Human-Machine Engineering For Security Critical and Resilient Systems Practicum

E. Brezhniev, A. Oriekhova, A. Oriekhov,
A. Lutskiv, I. Skarha-Bandurova
Edited by V.S. Kharchenko

Foundations of HME for resilient systems

Resilient cooperative HMS

Human authentication and biometry identification for security purposes

Human aspects in operator teamwork

Human-Machine Engineering for Security Critical and Resilient Systems. Practicum

PRACTICUM

HUMAN-MACHINE ENGINEERING FOR SECURITY-CRITICAL AND RESILIENT SYSTEMS

2017

Co-funded by the Tempus Programme of the European Union

Ministry of Education and Science of Ukraine
Volodymyr Dahl East Ukrainian National University
National Aerospace University "KhAI"

I.S. Skarga-Bandurova, A.Y. Velykzhanin

HUMAN-MACHINE ENGINEERING FOR SECURITY CRITICAL AND RESILIENT SYSTEMS

Training support package

Edited by V.S. Kharchenko

Prepared within the project TEMPUS SEREIN "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains".
(543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Severodonetsk – Kharkiv
2017

UDC 004.49+004.832.2
C42

Skarga-Bandurova I.S., Velykzhanin A.Y.
Human-Machine Engineering for Resilient Systems. Module CM 3.4: Human aspects of operator team-work and modeling group decisions : Training support package / Kharchenko V.S. (ed.) – Ministry of Education and Science of Ukraine, Volodymir Dahl East Ukrainian National University, National Aerospace University "KhAI", 2016. – 106 p.

C42

Reviewers:
– Prof. Todor Tagarev, Centre for Security and Defence Management, Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences;
– Prof. Stefano Russo, Consorzio Interuniversitario Nazionale per l'Informatica (Naples, Italy)

Training support package for course "Human-Machine Engineering for Resilient Systems", was designed for master students within the framework TEMPUS project "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains" co-founded by the Tempus Programme of the Europe Union. Project Number: 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR.

The main aim of the course is to improve our understanding of the role of human factors in system robustness and resilience. This chapter will explore how cyber security concerns related to the uncertainty of emergency management tasks can be addressed for secure EM and suggest possible approaches to improving resilience to cyber-attacks at individual, team and organization level; to develop human factors support tools for enhancing individual and group cyber security sensitivity. The course is a combination of lectures, seminars and laboratory exercises directed to gaining experience in both industrial security concepts and advanced use of particular tools.

Training support package includes a course outline, ad hoc teaching materials, borrowed open-source software and native software.

The book is mainly devoted to MSc, PhD students of universities in such fields as computer security, computer and program engineering when studying methods and tools for safety critical systems. It could be useful for lecturers and professors who conduct classes on corresponding courses.

Fig.: 25. Tab.: 6 Ref.: 27.

UDC 004.49+004.832.2

ACRONYMS AND ABBREVIATIONS

AHP	Analytical Hierarchy Process
ANP	Analytic Network Process
BPA	Basic Probability Assignments
CCO	Chief Compliance Officer
CSIRT	Cyber Security Incidence Response Team
DM	Decision-Maker
DSE	Dempster-Shafer Engine
DSI	Dempster-Shafer with Intervals
DSS	Decision Support System
EDM	Emergency Decision Making
IBLT	Instance-Based Learning Theory
IDS	Intrusion Detection System
IE	Internet Emergency
IFWG	Intuitionistic Fuzzy Weighted Geometric operator
GDM	Group Decision-Making
GDMM	Group Decision-Making Methodology
GDSS	Group Decision Support System
HF	Human Factor
MCDA	Multi-Criteria Decision Analysis
MCGDM	Multi-Criteria Group Decision-Making
MRP	Material Requirements Planning
NFS	Network File System
RSSFG	Rough Set Scenario Flow Graph
SA	Situation Awareness
WPAM	Work Process Analysis Model

INTRODUCTION

Training support package for course "Human-Machine Engineering for Resilient Systems" (Module CM 3.4 "Human aspects of operator team-work and modeling group decisions") was designed for master students within the framework TEMPUS project "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains" co-founded by the Tempus Programme of the Europe Union. Project Number: 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR[1].

This course will involve you actively as a learner by including activities and exercises that highlight basic concepts the role of human factors in system robustness and resilience. It will also provide you with guidance on actions required in specific situations through the use of field-specific case studies.

The main aim of the course is to improve our understanding of the role of human factors in system robustness and resilience. This chapter will explore how cyber security concerns related to the uncertainty of Emergency Management (EM) tasks can be addressed for secure EM and suggest possible approaches to improving resilience to cyber-attacks at individual, team and organization level; to develop human factors support tools for enhancing individual and group cyber security sensitivity.

The universe of cyber security is an artificially constructed abstraction that is only weakly tied to physical systems. Therefore, there are few a priori constraints on either the attackers or the defenders. Also, one of the most significant challenges in defining cyber security within the context of EM, is the fact that most of the threats associated with cyber security are dynamic in that the nature and agenda of adversaries is continually changing. In addition, the type of attacks encountered evolves over time, partly in response to defensive actions. The question for EM organizations is how they will handle cyber security situational awareness within the context of the cyber infrastructure resources they depend on and how will they develop cyber security abstraction models that exploit the knowledge and experience of sophisticated members of their community as well as provide a framework for discussion of cyber security issues.

[1] *This project has been funded with support from the European Commission. This publication (communication) reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*

Decision-making in emergencies requires non-traditional approach and tools characterized by non-hierarchical structure and flexibility. The quick response and decision-making for emergencies has attracted lots of research to resolve this problem by refining reaction strategy or designing preventive plan previously. Most of those researches describe a decision-making process with single decision maker. However, it is seldom that single person can own comprehensive understanding of all phases of emergency and the limitation of personal ability is more likely to be the bottleneck of crisis management. Therefore, further research is needed to improve the system robustness and resilience through effectiveness and efficiency of Emergency Decision-Making.

In this part of course "Human-Machine Engineering for Resilient Systems" you will learn the decision-making models that can be used to make decisions and solve problems in both security emergency and day-to-day situations.

You will benefit in several ways by taking this course:

– you will learn how to identify a problem – as distinguished from its causes or symptoms;

– you will learn special group decision-making methods to deal with the inadequate information, uncertainty and dynamical trend;

– you will become more aware of your own personal attributes as a decision maker and use that awareness as a starting point for improving your decision-making ability.

Training support package includes a course outline, ad hoc teaching materials, borrowed open-source software and native software. The labs we proposed for the course were on the following topics, with particular tools written in parentheses: (1) Discovery of Group Decision-Making Mechanism of Internet Emergency; (2) Emergency Management and Decision Making in Complex Environments; (3) Analysis of GDM and Emergency Management Model Based on Intuitionistic Fuzzy Sets; (4) A Group Decision Support Technique for Cyber Incident Response Teams; (5) Designing Gaming Situations for the Improvement of Team Awareness on Cyber Incidents.

The structure of the study program contains three complementary educational aspects. First, the core educational component combines an intensive training with the small groups on labs. Second, this course provides the students with the opportunity to enhance their skills by wide involvement industrial practice and case study. Case study enables students

to develop realistic solutions to the industrial security problems and to understand crucial nature of complex analysis both specifically and generally. Finally, we try to encourage the students to use their knowledge and ambitions into their research activity.

By the end of semester, the successful student should be able to:

– understand the basic terms and concepts of human factors engineering;

– identify and analyze sources of human and organizational error in complex systems;

– analyze protocols of operators with the system interaction;

– understand basic principles of access control;

– develop flexible and robust operators authentication system;

– explain the need for decision-making and problem-solving skills in emergency management;

– describe how decisions made before an emergency help the decision making process during an emergency;

– apply the methods of human factors evaluation and decision making under multiple and conflicting goals;

– apply a model for problem solving and decision making to emergency management scenarios.

As acquired professional competencies we expect an) effective analytical and problem-solving skills to contribute to creative solutions to complex cyber security and emergency problems, b) gaining experience in working in team under limited direction within scope of the assignment and using independent judgment in choosing methods, techniques, software, and evaluation criteria and c) ability to interact effectively with peers and customers.

Training support package prepared by Professor, Head of Computer Engineering department of V. Dahl East Ukrainian National University, D.Sc. Inna Skarga-Bandurova and master student Artem Velykzhanin who fulfilled in good faith all practical tasks and adjusted laboratory works. General editing was performed by Professor, Head of Computer systems and networks department of Kharkiv National Aerospace University "KhAI", D.Sc. Vyacheslav S. Kharchenko.

Much of the work was inspired and supported by our colleagues on TEMPUS SEREIN project. We are very grateful for this and thank for their contribution to this book.

Laboratory work 1
DISCOVERY OF GROUP DECISION-MAKING MECHANISM OF INTERNET EMERGENCY

Goal and objectives: This laboratory work is devoted to a group decision-making mechanism based on rough set scenario flow graphs. We'll discover characteristics and main factors of internet emergency management, study the process and general operations of the group decision-making in internet emergency.

Learning objectives:

- study basics of internet emergency management;
- study how to use qualitative data to dig into the evolution rules of the general situation;
- study reasoning method that combines the rough set, the flow graph and scenario analysis to mining and forecasting network emergency evolution in the process of emergency response.

Practical tasks:

- acquire practical skills in working with rough set scenario flow graphs;
- draw the whole rough set scenario flow graph of situation evolution.
- acquire practical skills to construct the elements of emergency decision-making system based on large group decision, which demands decision-makers independent in decision-making as well as complement each other.

Exploring tasks:

- discover characteristics, and main factors of internet emergency management;
- investigate how the group decision-making mechanism can be applied to internet emergency decision-making.

Setting up

In preparation for laboratory work it is necessary:

- to clear the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1-3];
- to familiarize oneself with the main procedures and specify the exploration program according to defined task.

1.1 Synopsis

Comparing with the common emergency, internet emergency (IE) has some characteristics, such as medium dependence, widespread impact, great destruction, and origin enshrouding. Based on these characteristics, IE management system should be constructed to deal with IE and it should include early-warning system, emergency response system, and supervisory control system. The IE management system is also based on the group decision-making, but it needs not only the independent decision-making but also the collective decision-making. In this laboratory work the influences of decision-making on the evolution of IE will be discussed in order to make scientific decision from independent decision, collective decision and their combining result.

1.2 Brief theoretical information:

1.2.1 Internet emergency management

IE is one kind of unexpected event based on internet media, which the subjects such as natural force and human power, caused by network media, and effects the objects such as network-users, internet organization and equipment. Therefore, IE means an unexpected event which is caused by natural factors or human factors, and is destroyed to some important computer network or to large scope of computer network, seriously threats the security of country, society, person and property.

Emergency response introduces a new level of environmental complexity in terms of heterogeneity, multiple spatial and temporal scale, uncertainty, resource constraints, distributed computing, and autonomy. It is a “wicked problem”, with large interdependencies, no single optimal solution, and nonlinear behavior. Adding humans to the loop will further increase the need to address these challenges while simultaneously presenting new ones, e.g., environments necessarily introduce synchrony while the human element results in asynchrony. Therefore, strategies must be developed that can deal with discrete and continuous systems on multiple time scales in different time domains.

1.2.1.1 Classification of internet emergency

In conformity with the cause, objects and affected region, internet emergency events can be categorized as follows:

(1) According to the cause, they are divided into two categories, hardware-damaged emergency and software-destroyed internet emergency. The former refers to network interruption and network service termination for widespread of communication lines and equipment. The latter refers to such event as operation of network terminals and losing of stored data as computer is destroyed;

(2) According to the objects, three categories are divided as commercial internet emergency, government internet emergency and civil IE. Commercial network is mostly used by enterprises, so commercial IE affects enterprise network and causes economic losses, even economy in one region. Governments are mainly users of government network, so government IE can cause governmental information flow to government administration system to fail and national secret information to the users of civil network are mainly social citizens, so civil internet y can bring threats to the security of person and property, then give birth to social panic and unrest;

(3) According to the affected region, there are two categories as follows: fixed-region IE and non-fixed-region internet emergency. The former refers to an unexpected event that happens in one or several regions and hardly affects other areas. The latter refers to an unexpected event that its affected areas are uncertain.

1.2.2.2 Characteristics of internet emergency

As an unconventional event, besides internet emergency owns the general characteristics of emergency events, there are special characteristics as follows:

(a) Unconventional and unexpected. It means IE is very rare and its is very unobvious before happening, the process of happening and evolution are irregular, so it is very difficult to be forecasted and controlled according to past experience, which means it’s very difficult to early-warning and effective action.

(b) Dependence of media. Form beginning to end of IE, computer network is a very important even internet emergency doesn’t exist without media.

(c) Extensive influence. Internet connects many areas and fields, so the influence of emergency usually crosses the boundary of one area, region or field. In addition, network is a net-like structure, so, when one

side of terminal is affected, the other sides of terminal in the whole computer network also can be affected.

(d) Intense destructive force. The destructive force of IE is in three respects as follows: First, from economy perspective, IE could cause internal information interruption in enterprises, betray of secrets etc., which may lead to economy losses of individuals and enterprises. Second, from social perspective, IE probably cause social panic. Third, from maintainability perspective, the losses for IE destruction are difficult to be repaired especially when computer stored data is lost and computer hardware equipment is destroyed;

(e) Its source is difficult to be discerned. Since computer network is extensively used and network is widely distributed, it is hard to discern its initiating trigger factors once internet emergency happens.

1.2.1.3 Main factors of internet emergency

IE consists of three factors: cause factor, media factor and subject factor. The cause factor of internet emergency refers to the factor that leads to internet emergency events. The cause factor includes human factor, natural factor and other factors. The human factor refers to individual or organizational unconscious or intentional damaging activities to computer network. The natural factor refers to natural disasters or natural power which destroys computer network. Other factors refer to the special factors that cause computer network destructive. The cause factor directly determines how to find the reason of IE and how to category internet emergency, which plays an important role in the process of internet emergency management. The media factor of internet emergency refers to the damaged parts of computer network, including network optical cables, network service, optical network terminal and optical network terminal software etc. It is the basis of internet emergency scheme and determines the orientations of internet emergency response. The subject of IE consists of two parts as follows: affected subject and decision-making subject. The former can be divided into four levels: First level is national emergency mechanism including police office and security department etc.; Second level is social infrastructure including bank, water supply system and power supply department etc.; Third level is social organizations including schools, scientific research institutes and enterprises etc.; Fourth level is personal computer users. The decision-making subject refers to the departments of

internet emergency response, for example, police office, network management department, news media, and network technology department etc. Moreover, spread speed and influence scope are two attribute factors of IE. The former refers to the changing number of affected individual, regional area and losses per unit time, which decides diffusion ability of internet emergency and is the vital basis of internet emergency action. The latter includes the affected areas and objects and its spread tendency, which is the basis of the control measures in the process of internet emergency response. The relationship among the three internet emergency factors is shown in fig. 1.1 as follows:

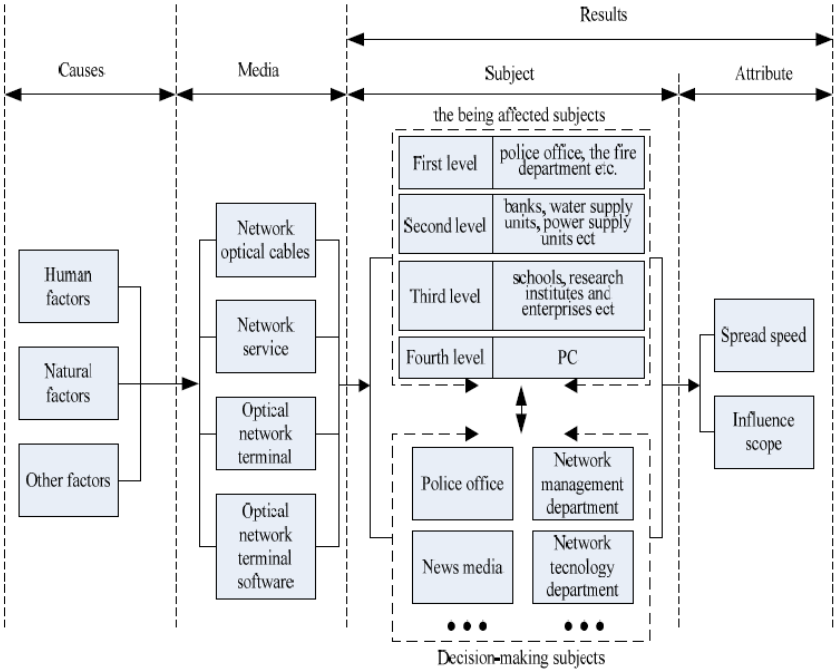


Figure 1.1 – The factor relationship of the internet emergency [1]

1.2.1.4 General operation mechanism of group decision-making in internet emergency management

Based on the essential characteristics of internet emergency, the process of the **group decision-making** in internet emergency **is quite**

different from the common decision making process. The differences are listed as follows:

a. Decision makers should response emergency events more rapidly and take decision schemes more quickly. Internet emergency usually has extensive effect and destructive force. Therefore, internet emergency events will become too severe to control if the decision makers do not make the best decision early enough;

b. Internet emergency events are so complicated that many groups, including departments, enterprises and other individuals, will all participate in the decision making process. Therefore, group decision-making requires a considerable level of cooperation to protect internet emergency action from disorder;

c. Internet emergency is highly unpredictable and changeable. Therefore, in order to make adaptable decisions, decision makers should track the emergency events unceasingly, test and correct decision schemes without delay.

Consequently, definition of group decision-making of internet emergency management is making choices in joint actions among several decision-making groups which consist of different decision-making subjects who act for the common purpose or benefit, or make profits for their own in the process of internet emergency.

To achieve the goal of agile response and adaptable decision, three systems are needed to combine group decision-making mechanism of internet emergency. They are internet emergency early warning system, internet emergency response system, and supervisory control system. The chief responsibilities of internet emergency early warning system are to predict the possible emergency and to sound the alarm. Internet emergency response system is in charge of analyzing the present state of emergency events, proposing internet emergency decision schemes, making decisions, and then executing the schemes by taking full advantage of all kinds of resources. Internet emergency supervisory control system is in charge of supervising the whole process of emergency decision-making, dealing with the subsequent controlling work, and sending feedback the decision results. The general mechanism of group decision making in internet emergency can be shown in fig. 1.2. The figure shows the laws and principles of group decision-making in internet emergency.

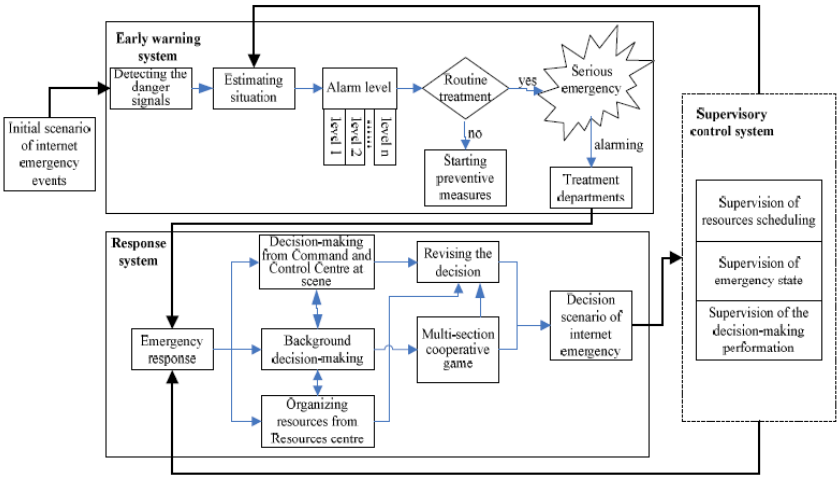


Figure 1.2 – Group decision-making systems of internet emergency, from [1]

The group decision-making mechanism of internet emergency consists of early warning system, response system and supervisory control system.

The three systems combine into a comparatively complete mechanism.

Early-warning system is the prerequisite of the mechanism. Once early-warning system detects danger signals, response system and supervisory control system will be activated immediately.

Response system is the core of the mechanism. In one way, response system takes the corresponding level of emergency scheme according to the severity that early-warning system provided. In other way, response system adjusts its decisions according to the emergency information or the analysis results of supervisory control system.

Supervisory control system is the guarantee of the mechanism. It supervises the whole emergency management actions, feedbacks the results to early-warning system in order to re-evaluate the emergency severity, and feedbacks the latest situation of internet emergency and the results to response system in order to adjust its decision.

1.2.1.5 Three systems of internet emergency group decision-making

1. The process analysis of internet emergency early-warning system Early-warning system consists of detecting information, estimating situation, alarm level and responding emergency. Firstly, it observes emergency information factors. The subject factors include internet optical cable, internet server, internet terminal equipment, etc. The environmental factors include weather, economic condition, social condition and other important factors. If the system detects danger signals from these factors, it will be reported to the detect centre of early-warning system. Secondly, the system makes a judgment to the observed events and determines the alarm level. Generally, the higher the alarm level, the more urgent and intensive it has. Thirdly, it will start the emergency scheme of the same level if the emergency can be solved by existing resources and abilities. If not, then it will start the alarm immediately and inform the related departments to take action.

2. The process analysis of internet emergency response system Response system is the core part of the whole decision-making mechanism. Internet emergency is so serious that many corresponding departments and individuals will participate in the emergency management actions. Therefore, there are many groups to make decision. It forms multi-schemes by the groups in the decision process. The final decision is been made by the game process of the groups. Internet emergency response system is divided into three parts as follows: decision-making from the command and control centre at scene, background decision-making, and resource allocation decision-making. While, foreground decision-making is the execution unit of internet emergency response, which is under the direction of the background decision-making, is bound by resource allocation decision-making and is interfered by emergency situation. Resource allocation decision-making is the insurance unit of the needed resources to internet emergency response. It is under the direction of background decision-making. Background decision-making is the core unit of emergency response, which is based on the foreground information and resource information. The three decision-making processes have interaction to each other and is usually a multi-agent decision-making. Multi-agent decision-making may lead to the different decision schemes which can result in internal decision-making game.

3. The process analysis of supervisory control system Supervisory control system is in charge of supervising the whole emergency management actions, having the subsequent control, and feedbacking the results and existing problem. When internet emergency is confirmed by early-warning system, supervisory control system starts to detect and track. In emergency management action, it collects some valuable information from emergency response system, such as resource usage, resource allocation, emergency situation and decision effect. In one way, it transfers them to early-warning system at intervals to observe whether internet emergency is perfectly controlled or not. If IE has been controlled to the special level, the alarm will stop. In other way, it transmits those information to emergency response system at intervals in order to update emergency information of emergency response system which can response agilely and adjust the decision schemes to have the better effect.

1.2.2 Models of group decision-making mechanism of internet emergency management

Flow graph proposed by Z. Pawlak in [3] was used to analyze the information flow decision. Flow graph can measure the relationship between nodes by using flow distribution among them. That is, it analyzes and reasons the data from the view of quantization, and it requires a stable structure of the flow internet. That is the main reason that traditional flow graphs aren't suitable for internet emergency decision-making, but if we add the Scenario Analysis to flow graph it could be employed in group decision-making of internet emergency management and it is defined as Rough Set Scenario Flow Graph.

1.2.2.1 Rough scenario flow graph and group decision support

Rough Set Scenario Flow Graph (RSSFG) is directed acyclic graph $G=(N,B,\varphi)$, in which, N is node set, $B\subseteq N\times N$ is directed arc set, $\varphi: B\to 2^E$ is object set who flows arc.

Assume x_{ti}, y_{tj} and z_{tk} respectively denote situation scenario node, situation response node and situation system scenario node; x_t, y_t and z_t respectively denote situation scenario node set, situation response node set and situation system scenario node set, $x_{ti}\in x_t\subset B$, $y_{tj}\in y_t\subset B$, $z_{tj}\in z_t\subset B$. Here situation scenario node x_{ti} is defined as the input of

situation response node y_{tj}, situation scenario node y_{tj} is defined as the output of situation scenario node x_{ti}, $x_{ti} \rightarrow y_{tj}$ is situation rough set response arc, $\varphi(x_{ti}, y_{tj})$, is the flow rate of $x_{ti} \rightarrow y_{tj}$, then

$$\varphi(x_{ti}, y_{tj}) = CD(x_{ti} \rightarrow y_{tj}) \tag{1.1}$$

Where, $CD(x_{ti} \rightarrow y_{tj})$ refers to the confidence of decision rule $x_{ti} \rightarrow y_{tj}$. Then, the probability of the situation response y_{tj} in situation scenario $\varphi(y_{tj} | x_{ti}) = \varphi(x_{ti}, y_{tj})$.

Moreover, situation response node y_{tj} is defined as the input of situation system scenario node z_{tk}, situation scenario node z_{tk} is defined as the output of situation response node y_{tj}, $y_{tj} \rightarrow z_{tk}$ is situation response scenario analysis arc. In an open system, situation scenario x_t may trigger several situation responses y_{tj} (j=1, 2, …, m_t). According to scenario analysis theory, several situation responses y_{tj} combine randomly based on different levels, which can lead to situation more complex and present several situation system scenarios z_{tk}. In a situation system scenario z_{tk}, any situation response y_{tj} may be the "major factor" or "minor factor", so mt situation responses y_{tj} can combine randomly into 2^{m_t} situation system scenario z_{tk}. Obviously, whether a situation response y_{tj} is "major factor" or "minor factor" is correlated with its probability $\varphi(y_{tj} | x_{ti})$.

When the probability $\varphi(y_{tj} | x_{ti})$ is very big, the situation response y_{tj} is more likely the major factor of situation system scenario z_{tk}; otherwise, it is more likely the minor factor of situation system scenario z_{tk}. Therefore, in the situation system scenario z_{tk}, the probabilities that situation response y_{tj} is a major factor or minor factor can be described as $\varphi(y_{tj} | x_{ti})$ and $1 - \varphi(y_{tj} | x_{ti})$. Moreover, situation system scenario contains some elements such as situation scenario and situation response, so, the probability of situation system scenario z_{tk} is related with whether its inputting situation responses y_{tj} are major factors or minor factors and their combination, and it can be solved as formula (1.2).

$$\varphi(z_{tk} | x_{ti}) = \underset{j=1,2,..,m_t}{f}(\varphi(y_{t1} | x_{ti}), \varphi(y_{t2} | x_{ti}), \ ... \ , \varphi(y_{tm_t} | x_{ti})). \tag{1.2}$$

For example, as shown in fig. 1, there are two situation response node $y_{0,1}$, $y_{0,2}$ after situation scenario node $x_{0,1}$.

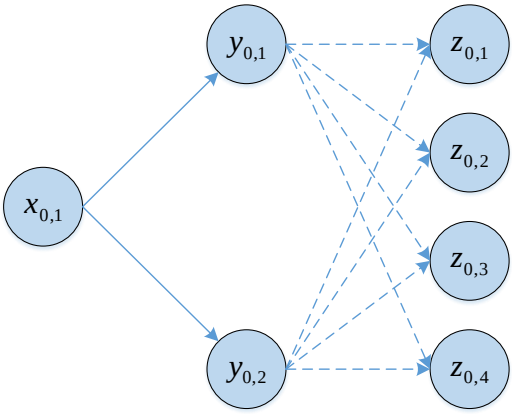


Figure 1.3 – An example of Rough Set Scenario Flow Graph

Then $2^2 = 4$ situation system scenario nodes z_t can be formed by random combination of situation responses $y_{0,1}$, $y_{0,2}$ as following:

$$z_{0,1} = \left\{x_{0,1}, \underline{y_{0,1}}, \underline{y_{0,2}}\right\};$$
$$z_{0,1} = \left\{x_{0,1}, \overline{y_{0,1}}, \overline{y_{0,2}}\right\};$$
$$z_{0,1} = \left\{x_{0,1}, \overline{y_{0,1}}, \underline{y_{0,2}}\right\};$$
$$z_{0,1} = \left\{x_{0,1}, \underline{y_{0,1}}, \overline{y_{0,2}}\right\};$$

$\overline{y_{0,j}}$ and $\underline{y_{0,j}}$ denote respectively as "$\overline{y_{0,j}}$ is a major factor" and "$\underline{y_{0,j}}$ is a minor factor".

Therefore, their probabilities can be solved according to formula (1.2) as following:

$$\varphi(z_{0,1} \mid x_{0,1}) = [1 - \varphi(y_{0,1})][1 - \varphi(y_{0,2})];$$

$$\varphi(z_{0,2}\left|x_{0,1}\right.)=\varphi(y_{0,1})\varphi(y_{0,2});$$
$$\varphi(z_{0,3}\left|x_{0,1}\right.)=\varphi(y_{0,1})[1-\varphi(y_{0,2})];$$
$$\varphi(z_{0,4}\left|x_{0,1}\right.)=[1-\varphi(y_{0,1})]\varphi(y_{0,2}).$$

Situation system scenario could promote the evolution of situation, that is $z_{tk}\rightarrow x_{t+1,i}$.

So there are different evolution tendencies in different situation system scenarios. Here the path between situation system scenario node z_{tk} and situation scenario node $x_{t+1,i}$ in the next stage is defined as situation evolution arc. Supposing that $\varphi(z_{tk},x_{t+1,i})$ is the flow rate of $z_{tk}\rightarrow x_{t+1,i}$, then,

$$\varphi(z_{tk},x_{t+1,i})=CD(z_{tk}\rightarrow x_{t+1,i}) \quad (1.3)$$

Where, $CD(z_{tk}\rightarrow x_{t+1,i})$ refers to the confidence of decision rule $z_{tk}\rightarrow x_{t+1,i}$.

Then, the probability of $x_{t+1,i}$ who is forced by situation scenario z_{tk} is as follows: $\varphi(x_{t+1,i}\left|z_{tk}\right.)=\varphi(z_{tk},x_{t+1,i})$. So, based on situation scenario $x_{t,i}$ its situation evolves to situation scenario $x_{t+1,i}$ in the next stage, its probability is as follows:

$$\varphi(x_{t+1,i}\left|x_{t,i}\right.)=(\varphi(x_{t+1,i}\left|z_{tk}\right.)\cdot\varphi(z_{tk}\left|x_{t,i}\right.)=\varphi(z_{tk},x_{t+1,i})\cdot\varphi(z_{tk}\left|x_{t,i}\right.). \quad (1.4)$$

In formula (1.4), $\varphi(x_{t+1,i}\left|x_{t,i}\right.)$ is the flow rate of $x_{t,i}\rightarrow x_{t+1,i}$, which reveals the basic rules the situation evolves from scenario $x_{t,i}$ to scenario $x_{t+1,i}$.

So, RSSFG is a reasoning method to qualitative data by using rough set and scenario analysis, and can dig into the evolution rules of the general situation and draw the whole rough set scenario flow graph of situation evolution. The general rules of situation evolution can be dug by the ways of following methods:

a. By comparing between situation scenarios of two continuous stages, the deteriorated, stable or optimized trend can be examined.

b. By comparing situation scenario x_t with the early-warning threshold λ_t in the same stage, which is an early-warning to the situation evolution.

c. By comparing the situation scenario x_{t*} in the target time t* with the final aim, which can help select the best situation evolution paths and determine the best control variable z_{tk} in every stage.

1.2.2.2 The RSSFG of internet emergency group decision-making

In RSSFG, $x_{ti} \rightarrow y_{tj}$ and $y_{tj} \rightarrow z_{tk}$ can respectively represent a situation response rule and a situation evolution rule. In the process of internet emergency group decision-making, different internet emergency scenarios ask for different emergency decision; Even under the same internet emergency scenarios, different groups may have different emergency decisions. That is to say that there is game among group decision-making, which could affect the evolution of internet emergency. Therefore, the RSSFG of internet emergency group decision-making can be drawn based on the above method.

Define concretely,

a. Every decision-maker has his decision in different situation scenario of internet emergency, which can form some decision information system.

$$S_{x_t \rightarrow y_j} = (U, C_{x_t}, D_{y_j}).$$

All decision rules $x_{ti} \rightarrow y_{tj}$ and their confidences $\varphi(x_{ti}, y_{tj})$ can be determined by analyzing the information systems.

b. Based on scenario analysis theory, some situation system scenarios z_t are formed by random combination to all correlative decision rules. The probability of any situation system scenario z_{tk} can be obtained according to formula (1.2).

c. Internet emergency can evolve to different situation scenario x_{t+1} under the forces of situation system scenario z_t, the information system $S_{z_t \rightarrow x_{t+1}} = (U, C_{z_t}, D_{x_{t+1}})$ between z_t and x_{t+1} can be formed by collecting the information. Hereby, all evolution rules $z_{tk} \rightarrow x_{t+1,i}$ and their

confidences $\varphi(z_{tk}, x_{t+1,i})$ can be determined by analyzing the information systems.

d. Turn to step a. and analyze the next stage of internet emergency until meet the following condition, then the rough set flow stop and the RSSFG isn't extended again.

i. Exceed the research time;

ii. Achieve the control goal;

iii. Make the risk transfer.

Table 1.1. The confidence and support of decision rules

Spread speed	Conf.	Support
Very rapid spread, very extensive effect	85-100%	30-100%
Slow spread, not widespread	40-85%	20-30%
Very slow spread, small extent	0-40%	0-20%

1.2.2.3 Group decision-making rule of internet emergency and situation evolution path

Based on the RSSFG of internet emergency group decision-making, several evolution paths of internet emergency $x_0 \rightarrow x_1 \rightarrow \ldots \rightarrow x_{t^*}$ can be determined on the condition of multi-stage group decision-making. Supposing there are Γ paths which can achieve the control goal, every path depends on t_l. If $t_{l'} = \min_{l=1,2,..,\Gamma}(t_l)$, internet emergency evolution path $x_{0,i'} \rightarrow z_{0,k'} \rightarrow x_{1,i'} \rightarrow z_{1,k'} \rightarrow z_{t'k'} \rightarrow x_{t',k'}$ is the best control path, $z_{0,k'}$, $z_{1,k'}$, …, $z_{t'k'}$ are respectively the best decisions of every stage in [0,t'] .

1.3 Execution order and discovery questions:

1. Familiarize yourself with supplement materials in Appendix 1 (An example of the execution of the Lab 1).

2. Perform search for information on the Internet according to your assignment. Search all of the existing literature for data regarding your type of emergency management problem.

3. Develop an elimination scheme to combat the target virus. The scheme should include all the possible activity and events gathered on the previous stage.

4. Construct a functioning virus scheme.

5. Determine the primary and secondary methods of dealing with the targeted virus relying on the elimination scheme and the assessment of

probabilities. The probability of any situation system scenario can be obtained according to formula (1.2). Also you can choose the confidence and support values for your practice assignment from the table 1.1.

6. Calculate and rank the possible scenarios for eliminating virus spread.

7. Draw a rough set scenario flow graph and prioritize the implementation of best decision scenarios.

1.4 Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

- (I): background / theory, purpose and discovery questions
- (M): complete description of the procedures which was followed in the experiment, experiment overview, figures / schemes:
- (R): narrate (like a story), tables, indicate final results;
- (D): answers on discovery questions, conclusion / summary.

1.5 Test questions:

1. Name the main factors of internet emergency.
2. Why internet emergency management needs collective decision making?
3. What are the main differences between the group decision-making in internet emergency the common decision making process?

1.6 Recommended literature:

1. Xie K. Research on Group Decision-Making Mechanism of Internet Emergency Management / K. Xie, G.Chen, W. Qian, and Z. Shi // http://telematika.kstu.kg/server/books/ger/ebuziness/2.pdf

2. Kowalski, K. Judgment and decision making under stress: an overview for emergency managers / K. Kowalski, C. Trakofler // Int. Journal of Emerg. Management. – 2003. – vol. 1(3) – pp. 278–289.

3. Pawlak, Z. Flow Graphs and Decision Algorithms. / Z. Pawlak // Proc. Ninth International Conference on Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing. – 2003. – pp. 2463–2468.

1.7 Assignments to the laboratory work

Undertake a study one of the following viruses: (1) Flame; (2) Gauss; (3) Duqu; (4) Regin; (5) Shamoon; (7) Zeus; (8) Narilam.

Laboratory work 2
EMERGENCY MANAGEMENT AND DECISION MAKING IN COMPLEX ENVIRONMENTS

Goal and objectives: In this laboratory work we'll discover a formal decision-making framework and study how to optimize decision making when one is faced with a mix of qualitative, quantitative, and conflicting factors that are taken into consideration during emergency management in complex environments.

Learning objectives:

- study the main techniques of Multi-Criteria Decision Analysis (MDCA) applicable for group decision making in cybersecurity and resilience;
- gain basic knowledge about multiple choice decision analysis;
- study the multi-criteria decision analysis methods suitable for complex environments;

Practical tasks:

- acquire practical skills in working with typical MCDA method;
- master the process of developing models for emergency management in respect to cybersecurity problem;
- acquire practical skills in working with decision making software based on the AHP and the ANP.

Exploring tasks:

- discover how GDM can improve emergency management effectiveness in complex environments;
- investigate MDCA techniques to deal with incomplete and imprecise information in different emergency situations.

Setting up

In preparation for laboratory work it is necessary:

- to clear the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1,2];
- to familiarize oneself with the main procedures and specify the exploration program according to defined task.

Recommended software and resources: *SuperDecisions* (http://www.superdecisions.com/)

2.1 Synopsis

Human decision-making involves the use of intelligence, wisdom and creativity in order to satisfy basic needs or to survive. Evaluating a decision requires several considerations such as the benefits derived from making the right decision, the costs, the risks, and losses resulting from the actions (or non-actions) taken if the wrong decision is made.

2.2 Brief theoretical information:

As the emergency is always complex and involves many aspects, it needs the consensus decision that is made by experts, government workers, the public and other relevant departments. Accordingly, using group decision support systems (GDSS) to handle emergency decision problems could be extremely valuable.

Streamlined process of solving problems and tasks involves the following steps, if necessary, performed simultaneously, in parallel, iteratively, to return to the execution of the previous steps:

1. The situation analysis (problem situation analysis);
2. Identifying the problem and goal setting;
3. Search the information you need;
4. Formation of a set of possible solutions;
5. Formation of making the evaluation criteria;
6. The development of indicators and criteria for monitoring the implementation of decisions;
7. Evaluation of solutions;
8. Choosing the best solutions;
9. Implementation;
10. Monitoring of the implementation;
11. Evaluation of results.

2.2.1 Multi-Criteria Decision Analysis methods

There is no doubt that group decision making in cybersecurity and resilience has multiple criteria to meet simultaneously. Such decisions can envelop quantitative, qualitative, tangible and intangible factors. Multi-Criteria Decision Analysis (MCDA) is a generic approach that can empower decision makers to consider all the decision criteria and decision factors, resolve the conflicts between them, and arrive at justified choice. Over the past three decades, several variants of MCDA

have been developed. This section compares four widely used MCDA methods: AHP, ANP, fuzzy set theory and fuzzy AHP/ANP.

2.2.1.1 Analytical Hierarchy Process (AHP)

Analytical Hierarchy Process (AHP) was introduced by T. Saaty [1] for solving unstructured problems. Since its introduction, AHP has become one of the most widely used analysis methods for multi-criteria decision making.

AHP uses the judgments of decision makers to form a decomposition of problems into hierarchies. Problem complexity is represented by the number of levels in the hierarchy which combine with the decision-maker's model of the problem to be solved. The hierarchy is used to derive ratio-scaled measures for decision alternatives and the relative value that alternatives have against organizational goals (customer satisfaction, product/service, financial, human resource, and organizational effectiveness) and project risks. AHP uses matrix algebra to sort out factors to arrive at a mathematically optimal solution. AHP is a time-tested method that has been used in multi-billion dollar decisions.

Typical applications where AHP has been used are in:

– Prioritizing factors and requirements that impact software development and productivity,

– Choosing among several strategies for improving safety features in motor vehicles,

– Estimating cost and scheduling options for material requirements planning (MRP),

– Selecting desired software components from several software vendors,

– Evaluating the quality of research or investment proposals.

AHP also uses actual measures like price, counts, or subjective opinions as inputs into a numerical matrix. The outputs include ratio scales and consistency indices derived by computing eigenvalues and eigenvectors.

The strength of AHP is that it can handle situations in which the unique subjective judgments of the individual decision makers constitute an important part of the decision making process. However, its key drawback is that it does not take into account of the relationships between different decision factors.

2.2.1.2 Analytic Network Process

Analytic Network Process (ANP) is the evolution of AHP. Given the limitations of AHP such as sole consideration of one way hierarchical relationships among decision factors, failure to consider interaction between various factors and "rank reversal", ANP has been developed as a more realistic decision method. Many decision problems cannot be built as hierarchical as in AHP because of dependencies (inner/ outer) and influences between and within clusters (goals, criteria and alternatives). ANP provides a more comprehensive framework to deal with decisions without making assumptions about the independence of elements between different levels and within the same level. In fact, ANP uses a network without the need to specify levels as in a hierarchy and allows both interaction and feedback within clusters of elements (inner dependence) and between clusters (outer dependence). Both AHP and ANP share the same drawbacks:

(a) With numerous pairwise comparisons, perfect consistency is difficult to achieve. In fact, some degree of inconsistency can be expected to exist in almost any set of pairwise comparisons.

(b) They can only deal with definite scales in reality, i.e. decision makers are able to give fixed value judgments to the relative importance of the pair wise attributes. In fact, decision makers are usually more confident giving interval judgments rather than fixed value judgments.

Furthermore, on some occasions, decision makers may not be able to compare two attributes at all due to the lack of adequate information. In these cases, a typical AHP/ANP method will become unsuitable because of the existence of fuzzy or incomplete comparisons. It is believed that if uncertainty (or fuzziness) of human decision making is not taken into account, the results can be misleading.

2.2.1.3 Fuzzy set theory

To deal quantitatively with such imprecision or uncertainty, fuzzy set theory is appropriate. Fuzzy set theory was designed specifically to mathematically represent uncertainty and vagueness, and to provide formalized tools for dealing with the imprecision intrinsic to multi-criteria decision problems. The main benefit of extending crisp analysis methods to fuzzy technique is in its strength

that it can solve real-world problems, which have imprecision in the variables and parameters measured and processed for the application.

2.2.1.4 Fuzzy AHP/ ANP

Fuzzy AHP/ANP is considered as an important extension of the conventional AHP/ANP. A key advantage of the fuzzy AHP/ANP is that it allows decision makers to flexibly use a large evaluation pool including linguistic terms, fuzzy numbers, precise numerical values and ranges of numerical values. Hence, it provides the capability of taking care of more comprehensive evaluations to provide more effective decision support. Details of the key features, strengths and weaknesses of different MCDA methods are compared in Table 2.1.

Table 2.1. Comparison between different MCDA methods (adapted from [6])

Analysis methods	Key elements	Strengths	Weaknesses
AHP	Multi-criteria and multi-attributes hierarchy; Pair wise comparison; graphical representation.	Can handle situations in which decision maker's subjective judgments constitute a key part of the decision making process	Relationships between decision factors are not considered; inconsistency of the pairwise judgments; cannot deal with uncertainty and vagueness
ANP	Control network with sub-networks of influence	Allows interaction and feedback between different decision factors	Inconsistency of the pairwise judgments; cannot handle situations where decision makers can only give interval value judgments or cannot give values at all
Fuzzy set theory	Mathematical representation; handle uncertainty, vagueness and imprecision; grouping data with loosely defined boundaries.	Can solve real-world decision problems with imprecision variables	Lack of a systematic weighting system

Table 2.1 Comparison between different MCDA methods (continuation)

Fuzzy AHP/ ANP	Fuzzy membership functions together with priority weights of attributes	Combined strengths of fuzzy set theory and AHP/ANP	Time consuming; complexity.

2.2.2 General information about *SuperDecisions* software

SuperDecisions is decision making software based on the Analytic Hierarchy Process (AHP) and the Analytic Network Process (ANP). Decision making is all about setting priorities and the AHP and ANP, award-winning decision processes are the way to do that.

In the *SuperDecisions* software priorities are derived through a series of pairwise comparisons on the factors of the problem that can include both tangibles and intangibles.

2.2.2.1 Creating a new model in the SuperDecisions

Let's assume we need to choose the best plan of action during the accident on the railway (e.g., rail tank car with hazardous chemical substance had been turned over and emergency response required), with the specified criteria. The plan is shared.

To create a new model select Design→ Cluster→ New to create cluster (fig.2.1).

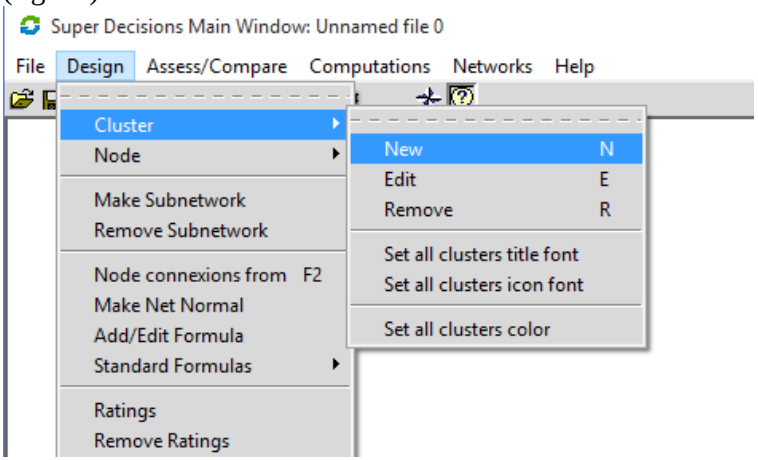


Figure 2.1 – Pop-up windows to creating a new model

Enter cluster name, short description and save your notes.

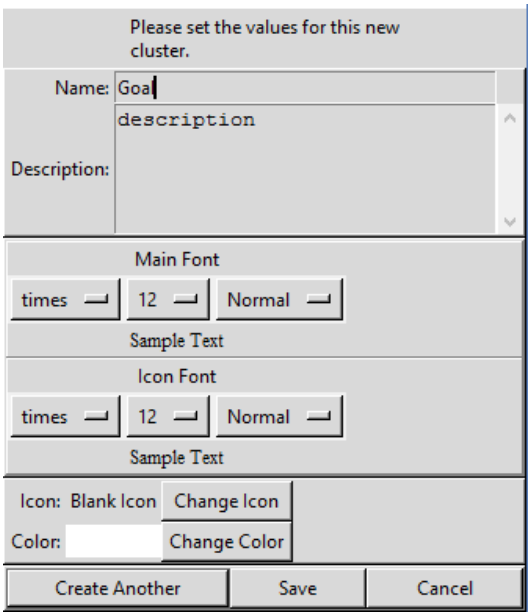


Figure 2.2 – Setting the values for new cluster

Right-click on cluster background will open a dropdown menu. Click “create node in cluster”.

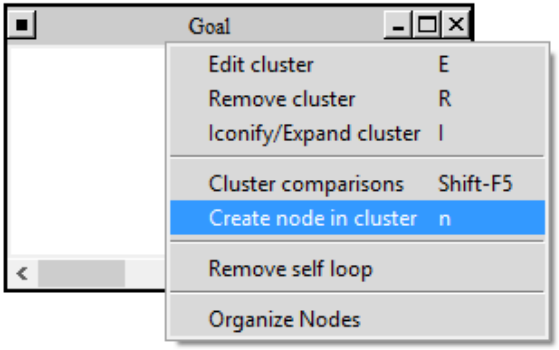


Figure 2.3 – Pop-up windows to creating a node in cluster

Enter node name “The Best Plan of Action” and description (optional).

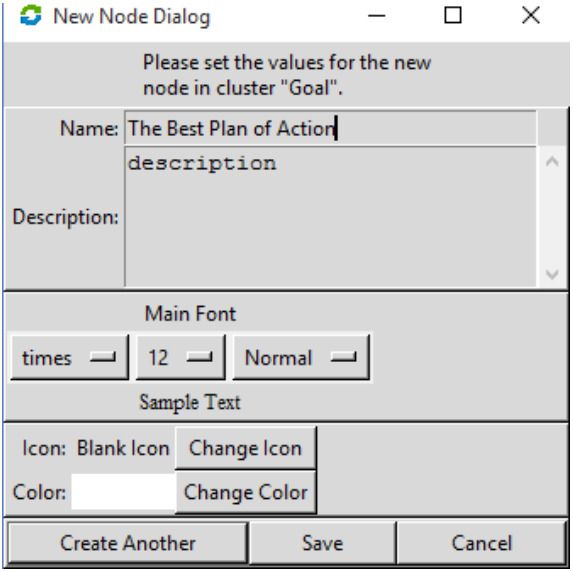
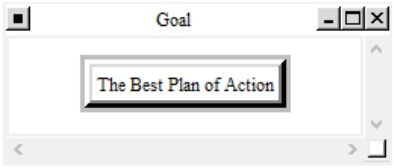


Figure 2.4 – New Node window

Add another cluster with 3 alternatives of accidents on chemically hazardous objects: transport accident, accident on enterprise workshops, and accident on warehouses.



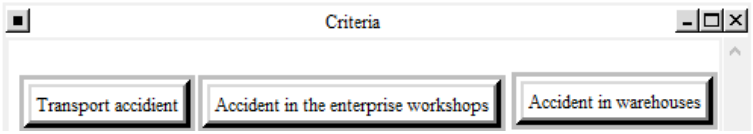


Figure 2.5 – Adding alternatives

Left-click “Do connections” icon to depress it and enter “make connections” mode.

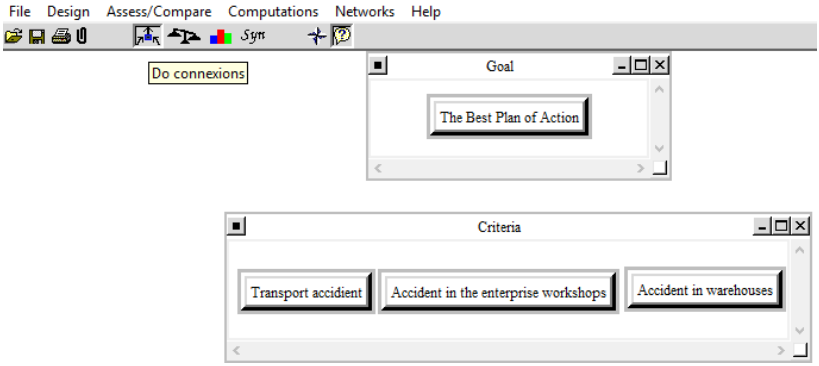


Figure 2.6 – Making connections

Left-click on “from” or parent node.

Right-click successively on “to” or children nodes. Link is been automatically appears between clusters.

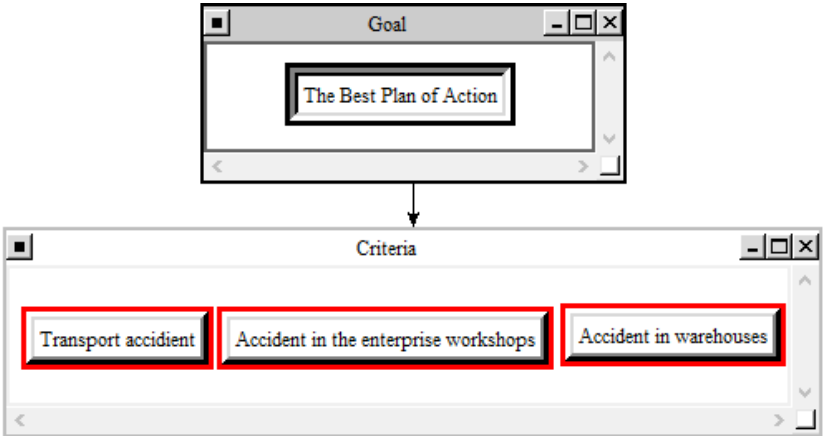


Figure 2.7 – Connecting alternatives

Left-click on “parent node” then left-click on “comparisons” icon  to launch comparison node selector. Left-click on “Node”.

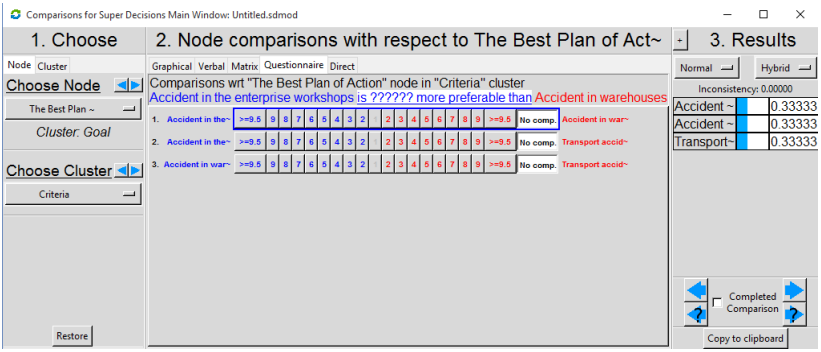


Figure 2.8 – Launching comparison node selector

Select “Questionnaire”. Select “Comparisons words” and change comparison word to preference (optional) and save changes.

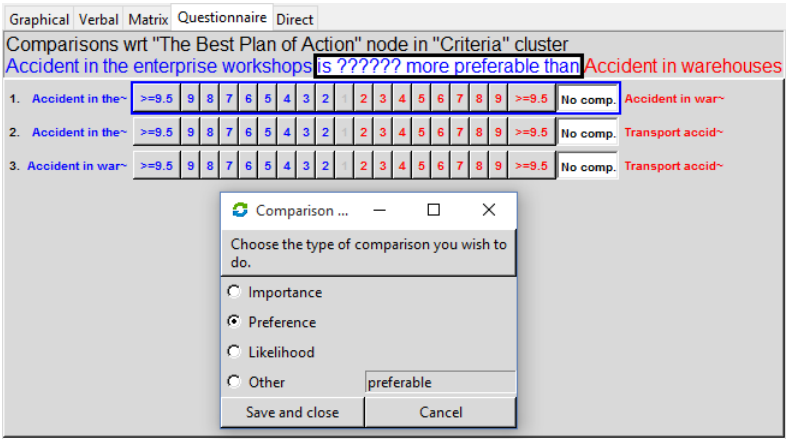


Figure 2.9 – Setting the type of comparison options

Set the value. Since we consider the case with the transport incident that introduces such values.

Figure 2.10 – Setting parameter value

In the lower right corner, put a checkmark and close.

Adding further criteria, as a result we get the following scheme in case of accidents on chemically hazardous object (fig.2.11).

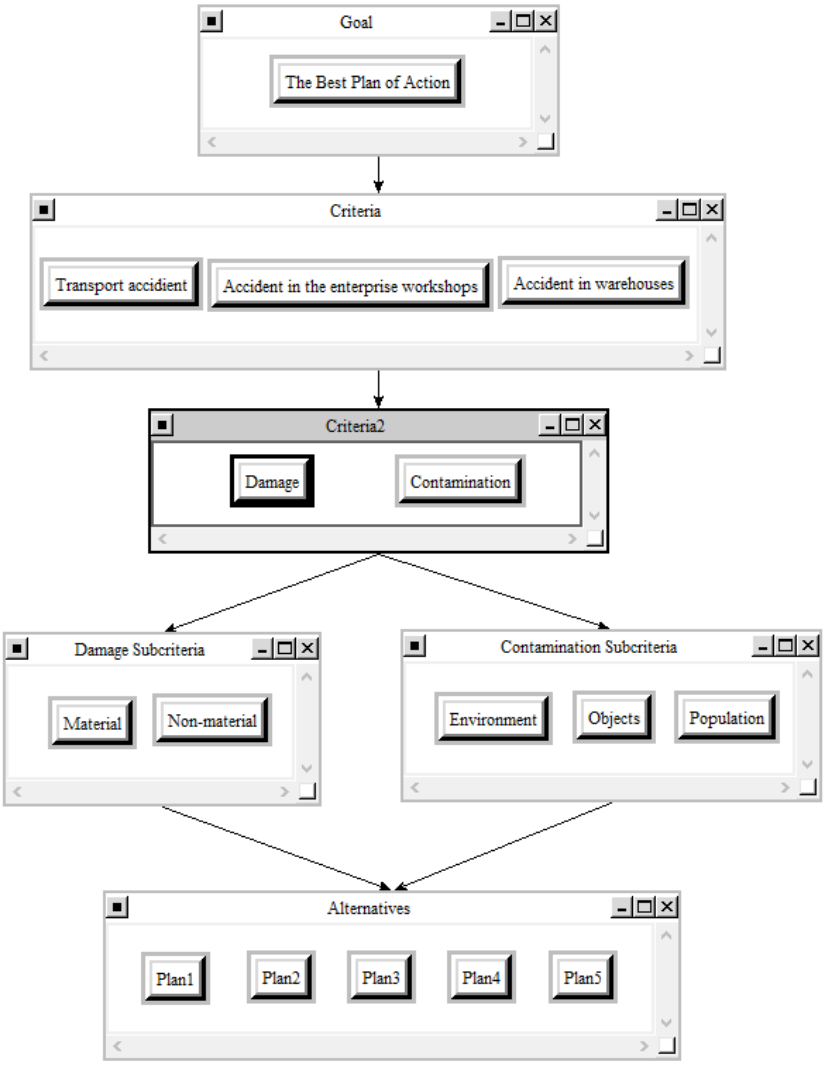
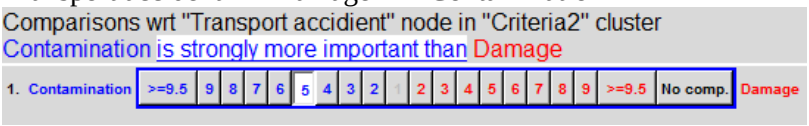


Figure 2.11 – An example of the action plan in case of accidents on chemically hazardous objects

2.2.2.2 Work out the different action plans at targeted emergency

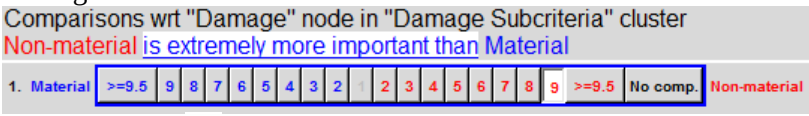
To analyze different plans you need to construct all schema relations. Comparison process can be represented in the following.

Transport accident → Damage <-> Contamination

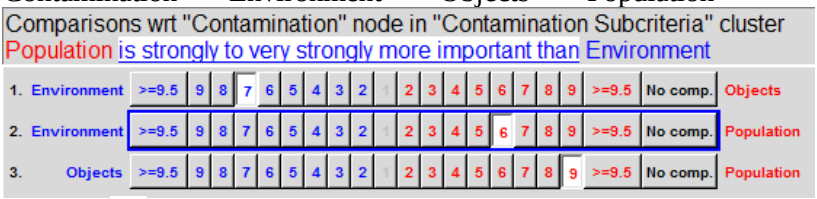


Since we are considering only traffic accident here, so we excluded the other criteria (enterprise workshops, warehouses), subject to the same.

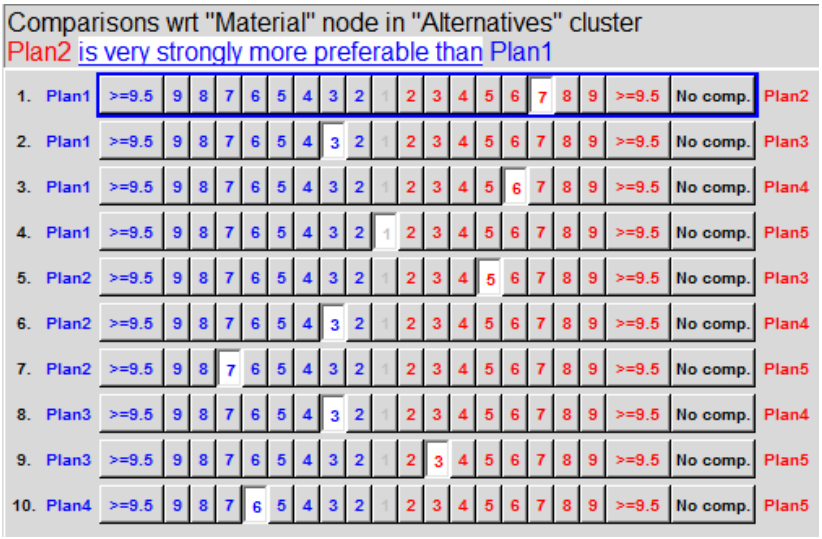
Damage→ Material<->Non-material



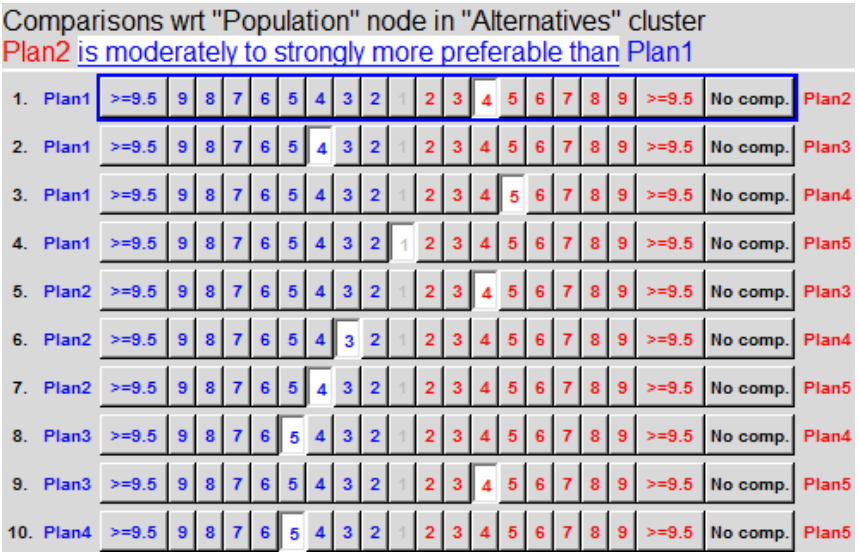
Contamination → Environment <-> Objects <-> Population



Material → Plan 1 <-> Plan 2 <-> Plan 3 <-> Plan 4 <-> Plan 5



The same with other parameters:
Non-material → Plan 1 <-> Plan 2 <-> Plan 3 <-> Plan 4 <-> Plan 5
Environment → Plan 1 <-> Plan 2 <-> Plan 3 <-> Plan 4 <-> Plan 5
Objects → Plan 1 <-> Plan 2 <-> Plan 3 <-> Plan 4 <-> Plan 5
Population → Plan 1 <-> Plan 2 <-> Plan 3 <-> Plan 4 <-> Plan 5



When all values are entered you need to click Syn on the top bar of the main window.

This opens a window that displays all the alternative plans with their coefficients (fig.2.12).

Name	Graphic	Ideals	Normals	Raw
Plan1		0.592251	0.156674	0.039169
Plan2		1.000000	0.264540	0.066135
Plan3		0.759530	0.200926	0.050232
Plan4		0.869487	0.230014	0.057503
Plan5		0.558879	0.147846	0.036961

Figure 2.12 – Visible representations of the global priorities for five alternatives

Here we can observe that the best action plan during the transport incident would be a Plan 2.

2.2.2.3 Other comparison mode

To demonstrate effectiveness of different scenario of emergency management you can use additional tools (fig. 2.13-2.16).

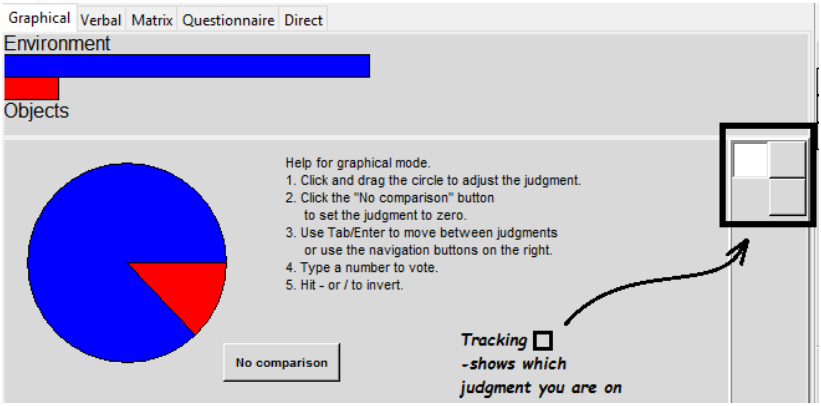


Figure 2.13 – Graphical representation

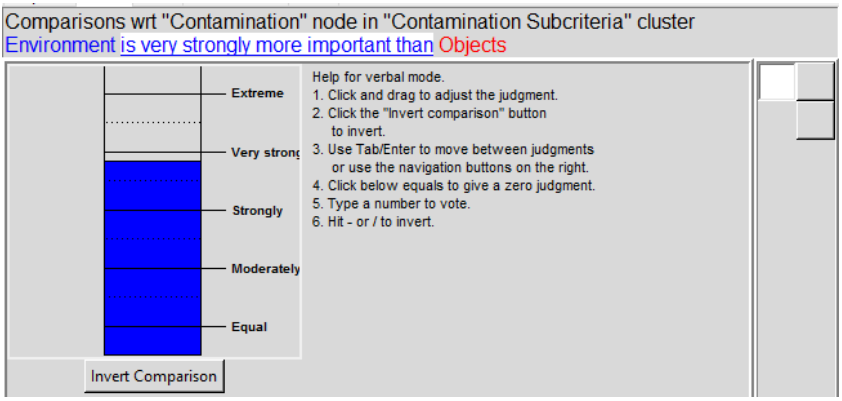


Figure 2.14 – Verbal mode

The Matrix mode for entering judgments is shown in fig.2.15. These are equivalent to the judgments shown in the Questionnaire Mode.

Note that the arrow next to the judgment points to the preferred member of the pair.

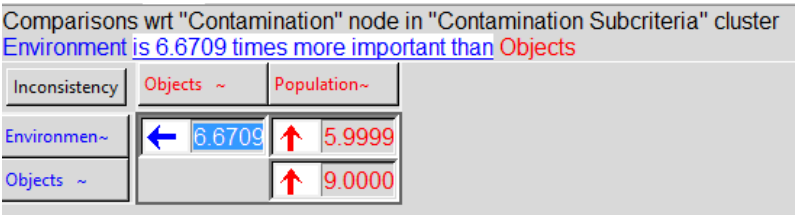


Figure 2.15 – Matrix representation

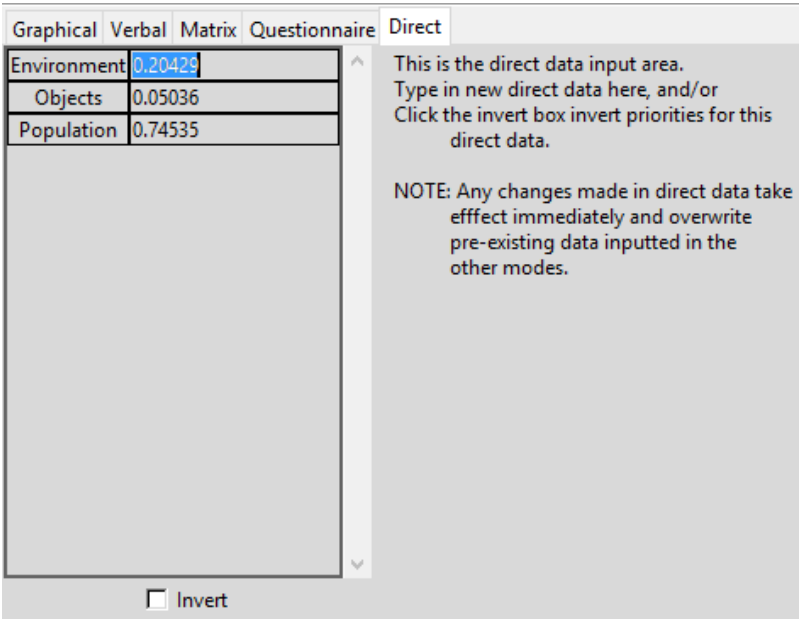


Figure 2.16 – Direct data input area

2.3 Execution order and discovery questions:

1. Obtain the initial data to perform individual task (see section 2.7).

2. Using multiply sources (Internet search, local ‘experts’, site plans, diagrams, etc.), perform problem situation analysis and identify the problem, goal, and tasks. Think about the main elements and decide what

kind of logical groupings of nodes and clusters would best describe the problem;

3. Search the information you need to decision making;

4. Draw up a table with a set of alternatives of accidents ('worst case scenario'), links, possible solutions, and evaluation criteria;

5. Develop indicators and criteria for monitoring the implementation of decisions;

6. Set up your lab environment according to the specifications below.

6.1. To installing the *SuperDecisions* software visit website http://www.superdecisions.com/;

6.2. Register on this website then login.

6.3. Download *SuperDecision* software. To do this select the install file you need for your computer's operating system and click the Download button. You must be logged in and agree to the license before you can download the software. It runs on Windows 7, Windows 10, the Mac and Linux.

6.4. Go to http://www.superdecisions.com/get-serial-number/.

6.5. Get your serial number and register your program. To obtain the serial number you must be logged in.

7. With *SuperDecisions* software, develop a model for emergency management and draw an action plan in case of accidents. For more information refer to [3-5].

8. Work out the different plans of action at targeted emergency and choose the set of best solutions;

9. Evaluate results.

2.4 Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

- (I): background / theory, purpose and discovery questions
- (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures
- (R): narrate (like a story), tables, indicate final results;
- (D): answers on discovery questions, explanation of results, conclusion / summary

2.5 Test questions:

2. What mathematical theory can be used to deal systematically with all kinds of dependence and feedback?
3. The main steps to build an Analytic Network Process (ANP) network.
4. Criteria for evaluating alternative solutions.
5. How do you know when you've obtained best decision?

2.6 Recommended literature:

1. Saaty T.L, Vargas L.G Models, Methods, Concepts and Applications of the Analytic Hierarchy Process / Kluwer, Dordrecht, Springer US (2001). – 333 p.
2. Noyes J., Cook M. Decision Making in Complex Environments / CRC Press (2007). – 458 p.
3. Manual for building ANP Decision Models [Digital edition] - http://www.superdecisions.com/wp-content/uploads/Manual-for-building-ANP-Decision-Models.doc
4. Tutorial on SuperDecisions software [Digital edition] - http://www.superdecisions.com/category/support/tutorials/
5. SuperDecision Software Guide [Digital edition] - http://www.ii.spb.ru/admin/docs/SuperDecisionsHelp2011.pdf
6. Velasquez M., Hester P. T. An Analysis of Multi-Criteria Decision Making Methods // International Journal of Operations Research Vol. 10, No. 2, (2013) – pp. 56–66. [Digital edition] - http://www.orstw.org.tw/ijor/vol10no2/ijor_vol10_no2_p56_p66.pdf

2.7 Assignments to the laboratory work

Undertake a study of one of the following emergences:

(1) Power outage; (2) Internet Blackout; (3) Act of terrorism; (4) The explosion in the reactor compartment of nuclear power stations

Laboratory work 3
ANALYSIS OF GROUP DECISION MAKING AND EMERGENCY MANAGEMENT MODEL BASED ON INTUITIONISTIC FUZZY SETS

Goal and objectives: In this laboratory work we'll discover how a group decision-making methodology (GDMM) based on intuitionistic fuzzy sets can be used to solve the emergency group decision-making problem. The main purpose of the multi-criteria GDMM is to improve decision accuracy, and to enhance decision transparency and thus to increase decision effectiveness.

Learning objectives:

- study the general framework for the group decision-making methodology;
- gain basic knowledge of intuitionistic fuzzy sets
- study IFWG operators to aggregate individual's preference into the group preference;

Practical tasks:

- acquire practical skills in working with group decision making model base on intuitionistic fuzzy sets;
- use score function to judge the intuitionistic fuzzy numbers;
- acquire practical skills in developing models for group decision support system (GDSS) in emergency response.

Exploring tasks:

- discover how GDSS can improve emergency management effectiveness and decision transparency;
- investigate how the incomplete intuitionistic judgment matrix is constructed to convey the information of experts in group decision making.

Setting up

In preparation for laboratory work it is necessary:

- to clear the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1,2];
- to familiarize oneself with the main procedures and specify the exploration program according to defined task.

Recommended software and resources: *GDSS*

3.1 Synopsis

In emergency decision making, the decision makers may be hesitated and lack of knowledge. To solve this group decision making problem, a method that based on incomplete intuitionistic judgment matrix will be analyzed for emergency management. In this laboratory work, the incomplete intuitionistic judgment matrix is constructed to convey the information of experts in group decision making.

The reality of a group decision making generates a requirement for creating communication links between the members of the decision-making group with a common understanding of the syntax and semantics of the underlying cybersecurity issues. Decisions made in an ad-hoc, unstructured or semi-structured manner, based on the availability of only a subset of the decision-making group at the time of decisions, has a high probability of being not just suboptimal but utterly wrong, with disastrous results.

3.2 Brief theoretical information:

3.2.1 Description of the emergency decision problem

As the emergency is always unconventional, sudden and complex, it is necessary to invite experts from different fields to make decisions. It is impossible to make an emergency plan considering all aspects of the emergency. The realistic choice is that we should have many emergency plans and let the decision makers to choose a best one. So, the emergency decision is a group decision-making problem. As the emergency decision-making must be made in a short time using partial or incomplete information, the decision makers may be hesitant and unfamiliar with some aspects of the emergency.

In this laboratory work we'll use intuitionistic fuzzy sets to solve the problem.

The description of the emergency group decision-making problem is as the following:

$Y=(Y_1, Y_2,\ldots,Y_n)$: the emergency plans that are made by emergency department to deal with the emergency.

Y_i stands for the i-th emergency plan, i =1,2,…, n.

$E=(e_1, e_2,\ldots,e_l)^T$: the decision makers from different field to deal with the emergency, e_k stands for the k-th decision maker.

$\mu_{ij}^{(k)}$: the certain degree to which Y_j is preferred to Y_i that is assessed by emergency decision maker e_k.

$v_{ij}^{(k)}$: the certain degree to which Y_j is preferred to Y_i that is assessed by emergency decision maker e_k.

$1-\mu_{ij}^{(k)}-v_{ij}^{(k)}$: the uncertain degree to which Y_j is preferred to Y_i that is assessed by emergency decision maker e_k.

$\xi=(\xi_1, \xi_2,\ldots, \xi_l)^T$: the weight vector of the emergency decision makers.

The general framework for the GDMM is given in fig.1.

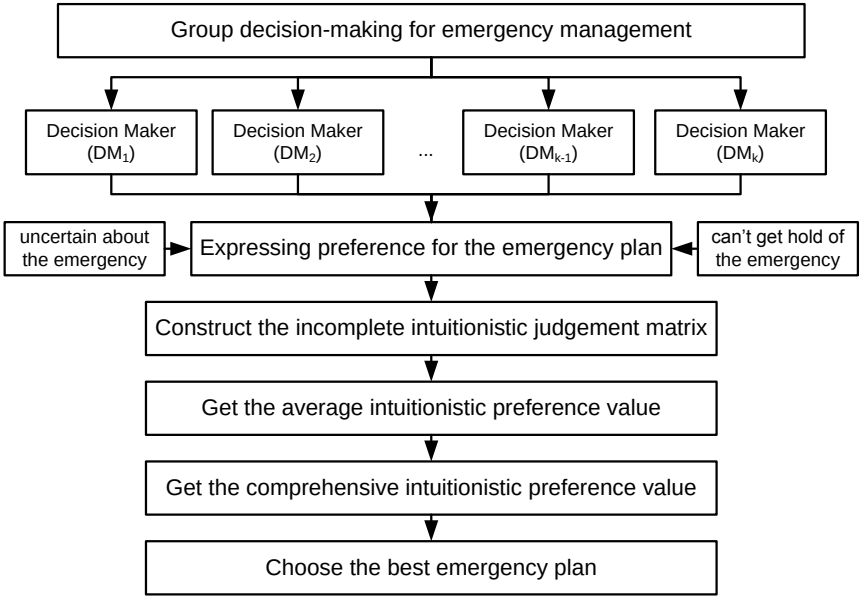


Figure 3.1 – General framework for the GDMM [2].

First, the emergency group decision making problem is described. As the emergency is always complex, the decision maker is usually hesitant and cannot get hold of the emergency because of the lack of information. So the incomplete intuitionistic judgment matrix is proposed when the decision makers express their preference for the emergency plan. Based on intuitionistic fuzzy set, we can get the average intuitionistic preference value and the comprehensive

intuitionistic preference value. Finally, choose the best emergency plan to deal with the emergency.

3.2.2 Basic knowledge of intuitionistic fuzzy sets

Definition 1: Let $Q = (q_{ij})_{n\times n}$ be the intuitionistic judgment matrix [3], where $q_{ij} = (\mu_{ij}, v_{ij})$, i,j=1,2,…,n, μ_{ij} stands for the decision maker's preference to Y_i when they compare Y_i with Y_j, v_{ij} stands for the decision maker's preference

$$\begin{aligned}&\mu_{ij} \in [0,1],\ v_{ij} \in [0,1],\ 0 \le \mu_{ij} + v_{ij} \le 1,\ \mu_{ji} = v_{ij},\ \mu_{ii} = v_{ii} = 0,5\\&(i, j = 1, 2, ..., n)\end{aligned} \tag{3.1}$$

then we call Q the intuitionistic judgment matrix.

Definition 2: Let $Q = (q_{ij})_{n\times n}$ be the intuitionistic judgment matrix, if it contains incomplete elements and complete elements, be the incomplete elements, if

$$\begin{aligned}&0 \le \mu_{ij} + v_{ij} \le 1,\ \mu_{ji} = v_{ij},\ v_{ji} = \mu_{ij},\ \mu_{ii} = v_{ii} = 0,5\\&(i, j = 1, 2, ..., n)\end{aligned} \tag{3.2}$$

then we call Q the intuitionistic judgment matrix.

Definition 3: If $q_{ij}=(\mu_{ij}, v_{ij})$ and $q_{kl}=(\mu_{kl}, v_{kl})$ are two intuitionistic fuzzy values, then

(1) $q_{ij} = (v_{ij}, \mu_{ij})$.

(2) $q_{ij} + q_{kl} = (\mu_{ij} + \mu_{kl} - \mu_{ij} \cdot \mu_{kl},\ v_{ij} \cdot v_{ij})$.

(3) $q_{ij} \cdot q_{kl} = (\mu_{ij} \cdot \mu_{ij},\ v_{ij} + v_{kl} - v_{ij} \cdot v_{kl})$.

(4) $\lambda q_{ij} = (1-(1-\mu_{ij})^{\lambda},\ v_{ij}^{\lambda}),\ \ \lambda > 0.$

(5) $q_{ij}^{\lambda} = (\mu_{ij}^{\lambda},\ 1-(1-v_{ij})^{\lambda}),\ \ \lambda > 0.$

Definition 4: Let $Q = (q_{ij})_{n\times n}$ be the incomplete intuitionistic judgment matrix, if $q_{ij} = q_{ik} \otimes q_{ki}$, $q_{ij}, q_{ik}, q_{ki} \in \Omega$, then we call Q the consistency incomplete intuitionistic judgment matrix.

Definition 5: Let $Q = (q_{ij})_{n\times n}$ be the incomplete intuitionistic judgment matrix, if $(i, j)\cap(k, l) \neq \acute{O}$, then we call the element q_{ij} and q_{kl} are adjacent.

Definition 6: Let $Q = (q_{ij})_{n\times n}$ be the incomplete intuitionistic judgment matrix, if each unknown element can be got from its adjacent elements, Q is acceptable, or Q is unacceptable.

In the face of the emergency, the decision maker ($e_k \in E$) is usually hesitant and uncertain, they gives the preference after compare two contingency plans, and we can get $q_{ij}^{(k)} = (\mu_{ij}^{(k)}, v_{ij}^{(k)})$, where μ_{ij} stands for the decision maker's preference to Y_i when they compare Y_i with Y_j, v_{ij} stands for the decision maker's preference.

Let $q_{ij}^{(1)}, q_{ij}^{(2)}, ..., q_{ij}^{(m)}$ be m intuitionistic fuzzy values, where $q_{ij}^{(c)} = (\mu_{ij}^{(c)}, v_{ij}^{(c)})$, c=1,2,…,m, and let $w = (w_1, w_2, ..., w_m)^T$ be the weight vector of $q_{ij}^{(1)}, q_{ij}^{(2)}, ..., q_{ij}^{(m)}$, then the aggregated value q_{ij} of $q_{ij}^{(1)}, q_{ij}^{(2)}, ..., q_{ij}^{(m)}$ is also an intuitionisitic fuzzy value, where q_{ij} is obtained by using the intuitionisitic fuzzy weighted arithmetic averaging operator:

$$q_{ij} = \sum_{c=1}^{m} w_c q_{ij}^{(c)}, \quad i, j = 1, 2, ..., n, \tag{3.3}$$

or by using the intuitionist fuzzy weighted geometric averaging operator:

$$q_{ij} = \prod_{c=1}^{m} (q_{ij}^{(c)})^{w_c} \quad i, j = 1, 2, ..., n. \tag{3.4}$$

In particular, if $w = (1/m, 1/m, ..., 1/m)^T$, then (3.3) and (3.4) are, respectively, reduced to the intuitionistic fuzzy arithmetic averaging operator:

$$q_{ij} = \frac{1}{c}\sum_{c=1}^{c} w_c q_{ij}^{(c)}, \quad i, j = 1, 2, ..., n \tag{3.5}$$

and the intuitionisitic fyzzy geometric averaging operator:

$$q_{ij} = \prod_{c=1}^{m} (q_{ij}^{(c)})^{\frac{1}{m}} \quad i, j = 1, 2, ..., n. \tag{3.6}$$

3.2.3 Group decision making model base on intuitionistic fuzzy sets

Here we introduce the incomplete intuitional judgment matrix to express the preference of the decision maker. The decision makers express their preference according the knowledge about the emergency and we will aggregate individual preference to group preference, and finally get the best emergency plan.

Step 1: Construct the incomplete intuitionistic judgment matrix

As the emergency is complex and sudden, the decision maker may be hesitant and can't get enough knowledge, they can make space when express the preference, then we can get the incomplete intuitional judgment matrix $Q_k = (q_{ij}^{(k)})_{n\times n}$, where

$$q_{ij}^{(k)} = (\mu_{ij}^{(k)}, \nu_{ij}^{(k)}), \quad 0 \le \mu_{ij}^{(k)} + \nu_{ij}^{(k)} \le 1, \quad \mu_{ji}^{(k)} = \nu_{ij}^{(k)}, \quad \nu_{ji} = \mu_{ij},$$
$$\mu_{ii}^{(k)} = \nu_{ii}^{(k)} = 0.5 \quad (i, j \in \Omega).$$

As defined in 3.2.2, Q_k should be acceptable. If Q_k is unacceptable, the decision maker needs to construct a new one until it is acceptable.

Step 2: Construct the improved incomplete intuitionistic judgment matrix

As described in previous step, we can get the acceptable incomplete intuitionistic judgment matrix from each emergency decision maker. As there are incomplete and unknown elements in the intuitionistic judgment matrix, we should estimate them through other known elements.

Let $Q_k = (q_{ij}^{(k)})_{n\times n}$ be the acceptable incomplete intuitionistic judgment matrix, if each unknown element can be got through

$$q_{ij} = (\bigotimes_{k\in N_{ij}} (q_{ik} \otimes q_{kj}))^{\frac{1}{n_{ij}}}, \tag{3.7}$$

where $N_{ij} = \{k \,|\, q_{ik}, \quad q_{kj} \in \Delta\}$, then we get the improved $Q_k = (q_{ij}^{(k)})_{n\times n}$:

$$q_{ij} = \begin{cases} q_{ij}, & q_{ij} \in \Omega, \\ q_{ij}, & q_{ij} \notin \Omega. \end{cases} \tag{3.8}$$

The improved intuitionistic judgment matrix contains both the direct intuitionistic preference information given by the emergency decision maker and the indirect intuitionistic preference information derived from the known intuitionistic preference information.

Step 3: Get the average intuitionistic preference value through IFWA operators Through Institutionistic Fuzzy Weighted Aggregation (IFWA) operators:

$$q_i^{(k)} = \frac{1}{n}(q_{i1}^{(k)} \oplus q_{i2}^{(k)} \oplus \ldots \oplus q_{in}^{(k)}) \tag{3.9}$$

we can aggregate the intuitionistic preference value of emergency plan, then get the average intuitionistic preference value.

Step 4: Get the comprehensive intuitionistic preference value through IFWG operators

Through Intuitionistic Fuzzy Weighted Geometric (IFWG) operator:

$$q_i = (\xi_1 q_i^{(1)} \oplus \xi_2 q_i^{(2)} \oplus \ldots \oplus \xi_l q_i^{(l)}). \tag{3.10}$$

We can aggregate the intuitionistic preference value of emergency plan, and then get the comprehensive intuitionistic preference value.

Step 5: Choose the best emergency plan

Definition 6: For any intuitionistic fuzzy number $q_{ij} = (\mu_{ij}, v_{ij})$, we can asses it through the score function $s(q_{ij})$:

$$s(q_{ij}) = \mu_{ij} - v_{ij} \tag{3.11}$$

Where $s(q_{ij})$ is the score value, $s(q_{ij}) \in [-1, 1]$.The larger the score $s(q_{ij})$, the greater the intutionistic fuzzy value q_{ij}.

Definition 7: For any intuitionistic fuzzy number, we can asses it through the accuracy function:

$$h(q_{ij}) = \mu_{ij} + v_{ij} \tag{3.12}$$

to evaluate the degree of accuracy of the intuitionistic fuzzy value *i* q_{ij}, where $h(q_{ij}) \in [-1, 1]$. The larger the value of $h(q_{ij})$, the more the degree of accuracy of the intuitionistic fuzzy value q_{ij}.

Normally, we use score function to judge the intuitionistic fuzzy numbers, in some special circumstances, such as the score value of two groups of intuitionistic fuzzy number is the same and it cannot through the score function to judge, then we can use the accuracy function to judge.

Definition 8: Let $q_{ij} = (\mu_{ij}, v_{ij})$ and $q_{kl} = (\mu_{kl}, v_{kl})$ be two intuitionistic fuzzy values, $s(q_{ij}) = \mu_{ij} - v_{ij}$ and $s(q_{kl}) = \mu_{kl} - v_{kl}$ be the scores of q_{ij} and q_{kl}, respectively, and let $h(q_{ij}) = \mu_{ij} + v_{ij}$ and $h(q_{kl}) = \mu_{kl} + v_{kl}$ be the accuracy degrees of q_{ij} and q_{kl}, respectively, then

If $s(q_{ij}) < s(q_{kl})$, then q_{ij} is smaller than , denoted by $q_{ij} < q_{kl}$.

If $s(q_{ij}) = s(q_{kl})$, then

(1) If $h(q_{ij}) = h(q_{kl})$, then q_{ij} and q_{kl} represent the same information, denoted by $q_{ij} = q_{kl}$.

(2) If $h(q_{ij}) < h(q_{kl})$, then q_{ij} is smaller than q_{kl}, denoted by $q_{ij} < q_{kl}$.

According formula (3.5) and (3.6), we can sort the comprehensive intuitionistic preference value q_i (i=1,2, …,n), then we can sort the emergency plans Y_i (i =1,2, …,n) and choose the best one.

3.3 Execution order and discovery questions:

1. Set up your lab environment according to the specifications below; draw and annotate your testing environment.
2. According to your personal task, analyze four emergency plans considering with different emergency situations.
3. Construct the incomplete intuitionistic judgment matrix.
4. Use (3.7) to construct the improved intuitionistic judgment matrix.
5. Use (3.3) to aggregate all corresponding to the emergency plan Yi, and then get the averaged intuitionistic fuzzy value of the emergency plan over all the other emergency plans.
6. Use (3.4) to aggregate all into a collective intuitionistic fuzzy value of the emergency plan over all the other emergency plans.
7. Choose the best emergency plan through formula (3.11).
8. Evaluate results.

3.4 Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

- (I): background / theory, purpose and discovery questions
- (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures
- (R): narrate (like a story), tables, indicate final results;
- (D): answers on discovery questions, explanation of anomalies, conclusion / summary

3.5 Test questions:

1. Describe the emergency group decision-making problem in terms of cybersecurity issues.
2. For what purpose incomplete intuitionistic judgment matrix can be used?
3. What is the core of GDMM?

4. How to choose the best emergency plan to deal with the emergency with GDMM?

3.6 Recommended literature:

1. Miller S., Garibaldi J.M., Appleby S. Evolving OWA Operators for Cyber Security Decision Making Problems [Digital edition] - http://ima.ac.uk/papers/SSCI2013_SMM_300113_rev.pdf

2. Cheng T., Wu F., Chen Y. A Group Decision Making Methodology for Emergency Decision / IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 3 (2013).– pp. 151-157. [Digital edition] - http://ijcsi.org/papers/IJCSI-10-1-3-151-157.pdf

3. Xu Z S. Intuitionistic Fuzzy Information Aggregation: Theory and Applications / Beijing. Sciences Press (2008). – pp. 134-140.

4. Fan Z.P, Liu Y, Shen R.J. Risk decision analysis method for emergency response based on prospect theory // System Engineering Theory and Practice, Vol.32, No.5, (2012) – pp. 977-984.

5. Bertsch V., Geldermann J. Preference elicitation and sensitivity analysis in multicriteria group decision support for industrial risk and emergency management // International Journal of Emergency Management, Vol.5,No.1-2 (2008). – pp. 7-24.

2.7 Assignment to the laboratory work:

We suppose that there are four decision makers e_k (k =1, 2, 3, 4) (whose weight vector is ξ) to choose the best plan from four emergency plans with respect to cyber infrastructure resources.

To assess the emergency plans, we consider the following four aspects: economic loss, personnel losses, environmental impact and social influence.

In order to deal with the emergency, the emergency department has made four emergency plans considering with different situations. Decision makers has been set up to provide their preference information by incomplete intuitionistic judgment matrix $Q^{(k)}=(q^k_{ij})_{4\times4}$ (k =1, 2, 3, 4) respectively: Q_1, Q_2, Q_3, and Q_4. You need to choose the best emergency plan to deal with the target emergency.

V1

$\xi=(0.22,0.25,0.3,0.23)^T$.

$$Q_1=\begin{pmatrix}(0.5,0.5) & (0.4,0.5) & (x_1,x_2) & (0.3,0.5)\\ (0.5,0.4) & (0.5,0.5) & (0.5,0.3) & (0.4,0.5)\\ (x_2,x_1) & (0.3,0.5) & (0.5,0.5) & (0.3,0.6)\\ (0.5,0.3) & (0.5,0.4) & (0.6,0.3) & (0.5,0.5)\end{pmatrix}$$

$$Q_2=\begin{pmatrix}(0.5,0.5) & (0.4,0.5) & (0.5,0.3) & (0.3,0.5)\\ (0.5,0.3) & (0.5,0.5) & (0.6,0.3) & (x_3,x_4)\\ (0.5,0.3) & (0.3,0.5) & (0.5,0.5) & (0.3,0.6)\\ (x_4,x_3) & (0.4,0.5) & (0.5,0.4) & (0.5,0.5)\end{pmatrix}$$

$$Q_3=\begin{pmatrix}(0.5,0.5) & (x_5,x_6) & (0.4,0.5) & (0.3,0.5)\\ (x_6,x_5) & (0.5,0.5) & (0.5,0.3) & (0.4,0.5)\\ (0.4,0.5) & (0.3,0.5) & (0.4,0.5) & (0.5,0.5)\\ (0.6,0.3) & (0.5,0.4) & (0.6,0.3) & (0.5,0.4)\end{pmatrix}$$

$$Q_4=\begin{pmatrix}(0.5,0.5) & (0.3,0.5) & (0.5,0.3) & (0.3,0.6)\\ (0.5,0.4) & (0.5,0.5) & (x_7,x_8) & (0.3,0.6)\\ (0.3,0.5) & (x_8,x_7) & (0.5,0.5) & (0.5,0.4)\\ (0.5,0.3) & (0.5,0.4) & (0.6,0.3) & (0.5,0.5)\end{pmatrix}$$

V2

$\xi=(0.24,0.24,0.3,0.22)^T$.

$$Q_1=\begin{pmatrix}(0.5,0.4) & (0.4,0.5) & (x_1,x_2) & (0.3,0.5)\\ (0.5,0.5) & (0.5,0.4) & (0.5,0.3) & (0.5,0.5)\\ (x_2,x_1) & (0.4,0.5) & (0.5,0.5) & (0.3,0.6)\\ (0.5,0.3) & (0.5,0.4) & (0.6,0.3) & (0.5,0.5)\end{pmatrix}$$

$$Q_2=\begin{pmatrix}(0.4,0.5) & (0.4,0.5) & (0.5,0.4) & (0.3,0.5)\\ (0.5,0.3) & (0.5,0.5) & (0.6,0.3) & (x_3,x_4)\\ (0.5,0.3) & (0.3,0.5) & (0.4,0.5) & (0.3,0.6)\\ (x_4,x_3) & (0.5,0.5) & (0.5,0.4) & (0.5,0.4)\end{pmatrix}$$

$$Q_3 = \begin{pmatrix} (0.4,0.5) & (x_5,x_6) & (0.4,0.5) & (0.3,0.5) \\ (x_6,x_5) & (0.5,0.5) & (0.5,0.3) & (0.4,0.5) \\ (0.4,0.5) & (0.3,0.5) & (0.4,0.5) & (0.4,0.5) \\ (0.5,0.4) & (0.5,0.4) & (0.6,0.3) & (0.5,0.5) \end{pmatrix}$$

$$Q_4 = \begin{pmatrix} (0.5,0.5) & (0.3,0.5) & (0.5,0.3) & (0.3,0.6) \\ (0.5,0.5) & (0.5,0.5) & (x_7,x_8) & (0.3,0.6) \\ (0.4,0.5) & (x_8,x_7) & (0.5,0.5) & (0.5,0.4) \\ (0.5,0.4) & (0.5,0.3) & (0.6,0.3) & (0.5,0.5) \end{pmatrix}$$

V3

$\xi=(0.25,0.27,0.2,0.28)^T$.

$$Q_1 = \begin{pmatrix} (0.4,0.5) & (0.4,0.5) & (x_1,x_2) & (0.3,0.5) \\ (0.5,0.4) & (0.5,0.5) & (0.5,0.3) & (0.4,0.5) \\ (x_2,x_1) & (0.3,0.5) & (0.5,0.5) & (0.3,0.6) \\ (0.5,0.3) & (0.5,0.4) & (0.6,0.3) & (0.5,0.4) \end{pmatrix}$$

$$Q_2 = \begin{pmatrix} (0.4,0.5) & (0.4,0.5) & (0.5,0.3) & (0.3,0.5) \\ (0.5,0.3) & (0.5,0.5) & (0.6,0.3) & (x_3,x_4) \\ (0.5,0.3) & (0.3,0.5) & (0.5,0.5) & (0.3,0.6) \\ (x_4,x_3) & (0.4,0.5) & (0.5,0.4) & (0.3,0.6) \end{pmatrix}$$

$$Q_3 = \begin{pmatrix} (0.5,0.4) & (x_5,x_6) & (0.4,0.5) & (0.3,0.5) \\ (x_6,x_5) & (0.5,0.5) & (0.5,0.3) & (0.4,0.5) \\ (0.4,0.5) & (0.3,0.5) & (0.4,0.5) & (0.5,0.5) \\ (0.5,0.5) & (0.5,0.4) & (0.6,0.3) & (0.5,0.4) \end{pmatrix}$$

$$Q_4 = \begin{pmatrix} (0.5,0.4) & (0.3,0.5) & (0.5,0.3) & (0.3,0.6) \\ (0.5,0.4) & (0.5,0.5) & (x_7,x_8) & (0.3,0.6) \\ (0.3,0.5) & (x_8,x_7) & (0.5,0.5) & (0.6,0.3) \\ (0.5,0.4) & (0.5,0.4) & (0.6,0.3) & (0.5,0.4) \end{pmatrix}$$

Laboratory work 4
A GROUP DECISION SUPPORT TECHNIQUE FOR CYBER INCIDENT RESPONSE TEAMS

Goal and objectives: In this laboratory work, we'll explore a group decision support techniques that allows taking into consideration the subjective expert information formalized in the form of family of estimations based on the combination of hypotheses and ordered weighted average operators to effective cyber security risk management in different critical application.

Learning objectives:

- study a formal semantics of decision-making based on the theory of evidence and Dempster-Shafer belief structures;
- study a method of decision support that allows take into account the subjective expert information formalized in the form of family of estimations based on the combination of hypotheses and ordered weighted average operators (OWA).

Practical tasks:

- formulate the group decision problem in terms of the belief structures and evaluate the minimum and maximum objectives and differing types of aggregation of the operators;
- acquire practical skills working with group DSS.

Exploring tasks:

- investigate how to ensure variation in the goals with different types of ordering alternatives depending on the type of the specific problem.
- explore how matrix of possible solutions can be represented in the form of a payoff matrix or in the form of a risk matrix corresponding losses on the specific combinations of decisions.

Setting up

In preparation for laboratory work it is necessary:

- to clear the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1,2];
- to familiarize oneself with the main procedures and specify the exploration program according to defined task.

Recommended software and resources: *Dempster-Shafer Engine* (http://www.aonaware.com/dse.htm), or *DSI Toolbox* from official page of the Society for Imprecise Probability: Theories and Applications: http://www.sipta.org.

4.1 Synopsis

Cyber attacks and the resulting security breaches are part of a rapidly expanding international cyber threat that costs companies billions of dollars each year in lost information and response costs. Company executives are under increasing pressure to prevent these attacks and must act immediately to contain any damage once an attack occurs.

Let's suppose there is a problem selecting strategies to mitigate targeted cyber intrusions. This problem can be solved by combining subjective threat judgment information received from the in response team members (decision makers) based on their professional experience.

4.2 Brief theoretical information:

The cyber response team is responsible for developing the written cyber incident response plan and for investigating and responding to cyber attacks in accordance with that plan. Specifically, the response team, working with the CCO as appropriate, should [3]:

- Develop the cyber incident response plan.
- Identify and classify cyber attack scenarios.
- Determine the tools and technology used to detect and prevent attacks.
- Secure the company's computer network.
- Develop a checklist for handling initial investigations of cyber attacks.
- Determine the scope of an internal investigation once an attack has occurred.
- Conduct any investigations within the determined scope.
- Promote cyber security awareness within the company.
- Address data breach issues, including notification requirements.
- Conduct follow up reviews on the effectiveness of the company's response to an actual attack.

If a cyber attack has occurred, the response team should follow the investigation checklist set out in the cyber incident response plan to conduct the initial investigation. The initial response varies depending on the type of attack and level of seriousness. However, the response team should stop the cyber intrusions from spreading further into the company's computer systems.

Group decision-making is a situation where two or more decision makers in response team are involved in the decision of a joint problem whereas each of them has their own understanding of the problem and the decision consequences (competing hypotheses). Formally, competing hypotheses or conflict set is considered as a set of objects where there is no consensus of opinion among at least two experts.

Conceptual model *M* of a typical situation assessment problem in the presence of competing hypotheses

$$M = <A, S, P, D>$$

where *A* is a set of possible conclusions about the situation (alternatives), a generalization of logic experts; *S* is a set of baseline data on the situation which is measured in quantitative and qualitative scales; *P* are the analytical dependences, which provide formation of conclusions $a \in A$ according to the data *S*; and *D* are the techniques that allow to select the most important information from *S*.

To reduce a risk of decision-making in response team and ensure the reliability and accuracy of the decisions the group decision-making techniques can be suitable.

The next sections present the theoretical provisions based on the extended Dempster-Shafer belief structure and a method for automated decision support based on evidence-based reasoning. We have implemented this method on top of decision-support software tool, so it can be easily applied to the real critical application environment.

4.2.1 The challenge of decision making under competition

Let *A* be a set of alternatives {A1; A2; ...; Aq} whose values describe variants of the decision; *S* be a set of object states $\{s_1; s_2; ...; s_n\}$, characterizing the possible scenarios; values c_{11}; c_{12}; c_{1n}; c_{21}; c_{22}; c_{2n}; c_{n1}; c_{n2}; ...; c_{ln} – are the specific level of effectiveness of the solution corresponding to a specific alternative in a certain situation.

Knowledge of the safety conditions fixed in terms of belief structure m. B_1,..., B_r are the focal elements of m and m(B_k) are the associated weights.

The task involves finding the best alternative that delivers the payoff to the decision makers.

Moreover, to solve the problem, consider the following conditions:

– the presence of subjective quality expert information, characterized by a set of competing hypotheses and requiring aggregation;

– form of the matrix of solutions may vary depending on the selected performance indicators;

– method should provide support for decision-making, in order to lookup minimal losses as well as for the problem of finding maximum efficiency.

4.2.2 The procedure of group decision making in cyber incident response team

To get the best alternative in the group decision-making, the following steps are involved:

Step 1: Construction a decision matrix

Depending on the type of the problem, the matrix of possible solutions can be represented as a payoff matrix including performance indicators, or in the form of a risk matrix consists of financial loss indexes. It corresponds to certain combinations of alternatives to decision-making and possible scenarios.

	s_1	s_2	…	s_n
A1	c_{11}	c_{12}	…	c_{1n}
A2	c_{21}	c_{22}	…	c_{2n}
⋮	⋮	⋮	…	⋮
Al	c_{l1}	c_{l2}	…	c_{ln}

Step 2: Definition of a set focal elements $B \subseteq \Theta$ and the appointment of the main mass of probability to subsets

$$B^1 = (B_1^1, B_2^1, ...B_i^1 ...B_q^1).$$

$$B^2 = (B_1^2, B_2^2, ...B_j^2 ...B_\tau^2).$$

Step 3: Calculation of belief function for the combined sets using

$$m(B_k) = \sum_{B^1 \cap B^2 = B} m_1(B_i^1) m_2(B_j^2). \quad (4.1)$$

Step 4: Determination of the weight coefficients collection used in the aggregation functions for the individual sets of focal elements: $w = (w_1, w_2 ..., w_n)$ such that $w_j \in [0,1]$; $\sum_{j=1}^{n} w_j = 1$.

To calculate weighting values w_j (1=1,…,n) we use formula (4.2) Each weight can be obtained by

$$w_j = Q\left(\frac{j}{n}\right) - Q\left(\frac{j-1}{n}\right). \quad (4.2)$$

Where Q is a function of fuzzy linguistic quantifiers defined as

$$Q(r) = \begin{cases} 0, & \text{if } r < \alpha, \\ \dfrac{r-\alpha}{\beta-\alpha}, & \text{if } \alpha \le r \le \beta, \\ 1, & \text{if } r > \beta. \end{cases} \quad (4.3)$$

1) $Q(0) = 0,\ Q(1) = 1;$

2) $r < t \Rightarrow Q(r) \le Q(t);$

3) $\sum_{j=1}^{n} w_j = \sum_{j=1}^{n} \left(Q\left(\frac{j}{n}\right) - Q\left(\frac{j-1}{n}\right)\right) = Q(1) - Q(0) = 1.$

Quantifier Q is defined as a linear membership function for all $\alpha, \beta, r \in [0,1]$.

The values α, β are determined depending on the linguistic meaning of the quantifier.

Step 5: Calculating a set N_{ik}, which is formed when the i-th alternative has selected and k-th focal element,

$$\forall i,\ k : N_{ik} = \left\{ c_{ij} \middle| s_j \in B_k \right\}.$$

Step 6: Ordering N_{ik} sets for each of the criteria

$$OWA_\sigma, OWG_\sigma : s_1 > s_2 > ... > s_j > ... > s_{n-1} > s_n,$$
$$OWA_s, OWG_s : s_1 < s_2 < ... < s_j < ... < s_{n-1} < s_n,$$
$$\forall s_j \in N_{ik},\ j = 1, ..., n.$$

Step 7: Calculation of aggregated values M_{ik}.

$$M_{ik} = \sum_{j=1}^{n} w_j \cdot s_j. \tag{4.4}$$

Step 8: Calculation of the expected value of the overall index for each alternative

$$C_i = \sum_{k=1}^{r} M_{ik} \cdot m(B_k). \tag{4.5}$$

Step 9: Ordering and selection of an alternative in accordance with the objectives and the current rules.

4.2.3 General information about *Dempster-Shafer Engine* and *DSI Toolbox*

For this laboratory work you can use wide range of software tools related for imprecise probabilities theories (i.e. Dempster-Shafer theory, possibility theory, etc.) or to write the code. If you want a GUI, then use it from *Rcommander* or *R Studio*, or *Rkward*.

4.2.3.1. Dempster-Shafer Engine

Dempster-Shafer Engine (DSE) is a system which implements features of Dempster Shafer theory (fig. 4.1).

Project page http://www.aonaware.com/dse.htm

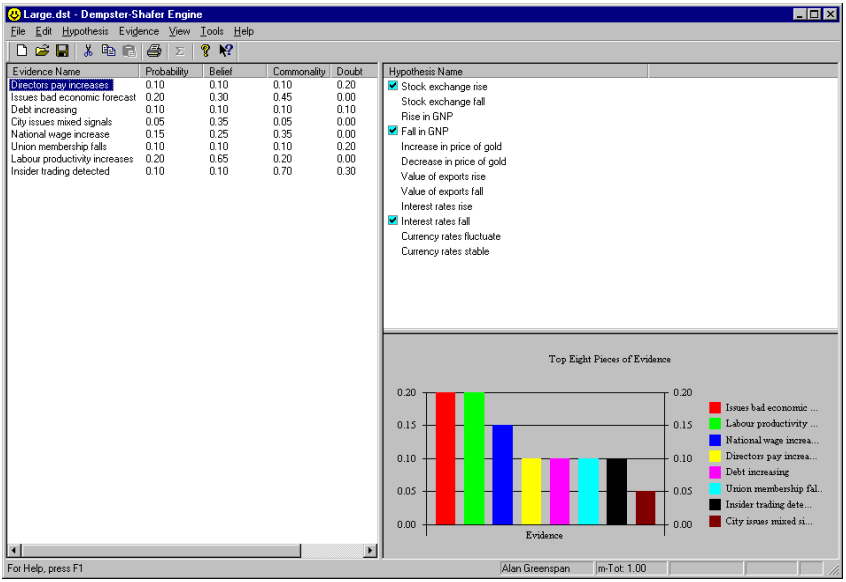


Figure 4.1 – Main window of *Dempster-Shafer Engine*

4.2.3.2 DSI Toolbox

DSI (for Dempster Shafer with Intervals) is a toolbox containing many methods related to the handling of belief functions in the setting of the general Dempster-Shafer theory. This includes dependence modeling through copulas: sensitivity analysis: aggregation functions (Dempster rule and the like): MC sampling and estimation of classical stastitical values (e.g. mean).

Methods for constructing basic probability assignments (BPA):

– Aggregation rules: Dempster's rule, (un)weighted mixing.

– Fast evaluation of (non-)monotonic system functions with Monte-Carlo sampling.

– Quantile-Quantile plots and plotting of BPAs.

– Verified results by using directed rounding and verified INTLAB functions.

The Dempster-Shafer with Intervals (DSI) toolbox is free for private use and for purely academic purposes. Proper reference is given acknowledging that the software package DSI has been developed by Gabor Rebner at University of Duisburg-Essen, Germany.

Project page - http://www.sipta.org/index.php?id=sfw

4.3 Execution order and discovery questions:

1. Set up your lab environment according to the specifications below; analyze and fix your targeted problem (intrusion mitigation program).
2. Analyze a decision matrix and expert judgments.
3. Define the set focal elements and appoint the mass of probability to subsets.
4. Calculate the belief function.
5. For individual sets of focal elements determine weight coefficients.
6. Calculate the aggregated values M_{ik}.
7. Calculate the overall index and define preference rule. It is necessary to prioritize the most suitable mitigation actions to implement in the target system.
8. Choose an alternative in accordance with your intrusion mitigation program.

4.4 Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

- (I): background / theory, purpose and discovery questions
- (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures
- (R): narrate (like a story), tables, indicate final results;
- (D): answers on discovery questions, explanation of anomalies, conclusion / summary

4.5 Test questions:

6. For what the cyber response team is responsible?
7. What areas the group decision support techniques can be used in the context of cyber security of critical infrastructures?
8. How to ensure variation in the goals with different types of ordering alternatives depending on the type of the specific problem?

9. How matrix of possible solutions can be represented in the form of a payoff matrix or in the form of a risk matrix corresponding losses on the specific combinations of decisions?

4.6 Recommended literature:

1. Chen Q., Aickelin U. Anomaly Detection Using the Dempster-Shafer Method [Digital edition] - http://arxiv.org/ftp/arxiv/papers/0803/0803.1568.pdf

2. Skarha-Bandurova, I. Nesterov M., Kovalenko Y. A Group Decision Support Technique for Critical IT Infrastructures // Theory and Engineering of Complex Systems and Dependability: Proc. of the Tenth Int. Conf. on Dependability and Complex Systems DepCoS-RELCOMEX, June 29-July 3 2015, Brunow, Poland. Advances in Intelligent Systems and Computing. - Volume 365. (2015). – pp 445-454.

3. Farhat V., McCarthy B., Raysman R., Cyber Attacks: Prevention and Proactive Responses // Holland & Knight LLP (2011). – 12 p.

4. Wu Q., Ferebee D., Lin Y., Dasgupta D. An Integrated Cyber Security Monitoring System Using Correlation-based Techniques // IEEE International Conference on System of Systems Engineering. – 2009. – pp. 1-6. [Digital edition] - https://www.researchgate.net/profile/Chase_Wu/publication/224602017_An_integrated_cyber_security_monitoring_system_using_correlation-based_techniques/links/55fc085b08aeafc8ac4200b7.pdf

4.7 Assignment to the laboratory work:

In this laboratory work you will face with one of following type of attack: (1) Browser attacks, (2) Brute force attacks, (3), Denial of service attacks, (4) SSL attacks, (5) Scans, (6) DNS attacks, (7) Backdoor attacks.

First of all you should choose 4 mitigation strategies. Thus, decision problem will have four mitigation strategies (alternatives A1, A2, A3, A4) with generalized metrics which allow assessing the mitigation actions in four process areas: s_1 - vulnerability management, s_2 - patch management, s_3 - configuration management, and s_4 - incident management as a base for analysis. To choose strategies to mitigate your targeted cyber intrusions please, refer to Appendix B.

Then you'll have two groups of experts, each of that defined their own judgment using the model of the belief structure for each alternative on each criterion as follows

Group 1: ({s_1, s_2, s_4}, 0,6; {s_2, s_3, s_4}, 0,3; {s_2, s_4}, 0,1).
Group 2: ({s_1, s_2, s_4}, 0,4; {s_2, s_3, s_4}, 0,2; {s_2, s_4}, 0,4).

The task is to select the best strategies to mitigate targeted cyber intrusion by combining subjective threat judgment information received from the decision makers based on their professional experience.

NB. If the main goal of your intrusion mitigation program formulated for improving system security or increasing confidence of security you should use descending order of operators, otherwise for example for risk reduction ordered weighted operators in ascending order will applicable.

4.8 Example of computational tables

1. Let decision problem has four mitigation strategies (alternatives A1, A2, A3, A4). To each strategy, we attribute generalized metrics which allow assessing the mitigation actions in four process areas: s_1, s_2, s_3, and s_4.

	s_1	s_2	s_3	s_4
A1	10	40	20	30
A2	15	20	25	30
A3	40	30	10	20
A4	40	50	10	30

2. Assume further that there are two groups of experts, each of that defined its own judgment using the model of the belief structure for each alternative on each criterion as follows.

Group 1: ({s_1, s_2, s_4}, 0,8; {s_2, s_3, s_4}, 0,1; {s_2, s_4}, 0,1).
Group 2: ({s_1, s_2, s_4}, 0,5; {s_2, s_3, s_4}, 0,4; {s_2, s_4}, 0,1).

Then the set of focal elements to merging sets can be represented as follows:

	$\{s_1,s_2,s_4\}$ 0,8	$\{s_2,s_3,s_4\}$ 0,1	$\{s_2,s_4\}$ 0,1
$\{s_1,s_2,s_4\}$0,5	$\{s_1,s_2,s_4\}$ 0,4	$\{s_2,s_4\}$ 0,05	$\{s_2,s_4\}$0,05
$\{s_2,s_3,s_4\}$0,4	$\{s_2,s_4\}$ 0,32	$\{s_2,s_3,s_4\}$0,04	$\{s_2,s_4\}$0,04
$\{s_2,s_4\}$ 0,1	$\{s_2,s_4\}$ 0,08	$\{s_2,s_4\}$ 0,01	$\{s_2,s_4\}$0,01

3. Calculation of the belief function carried out by (4.1):

B1	$\{s_1,s_2,s_4\}$	0,4
B2	$\{s_2,s_3,s_4\}$	0,04
B3	$\{s_2,s_4\}$	0,56

4. Determination of weight coefficients w, which are used for aggregation functions for the individual sets of focal elements.

$w_1 = (0,4; 0,6)$, and $w_2 = (0,3; 0,4; 0,4)$.

5. Defining sets N_{ik}.

6. Ordering sets $N_{ik} : a_{\sigma(i)} \geq a_{\sigma(i+1)}$, and $a_{s(i)} \leq a_{s(i+1)}$.

7. Calculation of aggregated values Mik performed by (4.4), the results are presented in Table 4.1.

Table 4.1. The results of calculation of aggregate values

Operator	Aggregate value					
	M_{11}	M_{12}	M_{13}	M_{21}	M_{22}	M_{23}
OWA_s	31	34	36	24,5	28	26
OWA_σ	28	32	34	23	27	24
OWG_s	24,2	29,8	35,6	21,6	25,1	25,5
OWG_σ	21,1	27,8	33,6	20,1	24,1	23,5
	M_{31}	M_{32}	M_{33}	M_{41}	M_{42}	M_{43}
OWA_s	34	23	26	45	35	42
OWA_σ	32	21	24	43	31	38
OWG_s	29,8	19,1	25,5	40,1	26,5	40,7
OWG_σ	27,8	17,1	23,5	38,1	22,5	36,8

8. Calculation of the overall index is performed by (4.5). The results are summarized in Table 4.2.

Table 4.2. The results of the calculation of the generalized index

	OWA_s	OWA_σ	OWG_s	OWG_σ
A1	33,92	31,52	30,81	28,37
A2	25,48	23,72	23,92	22,16
A3	29,08	27,08	26,96	24,96
A4	42,92	39,72	39,89	37,87

9. The choice of an alternative is performed in accordance with the preference rule presented in Table 4.3.

Table 4.3. The results ordering alternatives

Operators	The order of preference alternatives
OWA_s, OWG_s	$A2 \succ A3 \succ A1 \succ A4$
OWA_σ, OWG_σ	$A4 \succ A1 \succ A3 \succ A2$

For OWA_σ, OWG_σ operators, as the best solution chosen A4 because it gives the highest expected value. For OWA_s and OWG_s operators selected variant A2, since in these cases it is believed that the best result is the lowest.

Laboratory work 5
DESIGNING GAMING SITUATIONS FOR IMPROVING TEAM AWARENESS ON CYBER INCIDENTS

Goal and objectives: This laboratory work is devoted to studying how human factors can improve cyber security, investigating interaction and the effectiveness of team defense strategies according to the dynamics of cyber-security situations. Particular attention will be paid to improving the cyber defense training, exercises, and evaluation, as well as lessons learned.

Learning objectives:

- study basics of team situation awareness (SA) including information sharing, opinion integration and consensus SA generation;
- study the factors that impact the effectiveness of Cyber Security Incidence Response Team (CSIRT);
- understand the role of organizational culture and processes to increase cyber defense capacity.

Practical tasks:

- acquire practical skills in working in cybersecurity IDS game simulating environments;
- develop relevant decision making research paradigms that abstract most essential elements of the cybersecurity environment;
- acquire practical skills in decision making under complex interrelationships of seemingly unrelated events.

Exploring tasks:

- explore a computational cognitive model of team decision making in cyber-security situations.
- investigate how do humans recognize, process and accumulate information to make cyber-defense decisions.

Setting up

In preparation for laboratory work it is necessary:

- to clear the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1,2];
- to familiarize oneself with the main procedures and specify the exploration program according to defined task.

Recommended software and resources: *IBLTool* (http://www.hss.cmu.edu/departments/sds/ddmlab/downloads.html#ibltool) or the IBL model of the security analyst can be created using *Matlab* software.

5.1 Synopsis

The human factor may be a systems weakest link, but may also be a powerful resource to detect and mitigate developing threats. In this context situation awareness (SA) can be considered as a phenomenon that refers to extract environmental information, integrate it with previous knowledge to direct further perception and anticipate future events. Since SA is regarded as a dynamic and collaborative process, it is often required in a team. Team SA is commonly used in the human-computer interaction community where the concerns are to design computer interfaces so that a human operator can achieve SA in a timely fashion. Within large organizations, the investigation and resolution of cyber incidents rest upon the Cyber Security Incidence Response Team (CSIRT). The primary responsibility of a CSIRT is to review information from a variety of sources (e.g., intrusion detection systems, automated queries, user reports, notifications from other cyber professionals) to identify evidence of potential cyber threats. The corresponding tasks rely on general knowledge of computer and network systems and domain-specific knowledge of the local infrastructure, and an appreciation of adversary tactics and techniques. There is an emphasis on cognitive processes that enable inferential reasoning, pattern recognition, procedural memory, and communication.

In this laboratory work, we are going to analyze how human factor can improve or reduce cyber security through the interaction of team members on process identification situation and choosing defense strategies under dynamic cyber attacks.

5.2 Brief theoretical information:

Cyber attacks are the disruption in the normal functioning of computers and the loss of private information in a network due to malicious network events (threats), and they are becoming widespread. The nation’s cyber-security strategy is twofold: to improve the resilience to cyber incidents; and to reduce the cyber threat. To meet

these goals, the role of the security analyst (called "defender" onwards), a human decision maker who is in charge of protecting the online infrastructure of a corporate network from random or organized cyber-attacks, is indispensable. The defender protects a corporate network by identifying, as early and accurately as possible, threats and non-threats during cyber attacks.

5.2.1 A Simple Scenario of a Cyber Attack

The cyber-infrastructure in a corporate network typically consists of a web server and a fileserver. The web server handles customer interactions on a company's webpage. However, the fileserver handles the working of many workstations that are internal to the company and that allow company employees to do their daily operations. A bidirectional firewall (firewall 1 in Fig. 5.1) protects the path between the web server and the company's website on the Internet.

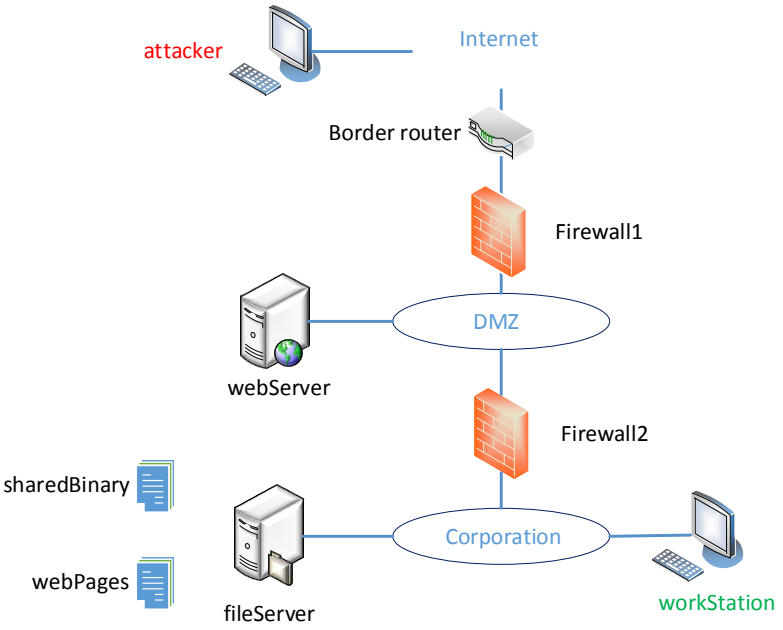


Figure 5.1 – A simplified network

Thus, firewall 1 allows both the incoming "request" traffic and the outgoing "response" traffic between the company's website and the web server. Another firewall (firewall 2 in Fig. 5.1) protects the path between the web server and the fileserver. Firewall 2 is a much stronger firewall than the firewall 1 as it only allows a very limited Network File System (NFS) access of the fileserver from the web server, but an easy access of the web server from the fileserver (this latter access allows company employees to make changes on the web server that would later show-up on the company's website).

For this cyber-infrastructure, attackers follow a sequence of an "island-hopping" attack, where the web server is compromised first, and then the web server is used to originate attacks on the fileserver and other company workstations (the workstations are directly connected to the fileserver) [3,4].

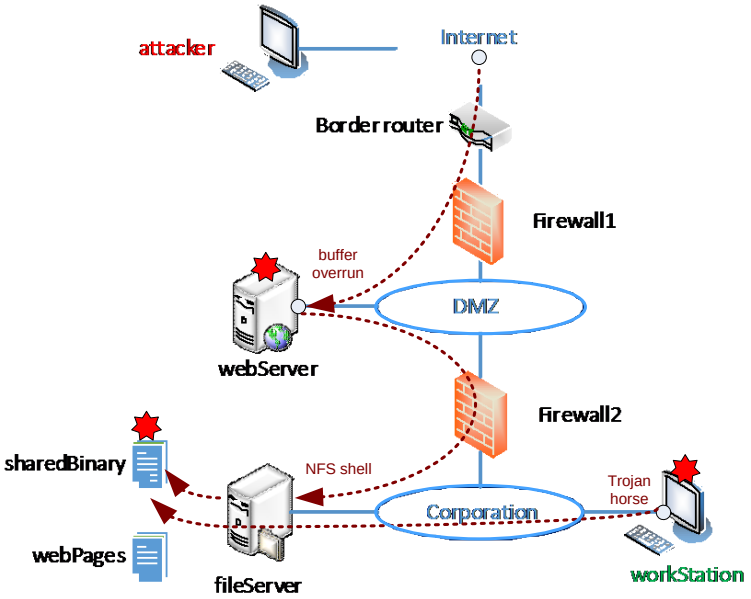


Figure 5.2 – An example of "island-hopping" attack

A simple scenario of an island-hopping cyber-attack within the cyber-infrastructure discussed above (see Figure 5.2) can be described by next simple steps stealing information from a workstation:

1. Normal operation
2. Attack httpd service
3. Penetrate through the hacked httpd service
4. Install sniffer to collect passwords
5. Hack into a workstation
6. Steal information
7. Create additional damage by sabotaging the network

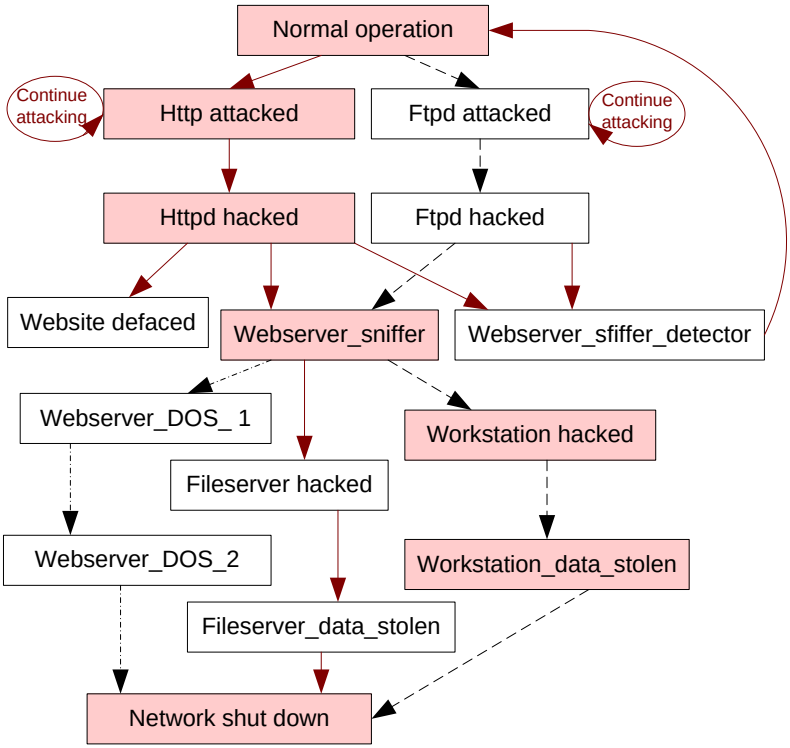


Figure 5.3 – Example of an attack

Four different types of cyber attacks which represent different intentions of an attacker: (1) Denial of Service (DoS), (2) Steal Information, (3) Install Sniffer, (4) Deface a website

During a cyber attack, there could be both malicious network events (threats) and benign network events (non-threats) occurring in a

sequence. Threats are generated by attackers, while non-threats are generated by friendly users of the network. In order to accurately and timely detect cyber attacks, a defender relies on highly sophisticated technologies that aid in the detection of threats. One of these cyber technologies is called an intrusion detection system (IDS), a program that alerts defenders of possible network threats. The IDS is not a perfect technology, however, and its predictions have both false positives and false negatives. Although there is ample current research on developing these technologies, and on evaluating and improving their efficiency, the role of the defender behavior, such as the defender's experience and tolerance to threats, is under-studied in the cyber-security literature [1,2,5,6]. In addition, it is likely that the nature of adversarial behavior also influences the defender's cyber SA. One characteristic of adversarial behavior is the attacker's strategy regarding the timing of threats during a cyber attack: An impatient attacker might inject all threats in the beginning of a sequence of network events; however, a patient attacker is likely to delay this injection to the very end of a sequence. For both these strategies, there is prevailing uncertainty in terms of exactly when threats might appear in a cyber attack. Thus, it is important for the defender to develop a timely and accurate threat perception to be able to detect a cyber attack. Thus, both the nature of the defender's and adversary's behaviors may greatly influence the defender's cyber SA

5.2.2 Instance-Based Learning Theory (IBLT) and IBL Model of Security Analyst

IBLT is a theory of how people make decisions from experience in a dynamic task [3,4]. In the past, computational models based on IBLT have proven to be accurate in generating predictions of human behavior in many dynamic-decision making situations like those faced by the security analyst. IBLT proposes that people represent every decision making situation as instances that are stored in memory. For each decision-making situation, an instance is retrieved from memory and reused depending on the similarity of the current situation's attributes to the attributes stored in instances in memory. An instance in IBLT is composed of three parts: situation (S) (the knowledge of situation attributes in a situation event), decision (D) (the course of action to take for a situation event), and utility (U) (i.e., a measure of the goodness of

a decision made or the course of action taken for a situation event). In the case of the decision situations faced by the security analyst, these attributes are those that characterize potential threat events in a corporate network and that needs to be investigated continuously by the analyst. The situation attributes that characterize potential threat events in the simple scenario are the IP address of the location (webserver, fileserver, or workstation) where the event took place, the directory location in which the event took place, whether the IDS raised an alert corresponding to the event, and whether the operation carried out as part of the event (e.g., a file execution) by a user of the network succeeded or failed.

These models reproduced human data obtained from experiments. Also, IBL models can be extended to represent strategic and non-asymmetric interactions beyond the individual: in 2x2 games and in cyberwar (multiplayer) games.

5.2.3 Cybersecurity IDS Game Simulator

IDS Game Simulator is a digital game that is designed to simulate the speed and complexity of an actual cyber breach. Fundamentally, Game Simulator was created to deliver a unique experience by allowing teams to feel pressure as they make fast paced decisions and to see potential consequences of their actions in real-time.

A model of the defender, based upon IBLT, is exposed to different island-hopping attack sequences (depending upon the two adversarial timing strategies). Each attack sequence is composed of 25 network events (a combination of both threats and non-threats), whose nature (threat or non-threat) is not known to the model. However, the model is able to observe alerts that correspond to some network events (that are regarded as threats) generated from the intrusion-detection system (IDS). Out of 25 events, there are 8 predefined threats that are initiated by an attacker (the rest of the events are initiated by benign users).

The model does not know which events are generated by the attacker and which are generated by corporate employees. By perceiving network events in a sequence as threats or non-threats, the model needs to identify, as early and accurately as possible, whether the sequence constitutes a cyber attack. In this cyber-infrastructure, we represented adversarial behavior by presenting event sequences with different timings for the 8 threats: an impatient strategy, where the eight

threats occur at the beginning of the sequence; and a patient strategy, where the eight threats occur at the end of the sequence.

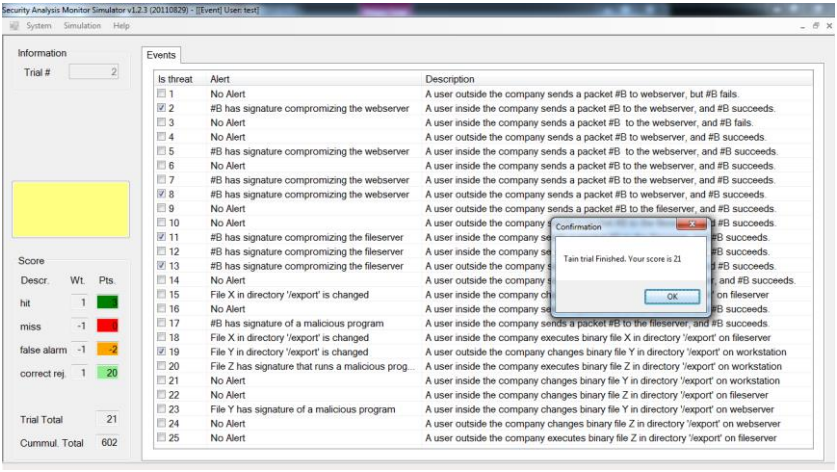


Figure 5.4 – The main window of Cybersecurity IDS Game Simulator

The events are colored in accordance with the type of breakdown, hits (green), misses (red), correct rejections (light green), and false alarms (yellow).

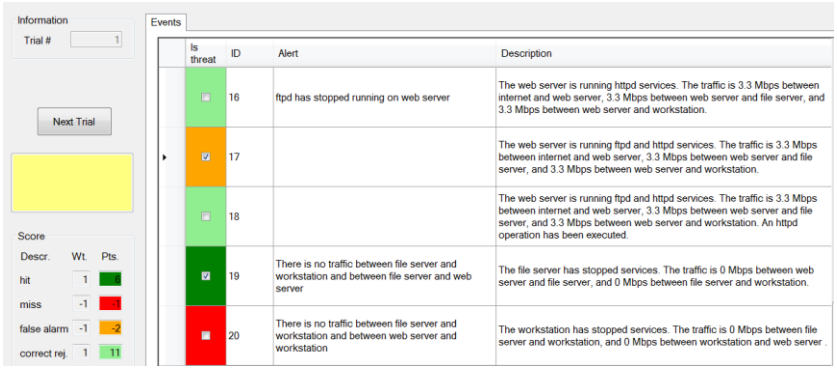


Figure 5.5 – Detailed feedback

Table 5.1. Instance structure with the possible values in the scenario

Type	Attribute name	Possible Value	Actual code
Situation	IP(Location)	Webserver	1
		Fileserver	2
		Workstation	3
	Directory	Missing value	-100
		FileX	1
	Operation	Successful	1
		Not successful	0
	Alert	Present	
		Absent	
Decision	Decision	Cyber-attack(calculated indirectly based upon U)	1
			0
Utility	Threat	Yes	1
		No	0

In the simple scenario, a security analyst is expose to a sequence of 25 network events (consisting of both threat and non-threat events) whose nature (threat or non-threat) is not precisely known to a security analyst. Out of the total of 25 events, there are 8 predefined threat events in the sequence that are initiated by an attacker.

The attacker, through some of these 8 events, first compromises the web server by remotely exploiting vulnerability on the web server and getting a local access to the web server. If the cyber-attack remains undetected by the security analyst by the 8th event out of a total of 25 events, then the attacker gains full access of the web server. Since typically in a corporate network and in the simple scenario, a web server is allowed to access the fileserver through only a NFS event, the attacker then modifies data on the fileserver through the vulnerability in the NFS event.

If the cyber-attack remains undetected by the security analyst by the 11th event out of a total of 25, then the attacker gains full access of the file server. Once the attacker gets an access to modify files on the fileserver, he then installs a Trojan-horse program (i.e., a virus) in the executable binaries on fileserver that is used by different workstations (event 19th out of 25). The attacker can now wait for an innocent user

on a workstation to execute the virus program and obtain control of user's workstation (event 21st out of 25).

During the course of the simple scenario, a security analyst is able to observe all the 25 events corresponding to file executions and packets of information transmitted on and between the webserver, fileserver, and different workstations. He is also able to observe alerts that correspond to some network events using an intrusion-detection system (IDS). The IDS raises an alert for a suspicious file execution or a packet transmission event that is generated on the corporate network. However, among the alerts generated by the IDS in the simple scenario, there is both a false-positive and a false-negative alert and one alert that correspond to the 8th event, but which is received by the analyst after the 13th event in the sequence (i.e., a time delayed alert).

Most importantly, due to the absence of a precise alert corresponding to a potential threat event, the analyst does not have precise information on whether a network event and its corresponding alert (from the IDS) are initiated by an attacker or by an innocent company employee. Even through the analyst lacks this precise information, he needs to decide, at the earliest possible and most accurately, whether the sequence of events in the simple scenario constitutes a cyber-attack. The earliest possible or proportion of timeliness is determined by subtracting the percentage of events seen by the analyst before he makes a decision about cyber-attack in the simple scenario to the total number of events (25) in the scenario from 100%. The accuracy of the analyst is determined by whether the analyst's decision was to ignore the sequence of events or declare a cyber-attack based upon the sequence of observed network events.

5.3 Execution order and discovery questions:

1. The game begins by generating a specified number of alerts. Each alert corresponds to an event that has triggered some form of automated network monitoring or other alerting function.

2. Set up your lab environment, run simulation software and load a sequence. This step is meant to simulate the experience where on any given morning, analysts arrive to find a queue containing some number of alerts that were either generated overnight or left unresolved from the previous day (Table 5.2).

Table 5.2. An example of simplified IDS that presents network traffic and possible threats to a human analyst

ID	Event
Event 1	Mallory (i.e. attacker) sends probing packet #B1 (after TCP 3-way handshake) to port 80 of webServer, but packet #B1 fails.
Event 2	Good packet #G1 gets into port 80 of webServer.
Event 3	Good packet #G2 gets into port 80 of webServer.
Event 4	Mallory sends probing packet #B2 to port 80 of webServer, but packet #B2 fails.
Event 5	Good packet #G3 gets into port 80 of webServer.
Event 6	Good packet #G4 gets into port 80 of webServer.
Event 7	Good packet #G5 gets into port 80 of webServer.
Event 8	Mallory sends probing packet #B3 to port 80 of webServer; packet #B3 succeeds.
Event 9	Mallory sends probing packet #B4 to RPC port on fileServer, but packet #B4 fails.
Event 10	Good packet #G6 gets into RPC port on fileServer.
Event 11	Mallory sends probing packet #B5 to RPC port of fileServer; packet #B5 succeeds. The network is now in the state specified by Node 32.
Event 12	Good packet #G7 gets into RPC port on fileServer.
Event 13	Good packet #G8 gets into RPC port on fileServer.
Event 14	Good packet #G9 gets into RPC port on fileServer.
Event 15	Binary file X in directory "/export" is changed by a good user.
Event 16	Binary file X in directory "/export" is changed by another good user.
Event 17	Mallory changes file X in directory "/export" to install a Trojan horse.
Event 18	Binary file Y in directory "/export" is changed by a good user.
Event 19	File X, the Trojan horse, is executed by admin. The Trojan horse executes code on workstation with root privilege.
Event 20	Binary file Y in directory "/export" is changed by another good user.
Event 21	File Y is executed by a regular user.
Event 22	Binary file Z in directory "/export" is changed by another good user.
Event 23	File Z is executed by a regular user.

3. On this step, the goal for every team members is to correctly classify each event as a threat or a non-threat by checking or unchecking the corresponding "is threat" box for each event.

4. Then IDS generates Alerts from Events. Take into account that they may contain noise (false alarms) and are generally imprecise (See Table 5.3).

Table 5.3. Example of Alerts

Label	Semantics
AE1	against Event 1: saying that packet #B1 matches a signature compromising webServer.
AE2	against Event 8: saying that packet #B1 matches a signature compromising webServer.
AE3	against Event 8 and #B3: However, due to detection latecy, this alert is raised after Event 13.
FN1	false negative against Event 11: the sensor did not rise any alert about #B5.
AE4	false positive: saying that webServer runs a malicious NSF shell.
AE5	against Event 15 saying that file X in directory "/export" is changed.
AE6	against Event 16 saying that file X in directory "/export" is changed.
AE7	against Event 17 saying that file X in directory "/export" is changed.
AE8	against Event 17 saying that file X is a Trojan horse.
AE9	against Event 19: saying that Trojan horse is being executed.

Most important effect of experience involves identification of attributes used by experts in detecting threats

5. Each player should make decisions whether to: Attack, Defend, or do nothing. Once an alert has been opened for investigation, it is determined which of thirteen tasks must be performed (See Table 5.4).

Table 5.4. Tasks incorporated into the simulation.

ID	Tasks
T01	Submit to sandbox
T02	Submit to analysis
T03	Retrieve machine proxy
T04	Reverse engineer executable
T05	Reverse engineer protocol
T06	Retrieve forensics data
T07	Analyze memory image
T08	Retrieve network data
T09	Retrieve email
T10	Add network signature
T11	Retrieve SSL keys
T12	Implement network block
T13	Implement additional alerts

6. Team members should collect data, generate awareness for a situation, and share them with other members aiming to get consensus awareness for the situation in the team.

Individual analysts should assign integer values from 1-10 to reflect both their level of expertise with a particular task and their expertise with the associated software tool. Expertise with tasks and tools serve as factors in determining the time required for an analyst to perform a given task and the effectiveness with which they will perform the task.

7. Each team should interacts with its own team members, and analyze the impact of their decisions in real-time on a shared monitor. All teams must make careful and strategic decisions in order to win. One of four outcomes may result: (1) the alert is correctly resolved; (2) the alert is erroneously resolved (i.e., false positive); (3) the alert is correctly unresolved; or (4) the alert is incorrectly unresolved (i.e., false negative). Where an alert is unresolved, there is a determination of the next task to be performed, with this process continuing until the alert is eventually resolved.

8. Post-game summary provides players with a detailed review of all actions and outcomes for all teams during the game.

5.4 Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

- (I): background / theory, purpose and discovery questions
- (M): complete description of the procedures which was followed in the experiment, experiment overview, figures / schemes:
- (R): narrate (like a story), tables, indicate final results;
- (D): answers on discovery questions, conclusion / summary.

5.5 Test questions:

4. What are the main factors impact the effectiveness of cyber security incidence response team?
5. When cyber security SA needs collective decision making?
6. How do humans recognize and process possible threats?
7. What are the main differences between the group team and individual decision-making?
8. How human factor can improve or reduce cyber security through the interaction of team members?

5.6 Recommended literature:

1. Thomas J. Mowbray. Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions / John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256, 2014.

2. Reed T., Abbott R. G., Anderson B., Nauer K., Forsythe C. Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams // Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting – 2014. – pp. 427-431. [Digital Edition] - http://pro.sagepub.com/content/58/1/427.full.pdf

3. Dutt V., Ahn Y.-S., Gonzalez C. Cyber Situation Awareness: Modeling Detection of Cyber Attacks with Instance-Based Learning Theory [Digital Edition] - http://hss.cmu.edu/departments/sds/ddmlab/papers/Dutt%20Ahn%20Gonzalez_CyberSA_HFES_28022012R_R3.pdf

4. Dutt V., Ahn Y.-S., Gonzalez C. Cyber Situation Awareness: Modeling the Security Analyst in a Cyber-Attack Scenario Through Instance Based Learning [Digital Edition] - https://pdfs.semanticscholar.org/f4af/8701f2e3e41534854f5ca97b5e0e88a18632.pdf

5. Gonzalez C. Game Theory and Cyber War: Paradigms for Understanding Human Decisions in Cyber Security [Digital Edition] - https://s2.ist.psu.edu/cybersa/review-SantaBarbara-2014/2014MURI-GameTheoryandCyberWar-CMU.pdf

6. Lu J., Zhang G., Wu F. Team Situation Awareness Using Web-Based Fuzzy Group Decision Support Systems // Int. Journal of Computational Intelligence Systems, Vol. 1, No. 1 (2008) – pp. 50–59.

5.7 Assignments to the laboratory work

This laboratory work was created to deliver an experience by allowing teams to feel pressure as they make fast paced decisions with minimal information and to see potential consequences of their actions in real-time.

In common situation, every five seconds there will be generated a new event and all teams should (1) classify event, (2) analyze alerts, and (3) make decisions. The winner is the team that scored the most points.

PROGRAM FOR THE SEMINARS

The major topics covered in the seminars are shown in Table.

No.	Topic	Details
1	The role of human factors in system robustness and resilience	The ability to sustain and protect the flow of information and data and the possibility to early detect, isolate and eliminate cyber hazards. Human interfaces associated with the offline tools for active co-operation between a decision aid tool and a human operator
2	The human dimension of cyber security	Cyber forensic analysis of common types of human-related security. Social engineering attacks. Malicious insiders.
3	Measuring the Human Factor of Cyber Security	Subjects, Techniques, Procedures, Instrumentation. Trust Framework of Human Factors in Cyber Security. Measuring Human Performance within Computer Security Incident Response Teams.
4	Tools and techniques for the co-design of safety and security critical interfaces.	Alarm management systems to prevent alarm inflation to be effective and informative in daily operation. Efficient collaboration tools for information and knowledge sharing. Decision support systems for detecting risk. Training initiatives for coping with emergencies. The Cisco Collaborative Operations solution.
5	Collaborative operational and research environments.	Basic factors affecting collaborative decision-making during emergency. How a shared collaboration surface may facilitate adequate team decision making on daily operation and planning and in risk situations and emergencies.

Appendix
An Example of the Execution of Lab 1

In this laboratory work we have undertaken a study of the Stuxnet virus. The main findings are based on the assessment of probabilities spreading Stuxnet. The analysis was performed in accordance to paragraph 1.3 ‘Execution order and discovery questions’ and represented in the form of 6 steps.

Step 1: An analysis of the assigned emergency management problem for Stuxnet worm

Following its discovery in June 2010, the Stuxnet worm triggered a worldwide sensation. It was the first publicly known root-kit attack targeted at industrial plants. It has infected tens of thousands of PCs, abusing and manipulating Windows-based automation software for its own purposes – to ultimately infiltrate malicious code into the controllers of specific real-world industrial installations. After Stuxnet, the threats from malware and insufficient IT security in automation networks, forecast by industry experts for a long time now, can no longer be ignored. The real danger looming out there, however, is not from Stuxnet itself, but rather from mutations likely to be created by imitators who could now circulate other arbitrary, malicious code utilizing the same basic techniques. And while Stuxnet focused on products from the Siemens SIMATIC family and on STEP 7 PLC projects with very specific properties, such mutations could affect components from other vendors as well, and turn out to be a lot less selective in their damaging impact. Apart from the fact that PCs in industrial use often are not (and cannot be) equipped with antivirus software, Stuxnet has also made it clear that conventional virus scanners do not provide protection against attacks of this caliber. In retrospect, the analysis of Stuxnet has shown that the worm had been out in the wild unnoticed for at least 12 months before its discovery and had not been detected by antivirus programs during that period for lack of any known signatures for the malware.

According to [1] Stuxnet has four main vectors for attack:

1. Infection of Windows PCs: The worm uses an aggressive mix of mechanisms to spread onto and contaminate both networked as well as non-networked Windows PCs (the latter via USB flash drives). For doing so, it utilizes a total of four zero-day exploits of previously unknown vulnerabilities which exist in several generations of Windows operating systems, and have only partially been fixed by security patches to date. In addition to a number of encrypted files which the worm stores in the %SystemRoot%\inf\ directory, Stuxnet installs the two device drivers MrxNet.sys and MrxCLS.sys in %SystemRoot%\system32\drivers\.

These drivers have been signed with stolen private digital keys from Realtek and JMicron and do therefore contain certificates which are rated as trustworthy by Windows systems.

2. Abuse and Manipulation of Automation Software: If Stuxnet comes across installations of WinCC visualization and/or STEP 7 engineering components on an infected PC, it abuses and manipulates any found WinCC databases and STEP 7 projects to ensure its further proliferation and persistency on the PC, and to spy out the controllers referenced in those projects as potential targets for step 3. Furthermore, Stuxnet renames the dynamic link library which is responsible for the communication between SIMATIC Manager and the projected S7 controllers (s7otbxdx.dll in the %SystemRoot%\system32\ thereby being renamed to s7otbxdsx.dll) and replaces it with a wrapper DLL of its own under the original name in the same directory, effectively hiding the modification.

3. Injection of Malicious Code into Controllers: This manipulated wrapper DLL enables Stuxnet to infiltrate arbitrary malicious code into the projected PLCs, to hide those manipulations from the programming engineer, and to safeguard them from later overwriting. The precise malicious code selectively injected by Stuxnet, only into controllers and projects with very specific properties, is of remarkable sophistication and – according to the latest expert findings – is supposed to permanently manipulate frequency converters and turbine controls as inconspicuously as possible, with the goal of disrupting the controlled processes and ultimately destroying the affected equipment. The malicious code targeted at

controller models of the S7-417 series in particular, is combining denialof-control and denial-of-view techniques into a man-in-the-middle attack in ways rarely considered until now. Under the attack, the legitimate PLC program completely loses control of the process without this being noticed by the PLC, or by the operating staff viewing their consoles in the control room. The underlying attack vector is generic and reproducible. It could be packaged into and provisioned by exploit tools such as Metasploit and then – contrary to common misconceptions – be used for attacks even by persons lacking in comprehensive insider knowledge.

4. Communication with Command & Control Servers on the Internet: From infected PCs, the worm attempts to contact its designated command & control servers on the Internet. When a connection gets established, information collected from the target and its environment can be uploaded to those servers as well as new instructions and updates to the worm, and its malicious payload can be received and executed. This adds an extra dynamic depth to the worm's potential for espionage and sabotage. Combined with the worm's capabilities to spread and update itself via peer-to-peer connections and USB flash drives, all of this can have collateral effects even on systems without a network connection or Internet access.

Step 2: Development of elimination scheme to combat the Stuxnet worm

Elimination Stuxnet scheme adapted from [2] is shown in fig.A.1.

Step 3: The functioning virus scheme

Stuxnet work scheme was taken and compiled from [3], (see fig. A.2.). According to scheme fig. A.2 Stuxnet had many paths to its victim PLCs. Green highlights infection path. Red highlights more direct paths which bypass existing security infection.

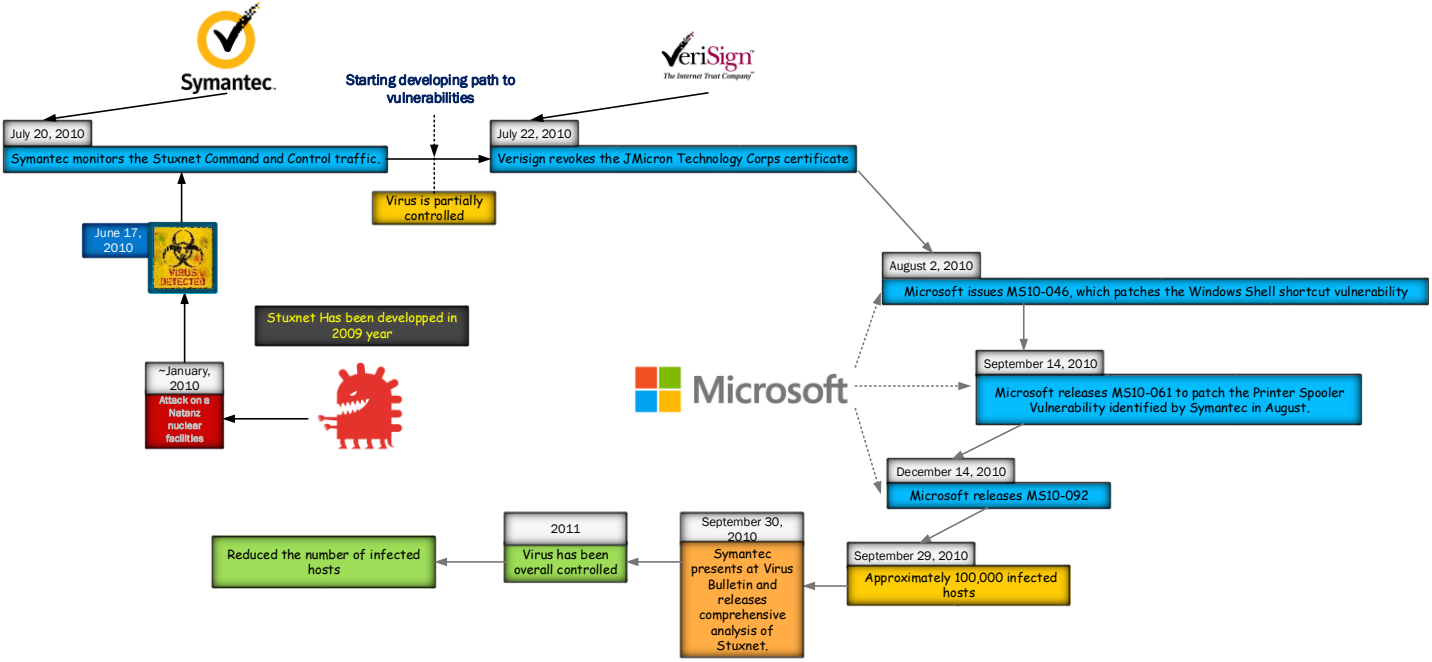


Figure A.1 – Elimination Stuxnet scheme [2]

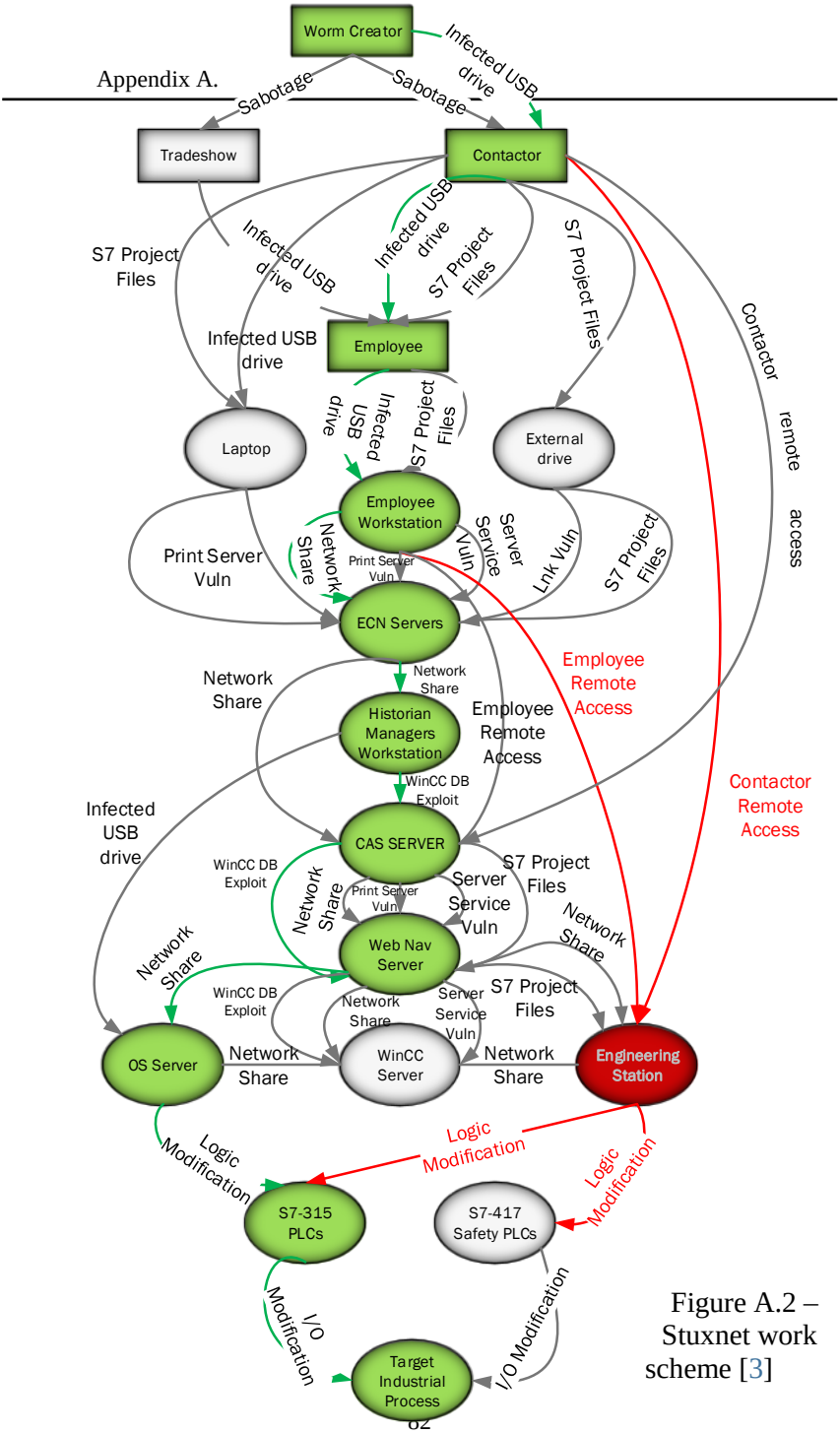


Figure A.2 – Stuxnet work scheme [3]

Step 4: Determining the primary and secondary methods of dealing with the Stuxnet virus relying on the elimination scheme and the assessment of probabilities.

Virus spread is a very important internet emergency, its spread speed and effect range are key factors to lead emergency unit to pay attention to. At the beginning of virus outbreak, most information about that computers is infected is feed backed to antivirus software companies. So the initial scenario that its spread is very rapid and its effect is very extensive is firstly inputted to them, and anti-virus software companies are the first unit to emergency decision-making.

On basic of the initial scenario ($x_{0,1}$ = {rapid spread, extensive effect}), they have two emergency countermeasures as follows:

$y_{0,1}$ = {develop patches},

$y_{0,2}$ ={develop anti-virus software}.

According to investigation, in order to deal with Worm Stuxnet virus, the decision rules of anti-virus software are explored by rough set as table A.1.

Table A.1. Emergency decision in initial scenario

Situation scenario			Decision	Confidence	Support
Code	Spread speed	Effect extension			
$x_{0,1}$	rapid	extensive	$y_{0,1}$	87%	80%
$x_{0,1}$	rapid	extensive	$y_{0,2}$	13%	20%

As far as we know the schemes to combat the virus, we are based on the opinions of experts, we can draw conclusions about the percentage of methods to combat the virus. Or we can take a priori values from Table A.1, the virus obtained after the classification. The example is based on expert opinion (Symantec, Kaspersky Internet Security, etc.).

Outcomes calculate according to the already known scheme of the virus. In our case, we have 2^m outcomes Z, where m – the number of situation response node, i.e. $2^m = 4$ outcomes.

According to table A.1, in the initial scenario $x_{0,1}$ ={rapid spread, extensive effect}, anti-virus software companies have two countermeasures, and the confidence and support of the decision rule

$x_{0,1} \rightarrow y_{0,1}$ are respectively 70% and 42%, the confidence and support of the decision rule $x_{0,1} \rightarrow y_{0,2}$ are respectively 30% and 18%.

On the effect of these two countermeasures, the virus spread event are in four scenarios as follows: $y_{0,1}$ and $y_{0,2}$ aren't major countermeasures to $x_{0,1}$, and the new countermeasure is continued to look for; $y_{0,1}$ and $y_{0,2}$ are major countermeasures to $x_{0,1}$; only $y_{0,1}$ is only a major countermeasures to $x_{0,1}$; only $y_{0,2}$ is only a major countermeasures to $x_{0,1}$.

These form four situation system scenarios of the virus spread as following $z_{0,1}$, $z_{0,2}$, $z_{0,3}$ and $z_{0,4}$

Step 5: Calculating and ranking the possible scenarios for eliminating virus spread.

Let us calculate possible scenarios (as it has been said before, we have four ones):

$$z_{0,1} = \{x_{0,1}, \underline{y_{0,1}}, \underline{y_{0,2}}\}$$
$$z_{0,2} = \{x_{0,1}, \overline{y_{0,1}}, \overline{y_{0,2}}\}$$
$$z_{0,3} = \{x_{0,1}, \overline{y_{0,1}}, \underline{y_{0,2}}\}$$
$$z_{0,4} = \{x_{0,1}, \underline{y_{0,1}}, \overline{y_{0,2}}\}$$

If we got scenario $\overline{y_{0,j}}$, then $\overline{y_{0,j}} = \varphi(y_{0,j})$, if $\underline{y_{0,j}}$, then $\underline{y_{0,j}} = [1 - \varphi(y_{0,2})]$.

$$\varphi(z_{0,1} \mid x_{0,1}) = [1 - \varphi(y_{0,1})][1 - \varphi(y_{0,2})]$$
$$\varphi(z_{0,2} \mid x_{0,1}) = \varphi(y_{0,1})\,\varphi(y_{0,2})$$
$$\varphi(z_{0,3} \mid x_{0,1}) = \varphi(y_{0,1})[1 - \varphi(y_{0,2})]$$
$$\varphi(z_{0,4} \mid x_{0,1}) = [1 - \varphi(y_{0,1})]\varphi(y_{0,2})$$

The table A.2. was build based on the already known virus scenarios.

Table A.2. Emergency decision in initial scenario

Situation scenario			Decision	Conf.	Support
Code	Spread speed	Effect extension			
$z_{0,1}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\underline{y_{0,1}}, \underline{y_{0,2}}$	$x_{1,1}$	100 %	25%
$z_{0,2}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\overline{y_{0,1}}, \overline{y_{0,2}}$	$x_{1,2}$	63%	15.75 %
$z_{0,2}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\overline{y_{0,1}}, \overline{y_{0,2}}$	$x_{1,3}$	37%	9.25%
$z_{0,3}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\overline{y_{0,1}}, \underline{y_{0,2}}$	$x_{1,2}$	79%	19.75 %
$z_{0,3}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\overline{y_{0,1}}, \underline{y_{0,2}}$	$x_{1,3}$	21%	5.25%
$z_{0,4}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\underline{y_{0,1}}, \overline{y_{0,2}}$	$x_{1,2}$	83%	20.75 %
$z_{0,4}$:	$x_{0,1}$ = {rapid spread, extensive effect}	$\underline{y_{0,1}}, \overline{y_{0,2}}$	$x_{1,3}$	17%	4.25%

Using the values of confidence and in accordance with the Table A.2 (10 % = 0.1):

$$y_{0,1} = 0.87;\ y_{0,2} = 0.13$$

$$\varphi(z_{0,1} \mid x_{0,1}) = [1 - 0.87][1 - 0.13];$$
$$\varphi(z_{0,2} \mid x_{0,1}) = 0.87 * 0.13;$$
$$\varphi(z_{0,3} \mid x_{0,1}) = 0.87 * 0.87;$$
$$\varphi(z_{0,4} \mid x_{0,1}) = 0.13 * 0.13.$$

After on substitution of the expression for x from (1.2); we get the probability scenarios

$$\varphi(z_{0,1} \mid x_{0,1}) = 0.11;$$
$$\varphi(z_{0,2} \mid x_{0,1}) = 0.11;$$
$$\varphi(z_{0,3} \mid x_{0,1}) = 0.76;$$
$$\varphi(z_{0,4} \mid x_{0,1}) = 0.017.$$

According to Table A.2, in the scenario $z_{0,1}$ = {$x_{0,1}$, $y_{0,1}$ and $y_{0,2}$ aren't effectively carried out}, the virus spread event makes further worse and its situation scenario evolves to $x_{1,1}$ = {very rapid spread, very extensive effect}, its confidence and support are respectively 100% and 25% . In the scenario $z_{0,2}$ = { $x_{0,1}$, $y_{0,1}$ and $y_{0,2}$ are major countermeasures and are carried out}, the virus spread event is controlled partially or completely, so its situation scenario could evolve to $x_{1,2}$ ={slow spread, not widespread} or $x_{1,3}$ ={very slow spread, small extent}, and their confidences are respectively 63% and 37%. In the scenario $z_{0,3}$ = { $x_{0,1}$, $y_{0,1}$ and $y_{0,2}$ are respectively major and auxiliary countermeasures and are carried out},the event is controlled partially or completely, so its situation scenario could evolve to $x_{1,2}$ ={slow spread, not widespread} or $x_{1,3}$={very slow spread, small extent}, and their confidences are respectively 79% and 21%. In the scenario $z_{0,4}$ = { $x_{0,1}$, $y_{0,1}$ and $y_{0,2}$ are respectively major and auxiliary countermeasures and are carried out}, the event is controlled partially or completely, so its situation scenario could evolve to $x_{1,2}$ ={slow spread, not widespread} or $x_{1,3}$ ={very slow spread, small extent}, and their confidences are respectively 83% and 17%. So, after the emergency action of anti-virus software companies, the event evolves to three results respectively, $x_{1,1}$, $x_{1,2}$ and $x_{1,3}$, (there were three versions of Stuxnet with different propagation velocity and exploiting different vulnerabilities) and their probabilities can be calculated by formula (1.4) as following:

$$\varphi(x_{1,1} \mid x_{0,1}) = \varphi(z_{0,1} \mid x_{0,1}) * \varphi(z_{0,1} \mid x_{0,1}) = 1 * 0.11 = 0.11$$
$$\varphi(x_{1,2} \mid x_{0,1}) = \varphi(z_{0,2} \mid x_{1,2}) * \varphi(z_{0,2} \mid x_{0,1}) = 0.63 * 0.11 = 0.069$$
$$\varphi(x_{1,2} \mid x_{0,1}) = \varphi(z_{0,3} \mid x_{1,2}) * \varphi(z_{0,3} \mid x_{0,1}) = 0.79 * 0.76 = 0.60$$
$$\varphi(x_{1,2} \mid x_{0,1}) = \varphi(z_{0,4} \mid x_{1,2}) * \varphi(z_{0,4} \mid x_{0,1}) = 0.83 * 0.017 = 0.014$$
$$\varphi(x_{1,2} \mid x_{0,1}) = 0.069 + 0.6 + 0.014 = 0.683$$
$$\varphi(x_{1,3} \mid x_{0,1}) = \varphi(z_{0,2} \mid x_{1,3}) * \varphi(z_{0,2} \mid x_{0,1}) = 0.37 * 0.11 = 0.0407$$
$$\varphi(x_{1,3} \mid x_{0,1}) = \varphi(z_{0,3} \mid x_{1,3}) * \varphi(z_{0,3} \mid x_{0,1}) = 0.21 * 0.76 = 0.1596$$
$$\varphi(x_{1,3} \mid x_{0,1}) = \varphi(z_{0,4} \mid x_{1,3}) * \varphi(z_{0,4} \mid x_{0,1}) = 0.17 * 0.017 = 0.00289$$
$$\varphi(x_{1,3} \mid x_{0,1}) = 0.0407 + 0.1596 + 0.00289 = 0.203$$

Step 6: Drawing a rough set scenario flow graph and prioritizing the best decision scenarios.

In view of the fact that we have to make a decision in a very short time, we'll consider an interval t = 0.

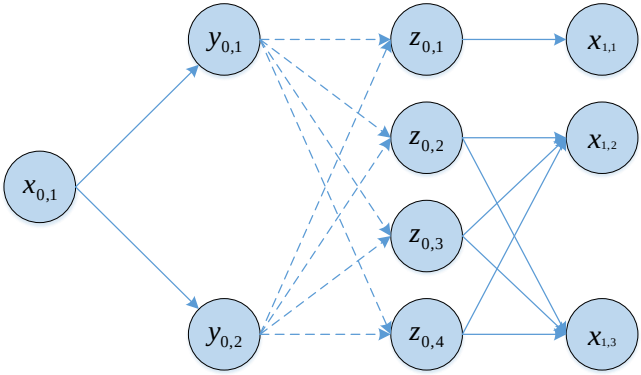


Figure A.4 - A rough set scenario flow graph for targeted internet emergency management problem

The evolution process of the virus spread event could be explored by above scenario analysis and rough set, and its rough set scenario flow graph could be drawn as fig. A.4. According to the graph, some group decision mechanisms of internet emergency management could be explored. In order to control the virus spread before t=1, some countermeasures which could lead $x_{0,1} \rightarrow x_{1,3}$ can be adopted, situation system scenarios $z_{0,2}$, $z_{0,3}$ and $z_{0,3}$ can lead the event to evolve from scenario $x_{0,1}$ to scenario $x_{1,3}$.

So, when t=0, the best decision scenario is $z_{0,2}$, that is both $y_{0,1}$ = {develop patches} and $y_{0,2}$ = {develop anti-virus software} are major countermeasures to $x_{0,1}$, when t = 0.

Bibliography Cited

1. Post-Stuxnet Industrial Security: Zero-Day Discovery and Risk Containment of Industrial Malware – http://www.phoenixcontact-cybersecurity.com/data/downloads/white_papers/post_stuxnet_industrial_security_en.pdf

2. W32.Stuxnet Dossier. Version 1.4 – Available from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

3. SCADA and CIP Security in SCADA and CIP Security in a Post-Stuxnet World: The Future of Critical Infrastructure Security – https://scadahacker.com/library/Documents/White_Papers/Tofino%20-%20SCADA%20and%20CIP%20Security%20in%20a%20Post%20Stuxnet%20World.pdf

Appendix B

Strategies to Mitigate Targeted Cyber Intrusions

(ASD's list of mitigation strategies)

	Mitigation Strategy	Overall Security Effectiveness	User resistance
1	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium
2	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low
3	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low
4	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium
5	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium
6	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low
7	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low
8	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low
9	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low
10	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low
11	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a	Excellent	Medium

	privileged action or access a sensitive information repository.		
12	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low
13	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium
14	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High
15	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low
16	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low
17	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High
18	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium
19	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High
20	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low
21	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium
22	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low
23	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low
24	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low
25	**Enforce a strong passphrase policy** covering complexity,	Good	Medium

	length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.		
26	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High
27	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low
28	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium
29	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low
30	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low
31	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low
32	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low
33	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low
34	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low
35	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low

ASD's (Australian Signals Directorate) list of mitigation strategies, first published in February 2010, is revised for 2014 based on ASD's most recent analysis of cyber intrusions across the Australian Government. This document provides a summary of key changes for 2014. Document and additional information about implementing the 35 mitigation strategies is available at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

COURSE PROGRAM

DESCRIPTION OF THE MODULE

TITLE OF THE MODULE	Code
Human-Machine Engineering for Resilient Systems	CM3

Teacher(s)	Department
Coordinating: **Dr. E. Brezhnev** **Others:** Prof. V. Kharchenko Prof. A. Orekhov, Dr. A. Orekhova Dr. A. Lutskiv, Prof. I. Skarha-Bandurova	Computer Systems and Networks, Computer Engineering

Study cycle	Level of the module	Type of the module
Master	A	Full-time tuition

Form of delivery	Duration	Langage(s)
Full-time tuition	One semester	English

Prerequisites	
Prerequisites: Probability Theory and Foundations of Mathematical Statistics; Foundation of Modeling; Software Engineering	**Co-requisites (if necessary):**

Credits of the module	Total student workload	Contact hours	Individual work hours
4	108	36	72

Aim of the module (course unit): competences foreseeen by the study programme		
This course is designed to provide students with a fundamental understanding of human factors that must be taken into account in the engineering of complex systems and understanding ways of reducing the potential for human behaviours that play a role in breaches of cyber security. The primary focus is the humans aspects of cyber-security, human-machine interaction and decision making within safety-critical industries.		
Learning outcomes of module (course unit)	**Teaching/learning methods**	**Assessment methods**
At the end of course, the successful student will be able to: 1. understand the basic terms and concepts used in human factors engineering	Interactive lectures, Seminar, Just-in-Time Teaching	Module Evaluation Questionnaire
2. identify and analyze sources of human and organizational error in complex systems	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
3. analyze protocols of operators with the system interaction	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
4. understand basic principles underlying the system of access control	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
5. develop flexible and robust operators authentication system	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
6. apply the methods of human factors evaluation and decision making under multiple and conflicting goals.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

Themes	Contact work hours							Time and tasks for individual work	
	Lectures	Consultations	Seminars	Practiclwork	Laboratorywork	Placements	**Total contact work**	**Individual work**	**Tasks**
1. Introduction into HF engineering. 1.1. Complex Systems and Human Factors. 1.2. Areas of Human Factors applications. 1.3. Characteristics of human behaviours. 1.4. Human Error Mechanisms. 1.5. Levels of Human cognitive behaviour. 1.6. Interactions between safety, security, dependability and the usability of complex systems.	2							7	1.7. Human error identification (HEI) technique
2. Human machine interaction safety assessment. 2.1 Interactions between human and machine in a given environment. 2.2. Models for operators' responses to disturbances. 2.3. Group and individual performance.	2		2					7	2.8. Stress, Workload, Boredom, and Fatigue

2.4. Human capabilities and performance. 2.5. Human performance indicators. 2.6. Memory and complex skills. 2.7. Situation awareness.									
3. Human factors and information security. 3.1. Information security and types of human factor errors. 3.2. Threats in human-machine interaction. 3.3. Human-operator readiness evaluation. 3.4. Human-operator readiness methodologies.	2							8	
4. Access control in safety-critical systems. 4.1. Human factors in user authentication. 4.2. Interaction protocols of operators and information system. 4.3. Security policies according to access control.	2							7	
5. Basic principles of authentication, authorization and accounting in information systems. 5.1. Unique identifying characteristics to authenticate user. 5.2. Authentication, authorization and	2				4			7	

accounting operators activity in modern information systems. 5.3. Authentication methods. RADIUS.									
6. Biometry authentication techniques. 6.1. Biometric Error Rates. 6.2. Biometry authentication by fingerprinting. 6.3. Biometry authentication by on-line signature.	2				4			7	
7. Safe Work Practices and Permit-to-Work Systems. 7.1. Specifics of security policies in process control systems. 7.2. Authentication, authorization and accounting in Permit-to-Work Systems.	2				4			7	
8. Security aspects of operators' teamwork. 8.1. Security operations: organizational aspects. 8.2. The work process analysis model (WPAM). 8.3. Team failures. 8.4. Defining the team and teamwork. 8.5. Problems of group decision making.	2			2					
9. **Group decision and accident prevention.** 9.1. Decision support for operators.	2								9.7. Collaborative operation

9.2. Situation for supporting the operator. 9.3. Types of decision support and roles of decision support systems. 9.4. The effects of leadership and group decision on accident prevention. 9.5. Managing multiple and conflicting goals in dynamic and complex situations. 9.6. Formal group decision support techniques.									al and research environment.
10. Training and technology for teams. 10.1. Empirical model of team collaboration. 10.2. Self-assessment and learning in simulation training. 10.3. Knowledge acquisition through repeated theoretical and practical training. 10.4. A computational system for investigating and supporting cognitive and collaborative sense-making processes.	2								10.5. Tools and techniques for the co-design of safety and security critical interfaces.
Iš viso	**20**		**2**	**2**	**12**			**72**	

Assessment strategy	Weight in %	Deadlines	Assessment criteria
Lecture activity, including fulfilling special self-tasks and seminars	10	7,14	85% – 100% Outstanding work, showing a full grasp of all the questions answered. 70% – 84% Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. 60% – 69% A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. 50% – 59% There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. 45% – 49% Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect. 40% – 44% There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range. 20% – 39% There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places. 0% – 19% Very little or nothing that is correct and relevant.
Learning in laboratories	30	7,14	85% – 100% An outstanding piece of work, superbly organised and presented, excellent achievement of the objectives, evidence of original thought. 70% – 84% Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organisation and presentation. 60% – 69% Students will show a clear

			understanding of the issues involved and the work should be well written and well organised. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. 50% – 59% The work should show evidence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organisation should be reasonably clear, and the objectives should at least be partially achieved. 45% – 49% Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. 40% – 44% There should be some work towards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem. 20% – 39% The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. 0% – 19% Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements.
Module Evaluation Quest	60	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	Year of issue	Title	No of periodical or volume	Place of printing. Printing house or intrenet link
Compulsory literature				
M. Teichmann	2013	Human Factors Engineering		Tallinn University of Technology, Estonia http://www.tpi.ee/digiope/hfe/
Editor: D. Growl. Authors: D. Attwood, P. Baybutt, C. Devlin, W. Fluharty, G. Hughes, D. Isaacson, P. Joyner, E. Lee, D. Lorenzo, L. Morrison, B. Ormsby.	2007	Human factors methods for improving performance in the process industries		A John Wiley & Sons, Inc., Publication
Editors: J. Misumi, B. Wilpert, R. Miller.	2005	Nuclear Safety: A Human Factors Perspective		Taylor & Francis Ltd, London, UK
Editors: J. Noyes and M. Bransby	2001	People in Control: Human factors in control room design		The institution of Engineering and technology, London, UK
Editors: D. J. Garland, J.A. Wise, and V. D. Hopkin.	2010	Handbook of aviation human factors	2nd ed.	CRC Press., Taylor & Francis Group, USA
Editors: M. P. Letsky, N. W. Warner, S.M. Fiore, C.A.P. Smith	2008	Macrocognition in Teams: Theories and Methodologies		Printed and bound in Geat Britian by MPG Books LTD. Ashgate

				Publishing Limited, Hampshire, England. Ashgate Publishing Company Burlington, USA.
B. Dayer	2006	Consideration of Human Errors in Risk management		Local Group Zurich, Switzerland
Administrator: J. C. Szaoo, Federal Railroad Administration	2014	Collaborative Incident Analysis and Human Performance Handbook		http://www.apta.com/gap/fedreg/Documents/Human%20Peformance%20%20Manual%20Final.pdf
S. T. Shorrock	2002	Development and Application of a Human Error Identification Tool for Air Traffic Control	Vol 33	Applied Ergonomics, Elsevier Science Ltd. pp. 319–336.
M. Mikkers, E. Henriqson, S. W. A. Dekker	2012	Managing multiple and conflicting goals in dynamic and complex situations: Exploring the practical field of maritime pilots.		Journal of Maritime Research, 9(2), 13-18.
N. A. Stanton, P. M. Salmon, G.H. Walker, C. Baber, D.P. Jenkins	2006	Human Factors Methods: A Practical Guide for Engineering And Design		Ashgate Publishing
Additional literature				
D. Lacely	2009	Managing the human		A John Wiley &

		factor in information security		Sons, Inc., Publication
D. Meister	2004	Conceptual Foundations of Human Factors Measurement		Lawrence Erlbaum Associates, Publishers Mahwah, New Jersey London
J.P. D'Arcy	2007	The Misuse of information systems: The impact of security countermeasures		LFB Scholary Publishing LLC, NY, USA
J. Baron	2008	Thinking and deciding		Cambridge Univ Press.
S. Dekker	2006	The Field Guide To Understanding Human Error		Aldershot, UK, AshgatePublishing Ltd.
R. Hastie, R.M. Dawes	2009	Rational choice in an uncertain world: The psychology of judgment and decision making		Sage Publications, Inc.
G. Gigerenzer	2008	Rationality for Mortals: How People Cope with Uncertainty (Evolution and Cognition)		Oxford University Press

ABSTRACT

UDC 004.49+004.832.2

Skarga-Bandurova I.S., Velykzhanin A.Y. Risk Analysis of SoS Security and Resilience / Edited by Kharchenko V. S. – Kharkiv: National Aerospace University named after N. E. Zhukovsky "KhAI", 2016. – 106 p.

Practical materials of study course "Human-Machine Engineering for Resilient Systems". Module CM 3.4: Human aspects of operator team-work and modeling group decisions, was designed for master students within the framework TEMPUS project "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains" co-founded by the Tempus Programme of the Europe Union. Project Number: 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR.

The course is devoted to the improving the understanding of the role of human factors in system robustness and resilience. This chapter will explore how cyber security concerns related to the uncertainty of emergency management tasks can be addressed for secure EM and suggest possible approaches to improving resilience to cyber-attacks at individual, team and organization level; to develop human factors support tools for enhancing individual and group cyber security sensitivity. The course is a combination of lectures, seminars and laboratory exercises directed to gaining experience in both industrial security concepts and advanced use of particular tools.

Training support package includes a course outline, ad hoc teaching materials, borrowed open-source software and native software.

The book is mainly devoted to MSc, PhD students of universities in such fields as computer security, computer and program engineering when studying methods and tools for safety critical systems. It could be useful for lecturers and professors who conduct classes on corresponding courses.

Fig.: 25. Tab.: 6 Ref.: 27.

CONTENTS

Inna Skarga-Bandurova
Artem Velykzhanin

HUMAN-MACHINE ENGINEERING FOR SECURITY CRITICAL AND RESILIENT SYSTEMS

Training

Kharchenko V.S. eds.

Зв. план, 2017
Підписаний до друку 25.01.2017 Формат
60x84 1/16. Папір офс. №2. Офс. друк.
Умов. друк. арк. 21,89. Уч.-вид. л. 22,31. Наклад 100 прим.
Замовлення 2/2. Ціна вільна

Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu