 1. Schematic illustration of key stakeholders and activities involved in the response and recovery operations following unauthorised persons on railway premises

What makes this case particularly interesting is the fact that the various stakeholders involved in response and recovery operations define the event differently (due to their various roles and mandates), and show different adaptation strategies to reach their individual goals. Starting with the rescue service, one of the tasks they are involved in relates to cleaning the train and tracks using their water hoses. Since the traction power line is electrified, there is great danger associated with spraying water high into the air. For this reason, electrical power is often turned off before the cleaning begins, and the power lines are normally earthed in order to ensure safe operations.

Since the rescue service (and in some cases, the same thing has been reported for the police) knows that power usually needs to be turned off at some stage in this type of event, they sometimes make this request at a very early stage. In some cases, this request has been made on the communication radio already before they have reached the site, in order to speed up their line of decisions. If the event is seen as an ordinary rescue operation (from a local rather than global system perspective), this action is fully rational, and enables an efficient response operation. This type of speedy decision-making is clearly in line with what is normally seen as a successful rescue operation; at the same time it guarantees safety (by turning off the power) and efficiency (by making the request already before arriving on site). However, the power system is constructed in such way that power supply to a small section cannot be turned off remotely. This means that when a request is made to the traffic control centre to turn off the power, a large area sometimes involving several railway lines (and subsequently many trains) is affected. Moreover, cleaning of the train and tracks is one of the last things that are carried out on site before train operation is resumed. Before this happens, the deceased person must have been removed from the site. As mentioned above, the police have contracted this task to funeral agencies. In this contract, a maximum time for arrival to the site of up to 2 h is sometimes stipulated, which means that significant time will pass before the body is removed and the cleaning of the train and tracks begins, and hence a long time of unnecessary cut off power to one or several railway lines. If the event is seen as a railway disturbance, it is thus not optimal from a global perspective to turn off the power for a large section of the railway system at an early stage of the response and recovery operation.

Consequently, seen from the perspective of each individual actor involved in the response and recovery of this type of event, they are adapting and making locally rational choices in pursuit of their respective goals. However, as will be further discussed later, these adaptations are sometimes in conflict with the global goals of the system, i.e. the sustained operation of the railway system. This is clear from analysing incident reports (e.g. Swedish Transport Administration, 2012) as well as from media coverage of this type of events, where significant criticism of the handling of these types of events has been raised. Before further discussing the implications in terms of the performance of the system, another example relating to breakdowns of traction power lines is described.

3.2 *Breakdown of traction power lines*

The second type of event relates to breakdown of traction power lines. Traction power lines, i.e. the power lines feeding electricity to the trains, are subjected to continuous wear due to the friction that occurs when the line is in contact with the pantograph on the roof of the train. It is quite common that a train tears down the power line, causing a short circuit, which in turn makes the entire railway line inoperable. In this case, evacuation of passengers is always necessary, since the damages render the train unmovable. Evacuation is carried out by means of buses, which are contracted by the train companies, and time of arrival of these buses depends on the availability of spare buses and drivers, as well as on the time of the day and the location of the incident. Due to the potential danger of coming into contact with the live power line that has fallen down, passengers are not allowed to evacuate the train until the site has been secured. In order to do this, and to restore the railway infrastructure, the Transport Administration has engaged maintenance contractors for different areas of the railway infrastructure. In the contracts, maximum times until arrival to the site are specified, ranging from 30 min to 120 min (depending on, for example, if the railway line is located in an urban or rural area). Once on site, maintenance contractors secure the site, and evacuation by buses can be initiated. In the same way as described with unauthorised persons on railway premises above, this type of event gives rise to significant disturbances in the railway system, and therefore leads to substantial re-scheduling work for all affected train operators. The activities carried out by each of the relevant actors are schematically illustrated in Figure 2.

1. Train driver reports that the traction power line has been torn down.
2. Maintenance contractor is called. Time to arrival between 30 to 120 min after being called.
3. Site secured and passengers allowed to evacuate to buses.
4. Restoration work undertaken and train is towed to service.
5. Train operation is resumed.

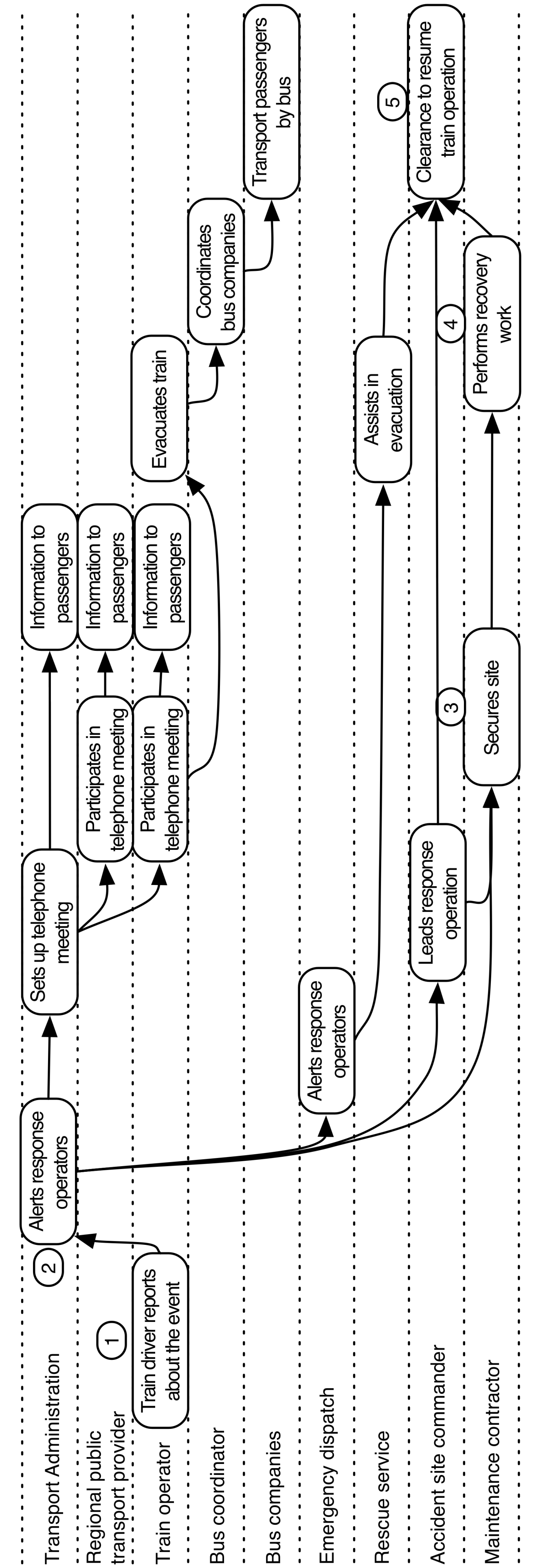

Figure 2. Schematic illustration of key stakeholders and activities involved in the response and recovery operations following a breakdown of a traction power line

From a micro-level point of view, it is interesting to highlight the way maintenance contractors have managed to strike a balance between economy and productivity. Based on the respondents' accounts, it appears that the maintenance contractors have optimised their response in such way that they often arrive to the site just before the specified time of arrival to the site expires. In other words, this time sometimes amounts to almost 2 hours after they have been called. As a matter of fact, an alleged strategy to meet established time limits is to send someone to the site just within required time limits in order to report to the contractor that staff is on site (which is defined by the contract), notwithstanding this person (according to some respondents) does not have the right competence to actually carry out the required work. This means that additional time passes until persons with the relevant qualifications reach the site. During this time, passengers are not allowed to leave the train, regardless of whether the train has stopped near a station (which on several occasions has given rise to outcries among passengers being stuck on trains, and these occurrences have been heavily covered by media, see e.g. Sydsvenskan, 2014). Once the site has been secured, the actual restoration work normally takes an additional 6-8 hours in an uncomplicated case, while a lot longer in difficult cases.

4 LOCAL SUCCESS, GLOBAL FAILURE

From the brief descriptions of response and recovery activities relating to the two types of railway accidents and disturbances outlined in the previous sections, it can be concluded that a number of actors are successful in solving their individual tasks on the local level. For example, the rescue service and the police are reported to demand a non-electrified traction line, even before they reach site. This guarantees a safe workplace and enables more rapid decision-making once on site, and can therefore be seen as a characteristic of a successful response from their point of view. However, when the power is turned off, disturbances propagate to a large part of the railway system. Thus, many trains (and passengers) are left standing on the tracks for a substantial period of time, obstructing railway services in a large part of the railway system and causing global failure. To maintenance contractors, success is at least partly measured in terms of the ability to meet the requirements of the contract in as cost-effective ways as possible. These contracts specify a maximum time until arrival to the site and unless the maintenance staff manages to meet this time limit, the contractor runs the risk of being fined by the Transport Administration for not fulfilling the contract. In this way, the ability to meet their time limits is ultimately one of their key indicators of whether the operation is deemed a success or a failure..

To a large extent, the various actors are successful in meeting the demands of their respective organisations, e.g. in terms of safety goals as well as productivity goals. However, interdependencies between the organisations' different tasks (and their different, sometimes even conflicting goals) create failures on the global level, in terms of problems of sustaining and quickly restoring railway operations (which is not the primary goal of any of the individual actors). This means that there is no single root cause to the sub-optimal outcome described above. Rather, the main challenge can be referred to as a problem of multi-actor coordination in a system characterised by several sub-contractors and dispersed responsibility. Since the goals of the various stakeholders largely are established from a local point of view, there are few incentives for each operator to ensure resilient rail operations for the system as a whole.

The different adaptation strategies have in common that they strive for increased efficiency from their individual point of view. Each stakeholder normally only consider a limited part of the system in question, and adjustment and optimisation of their performance thus occurs locally. Gradual deregulation of the Swedish railway system has resulted in institutional fragmentation, with an increased number of different stakeholders who individually optimise their work in pursuit of local goals. However, the more fragmented system, the larger becomes the resulting co-ordination problem (see e.g. Kramer, 2005). Consequently, although each stakeholder may become increasingly specialised and efficient in solving their respective tasks, the institutional fragmentation may have unintended side-effects that are not clearly visible from the individual players' points of view. More specifically, the division of roles and responsibilities means that they sometimes work at cross-purposes. Each stakeholder is locally adapting to changing conditions in their strivings for success, which does not seem to be clearly correlated with the uninterrupted operation of the system as a whole (cf. Branlat & Woods, 2010).

The problems related to response and recovery operations following railway disturbances do not mean that institutional fragmentation of critical infrastructure is a predominantly negative trend, or that CIs should be owned and operated by a single, central agency. Rather, this case study points at the fact that coordination and mutual understanding between the multitude of actors involved in the operation and restoration of these systems invokes some important challenges. Due to their diverse goals and mandates, it becomes important to share knowledge among the various stakeholders about the ways that each organisation's actions may affect the conditions for others as well as for the functioning of the system as a whole.

Local adaptation and optimisation clearly invokes a risk of sub-optimisation at the level of the system as a whole (such as the operation of a railway system), and possibly reduces the incentives to take proactive actions to avoid failures on the global level. One of the most important countermeasures to limit the potentially negative side-effects of this development therefore relates to the need for increased understanding of each other's roles and responsibilities among the various actors involved in response and recovery operations. The interdependencies between the tasks carried out by different actors may not be clearly visible to each one of them, and for this reason there is room for increasing the joint understanding of the tasks carried out by all other actors.

5 CONCLUDING REMARK

While previous research has reported that institutionally fragmented critical infrastructures operate at a remarkable high reliability, this paper raises a concern over the negative effects of increased institutional fragmentation once these types of critical infrastructures do break down.

As described in this paper, a number of different stakeholders are involved in the response and recovery operations following failures and disturbances in the Swedish railway system. The goals of these stakeholders are to a large extent established from a local point of view, and accordingly, there are few incentives for each operator to ensure uninterrupted rail operations for the system as a whole. In this way, the institutional fragmentation may have unintended side-effects that are not clearly visible from the individual players' points of view. The division of roles and responsibilities means that they sometimes work at cross-purposes, and the interdependencies between the different stakeholders' tasks create failures on the global level in terms of problems of sustaining and quickly restoring railway operations. These challenges point at the need for improved coordination and mutual understanding between the variety of actors involved in this type of operations.

REFERENCES

Alexandersson, G., Hultén, S., Nilsson, J.-E., & Pyddoke, R. (2012). *The Liberalization of Railway Passenger Transport in Sweden - Outstanding Regulatory Challenges*. CTS Working Paper 2012:5. Stockholm.

Almklov, P. G., & Antonsen, S. (2010). The Commoditization of Societal Safety. *Journal of Contingencies and Crisis Management*, *18*(3), 132–144.

Amin, M. (2001). Toward Self-Healing Energy Infrastructure Systems. *IEEE Computer Applications in Power*, *14*(1), 20–28.

Ansell, C., Boin, A., & Keller, A. (2010). Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. *Journal of Contingencies and Crisis Management*, *18*(4), 195–207.

Branlat, M., & Woods, D. D. (2010). How do Systems Manage Their Adaptive Capacity to Successfully Handle Disruptions? A Resilience Engineering Perspective. *Complex Adaptive Systems —Resilience, Robustness, and Evolvability, Proceedings From the Association for the Advancement of Artificial Intelligence Conference, Arlington, 11-13 November 2010*.

de Bruijne, M. (2006). *Networked reliability: Institutional fragmentation and the reliability of service provision in critical infrastructures*. Doctoral Thesis. Delft University.

de Bruijne, M., & van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management*, *15*(1), 18–29.

Cedergren, A. (2013a). *Exploring the Railway System from a Risk Governance Perspective*. Doctoral Thesis. Lund University, Sweden.

Cedergren, A. (2013b). Designing resilient infrastructure systems: a case study of decision-making challenges in railway tunnel projects. *Journal of Risk Research*, *16*(5), 563–582.

European Railway Agency. (2013). *Intermediate report on the development of railway safety in the European Union*. Valenciennes.

Kramer, R. M. (2005). A Failure to Communicate: 9/11 and the Tragedy of the Informational Commons. *International Public Management Journal*, *8*(3), 397–416.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25.

Swedish Transport Administration. (2012). *Utredningsrapport 2012-03-23, Arlöv Personpåkörning (In Swedish) [Investigation report Collision with person in Arlöv 2012-03-23]*.

Sydsvenskan. (2014). Tågpassagerare satt fast i timmar i onödan (In Swedish) [Train passengers were unnecessarily stuck for hours].