IDENTIFICATION OF FUTURE CYBER THREATS

RESEARCH EXPERIENCE AND DEVELOPMENT PERSPECTIVES

ASSOC. PROF. ZLATOGOR MINCHEV

E-MAIL: ZLATOGOR@BAS.BG

GARMISCH-PARTENKIRCHEN IX SCIENTIFIC CONFERENCE OF IISR CONSORTIUM APRIL 24, 2014

Digital Era Challenges & Beliefs

2000

Web 1.0

Web 2.0

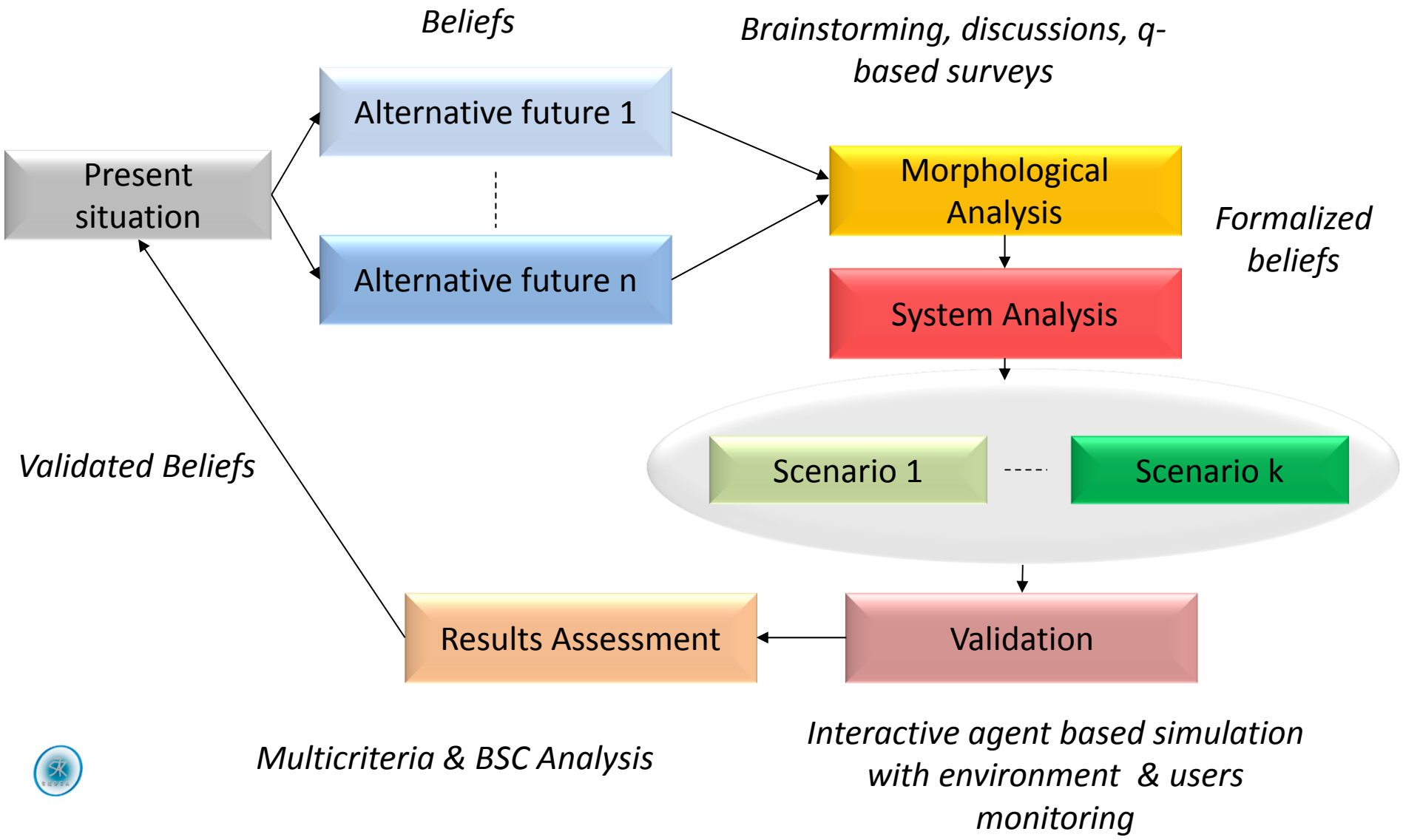
Web 5.0

2050

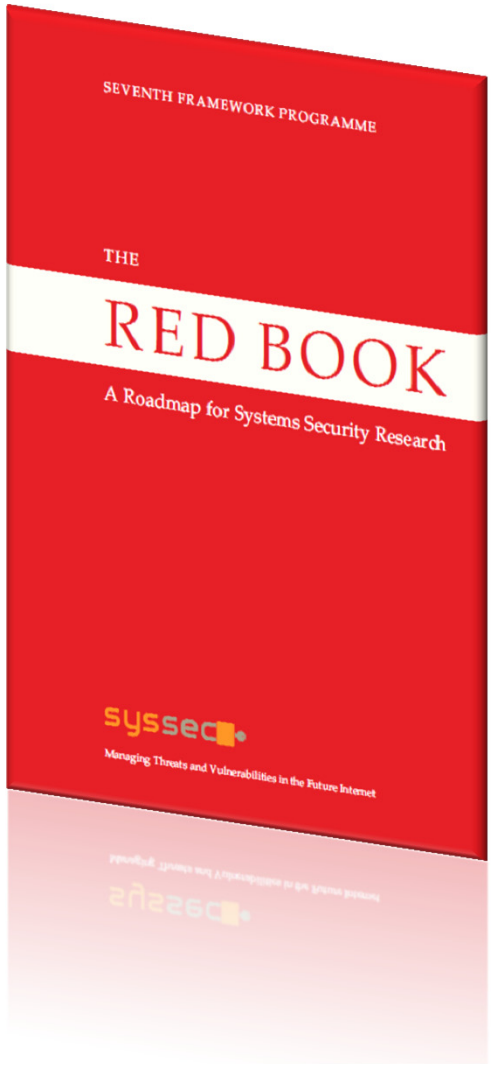
Web 4.0

Web 3.0

METHODOLOGICAL FRAMEWORK



A European Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet



www.syssec-project.eu

Trends Generalization Towards 2020

Threats

- Malware
- Targeted Attacks
- Social Engineering - Phishing

Areas

- Mobile Devices
- Social Networks
- Critical Infrastructures

Challenges

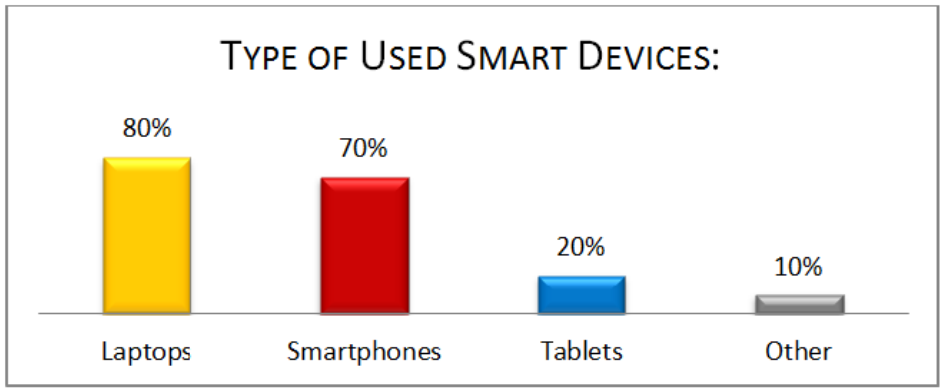
- No Device Should Be Compromisable
- Give Users Control Over Their Data
- Provide Private Moments in Public Places
- Develop Compromise-Tolerant Systems

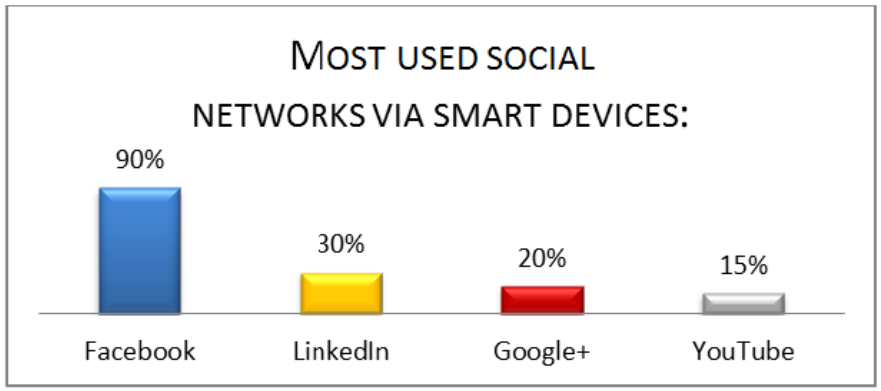
...Web 2.0 и Web 3.0...

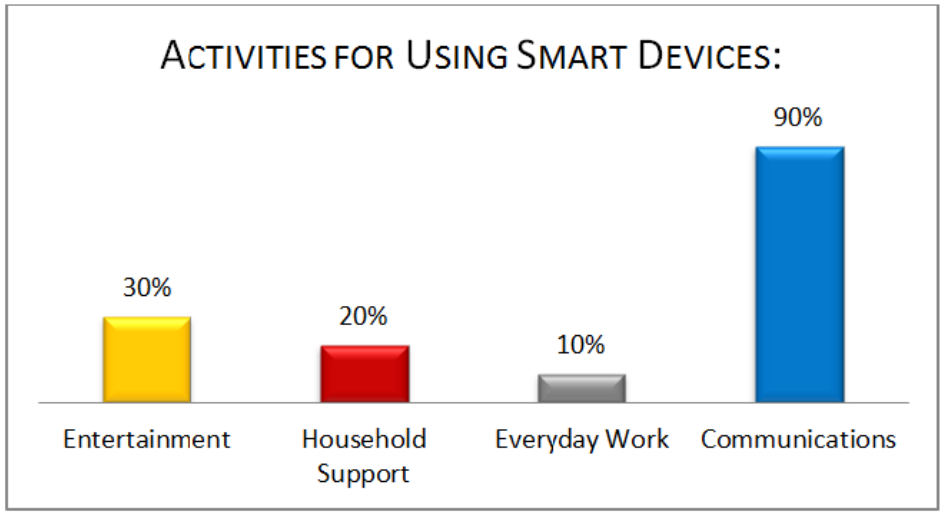
WEB TECHNOLOGIES TRENDS UP TO 2050 ARE QUITE UNCERTAIN...

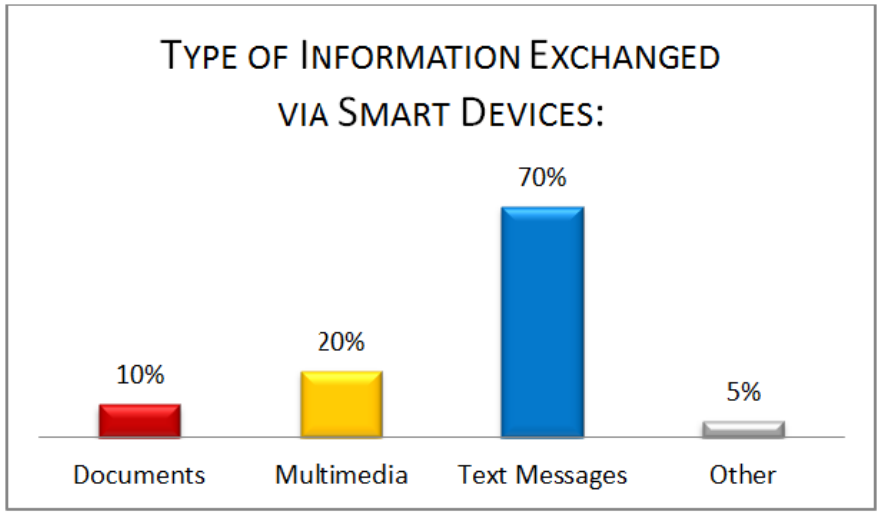
Technology/Dimension	Civil society	Banks & finances	State governance	Critical Infrastructure	Emerging technologies	Education
Web 1.0						
Web 2.0 / Web 3.0						
Web 4.0						
Web 5.0						

POTENTIAL SOURCES OF CYBERTHREATS GO SMART...







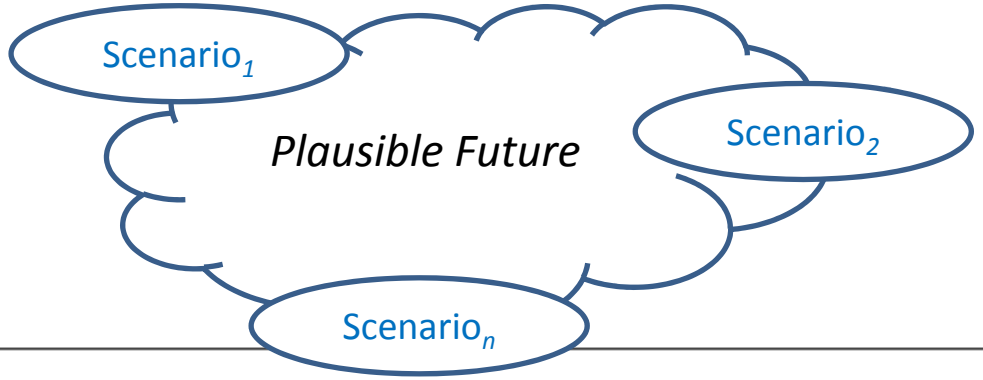


MORPHOLOGICAL ANALYSIS

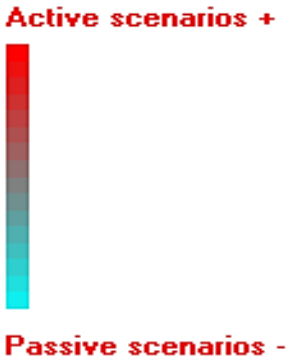
1620 scenario combinations

Morphological Analysis

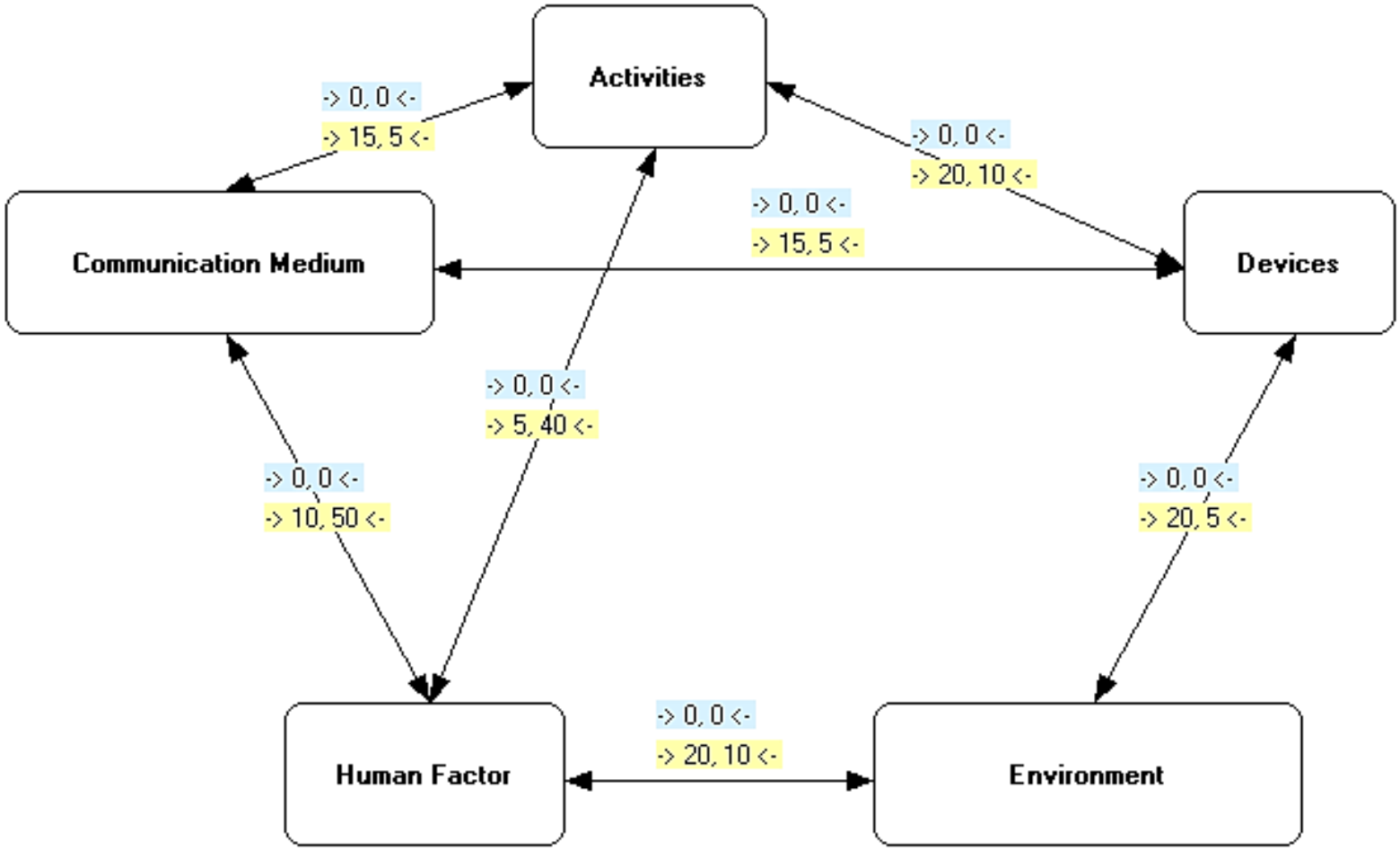
Devices	Activities	Communication Medium	Environment Characteristics	Human Factor Characteristics
Mobile Smart Devices	Entertainment	Cable Networks	Physical	Bioelecrics
Home Entertainment Systems	Communication	Wireless Networks	Structural	Spacial
Home Automation Systems	Everyday Work	Social Networks	Functional	Sensual
	Household Support			



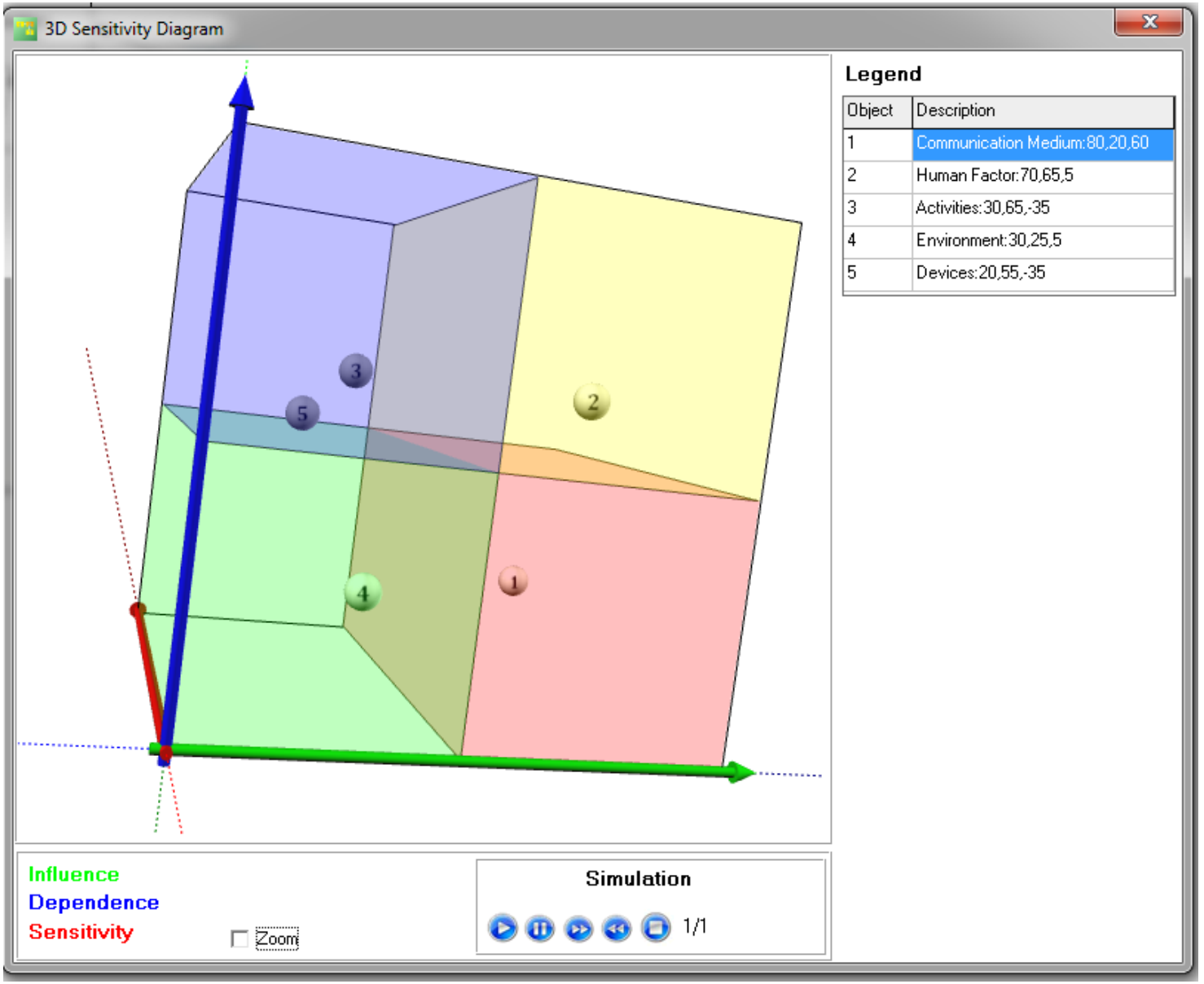
Index	Length	Weight	Name
1	5	170	Scenario1
2	5	125	Scenario2
3	5	265	Scenario3
4	5	145	Scenario4
5	5	195	Scenario5
6	5	195	Scenario6
7	5	140	Scenario7



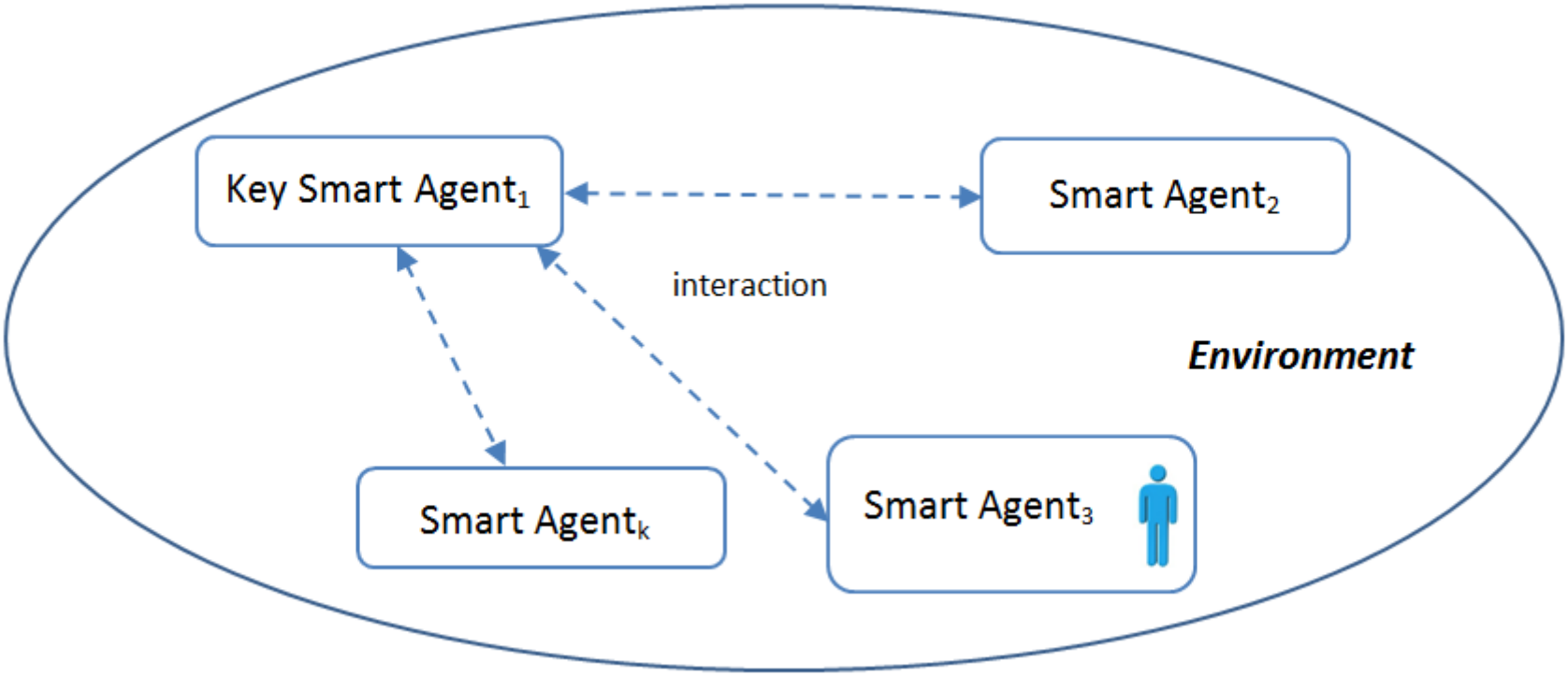
System Analysis



Resulting Classification



TEST-BED VALIDATION CONCEPT

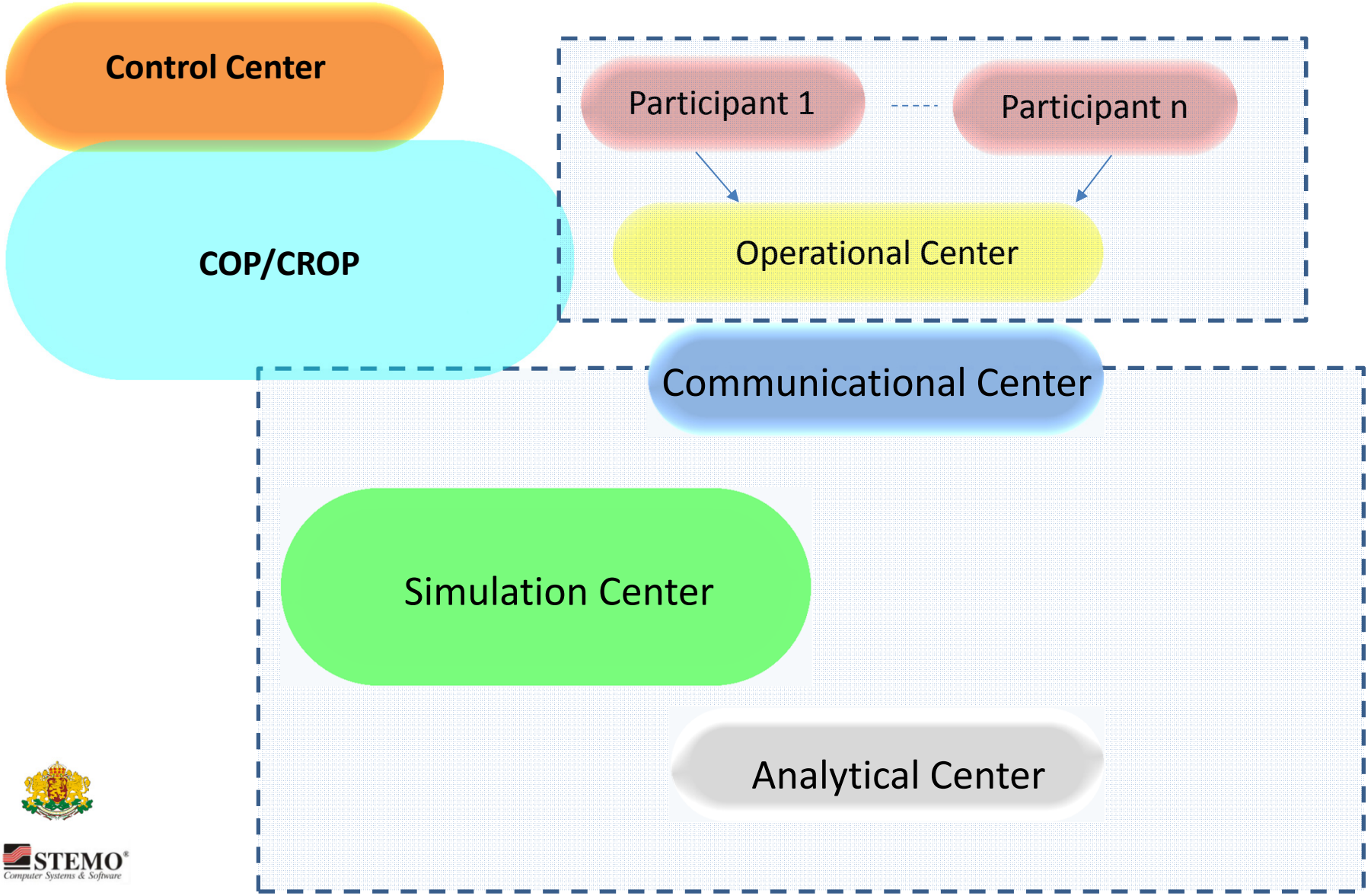


Concept Implementation

CAX

HFR Exploration

CAX KEY ORGANIZATION



STEMO
Computer Systems & Software

Human Factor Response Exploration

A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks

www.snfactor.com

A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes

www.smarthomesbg.com

EMOTION EXPLORATION & BIOFEEDBACK

Biosensors → ADC → DSP Processing & Feature Extraction → User Avatars

Lightweight device ← User working space

SEVENTH FRAMEWORK PROGRAMME
Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

syssec

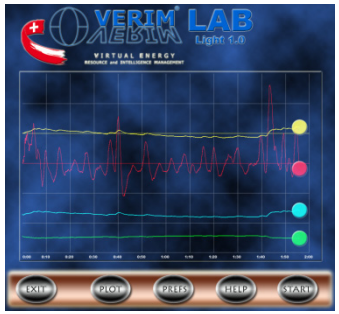
A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World*[1]

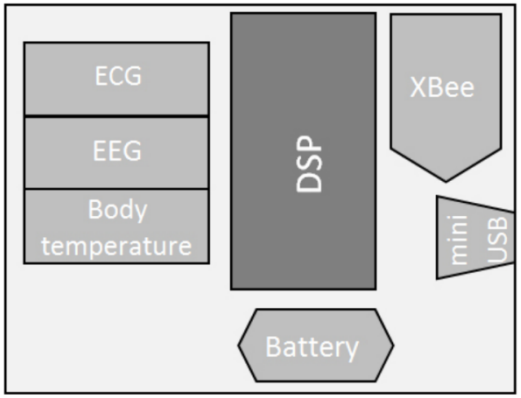
Deliverable D7.3: Advanced Report on Cyberattacks on Lightweight Devices

Abstract: In this deliverable, we will "*report our research results in the area of Cyberattacks on lightweight devices*". We begin by putting our work in the context of the SysSec roadmap, and specifically how our research results address the various threats identified. We then proceed in presenting the various tools and systems we have developed that address those threats. Finally we survey the research on the use of biometrics for improving the security of lightweight devices.

Contractual Date of Delivery	August 2013
Actual Date of Delivery	September 2013
Deliverable Dissemination Level	Public
Editors	Sotiris Ioannidis, Manolis Stamatogiannakis, Thanasis Petsas
Contributors	All SysSec Partners
Quality Assurance	Magnus Almgren, Ali Bezaki

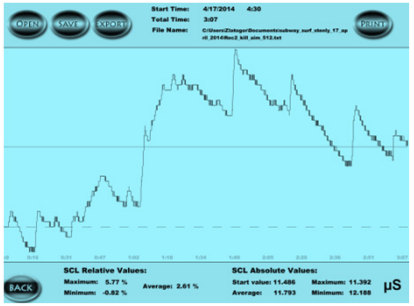
[1] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257007.

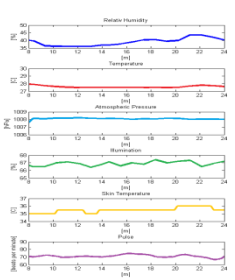


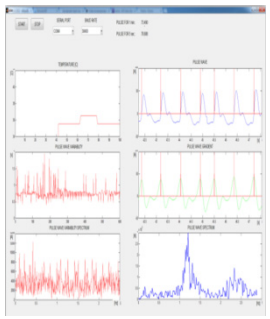


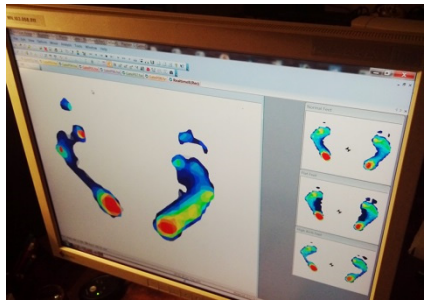
ViSensi Innovation

Entertainment Games Studies

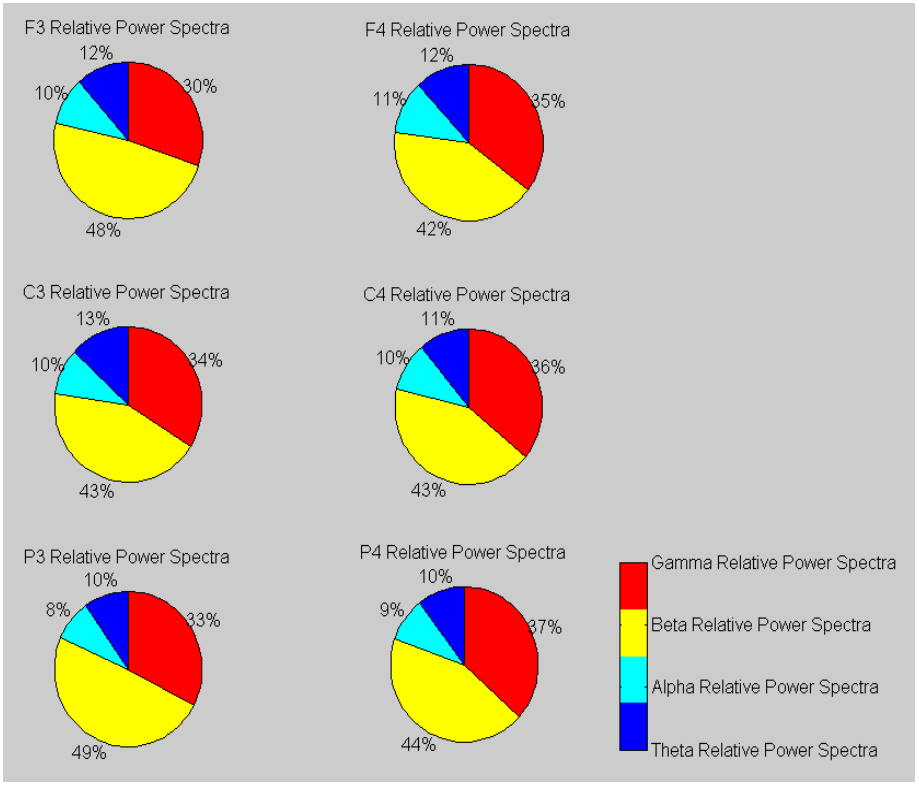




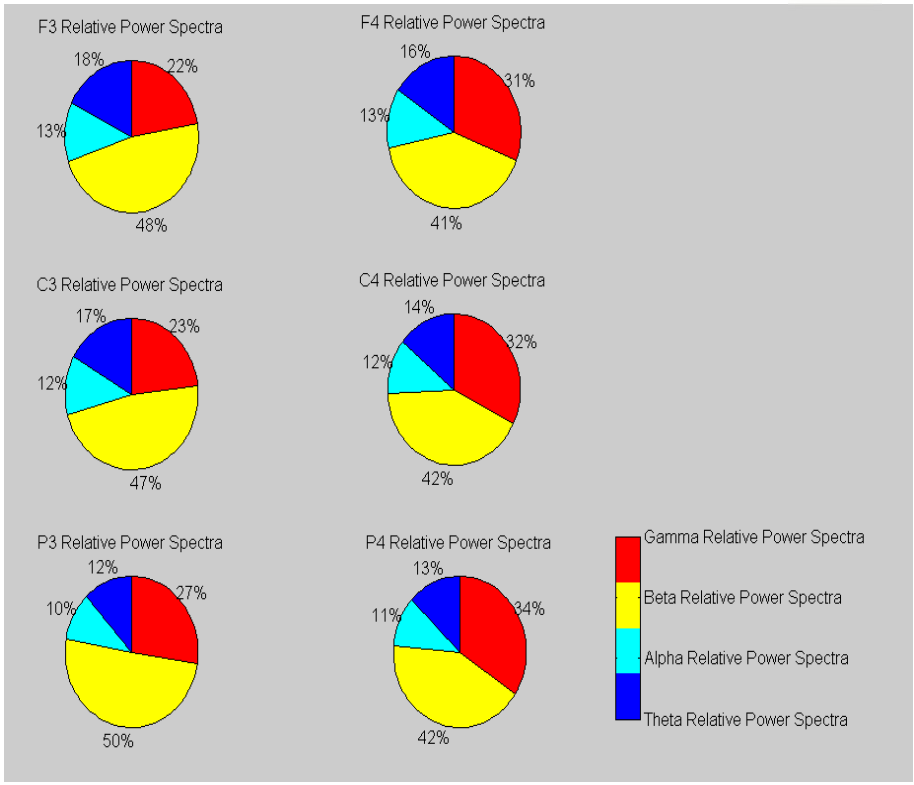




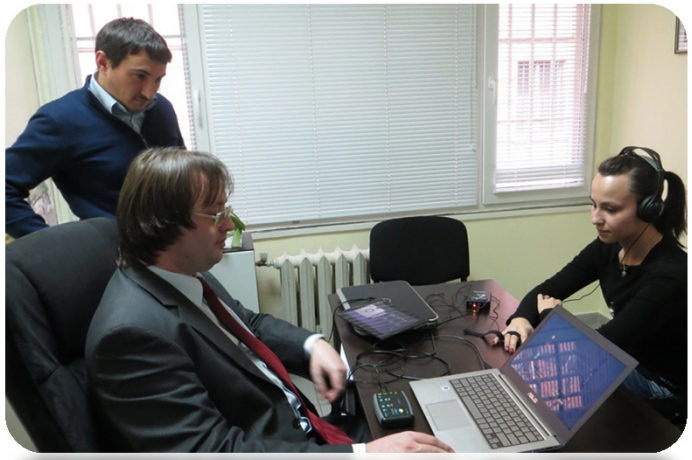
2D

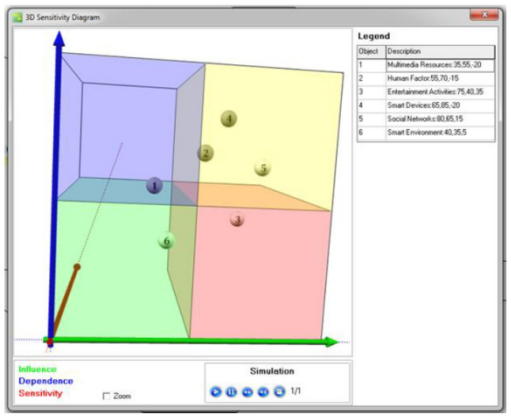


3D

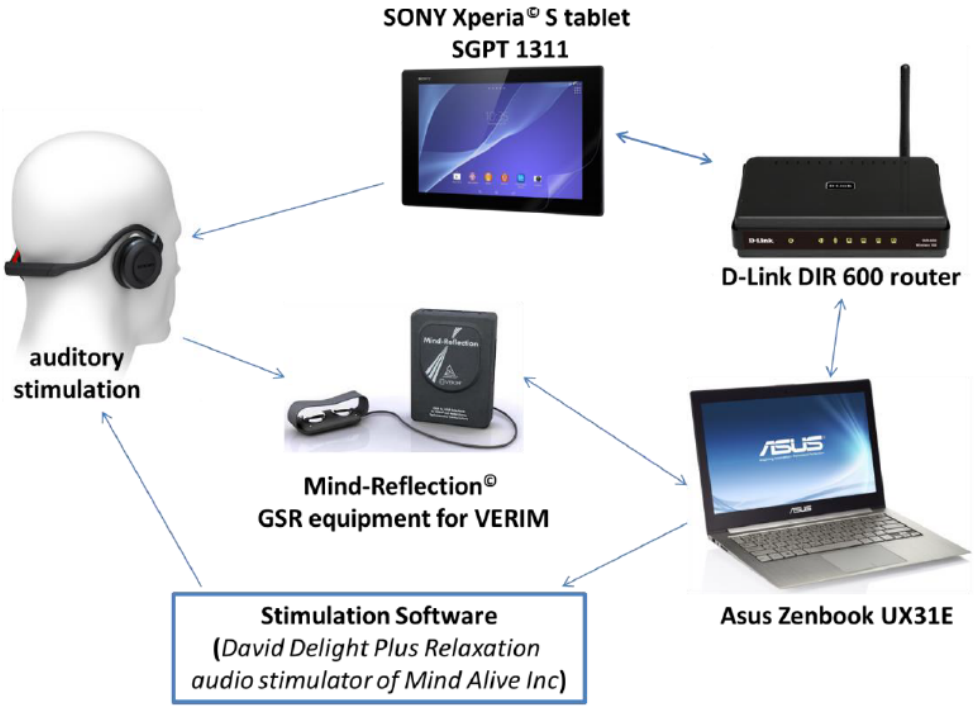


"Digital Drugs" Exploration

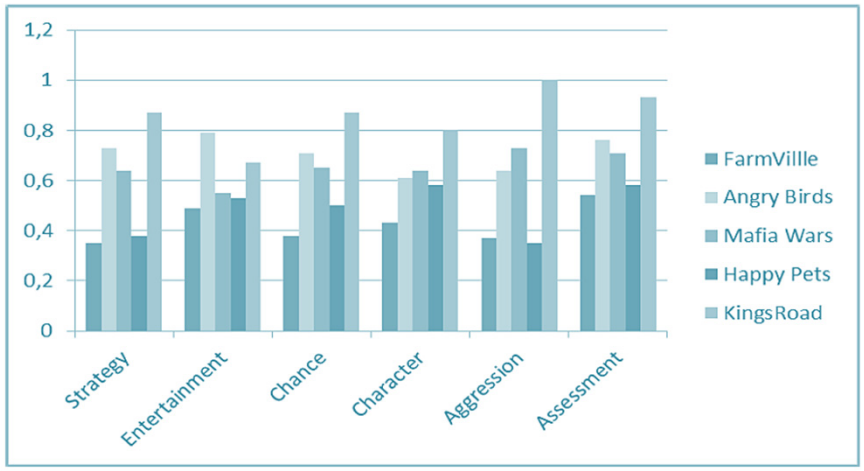


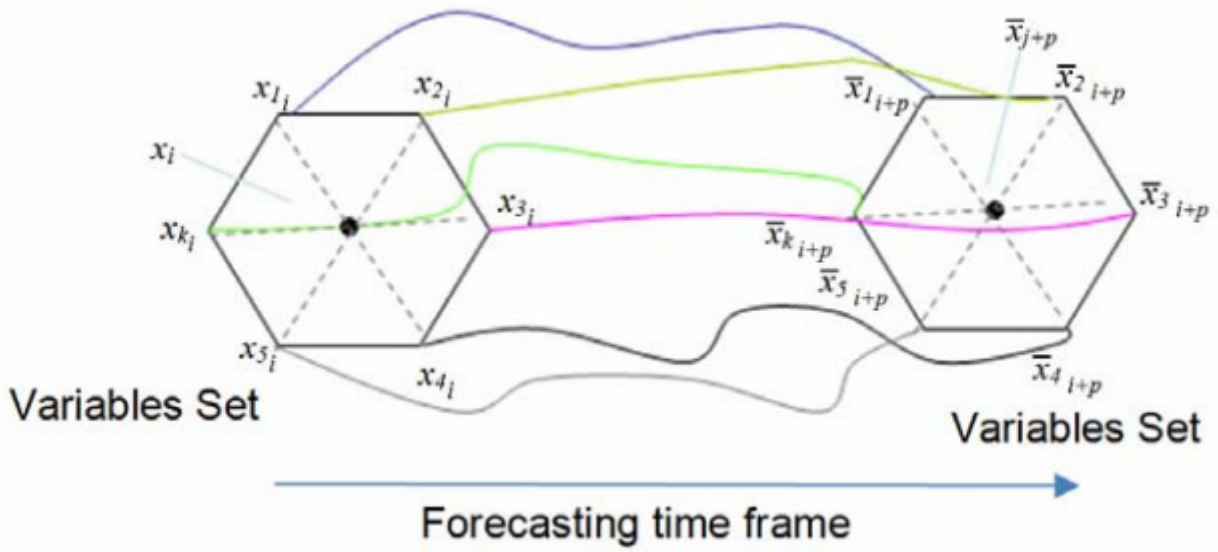


Multimedia Influence to nervous system response observation



RESULTS ASSESSMENT & VALIDATION





DISCUSSION

EVIDENTLY SECURING TODAY'S FAST PROGRESSING DIGITAL WORLD IS A COMPLEX TASK RELATED TO THE DEFINITION AND TEST OF A METHODOLOGICAL FRAMEWORK FOR EMERGING FUTURE CYBER THREATS IDENTIFICATION.

THE PRESENTED ONE IS FOCUSING THE HUMAN FACTOR AS A GENERATOR AND CONSUMER OF SUCH CYBERTHREATS TOGETHER WITH SOME USEFUL TECHNOLOGICAL APPROACHES AND ANALYSIS FOR DIFFERENT SCENARIO SITUATIONS.

THESE DO NOT ASSURE COMPREHENSIVENESS BUT GUARANTEES, AT LEAST, EXPLANATORY RESULTS NATURE THAT IS EXPERIMENTALLY VALIDATED ☺

Acknowledgements

The presented results & achievements have been financially supported by:

(I) EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet" – SysSec, FP7 Grant Agreement No. 257007, www.syssec-project.eu

(II) Bulgarian National Science Fund, Ministry of Education Youth & Science, grants:

(a) A Study on IT Threats and Users' Behaviour Dynamics in Online Social Networks", DMU03/22, Young Scientists Grant, www.snfactor.com

(b) A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes", Research Grant "Funding of Fundamental & Applied Scientific Research in Priority Fields", DFNI-T01/4, www.smarthomesbg.com

(c) Cortical Regulation of the Quiet Stance during Sensory Conflict, TK 02/60, www.cleverstance.com

THANK YOU FOR THE ATTENTION!