El Metodo
Managing Risks in Value Chains

Maarten Hoeve · Rieks Joosten · Edwin Matthijssen ·
Caroline van der Weerdt · Reinder Wolthuis

TNO
Netherlands Organization for Applied Research
www.tno.nl
{maarten.hoeve | rieks.joosten | caroline.vanderweerdt | edwin.matthijssen |
reinder.wolthuis}@tno.nl

Abstract

The ability to organize resource-allocation on the basis of actual need allows a business to become highly flexible, cost efficient and robust against crises. Doing so requires that functionalities and the associated responsibilities are properly defined, delegated to other parties where needed, and checked to ensure that the risks involved remain at an acceptable level. A framework called 'El Metodo' is presented that helps organizations do just that. Also, a simple use-case illustrates how 'El Metodo' supports the construction of an early-warning system that signals risks that become unacceptably high due to causes elsewhere in the resource chain. Finally, we present an overview of what businesses have to say about this method.

1 Introduction

Even though there is a lot of guidance with respect to (IT) risk management (e.g. [STGF02], [ISO31000], [ISF11]), its practice is generally still cumbersome. First, a comprehensive overview of (shackles in) value chains within an organization is rare as businesses become more service-oriented and hence complex. Consequently, it is difficult to determine what should be agreed upon in service level agreements (SLA's) between services adjacent in a value chain. When things turn sour, this can easily lead to finger-pointing. Secondly, risk management usually receives management attention when major incidents have occurred, but this attention wanes when the incident has been solved. Also, organizations may spend so much time continuously recovering from smaller incidents, that setting up risk management in a structured fashion doesn't seem to be an option. Finally, even when risks may be managed 'locally', solutions may not be optimal if the risks that adjacent shackles run (or manage) are not properly communicated.

Main features of the economy are the specialization and the division of work (e.g. [Sabe82], [PiSa90]). This is usually done by dividing companies into business units, departments or teams, each with their own responsibility. It also requires close cooperation and coordination. A well-known example is a production chain, where several companies or departments contribute until the product is complete. Another example is the supply chain that results in electrical energy being delivered to a wall outlet. Risk management across such value chains requires a clear delineation of the responsibilities between the shackles of value chains, so that risks (and the mitigation

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 1-10

thereof) can be explicitly assigned. Also, it requires a clear understanding of how the various shackles interoperate and cooperate to produce the final product, so that risks related to misunderstandings between shackles can be pinpointed.

El Metodo is a framework that helps to sort out the shackles, to assign responsibilities in case of disagreement, and to provide a clear understanding of how shackles interact with one another. Also, it provides managers with a means to do risk management within a shackle and relate that to the risks (and the management thereof) of 'adjacent' shackles. When multiple shackles decide to share risk information, El Metodo provides the basis for an early warning system that allows managers to be informed as risks start to 'line up', which may result in a catastrophe if not treated immediately.

This article is built up as follows. First, we introduce the basic concepts of El Metodo and illustrate them with examples. Then, using the same examples, we show how risk management is done both within functionalities and in value chains. using the same examples. This is followed by a discussion of the method, a specification of work to be done and conclusions.

2 El Metodo - the Method

To get a grasp on the division of work, El Metodo defines a functionality (a shackle in a value chain) as a coherent set of obligations, and a manager[1] that is responsible for fulfilling them. Functionalities come in many kinds: a company, a business unit or department, an information process, an IT system (or application), or even a project. Functionalities should be properly scoped, meaning that they should be distinct, and manageable.

The latter is important as managers, like all humans, have physiological limitations that make them err more as the scope grows [Mille56]. Therefore, functionalities with a scope whose size exceeds that what is humanly manageable, should be decomposed, resulting in (subsidiary) functionalities, each with its own obligations and its own manager. 'Outsourcing' these functionalities to their respective managers makes the scope of the outsourcing functionality smaller. Splitting of subsidiary functionalities should continue until the remaining scope has become manageable for its manager.

2.1 Designing Functionalities

Consider a functionality that provides IP-connectivity between various locations. Its manager defines the functionality by creating a list of its obligation, i.e. criteria or rules for the fulfillment of which he is responsible to some other functionality. Examples:

- IP-connectivity is provided for at least 99.9% of the time.
- IP-connectivity services comply with the Data Protection Act.
- Annual revenue of IP-connectivity is at least € R and annual costs are at most € C.

A manager can only meet his obligations if he can rely on some expectations to be fulfilled, either within his own scope of control (internal expectations) or by some other functionality (external expectations). The method requires that for every obligation of importance, the manager makes every expectation explicit that need to be fulfilled in order for him to fulfill the obligation. As an

1 We use the term ‚manager' to also include a management team.

example, the manager of the IP-connectivity functionality may associate the following expectations to the obligation that IP-connectivity is provided for at least 99.9% of the time:

- Every router has an availability of > 99.95%.
- At any time, every router is either powered by Energy Co, or by its UPS
- Routers X and Y are connected with two glassfiber networks (the A-net and B-net)
- At any time, either the A-net or the B-net is operational (or both).

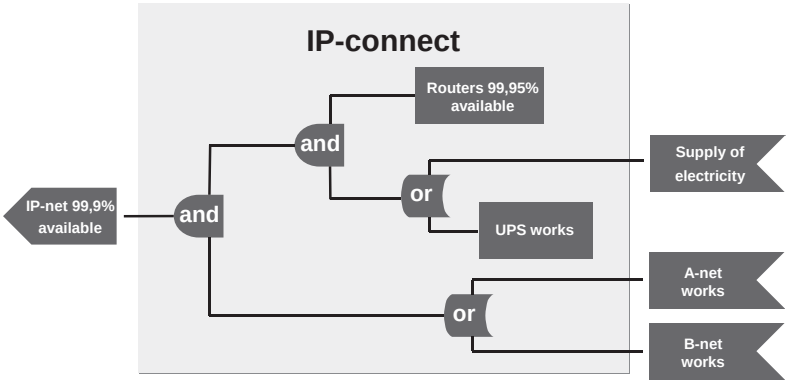

Fig. 1: Linking Expectations and Obligations

From the overview that the manager gets by linking expectations and obligations, he can judge whether or not he can fulfill his obligations.

Besides managing single functionalities, the method also helps to get a grip on the value chain by linking obligations and expectations of *different* functionalities. Every expectation of one functionality to another must correspond with an obligation of that other functionality to the expecting one. Signaling any lack of such correspondence allows the managers to take appropriate action and align their functionalities. Thus, there is no confusion later on about who is responsible for what.

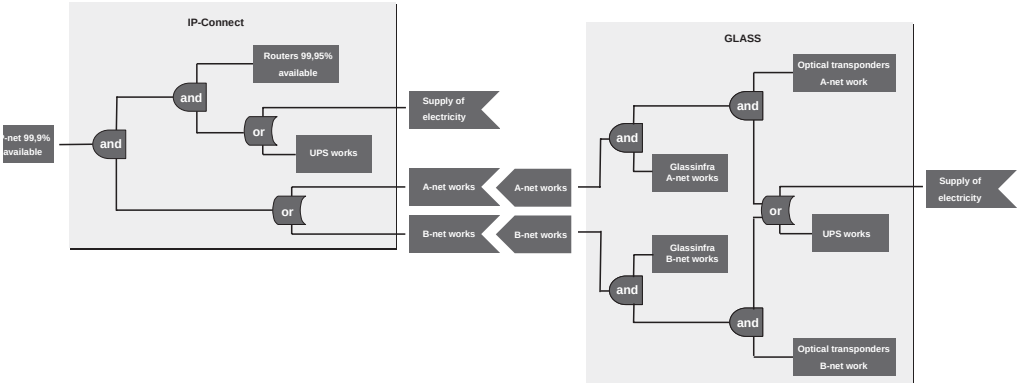

Fig. 2: Linking Obligations and Expectations Between Functionalities

Figure 2 illustrates the linking of expectations of the functionality 'IP-connect' with obligations of the functionality 'Glass'. Not only does this provide insight in functional dependencies, it also helps to (partly) automate risk management, as we shall see in the next section.

2.2 Managing Risk in Functionalities

Within organizations, risk management may take different forms, depending on the subject (financial, information, environment, health and safety, continuity), or the time horizon (long-term, medium term and short term) or hierarchical levels (e.g. organization, business unit and division). Many standard process models or frameworks provide guidance, such as ISO31000, MoR, ISO27001, BS25999 etc.

Roughly speaking, traditional risk management consists of determining the scope within which to manage risks and make an inventory of the (most important) risks within that scope. This is done by identifying threats, estimating the probability of occurrence and computing the risk using "Risk = Probability x Impact" (R=PxI). Then, the nature of these risks is assessed upon which it is decided to either accept them or choose and implement controls to mitigate them[2]. As this modifies the threats, probabilities and thus risks, the cycle starts again, until all remaining risks are accepted.

El Metodo equates functionalities with risk management scopes. Thus, every manager of a functionality runs his own risk management process. The idea behind this is that risks are limited to this scope, and the manager has the best knowledge for this.

Once the expectations, obligations and their interdependencies have been identified, they can be used to identify risks. Failure to fulfill a particular obligation constitutes a threat to a scope. For example, failure to fulfill "compliance with the Data Protection Act" is a threat as it may cause the government to impose a fine. Also, any expectation that is not fulfilled constitutes a threat to every obligation to which it is important. Thus, the charted obligations and expectations allows managers to estimate the probability of non-fulfillment, and associate a risk to each of them using the traditional formula R=PxI. Completeness of the risk assessment depends on completeness of the lists of obligations, expectations and their dependencies.

Changes in environmental conditions, customer numbers, laws and regulations all may cause changes in the list of obligations, expectations and dependencies. Therefore, it is necessary to update such lists every once in a while, which is readily complemented with an update of the estimates of likelihoods and risks.

Once obligations, expectations and dependencies are charted, risks can be computed using the traditional formula R=PxI. Determining probabilities and impacts is different for obligations and expectations.

The probability associated with an expectation of a manager is an estimate of the expectation not being fulfilled. For an internal expectation this is the probability something is wrong within the scope itself and should be readily assessable by the manager. For an external expectation, we may assume that there is an obligation of another functionality that corresponds with the expectation. Then, the probability associated with the expectation equals the probability of the other

2 Strictly speaking there are 2 other options, but they are not relevant for our purpose.

functionality not fulfilling its (corresponding) obligation. Ideally, this probability would be communicated so that the probability of the external expectation going sour is 'automatic'. However, if the manager of the other functionality is reluctant to share this information, the manager can estimate the likelihood himself basing it on trust, past experience, performance reports and/or audits.

The probability associated with an obligation of a manager is an estimate of the obligation not being fulfilled. When the dependencies between obligations and expectations are well-charted, the probability of not fulfilling an obligation can be derived using the probabilities of the expectations of which it depends, using dependency functions resembling those of Fault Tree Analysis.

The impact of an obligation is a measure of the maximum severity of the consequences of non-compliance with that obligation (disregarding any implementation knowledge). Managers assess the impact themselves; they may relate this e.g. to penalties as specified by law, penalties agreed in SLA's with customers, or morale. The impact of an expectation is an indicator of the importance of the expectation to the scope as it is derived from the impacts of all obligations to which the expectation is relevant.

Risks for every obligation and expectation can be computed based on their respective impacts and probabilities. Note that for management, qualitative measures such as Low/Medium/High, or number ranges (as done by the ISF) are useable. However, we also envisage that quantitative measures can be used in conjunction with qualitative assessments. After all, every scope will be able to produce a mapping between quantitative and qualitative measures as this mapping is, and remains, particular to that scope. We will use the characters L, M and H to denote Low, Medium and High respectively as we proceed with an example.

3 Putting El Metodo to Use - an Example

Looking back to the IP department of which the expectations and obligations have been linked, we see that failure of the "99.9% availability" obligation would have major consequences. Thus, the manager estimates the impact of this obligation as 'H'. The manager knows that the routers and UPS are very reliable, and hence sets the corresponding probabilities to 'L'. Since power is know to fail sometimes, he sets the probability to 'M'. Finally, the department 'Glass', which provides the physical connection between the routers, provides probabilities for all expectations towards that department. This results in the following overview:

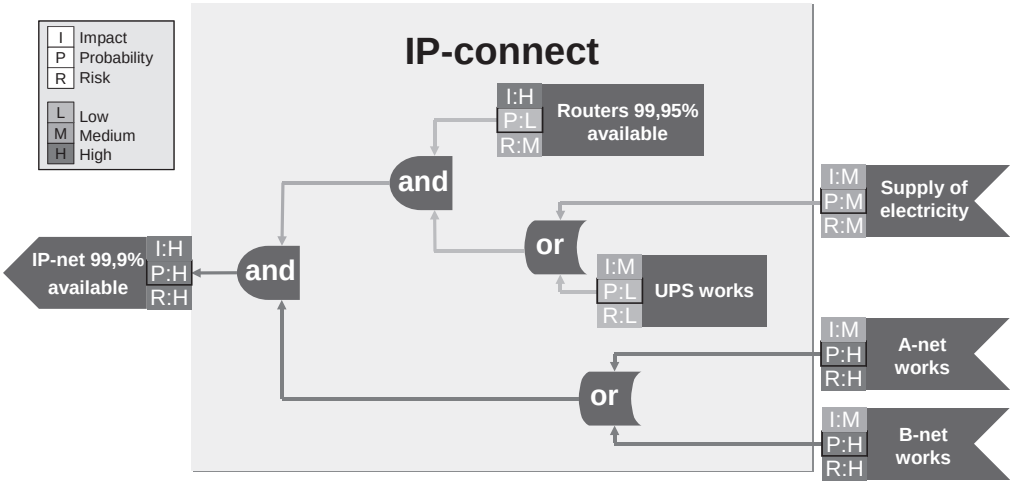

Fig 3: Computation of probability associated with an obligation

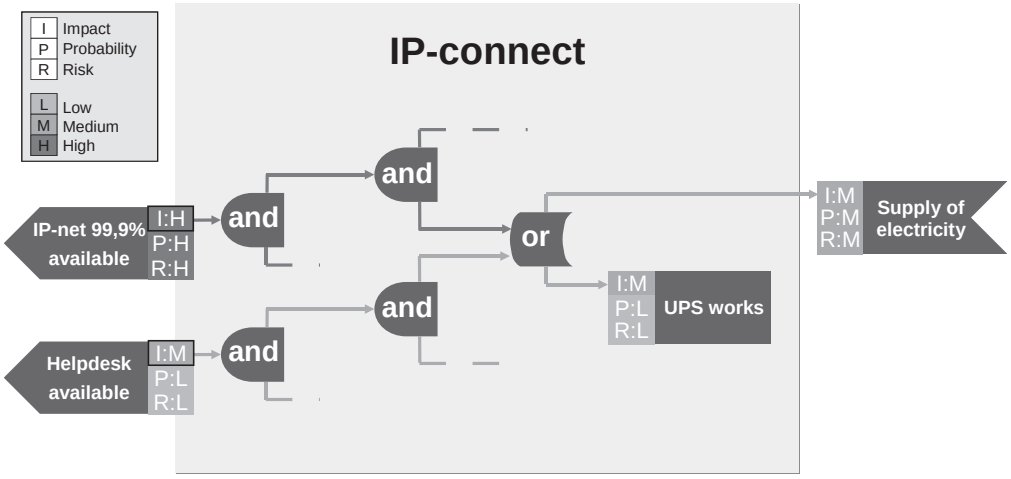

Fig 4: Computation of an impact associated to an expectation.

When a manager has computed the risks and finds one or more unacceptably high, he must take measures. If a risk associated with an external expectation is too high, he may decide to find a second supplier, a replacement supplier, or voice additional expectations to the supplier that will enhance its trust in the expectation being met. If a risk is associated with an internal expectation, the manager must reorganize the work within its own scope of control. If the risk associated with an obligation is too high, he may either search for causes - to be found in the set of expectations of which the obligation depends - adding or modifying this set until the risk becomes acceptable. Alternatively, he may do some 'expectations management' with the parties to which he has the obligation. The manager is free to choose between all of these options, as that is what his job consists of: taking responsibility for compliance with its obligations. Also, it helps to structure the negotiations between (managers of) different scopes.

In the example, the risk that the obligation can not be realized is unacceptably high. The manager sees that the problem is caused in the department 'Glass'. He will first consult with its manager to see if the problem can be solved. If not, he may look for another supplier for the glass network, or he manage the expectations of the customers of the IP network.

Ideally, scope managers communicate the probabilities of their obligations to the scopes that depend on them. Then, a chain (or better: web) of functionalities can be modeled and corresponding risks computed automatically. Especially for scopes within a single company this should be feasible because the required transparency is readily achievable. Communication of probabilities between scopes in different companies may not be that easy. However, the method still works, although scope managers will need to assess the probabilities of external expectations themselves.

Note that if all managers in a value chain really cooperate, they could see the effects that their risk treatment decisions have in other scopes. Also, risk mitigation can be optimized as risks that are run in a specific scope might well be mitigated by controls implemented in another scope. El Metodo itself is oblivious to the decisions of managers to the extent they wish to cooperate.

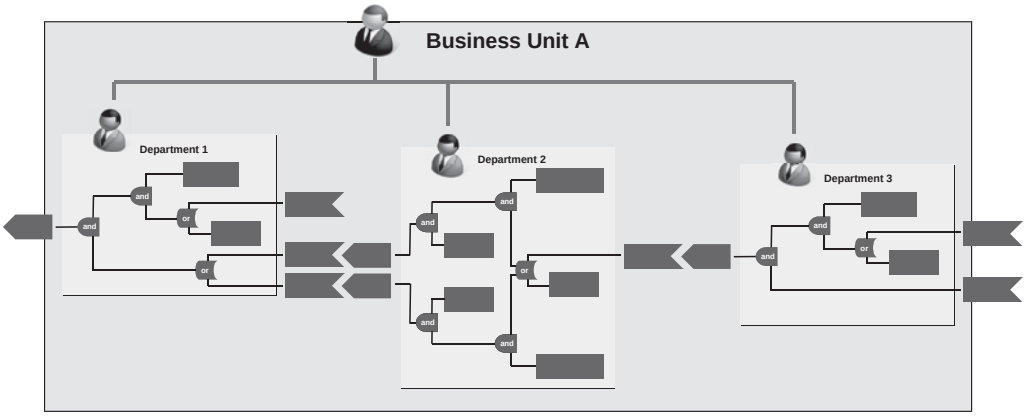

Fig 5: Risk Management across a value chain

By repeating the process over time and determining the effects of implemented measures and environmental conditions, an overview of the actual risks can be obtained relatively easy. Also, in the event that the implementation of an action takes a long time (long-term project), the progress of the project and its effects on reducing the risk have to be monitored.

4 Discussion

Starting to use the method requires organizations to change the way they do risk management. Rather than having a small group of risk managers responsible for managing all risks in an organization, this responsibility should be transferred to the people that already bear the responsibility of the business functionality from which the risk stems: line managers, product managers, project managers, as well as owners of processes, applications, systems, networks etc. After all, they should be running the risks, so that they decide which risks to mitigate, how to invest their resources and, if necessary, what additional resourcing to request for from higher management. Currently, and despite various efforts to quantify risks, such decisions are still often based on gut

feeling rather than on knowledge of causes and consequences. The method aims to have a risk management process in every scope and sets out to provide results of sufficient value to their managers that they will actually use it. This is very much in line with the list of practices from [FrAn11].

The method only works if the scope managers see the purpose of systematically identifying and assessing risks. They should be structural and honest with respect to filling in their part of the obligations and expectations. After all, it is in their own interest, because they will face the consequences of not living up to their obligations. But for many managers it may feel like an extra responsibility and extra bureaucracy. Moreover, it can be very confronting for a manager to make its obligations explicit.

It will take time and resources to implement the method. Scope managers must learn how the method works and obtain skills in keeping obligations and expectations. Also, after everything is set up, maintenance of the overview, even if it is only their own scope, will take effort.

If the method is used, it has a great advantage: risks are assessed by people who do this the best, namely the scope managers. The method ensures that the entire organization becomes aware of the risks and be responsible for managing those risks.

The method gives scope managers the tools to manage their own risks. They will identify and assess risks systematically, and will see the consequences of their choices. Also: the more complete the list of obligations and expectations, the more complete the overview of risks will be. They can compute probabilities, risks and impacts in a relatively straightforward way, and tooling that automates this process is readily thinkable. Also, they may confer with their colleague managers using a common risk language. Thus the method helps managers make decisions and better cooperate with one another.

The work of risk managers is simplified by the method. By using the method, an overview of value chains is created (and maintained) by the participants of that chain; risk managers only need to look for signals such as unaccepted risks, or expectations that are not matched with obligations, which is easy when the method is used with a supporting system. Every signal relates to a task that managers of the associated scopes need to do.

We have talked to the security officers (which also bear risk management responsibility) of a number of Dutch corporations to verify the ideas of our methodology. They recognize the problems that are sketched in section one. All security officers have to deal with a struggle for management attention, the companies do have to deal with risks stemming from their suppliers and they do not have a coherent overview of current risks. They appreciate our methodology to provide a structured manner to deal with risks. Although they do not consider the presented method to be a completely new way of thinking, they do see the usefulness of method, in which several useful elements are combined into one comprehensive and structural approach.

Currently, we are developing a tool for risk managers and scope managers so that they can get a quick overview of obligations, expectations, their dependencies and the associated impacts, probabilities and risks. For now, it will only provide them with a better understanding of where risks come from. In the future, this tool may automatically generate a risk register that keeps track of risks as they dynamically change.

5 A Look into the Future

At this moment the method provides a uniform manner at the operational level for understanding risks. This is useful for individual scope managers, as they get insight in their own scope and in the relations with other scopes, in terms of obligations and expectations. Managers also get insight in risks, what their impact is and what the probability is, since there is one for every obligation and expectation.

Supporting such managers with a single tool would be beneficial for them, as they could then simply write down or remove any obligation or expectation as and when necessary, and see the effects as they do so. We believe that this could be a valuable asset not only to managers, but also to others, e.g. marketeers or SLA managers.

Also, we think that (drawing) techniques used in e.g. fault tree analysis could be useful for having managers specify the functions that compute the probability of obligations not being met from the corresponding probabilities of the expectations on which such obligation depend.

A supporting system would even be more beneficial if multiple scopes started using the same system. This would not imply that everyone has access to everyone else's information, but it could mean that managers that trust each other's information, in particular the probability estimates, will be relieved of tasks that can be computed from such shared information. For example, if a manager trusts the probabilities computed in another scope, and such probabilities are shared, then the probability of every expectation to that scope can be computed from the probability of the corresponding obligation in that other scope.

Such cooperation on risk issues in a value chain would facilitate the propagation of risk estimates through a value chain. Consequently, if risks 'line up', i.e. if selected risks from various shackles in a chain become so high that delivery of the final product of the chain becomes risky, this will automatically be signalled provided each manager signals his own risk dynamically. Eventually, a system might even provide advice with respect to measures to be taken in order to prevent catastrophes taking place.

What should be further investigated is the added value of the method for chains with scopes in different organizations. The feeling is that this method offers advantages, but this depends largely on whether the organizations are willing to share information and what information it is.

6 Conclusion

In this article we presented a new way of treating risk in value chains. The method combines several existing elements into a new and structured method. This method can be automated very easily. The method does not use standard threat lists, but takes obligations of organizations and their expectations put upon themselves or others (e.g. suppliers) as a basis. In the method, completeness of the risk assessment depends on completeness of the lists of obligations, expectations and their dependencies.

An advantage of the method is that it brings risk assessment to the 'floor'. Rather than having a small group of risk managers (often on staff level) responsible for managing all risks in an organization, this responsibility can be transferred to the people that already bear the responsibility of

the business functionality from which the risk stems: line managers, product managers, project managers, as well as owners of processes, applications, systems, networks etc.

The method offers clear advantages for scopes within an organization. The idea is that this method also offers advantages to cross organization risk assessment (in value chains), but this depends largely on whether organizations are willing to share information. Even if organizations are not willing to share information, the method can still be used by estimating the necessary parameters based on trust, past experience, performance reports and/or audits. We will continue to perform research in this area.

We have checked the method with a number of Dutch corporations and they do see the advantages of this method and have indicated they want to be involved in or informed about the future development of the method.

References

[FrAn11] Frigo, M.L, Anderson, R.J.: Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. Journal of Corporate Accounting & Finance, Volume 22, Issue 3, pages 81–88, March/April 2011.

[ISF11] International Security Forum: The 2011 Standard of Good Practice for Information Security. ISF, June 2011.

[ISO31000] ISO 31000:2009: Risk management -- Principles and guidelines, November 2009.

[Mille56] Miller, George A.: The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information. In: The Psychological Review. 1956, vol. 63, p. 81-97.

[PiSa90] Piore, M.J, Sabel, C.F: Second Industrial Divide: Possibilities for Prosperity. Basic Books, 1990.

[Sabe82] Sabel, C.F: Work and politics: the division of labor in industry. Cambridge University Press, 1982.

[StGF02] Stoneburner, G, Goguen, A and Feringa, A: Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. National Institute of Standards and Technology, July 2002.