Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)

RAUNO PIRINEN, JYRI RAJAMÄKI, LILI AUNIMO
Laurea Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9, 02650 Espoo
FINLAND
rauno.pirinen@laurea.fi, jyri.rajamaki@laurea.fi, lili.aunimo@laurea.fi
http://www.laurea.fi

Abstract: - There are number of systems, such as transport and logistic, power and telecommunication, hydropower and nuclear power stations; that are critical systems for the functioning of day-to-day life of the society in Finland. When assessing possible risks, it is only seldom taken into account that power, hydropower and nuclear power plants are critically dependent on the reliability and security of information systems. Information security is often enhanced by purchasing and extending technical solutions without considering any systematic planning and knowledge of how to protect the different segments of the system. In this case study, the risk is not only to investing of the information security resources to the wrong targets but also to take more risks. As the unplanned integration of systems and the related information security components may even create new security risks. As a result, systems that are critical for society may not work as they should. The Rescuing of Intelligence and Electronic Security Core Applications (RIESCA) project is targeted to do contributive and constructive solutions to this problem. The research object is produce information security and continuity management methods that can be used to ensure the proper functioning of critical systems under varying circumstances. Furthermore, it also leads to the development of an integrative action and environment for critical systems development, management and evaluation. This study: (1) describes the RIESCA project; (2) proposes enhanced data mining collection and analysis architecture model for critical systems evaluation; (3) includes Business Continuing Management (BCM) method creation perspective to context of critical systems and (4) describes the RIESCA action and process implementation model.

Key-Words: - Critical system, method development, critical infrastructure, security core application, critical process and societal security, data maining

1 Introduction

An important part of the technical and functional infrastructures that is essential for the operation of business and society has traditionally been planned and realized in such a way that it has of high level of functionality in a wide range of situations. These systems must tolerate human errors or malfunctions of an individual part of the system without affecting or crashing entire system. The traditional distribution of electricity or logistics serves as examples. However, the situation has changed significantly after the introduction of information technology.

An increasing number of essential functions of the systems are more and more dependent on information systems. As a result, vulnerability increases. An increasing number of essential functions may slow down or cease to operate due to problems related to information systems. Problems related to logistic systems serve as an example of problems attributed to the increased dependency on information systems. An error in a single information system can cause catastrophic effect on important part of the traffic system of the Finnish railway company. Similarly, an information security problem may crash the energy distribution network or prevent the operations of a water plant without any problem related to the actual distribution infrastructure. Everyone reading newspapers is familiar with significant losses in profit when commercial information systems have not worked properly or have stopped the entire organization outright, e.g. Sampo Bank, a Finnish part of the major Nordic Danske Bank Group, lost thousands of customers during their system migration process in spring 2008.

The changed role of information systems is evident because, in practice, all operations of business and the society are somehow linked with

information technology. The penetration of information technology into new functions and systems that did not previously contain information technology has created a situation in which the operational reliability of systems and equipment has decreased.

The introduction of information technology to link information systems with new systems, functions and equipment has created a situation in which usability, reliability and functionality as well as their preconditions has significantly changed. Therefore, old and familiar quality aspects and ways of thinking are no longer valid enough. It is evident that the integration of information technology in increasing number of products will be accelerated.

Furthermore, cooperation of RIESCA represents one kind of Complex Collaborative Learning Community. The social learning theory, allows us to see the ways in which this learning and development environment not only make sense of the objects of the development work processes through the project, cooperator, interaction, task and technology, but it also continues learning and inspiration about project and knowledge sharing each other in this environment [6,7].

1.1 Critical Systems in Finland

If you turn off main switch of the electricity in your home, many routine works stop functioning or becomes impossible to carry out. You may continue working with your table top personal computer about 20 minute more if it is backed up by UPS and it may able to rescue any unsaved data and information. Electricity and UPS are critical systems for storing your personal information. But which are the highly critical systems in scale of whole Finnish society? For instance, Thunderstorm over Helsinki on 22nd August, 2007 taught us severe lessons: National news service of Finnish Broadcasting Corporations could not be broadcasted, several false alarms has messed up rescues services, traffic lights of entire city went into error mode – and these are just few examples. More than five thunder strikes into antennas brought down many elementary functions of nation's capital. What would be the scene after purposeful attacks against these systems?

Our Swiss colleague is amazed: how simple it was for Russians to buy the majority of such companies like Oerlikon and Sulzer [1]. The question is - what is for the sale and what is not? With companies like Telia-Sonera the decisive power is not in Finnish and Swedish hands.

On the company level several safeguard measures like anti-virus programs and firewalls are tested and tendered before purchasing. It is commonplace to leave update gateway wide open for 24/7 unguarded action. What if somebody manages to use these gateways to install a mole into your company's IT system?

Now, we have more sophisticated cyber threats, terrorists! Use of IT by terrorists is constantly increasing and expanding the scope and reach of their acts. In fact, urgency of addressing this issue draw attention of NATO and hence it was one of the top agenda in the recent NATO summit [21].

These kinds of questions have brought together a consortium of Laurea University of Applied Sciences and the Universities of Oulu and Kuopio with their industrial and societal partners to seek answers and improved safeguard measures.

1.2 Related Work

Eurobaltic Civil Protection Project II (2005-2007). The project established the CIVPRO Civil Protection Network, aims to increase cross-sector and transnational competence in managing emergencies and disasters situations in the Baltic Sea Region. The project, coordinated by the Swedish Rescue Services Agency (SRSA), focuses on three areas: first, risk management and spatial development, second, building transnational capacity - exercises, training, education and research and third, promoting safety over sectors and borders. [2]

Towards a Regional Strategy of Critical Infrastructure Protection in the Baltic Sea Region (2007). The project examined the protection of critical infrastructure networks from cross-border risks such as terrorist attacks and natural disasters. The project was steered by the Nordic Centre for Spatial Development (Nordregio) and supported the forthcoming European Programme for Critical Infrastructure Protection (EPCIP). The focus was on the specific perspective of the Baltic Sea Region. [3]

Civil Protection Early Warning (2007). The project aimed at developing risk assessment and management systems as well as improving knowledge and expertise especially from the perspective of civil protection early warning. It investigated, reviewed, compared, evaluated and developed early warning systems in general as well as within three issue areas of civil protection, namely floods, critical infrastructure protection and maritime safety. The project dealt particularly with the "bottleneck" puzzle of an early warning. This is the period between the first, sometimes rather "weak" signals, on the one hand, and the response, on the other hand. [4]

2 Implementation of the RIESCA Project and Method Description

There is a common need for holistic systems to evaluate and diminish risks in existing systems, and minimize risks in systems under development. The three-year RIESCA project produces risk analysis of these systems and a method to minimize risks in new systems. Furthermore, co-operation network of the actors will be organized for critical system's risk management within the project. With the help of foreign university partners and researcher's mobility best practices of latest international developments are collected to facilitate the project.

The research partners of the project are the University of Oulu, University of Kuopio, and Laurea University of Applied Sciences. The international research partners are Macquarie University, Sydney, Australia; University of Arizona, USA; and Software Competence Centre Hagenberg, Austria.

The basic structure of the project is cyclic. Each cycle lasts for about a year and consists of the following stages:

1. Theoretical research combined with the analysis and modeling of the status of the selected systems.
2. Method development.
3. Application of the methods to the chosen targets (piloting).
4. Analysis of the application results and decision on further measures.

The development of the method stage in the first cycle focuses to the identifying and assessing the impact of technology. The method development stage of the second cycle focuses on the minimization of the impact and that of the third cycle on methods that can be used to avoid information system related problems in new improved and upgraded modernized systems. The schedule for the different stages will be available at project's web site.

The subject of this study is a generation of new methods for critical system's analysis and evaluation, using new implemented constructions and the creation of the new collaborative learning and development environment as well as various constructions related to work packages. And so, it is obvious to use the design-science research [5] and constructive approach.

According to the project plan, the research work consists of the three-stage cycle on improving operations. The stages of the cycle are:

1. Planning.
2. Implementation/Piloting of the plan.
3. Evaluation of the results.

The entire project consists of two and a half cycles with an identical basic structure. The first cycle focuses on the evaluation of the theoretical framework and piloting whereas the second cycle focuses on the practical implementation of theoretical models. The objective of the third short cycle is to allow the implementation of corrective measures.

In methodological perspective, the implementation part of RIESCA project combines design science and constructive research approach [5] along with applied mathematics used in a system.

The theoretical and practical knowledge on method development (Business Activity Monitoring and Event Security Management for Critical Systems) is recognized. Special attention is paid to the theoretical areas which are included in the project through the operations and special interests of the participating organizations.

The areas are integrated using Laurea's Learning by Developing (LbD) development framework. The Learning by Developing (LbD) framework is pedagogical and communal approach in which learning is linked to applied research and development projects and culture. That means learning expertise which comes from various aspects of collective objects like social interaction, knowledge and competence sharing, researching and problem solving culture. The model emphasizes on cooperation and creation of a "learning and developing" culture. Not only that but also make it possible to use various scientific perspectives and methods of learning, researching and developing. In this case using LbD, the aim is to implement and integrate all methods of research, development, learning, cooperation and project practice. [6]

It is also evident that project has valued the importance of regional and international development, especially in the perspective of knowledge sharing and transformation. According to the role of Integrative Learning Environment in the innovation system and its area of operation related to the existence of a network. It also considers its active and systematic participation in it. It takes in to account, the integration of three statutory tasks, such as research and development, education and regional development of University of Applied Sciences. This case, promotes the

knowledge transformation of security networks of cooperators by transmitting and producing new knowledge competences. [7]

The areas of special interests of each participating organization are mapped out in detail during the theoretical stage. In addition to that theoretical research will be emphasizing according to the said areas of interest. The theoretical work highlights the development of methods that will guide the operations of the partners through the practical implementation of the project. Metrics for the assessment of the pilots are also created at this stage of the project.

3 Related RIESCA Models

Pirinen & Rajamäki (2008) proposed: Data Collection Model; The Grip Model; Multidimensional Data Architectural Model and Implementation Model [22]. This study extends perspectives of: Determinacy Analysis as a method that solves tasks of data mining [23]; necessity of ontology's instance for critical systems [24]; advances of Fundamental Modeling Concept in case of RIESCA [25] and using of tacit knowledge capturing in acquisition process of business continuing management (BCM) methods [26].

3.1 Models of Data Collection and Analysis

Theoretical work underscores the handling and formation of method development that allows the practical implementation of authentic critical process or operations of the cooperator during the project.

The approach and metrics for the assessment of the pilot studies are planned to create in perspective of multidimensional data collections. It verifies and applies variety of methods and algorithms for evaluation and presentation of multidimensional data cubes or structures using elements. Further, in order to more efficiently support data analysis and querying involving aggregations to the case of critical system method analysis.

The new construction named "the grip" represent abstract term of dynamic online data collection, it emphasize nature of abstract online interface to data construction that can be thought of as extensions to the two-dimensional array of a spreadsheet or data cubes. These methods of analyzing the data are known as dimensions. Furthermore, in case of critical systems method there should be more than three dimensions of variables. Even the hypercube term describes better analysis approach.

In general the grip means: what is the meaningful data and how is it collected from critical system process and what are open and cost-effective technologies for capturing critical data? Following Fig.3 illustrates multidimensional perspective of Critical Systems Analysis in RIESCA case:

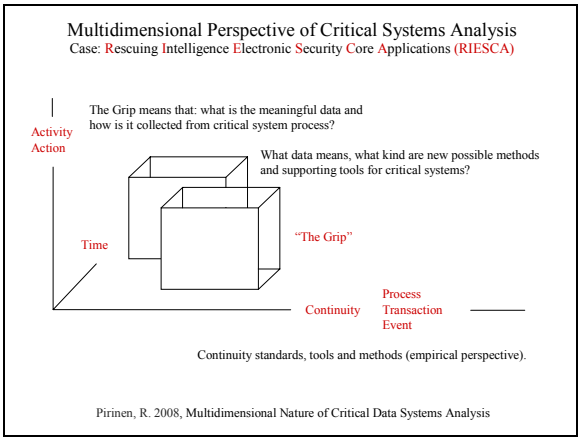

Fig. 3. Multidimensional Nature of Critical Data Systems Analysis.

The model consists of On-Line Analytical Processing (OLAP) principles. The applied solution should allow the actor (user or machine) to quickly analyze information online, information that has been summarized into multidimensional views and hierarchies. Model's tools and functions are used to perform trend and time analysis on critical system information which is collected using the grip construction. The aim is to enable and drill down of data mass in order to isolate activities or actions that are the most interesting for example in continuity management perspective. [13-17]

The designed model includes implementation of Multidimensional OLAP (MOLAP) that summarizes transactions into multidimensional views ahead of time. Data are organized into a cube structure that can be rotated by the actor, which is particularly suited for critical data summaries [18]. Relational databases are used and the analyses functions extract data. One possible first choice is to use SQL statements against relational tables, while another choice is to use Relational Online Analytical Processing (ROLAP) that is able to create multidimensional views on the fly. ROLAP solution tends to be used on data that has a large number of attributes, where it cannot be easily placed into a cube structure. [19]

The model of data collection and analysis includes authentic critical process implementation. The model emphasizes actors supervisory control improvements. The implemented system performs data acquisition and capturing from the critical

system plant and makes it possible to use the collected and analyzed data continuous criticality control and improvement purposes.

The main objects of model implementation are: development of new action and critical system security models, improvements of evaluation of critical systems and evaluation methods, contribution to crisis management and state transition management, improvements in Business Continuity Management (BCM) and testing of virtualization working in crisis management. The Model of Data Collection and Analysis configuration is presented in Fig. 4.

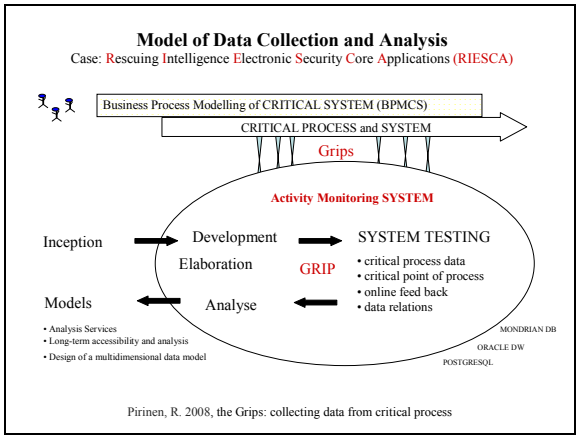

Fig. 4. Model of Data Collection and Analysis, 'a Grip' abstracts, incepts and elaborates: what, why and how the meaningful and only necessary data is colleted from critical process.

3.2 Open Architectural Model

The approach and purpose of the Open Architectural Model of RIESCA is to develop the framework of open critical system management for the institutions and enterprises, those who have importance of critical systems in the perspectives of societal and regional level (Fig. 6). The object of architecture is flexible enough in individual's perspective. That user and participant can be involved in the improvement phases of the implementation processes. In perspective of study the architectural contribution is new application of technology which is solved to critical processes and it develops usability of critical systems.

The Grip collects only necessary parallel or serial data or information from critical process for decision making. The grip means abstract term of configurable and trimming context of dynamic online data. Data constructions and analysis can be implemented thought of extensions to the two-dimensional array of a spreadsheet or data cubes. Architectural model of RIESCA implementation is illustrated in Fig. 5.

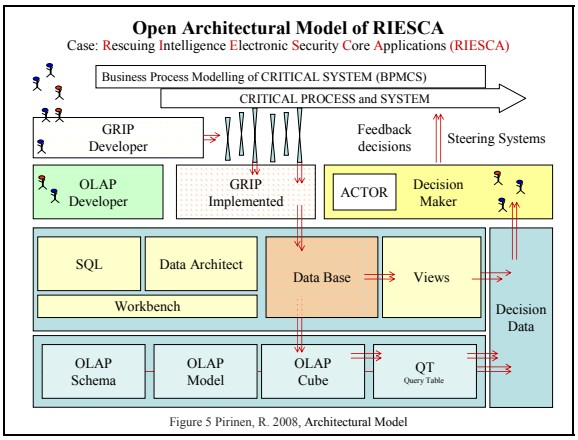

Fig. 5. Architectural Model of multi dimensional data analysing in RIESCA.

There are several implementation targets and models in technological perspective: multidimensional data model; snowflake schema used in relational databases; decision data reporting and architectural model and an implementation of the meta-data extensions with multidimensional query and analysis tools. The SQL (Structured Query Language) extensions including a "cube" object that returns row sets. Those are also "slices" of the cube. Implementation of the Service-Oriented Architecture (SOA) for OLAP (on-line analytical processing) provides meta-data for multidimensional data. XML (Extensible Markup Language) query results are also described in architectural model. [20]

3.3 RIESCA Process Implementation Model

Integrative Process model of RIESCA implementations are described and collected in trimming process model. The outcomes of the processes are new security methods and models: especially new security evaluation methods and models; new Business Continuity Management (BCM) models and methods; contribution of Crisis Management Models and terminology as well as evaluation of these methods and models.

All process phases are numbered from (1) to (11) in "implementation machine". In the operative level, the first positive outcome is the favorable conditions for new knowledge creation that created by objectivity of critical systems (6). This new instance and creation of Integrative Learning Environment [7] manages analysis and research process (7) which makes it possible to use feedback operations from

outcomes (8) to inputs (1-4) and steering and tuning of objects. The outcomes of research and analysis works (8) are useful to the new implementation of next research and analysis phases and cases. The project carried out in the integrative learning environments which allows constructive development (7) of context, objects and learning. The cyclic and elaborative process part (1-6) is then continued with linear analysis and research process, which includes implementation of critical systems method, integration of culture and community depending things cooperated with running and implementing construction. The RIESCA process implementation is illustrated in Fig. 6.

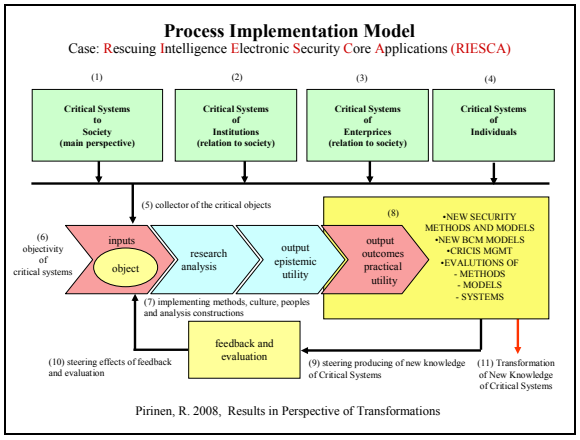

Fig. 6. Process Implementation Model integrates cyclic and creative world of innovations to linear development process for critical systems.

The RIESCA project will carry out in phases with implementing, evaluating and testing several research and analysis methods in phase (7), with the perspective of usability of applied mathematic applications for critical system analyst and evaluation. The results and outcomes (8) will produce new knowledge which are documented and tested as arguments. The value of new knowledge creation and its new prospects make it possible to knowledge transferring in participation perspective and the ability of transfer new knowledge to security innovations, new security services, improvements of productivity, new business linked to markets, vitality of network, safety, welfare and increased cooperation are all impacting values.

The little red arrow (11) illustrates possible execution and knowledge transformation process, from development and learning environment to value network [30]. The results are also possible and reachable on international and global scale [31].

3.4 Extending RIESCA

Lind and Kuusik (2008) proposed Determinacy Analysis as a method that solves tasks of data mining. In the case of RIESCA the Determinacy Analysis should answer the questions like how we can describe different actions and what distinguishes different risks from the others? [23]

Vincze, Szarvas and Csirik (2008) presented wordnets project and proposed two cases: financial domain ontology and the legal domain ontology. What is relation of critical system to ontology, does it contribute system security if critical system domain have instance of ontology or own sub ontology? [24]

Staines (2008) proposed Fundamental Modeling Concept (FCM) based on Unified Modeling Language (UML). The concept serves the capturing problem solving experience and knowledge for different domains at a high level. This could easily be shared whit different system stakeholders to come up with functional models offering optimized solution and better system comprehension [25].

According to Abdulmajid (2008) explicit knowledge is in the form of software artifacts and tacit knowledge is in the form of arguments that constitute the context behind the creation and validation criteria of knowledge [26]. Both, explicit and tacit knowledge is necessary to take into account in researching and acquisitions of empirical Business Continuing Management (BCM) methods in RIESCA case.

4. Propositions

The new proposition includes perspectives of: method creation of Business Continuity Management's (BCM) and second enhanced data mining architecture model for the discovery of unexpected sequences in critical data.

4.1 Business Continuity

Business continuity is about threatens onto business processes. It is about those threatens that substantially infringe the usual operation of business processes in a way that prevents the organization or enterprise to fulfil its mission with eventually severe impact onto costs or revenues. So, the threatens dealt within business continuity considerations are severe incidents that typically do not stem from the conditions of the respective business model but rather somehow from the environment the business operates in. Table 1 lists some of the typical threatens considered in the area of business continuity. Taken as an objective, business continuity is the ideal to reach a maximum of

stability of the business against those threatens. Therefore, business continuity management [32] is about becoming aware about as much threatens as possible and preparing the business for them as good as reasonable.

Table 1 results from a poll conducted by the Chartered Management Institute [37] on disruptions experienced in the UK in the year 2007. It clearly shows that loss of IT heads the list of experienced disruptions. However, the figures also tell that also those risks that are usually considered as non every-day risks like extreme weather conditions or fire clearly occur often enough to be considered for a systematic treatment. The table contains also other interesting figures. It shows that only a part of the respondents of the poll have systematically considered the several potential disruptions and eventually addressed them in their business continuity plans. Furthermore, it shows how many respondents were actually able to use an existing business continuity plan. The clear gap between these two latter figures is a key argument for further research and development of tools and techniques in the area of business continuity management.

Typical threatens	Experienced	BCP covered	BCP used
Loss of IT	38%	81%	9%
Loss of people	32%	53%	3%
Extreme weather e.g. flood/high winds	28%	58%	5%
Loss of telecommunications	25%	75%	5%
Utility outage e.g. electricity, gas, water, sewage	21%	57%	6%
Loss of key skills	20%	49%	2%
Negative publicity/coverage	19%	36%	2%
Employee health and safety incident	17%	52%	3%
Supply chain disruption	13%	37%	2%
Damage to corporate image/reputation/brand	11%	35%	2%
Pressure group protest	7%	23%	1%
Industrial action	7%	28%	2%
Environmental incident	6%	1%	2%
Customer health/product safety issue/incident	6%	1%	1%
Fire	6%	68%	2%
Terrorist damage	3%	57%	2%

Table 1. Disruptions experienced in UK in 2007 according to a poll conducted by the Chartered Management Institute with a base of 1257 respondents. Despite the percentage of respondents who experienced a certain disruption the tables also contains relative figures of those respondents whose business continuity plan (BCP) covered a certain incident and figures about those respondents who were actually able to use an existing business continuity plan in case of a certain incident.

4.1.1 The British Business Continuity Management Standard (BS 25999)

Business continuity management spawns the whole cycle of analyzing the business with respect to critical actions, systematically addressing critical actions, designing reactions to unavoidable incidents, and exercising and maintaining those reactions [27]. The British standard BS 25999 [28] is an internationally highly recognized standard in the area of business continuity management. BS 25999 considers business continuity management as a major crosscutting activity, which must be truly embedded in the company in the sense of awareness of it and support for it, in order to be successful. Fig. 7 shows the BS 25999 business continuity management lifecycle:

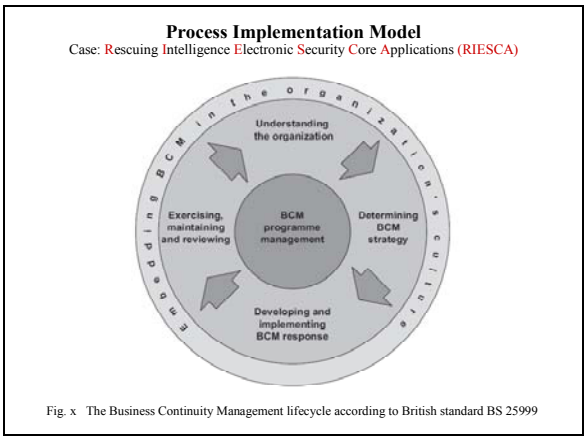

Fig. 7. The business continuity management lifecycle according to British standard BS 25999.

In lifecycle model: a major activity in the understanding of the organization is business impact analysis (BIA) is that the it identifies critical action and it is about determining the impact of failure of critical actions, i.e., eventually it tries to estimate direct and indirect costs of failure of critical actions. Furthermore, it has to be understood which incidents can yield to the disruption of critical actions. A kind of pervasive incident elicitation has to be conducted and then the probability of each single incident to actually occur has to be estimated. The stage of determining the business continuity strategy in Fig. 7 is about the important fact that the

preparation against threatens is not only about fixing reactions to possible incidents.

It has to be checked whether it is possible to change the existing business processes in a way that they become more stable against the identified threatens from the outset. In some cases it might be even possible to get entirely rid of some of the identified critical actions. It must also be considered to diminish the probability of incidents and risks wherever possible at reasonable costs. Also insurances against risks must be considered systematically. Eventually, for those risks for which you have decided to accept, appropriate response must be defined. All this is sometimes summed up roughly by a 4T model of dealing with risks: (1) treat, (2) tolerate, (3) transfer, or (4) terminate. Appropriate response to incidents is at the heart of business continuity management. Fig. 8 shows the incident timeline as presented by BS 25999:

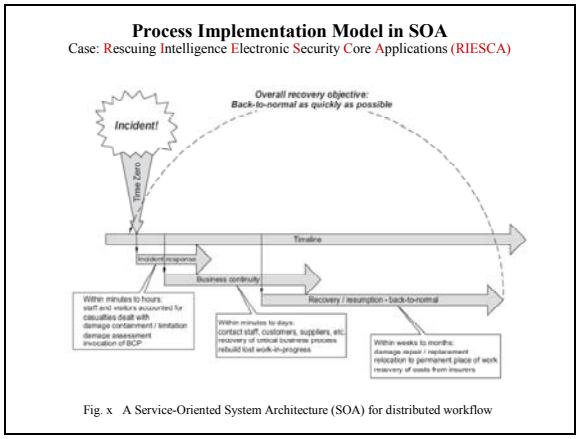

Fig. 8. A service-oriented system architecture for distributed workflow

The overall target of incident response is to resume to normal operation of the business as soon as possible. As an appropriate response to an incident a defined emergency mode of operation and services must be entered in which the absolutely necessary level of processes to fulfil the enterprise's or organization's mission can be guaranteed. The incident timeline shown in Fig. 8 distinguish between three phases, i.e., incident response, business continuity – here in the narrow sense – and recovery. The target is to have concrete plans for each of the three phases ready to execute. During incident response stakeholders are informed and necessary immediate actions are taken. The business continuity phase is about recovering and executing versions of critical business processes. The recovery phase leads the organization back to normal operation.

4.1.2 IT and Business Continuity Management

Business Continuity Management (BCM) does not address information technology outage as the only threaten. But of course it is an important one, because information technology is a mission critical asset and still the disruption of loss of information technology is the most often experienced one, e.g., according to Table 1. Depending on the branch and, of course, the concrete purpose of computer system, the impact in costs and revenues of information technology outage can be substantial for an enterprise. It is said that in banking the total outage of the core systems, i.e., those that deal with transactions on bank accounts, can yield to a bankrupt of bank already after two or three days. Therefore, for the core systems of a bank high availability technology like mainframe computers – often spatially replicated – or high availability clusters are used. Take a medium enterprise from the industrial production domain as another example. Here, the logistics applications that enable the company to deliver these products in extended supply chains are mission-critical. The outage of these applications do not lead to a bankrupt of the enterprise immediately as in the aforementioned banking example, however, actually every day or even every hour of outage can be directly measured in loss of revenue. Not to speak about the loss of customer satisfaction and trust and therefore indirect loss of revenue in the long run. For such medium-critical systems a real high availability solution might be considered overkill, but still a nearly high available system is desired. For example, midrange computers might yield a solution, in particular if there are spatially distributed.

Outage of information technology is a well-perceived in business continuity management. IT continuity management as a systematically approach to keep IT running exists in parallel to business continuity management efforts in enterprises. For example, ITIL (The Information Technology Infrastructure Library) explains IT service continuity management as supportive to overall business continuity management in an enterprise [33]. But then, a closer look to IT continuity management shows that mature IT continuity management efforts contain also the major activities seen in overall business management, like business impact analysis and risk analysis, of course, with a focus onto IT outage. Similarly, in IT service continuity management the same threatens as in overall business continuity management are

considered, e.g., extreme weather, utility outage – see Table 1. Of course, IT outage, is not a threaten considered in IT service continuity management, IT outage is rather the impact of the threatens. We believe that ideally teaming together overall business continuity management and IT service continuity management would mean to remove redundancies in activities and considered threatens on the level of IT service continuity management.

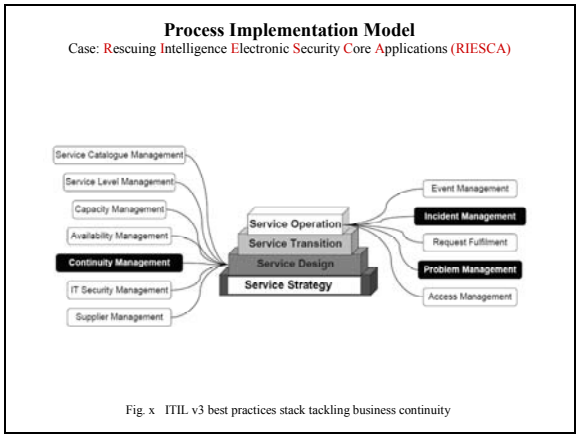

Fig. 9. ITIL v3 proposes best practices stack tackling business continuity.

Fig. 9 above represent an overview of the ITIL service lifecycle [35, 39] with a focus onto topics related to continuity management. Incident management deals with the malfunction of single services as perceived by users of services. A malfunction can be indeed the interruption of a service but also a reduction of quality of a service, e.g., in terms of usability. Incident management is not about reaction to major failover of an entire IT infrastructure or data center, it is about helping out from everyday incidents of IT services. Systematic incident management is about routing requests via a help desk, prioritizing request and reacting to them in a proper manner. Incident management is at the heart of IT infrastructure management. Therefore, incident management is typically the first ITIL service operation process in ITIL projects, i.e., the process that organizations introduce first when they start with ITIL. Problem management is a service operation process that has been introduced with ITIL version 3. Problem management is about the systematic collection of causes of incidents and events in the everyday IT infrastructure management. In ITIL a problem is not just a synonym for an incident but a source of a kind of incident. The gathered knowledge can be exploited in the sequel to find ways to prevent incidents from the outset. Incident management and problem management are processes of the service operation element [29] of ITIL. ITIL sees IT service continuity management as the means to resume to normal operation in case of major failover of IT infrastructure within predefined times. As a consequence, IT service continuity management is tackled within the service design element [36] of ITIL.

4.1.3 New methods and tools for BCM

So far, there are two incepted and promising empirical methods and one tool regarding to Business Continuity Management (BCM) context: the first method is life time errors and failures of system inside known time period at normal using conditions, this means age, reliability and impact of system as well as management of knowledge and key skills needed in system management and second is tacit undocumented methods of service production for producing supporting services of critical systems, this means that how and why the development objectives of supporting systems and tools are selected for service development; and third it is investigated how to bring Web 2.0 technology tools to the whole process of business continuity planning and implementation [34].

4.2 Discovery of Unexpected Sequences in Critical Data

Systems that are critical for security e.g. nuclear power plants, telecommunication and railway transportation systems produce masses of log data. This log data describes the past and current status of the system. By monitoring and analyzing this data, anomalies in the functioning of the system may be predicted. Analysis of the data is performed using data mining techniques. For instance, using data mining techniques, we have created a model on how a railway transportation system functions on a regular Monday morning on a winter day. Based on constant monitoring of new log data, any difference from the model is detected and thus irregular function – such as malfunction – can be predicted beforehand. In the case of successful analysis process, action can be taken when the very first signs of malfunction appear. Software error assessment and quantitative analysis of data produced by software in critical systems has been investigated in a variety of projects (See e.g. Lee [38] and Medhat et al. [41]). The architectural model that we propose in the following is based on decision tree and association rule induction and on their application on new data. The architecture is presented in Figures 10 and 11.

Figure 10 presents the architecture for the generation of decision trees and association rules from existing log data that has been created by ae critical system, e.g. some software in a nuclear power plant. This data may be enhanced by decision rules that are created by a human expert. The data produced by the critical system may be in e.g. the following formats: tuples of a relational database, a plain text file in the CSV format (comma separated values) or in the C4.5 format, which is the format of data developed for the C4.5 decision tree learning algorithm [40]. The proposed data mining engine is based on the open source Java data mining software named Weka [39]. In Figures 10 and 11, the components having the label "WEKA" use this software. The output of the process of classifier and rule generation are naturally a decision tree classifier and an association rule set.

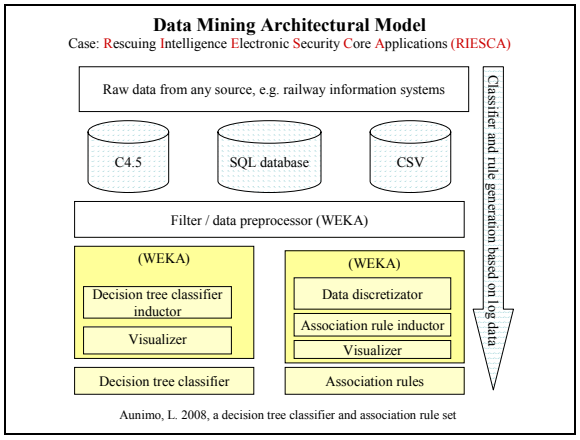

Fig. 10. The process of generating a decision tree classifier and a set of association rules based on log data produced by a critical system.

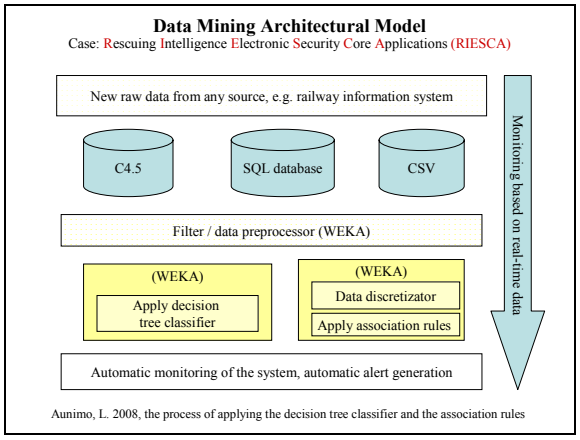

Fig. 11. The process of applying the decision tree classifier and the association rules to new data in order to automatically monitor system performance.

Fig. 11 presents the process of applying the decision tree classifier and the association rules created by the process illustrated in Fig. 10 on new data produced by a critical system. The result of this process may be an automatic alert sent to another system or a human agent. The input of the system is in the same format as in the process of classifier and rule induction. The major difference here is that the amount of input data is typically very small whereas in the previous process of tree and rule induction, the data sets are typically very large. As can be noted from Figure 11, a major part of the processing is performed using Weka. The output of this process is the real-time status information of the critical system in question as well as a prediction for its future status.

5 Conclusion

Western societies are surprisingly vulnerable considering their dependability of modern information and communication technology. In addition to that, the dependence on ICT has posed several questions to their functioning in and recovery from a crisis or catastrophe situation. It is not reasonable to assume that the recovery of ICT based society is as straightforward and easy to achieve compared with the recovery of societies that do not depend that much on ICT. The dependency on ICT is manifested by the fact that an increasing number of basic operations of the society do not work if one or more information system is inoperative.

Finnish society is highly dependent on different critical information systems that support society. Business secrets, patient records and credit card data of citizens, to name but a few, are in electronic form and it is, obviously, important that the said information is kept confidential and protected from unauthorized access. Therefore, it is crucial that information systems and software applications function in the correct way at the sufficient level in case of attempted cracking or human error. As a consequence, systems that are critical to the smooth running of society may not work as they should.

This study paper proposes model of discovery of unexpected sequences in data system and refers pre testing in practice. A critical system produces masses of log data; this log data describes the past and current status of the system. By monitoring and analyzing this data, anomalies in the functioning of the system may be predicted. Analysis of the data is performed using data mining techniques.

Business Continuity Management spawns the whole cycle of analyzing the business with respect

to critical actions, systematically addressing critical actions, designing reactions to unavoidable incidents, and exercising and maintaining those reactions. The ITIL (Information Technology Infrastructure Library) [29] sees IT service continuity management as the means to resume to normal operation in case of major failover of IT infrastructure within predefined times. As a consequence, RIESCA project takes booth standards in context and account.

There are two incepted and promising empirical methods and one tool regarding to Business Continuity Management (BCM) context: the first method is life time errors and failures of system inside known time period at normal using conditions, this means age, reliability and impact of system as well as management of knowledge and key skills needed in system management and second is tacit undocumented methods of service production for producing supporting services of critical systems, this means that how and why the development objectives of supporting systems and tools are selected for service development; and third it is investigated how to bring Web 2.0 technology tools to the whole process of business continuity planning and implementation [34].

The research partners of the project are the University of Oulu, University of Kuopio, and Laurea University of Applied Sciences. The international research partners are Macquarie University, Sydney, Australia; University of Arizona, USA; and Software Competence Centre Hagenberg, Austria. [8-12]

The RIESCA framework in Laurea's project main attention is pointed to the parts of; development of action and critical system security models, evaluation of critical systems and methods, crisis management and state transition management, definition of term crisis, Business Continuity Management (BCM) framework in perspective of its systems and methods, virtualization working in crisis management and inception phase of ITEA 2 - Project Outline (PO) and RIESCA – 2 project.

Acknowledgments

The authors thank TEKES (Finnish Funding Agency for Technology and Innovation), Ministry of the Interior, Ministry of Defence, Civil Crisis Management Center, Finavia, EADS Secure Networks Ltd., Ixonos Ltd., Softera Ltd., Portalify Ltd., Insta Ltd. and Laurea University of Applied Sciences for their contributions for the project funding. The authors thank Dr. Dirk Draheim for his contribution to RIESCA. The authors thank all students for their work and contribution for this authentic project, students has been equivalent researchers, developers and participants.

References:

1. Knuuttila, J. Rescuing of Intelligence and Electronic Security Core Applications (RIESCA). In: Laurea Research & Development 1/2008, p. 22. Lönnberg Print & Promo.
2. Eurobaltic Civil Protection Projects for a Less Vulnerable Society, http://www.raddningsverket.se (2008).
3. CIVPRO Civil Protection Network, http://www.aleksanteri.helsinki.fi/index.php (2008).
4. NORDREGIO Nordic Centre for Spatial Develop., http://www.nordregio.se/index.htm
5. Järvinen, P.: On Research Methods. Juvenes-Print, Tampere (2004).
6. Pirinen, R., Fränti, M. Learning by Developing. In: International Conference, Alytus College, Lithuania (2007).
7. Pirinen, R. Integrative Learning Environments in Perspective of Regional Development. In: Pascal International Conference, University of Limerick, Ireland (2008).
8. Tervo, H, Ahonen, J. IT and Infrastructure's Lost Dependability. In: IASTED International Conference Software Engineering, Innsbruck, Austria. pp. 31-36, ACTA Press (2008).
9. Wiander, T. Implementing the ISO/IEC 17799 Standard in Practice – Findings from Small and Medium Sized Software Organisations. In: 5th International Conference on Standardization and Innovation in Information Technology SIIT2007, Calgary, Canada (2007).
10. Wiander, T. ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners. In: 18th Australasian Conference on Information Systems (ACIS), the University of Southern Queensland, Toowoomba, Australia (2007).
11. Wiander, T. Positive and Negative Findings of the ISO/IEC 17799 Framework. In: 18th Australasian Conference on Information Systems (ACIS) 2007, the University of Southern Queensland, Toowoomba, Australia (2007).
12. Wiander, T. Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. In: The Australasian Information Security Conference (AISC), Wollongong, NSW, Australia (2008).
13. Codd, E., Codd S., Salley, C. Providing OLAP (On-Line Analytical Processing) to User Analyst: An IT Mandate. Technical report, http://www.arborsoft.com/OLAP.html (1993).

14. Dehne, F., Eavis, T., Liang, B. Compressing Data Cubes in Parallel OLAP Systems, CODATA Data Science Journal, Volume 6, pp. S184-S197 (2007).
15. Barclay, T., Barnes, R., Gray, J., Sundaresan, P. Loading databases using dataflow parallelism, ACM SIGMOD Record, v.23 n.4, pp.72-83, (1994).
16. Gupta, A., Mumick, I. Maintenance of Materialized Views: Problems, Techniques, and Applications. Data Eng. Bulletin, Vol. 18, No. 2, (1995).
17. Dekeyser, S., Kuijpers, B., Paredaens, J., Wijsen, J. Nested Data Cubes for OLAP Advances in Database Technologies. In: ER '98 Workshops on Data Warehousing and Data Mining, Mobile Data Access, and Collaborative Work Support and Spatio-Temporal Data Management, vol. 1552, pp. 129-140, Singapore (1998).
18. Sapia, C. On Modeling and Predicting Query Behavior in OLAP Systems. In: CaiSE99 Workshop on Design and Management of Data Warehouses 99 (DMDW99) (1999).
19. Chen, Y., Dehne, F., Eavis, T., Rau-Chaplin, A., Green, D., Sithirasenan, E. Efficient Parallel Generation and Querying of Terabyte Size ROLAP Data Cubes. In: 22nd International Conference on Data Engineering (ICDE 06), Atlanta, USA (2006).
20. Ruey-Chyi, W., Ruey-Shun, C., Chian, S. Design of product quality control system based on the use of data mining techniques. IIE Transactions (2006) 38, 39-51.
21. North Atlantic Treaty Organization (NATO) Summit documents, http://www.nato.int/docu/comm.htm (2008).
22. Pirinen, R., Rajamäki, J. Modeling and Simulation of Critical Infrastructures Case: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA). In: European Computing Conference. (ECC 08), WSEAS, Malta (2008), pp. 403-408.
23. Lind, G., Kuusik, R. Determinancy Analysis as a diclique extracting task. In: European Computing Conference. (ECC 08), WSEAS, Malta (2008), pp. 119-125.
24. Vincze, V., Szarvas, G., Csirik, J. Why are wordnets important? In: European Computing Conference. (ECC 08), WSEAS, Malta (2008), pp. 316 - 322.
25. Staines, A. Modeling UML Software Design Patterns Using Fundamental Modeling Concepts (FCM). In: European Computing Conference. (ECC 08), WSEAS, Malta (2008), pp. 192 - 197.
26. Abdulmajid, M. Capturing Software-Engineering Tacit Knowledge. In: European Computing Conference. (ECC 08), WSEAS, Malta (2008), pp. 192 - 197.
27. Bird, L. Selecting the Tools to Support the Process. In (P. Barnes, A. Hiles; Editors): The Definitive Handbook of Business Continuity Management. Wiley,2007, pp. 263–279.
28. British Standards Institution. Business Continuity Management – Part 1:Code of Practice. British Standard BS 25999–1:2006, BSI Group, 2006.
29. Cannon, D., Wheeldon, D. Service Operation – ITIL Version 3. Stationery Office Books, May 2007.
30. Drakos, N. Magic Quadrant for Team Collaboration and Social Software. Gartner RAS Core Research Note G00151493. Gartner, October 2007.
31. Grudin, J. Computer-Supported Cooperative Work: History and Focus. Computer, vol. 27, no. 5, IEEE Press, May 1994, pp. 19–26.
32. Hiles. A. The Definitive Handbook of Business Continuity Management, 2nd edition. Wiley, January, 2008.
33. Iqbal, M., Nieves, M. Service Strategy – ITIL Version 3. Stationery Office Books, May 2007.
34. Leuf, B., Cunningham, W. The Wiki Way – Quick Collaboration on the Web. Addison-Wesley, April 2001.
35. Office of Government Commerce. Official Introduction to the ITIL Service Lifecycle. Stationery Office Books, August 2007.
36. Rudd, C., Lloyd, V. Service Design – ITIL Version 3. Stationery Office Books, May 2007.
37. Woodman, P. Business Continuity Management. ISBN 0-85946-480-6, Chartered Management Institute, March 2007.
38. Prior Training of Data Mining System for Fault Detection Lee, C. Aerospace Conference, 2007 IEEE Volume , Issue , 3-10 March 2007 Page(s):1 – 6.
39. Witten, I., Eibe, F. Data Mining: Practical machine learning tools and techniques, 2nd Edition, Morgan Kaufmann, San Francisco, 2005.
40. Winston, P. Artificial Intelligence, Addison-Wesley (1992), Section 2, pp. 15-45.
41. Medhat, M., Zaslavsky, G., Krishnaswamy, S. Mining data streams: a review. ACM SIGMOD Record, Volume 34 Issue 2, June 2005.