The European Project STRUCTURES: Challenges and Results

S. van de Beek[1], J. F. Dawson[2], L. Dawson[2], I. D. Flintoft[2], H. Garbe[3], F. Leferink[4], B. Menssen[3], N. Mora[5], F. Rachidi[5], M. Righero[6], M. Rubinstein[7] and M. Stojilovic[7]

[1]*University of Twente, Enschede, The Netherlands*
[2]*University of York, York, UK*
[3]*Leibniz Universitat Hannover, Germany*
[4]*Thales Nederland B.V., Hengelo, The Netherlands*
[5]*Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland*
[6]*Istituto Superiore Mario Boella, Torino, Italy*
[7]*University of Applied Sciences and Arts Western Switzerland, Yverdon-les-Bains, Switzerland*

Published at the 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, Germany, 16-22 Aug., 2015, pp. 1095-1100.

DOI: 10.1109/ISEMC.2015.7256321

The European Project STRUCTURES: Challenges and Results

Stefan van de Beek *, John Dawson†, Linda Dawson†, Ian Flintoft†,
Heyno Garbe ‡, Frank Leferink*§, Benjamin Menssen ‡, Nicolas Mora¶,
Farhad Rachidi¶, Marco Righero‖, Marcos Rubinstein **, and Mirjana Stojilović **
*University of Twente, Enschede, The Netherlands, {g.s.vandebeek, f.leferink}@utwente.nl
†University of York, York, United Kingdom, {l.dawson, john.dawson, ian.flintoft}@york.ac.uk
‡Leibniz Universität Hannover, Germany, {menssen, garbe}@geml.uni-hannover.de
§Thales Nederland B.V., Hengelo, The Netherlands
¶Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland, {nicolas.mora, farhad.rachidi}@epfl.ch
‖Istituto Superiore Mario Boella, Torino, Italy, righero@ismb.it
**University of Applied Sciences and Arts Western Switzerland, Yverdon-les-Bains, Switzerland,
{marcos.rubinstein, mirjana.stojilovic}@heig-vd.ch

***Abstract*—The project STRUCTURES, funded by the European Union, started in July 2012 to study problems related to the emerging threats of electromagnetic attacks to critical infrastructures. Partners of the team have worked to list possible threats, identify the main characteristics of the critical infrastructures our way of living depends on, test current protection strategies with different simulation and measurement techniques, and condensate the results in guidelines accessible to an audience wider than the one of people working in the field. Here, we summarize the challenges, the solutions, and the results of almost three years of work.**

I. Introduction

The continuous and coordinated performance of a set of infrastructures is crucial for the security and quality of life in industrialized countries. These critical infrastructures (CIs) include electrical energy distribution networks, communication networks, transportation networks such as railways, motorways and airways, law enforcement structures, and public health facilities. Their growing interdependency increases even more their vulnerability to external attacks aimed at interrupting some of their services.

In recent years, the threat of reducing the functionality of such infrastructures using electromagnetic fields to jam, damage, or shut down the electric and electronic systems instrumental to their good performance has become more and more effective [1], [2].

The European Commission opened a call in the context of the overall FP7 Security Call SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platform and networks) against Electromagnetic (High Power Microwave (HPM)) Attacks, to investigate such threats. The diversity of structures to be considered, the intrinsic complexity of the electromagnetic phenomena, the plethora of existing (and foreseen) attacks, the numerous and different issues to be studied (modelling of the attacks, design of sensors, design of shielding, etc.) required a multi-disciplinary approach from highly skilled partners.

The project STRUCTURES started the 1st of July 2012 to address the call.

The project is split into three main phases, with a managing and a dissemination work package (WP) running along the whole duration [3]–[5].

In the first phase, presented in Section II, the simulation tools were adapted and the most significant points to be studied were identified. In particular, in the *physical scenario assessment* part, we conducted an extensive literature review to identify and classify possible electromagnetic threats and possible targets, highlighting their most prominent characteristics. In the *analysis scenario assessment* part, we explored the available simulation tools and how they can interact with each other to model the relevant scenarios identified in the previous part.

In the second phase, to which Section III is devoted, we conducted the actual analysis and design work. In the *risk investigation and protection* part, the archetypal models of critical infrastructures and IEMI threats devised in the physical scenario assessment were simulated using the computational chains identified in the analysis scenario assessment. Important susceptible items were experimentally characterized. Current protection strategies were tested. Using the results of this analysis, we propose some possible improvement of protection. In the *Awareness* part, we designed a sensor for real-time detection of IEMI attacks and an embedded system for identification and localisation of the source.

The third phase, described in Section IV, collects the results and processes them to define a series of guidelines for technicians and caveats for policy makers.

The diagram in Figure 1 shows the division of the activities across the different work packages.

II. Phase I

A. Physical scenario assessment

For a complete physical scenario assessment it is necessary to analyze both the IEMI threat (the electromagnetic source) and the victim (the critical infrastructure). The physical scenario assessment is subdivided into two work packages:

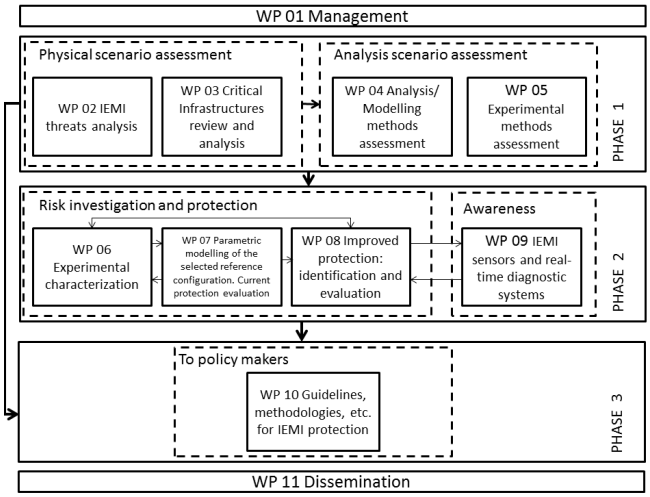

Fig. 1. Schematics of the work packages division in the project STRUCTURES.

- WP 2—IEMI threat analysis, and
- WP 3—Review and analysis of critical infrastructures.

In WP 2, we started by collecting a list of possible sources of an electromagnetic attack available from literature. The focus within STRUCTURES is on sources capable of creating high power electromagnetics (HPEM). HPEM is defined in [6] as: "*the general area of technology involved in producing intense electromagnetic radiated fields or conducted voltages and currents which have the capability to damage or upset electronic systems. Generally, the disturbance exceeds those produced under normal conditions (e.g. 100 V/m and 100 V).*" In total, we collected information on 65 sources, both radiated and conducted [2]. The sources are classified by technical attributes, e.g., frequency content [7], peak electric field or peak voltage, and pulse repetition frequency. The generation and propagation of HPEM is fundamentally limited by physical constraints, such as electric breakdown. These limitations were analysed for different types of sources. To estimate the risk potential of an RF source, it is not sufficient to only take technical attributes into account [8]. Non-technical attributes should also be used to classify the likelihood of the occurrence of an attack with a certain RF source. For this reason, all analysed RF sources were classified by the following non-technical attributes:

- **Source technology:** Sources can be classified by the technical sophistication level in assembling and deploying such systems. As described in [9], classification is based on three different levels: low-tech, medium-tech, and high-tech generator systems.
- **Portability:** The portability of the sources is subdivided into four different levels as described in [10]: pocket-sized, briefcase-sized, motor-vehicle sized, and trailer-sized.
- **Availability:** Measure of both cost and the technological sophistication as described in [10]. Four levels are defined, ranging from low availability to high availability.

The main objective of WP 3 was the identification, review, and analysis of critical infrastructures. Within STRUCTURES, we focused on six different CIs:

1) Power plant,
2) Communication exchange,
3) Transport based on train,
4) Bank/financial office,
5) Airport, and
6) Computer network.

The listed infrastructures are highly complex and increasingly reliant on electronic systems. To keep the complexity manageable, a reference configuration was derived for each infrastructure and the critical subsystems and components were identified [11]. A literature review, which addresses several EMC aspects relevant to critical infrastructures, was performed. First of all, past experience with IEMI effects was listed to analyse the susceptibility issues with these events. Furthermore, existing protection and mitigation concepts against IEMI interferences are summarized. The electromagnetic features of shielding, cable screening, filters, surge protection devices, and others are addressed. Finally, the susceptibility thresholds of relevant electronic components and subsystems available from the literature were analysed and documented.

Another important aspect of WP 3 was the Business Continuity Management (BCM) approach, as defined in the ISO standards starting from ISO 22301 [12]. The theoretical approach was presented and the actual situation was assessed using a questionnaire distributed among selected critical infrastructure organizations. Awareness about IEMI attacks appears to be underestimated by the organizations due to the lack of the experience with IEMI effects. Hence, the lessons learned will help to set up guidelines and methodologies in Phase III of the project.

B. Analysis scenario assessment

In order to perform approximate analyses of the response of complex systems, the Electromagnetic Topology (EMT) concepts [13]–[15] have played a key role since they permit dividing a complicated chain of EM interaction events into a number of simpler parts. Within an EMT-based analysis, the response of a system is obtained by considering independently all the interaction problems that occur; starting from the knowledge of the incident field and ending with the internal component response [16]. Civil infrastructures like office buildings or commercial infrastructures without any special EMC requirement (e.g. communications grounding systems, or similar) are typically designed without an EM topological division of zones. This complicates the decomposition of critical infrastructures into topological layers since they are not very well defined. Also, many of the EM hardening concepts can be violated.

Given the complexity of the problems under study in this project, in the first part of WP 4 a simulation policy was defined in which the main simulation task is decomposed into

simpler calculation objectives and all the results are combined to retrieve the total response. The adopted workflow for the numerical analysis process was defined as follows:

- The reference geometry of the case under study is defined and the susceptible equipment and their position inside the CI are located. The possible IEMI sources and their possible positions with respect to the CI are listed.
- A topological analysis of the reference configurations is performed to identify the relevant coupling paths between the source positions and the susceptible equipment.
- Each coupling path is decomposed into simpler transfer functions that will be modelled with appropriate numerical or analytical methods depending on the physical nature and complexity of the problem under study [17]–[20]. The transfer functions are cascaded together to obtain an overall result. In order to overcome the difficulties imposed by the uncertainty in some of the real scenarios, the method in [21] has been used to perform parametric simulations with less computational effort.
- Finally, a suitable safety margin is defined and applied in the evaluation of the interference risk, to take into account the reduced accuracy of the model. To assess the risk, the susceptibility thresholds (field, power, voltage, or current levels) of the critical equipment with respect to the different IEMI threats are assumed to be known.

A typical simulation problem includes the simulation of the fields generated by a given source, its propagation in an outdoor environment, the penetration of the fields into buildings through critical apertures, conductive penetrations or wall diffusion, and the indoor field distribution calculation. Once the indoor fields are calculated, a direct illumination of the susceptible equipment can be considered, or an indirect coupling to the equipment through its communication or power lines due to the field-to-wire coupling can also be studied. One of the major challenges in building realistic models of CIs is the determination of the high frequency characteristics of the constitutive materials of windows, cables, and polymers for which very little information is available in the literature or for which no simulation experience has been reported. Some parts of the experimental characterization campaigns of WP 5 and WP 6 were aimed at fine tuning the simulation models or at validating the accuracy of the adopted approximations in the calculation of the simplified transfer functions [22]. In the case of cable simulations, the input impedances of the communication circuits and power sources of the critical equipment are required for loading the MTL models and calculating the voltage and current transfer functions. A method to retrieve the differential input impedance of the communication and power ports of critical equipment with the aid of a two-port VNA was presented in [23].

At higher IEMI frequencies (above about 1 GHz), coupling to cables can only be considered statistically due to the uncontrolled variations in cable bundles and critically in the connection interface geometries. Since Ethernet cables are a critical component in many CI scenarios which depend on IT equipment, empirical data on the statistical variation of Ethernet cable and connector transfer functions were collected from 200 MHz to 6 GHz using reverberation chamber measurements. Transfer function envelopes were derived from the measurement data for use in WP 7.

III. Phase II

A. Risk investigation and protection

The risk analyses of the six types of infrastructures listed in Section II-A have been performed in WP 7 by using the agreed workflow. For each case, a reference configuration, including 3D CAD files and a list of critical equipment under study, and the appropriate numerical methods for its simulation have been elaborated by the consortium partners.

For example, the chosen reference configuration for the communication exchange infrastructure is a TETRA station, for which the susceptibility thresholds and other useful information were provided in WP 6 [24]–[26]. The simulation setup is illustrated in Figure 2. The equipment is mounted on an outdoor structure (mounting pole) typically built with metal and located above the ground. The critical equipment inside the base-stations consists of RF receivers connected to monopole antennas through RG214 coaxial cables, GPS receivers connected to the GPS antenna through RG58 coaxial cables, and network cards connected to the service box through Ethernet cables. The mounting pole is illuminated with a plane wave arriving from several possible directions. The transfer functions between the amplitude of the illuminating field and the induced voltage and current at the input of the receivers have been numerically calculated with a computational chain composed of time domain and frequency domain full wave methods for the field distribution and antenna coupling calculations, and MTL plus circuit codes for the field-to-wire coupling and propagation to the loads. The input impedance and the transfer functions of the front-end filters and the network equipment were previously obtained in the experimental campaigns of WP 6.

Another reference configuration for a transport infrastructure considered front-door coupling to the communication antennas on a train. The configuration is shown schematically in Figure 3. In Levels 2 of the European Train Control System (ETCS) both a GSM-R radio link and the fixed data balises are used in the signaling control loop between the signaling control centre and on-board computer (EVC). The balises operate as location markers to allow the train EVC to determine the train location which is then sent to the signaling control centre via a GSM-R radio link. Movement authority is then returned to the EVC by the GSM-R link. The critical equipment is the receiver front-ends in the GSM-R receivers and balise antenna units. The loop antennas system used by the balise may also offer an out-of-band attack front-door on the on-board computer system. The system is illuminated by plane-waves from various directions and by dipole antennas located in the passenger compartment of the train to yield transfer functions between IEMI source amplitudes and received voltage. The computational chain uses full-wave FDTD

simulations of the train coupled with MoM models of the GSM-R and balise antennas. In this case, the receiver input impedance and susceptibility profiles are obtained from the literature.

Data from the analysis of the six archetypal CIs are used for the following WP 8. The aim of WP 8 is to identify strategies and means of improving current protection levels for CIs. To this end, the work package is broken down into three tasks which provide a structured approach to the work. The first task is to define the protection levels which are required to mitigate the potential IEMI threat. The results of WP 6 and WP 7 are being used to define the protection level requirements (e.g., current level, voltage level, field level, frequency range) for the components of each critical infrastructure. The possible need for protection is being derived from the probability of failure of critical systems when subjected to the IEMI effects in the larger context of its relation with other components within the infrastructure containing the system of concern. The second task is a study of the protection technologies and strategies that can be used to achieve the desired protection levels specified in the first task. Specific protection strategies (hardware and software) are being applied for front-door and back-door IEMI attacks, which can be either conducted or radiated. Passive EM hardware protection techniques applied to the system of concern (e.g., filtering, shielding, SPDs, system layout) are being considered along with the integration of innovative active hardening measures (e.g., frequency selective surfaces in radomes, smart antennas). Special attention is being given to the fact that good coordination between hardware and software hardening (e.g., error detection codes, fault diagnosis, error recovery) must be achieved, as well as the fact that an upgrade of available traditional protective devices may be needed (e.g., parasitic effects in SPDs). The third task is an evaluation of the effectiveness of the proposed protection strategies and technologies through modeling, case simulations, and laboratory measurements. For the analysis, test cases defined in WP 7 will be used, considering both conducted and radiated scenarios. The cost and relevance will be considered to evaluate the convenience of the protection technologies and strategies.

B. Awareness

A failure of an electronic component or system due to IEMI may be blamed on faulty hardware or software, and much time and money may be wasted on searching for the cause, particularly if the failure is intermittent. It is therefore beneficial to consider how IEMI attacks may be detected. The three most important requirements for the detection system are the ability to detect an IEMI attack and generate an alarm, to send the received data for logging and post-processing, and to be cost-efficient. We have developed a low cost system that achieves these requirements [27], [28]. Additional features, such as locating and/or identifying the source of the attack, require designing a significantly more complex system, which is thus likely to be more expensive. However, in some applications, these features may be required, so we have also developed an IEMI detection system with location and identification

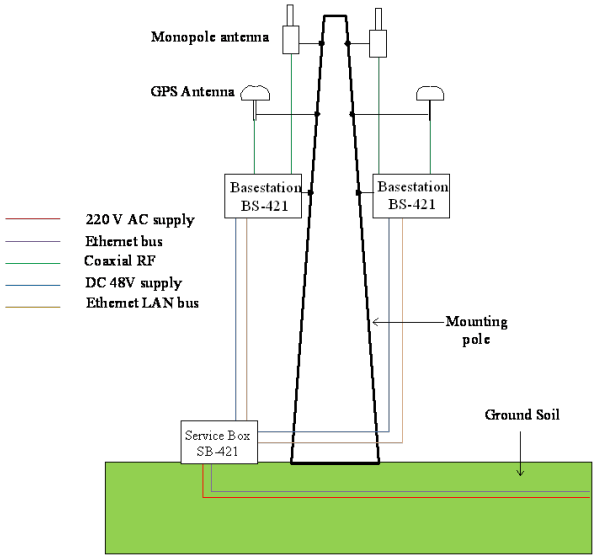

Fig. 2. Schematic diagram of the communication infrastructure. Image adapted from [24].

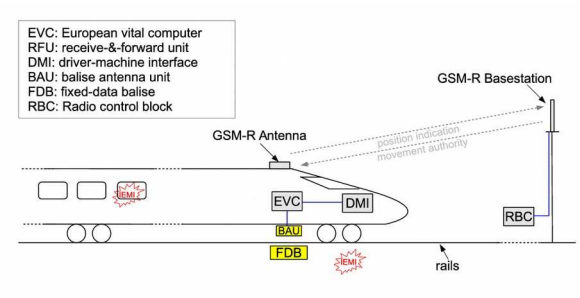

Fig. 3. Schematic diagram of the rail infrastructure reference case. Front-door coupling between IEMI sources at trackside and on the train to the onboard GSM-R and balise antenna units have been considered.

capabilities [29], [30]. This has been done as part of WP 9.

The low cost detector system uses a simple diode detector with a logarithmic amplifier and peak hold, sampled by a microcontroller, see Figure 4. It has a fibre-optic communications link to a monitoring station. It can detect CW signals over the frequency range 100 MHz to 6 GHz with a sensitivity better than 10 V/m. For short pulsed signals, the detector is less sensitive but able to detect signals of about 200 V/m for pulse widths of about 250 ps. A conducted IEMI sensor is also being developed. The design is capable of operating with a low power consumption so that it may be solar powered if used outside and will operate off internal batteries for a period of days in case of power loss.

When the design of the IEMI location and identification system started, a number of different localisation algorithms were analyzed to compare their applicability to locating IEMI sources. Most of them were found to have limitations due to the broad bandwidth, fast pulse-widths, and high directivity of IEMI sources. The time difference of arrival (TDoA)

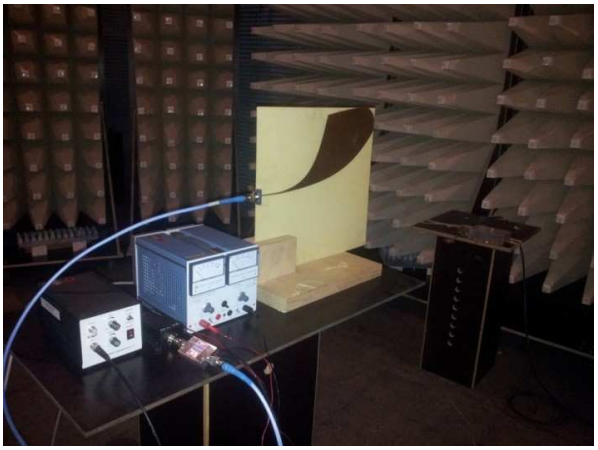

Fig. 4. The low cost IEMI detector prototype under test with double exponential pulse generator at Rheinmetal test facility Unterleuss.

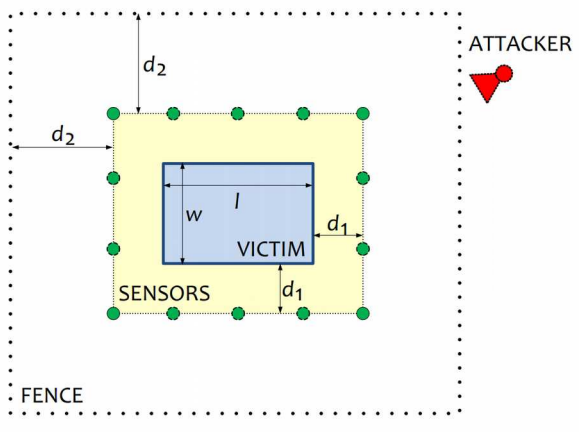

Fig. 5. An example scenario of the IEMI attack. The victim equipment is inside a building of length l and width w. A set of EM field sensors, marked in green, is distributed around the building. The separation between the building and the sensors is at least d_1 and between the sensors and the fence at least d_2. An IEMI source, marked in red, is somewhere outside the protected area [29].

algorithm was estimated the best [29]. This algorithm requires a relatively small number of simple sensors to calculate the source location from the difference in arrival time of the emitted pulse at each sensor. Due to high directivity of many IEMI sources, the sensors should be distributed around the periphery of an installation to be protected (Figure 5).

The IEMI location and identification system uses a novel one-bit digitisation method, allowing efficient identification of the type of source waveform [30]. The device is modular (Figure 6). It is designed to accept up to five EM-field sensors, e.g., D-dot sensors SFE3-5G from Montena Technology SA. The main components of the device are the sensor boards, one for every sensor, the interface board, and the FPGA signal-processing board. The sensor boards are analog interface boards, designed to accept sharp voltage impulses or oscillatory signals, estimate their amplitude, and perform one-bit digitization. The interface board collects digital data from all sensor boards and passes it to the Xilinx FPGA Kintex-7 Evaluation board. The FPGA is programmed to perform attack detection and data preprocessing. At the same time, the evaluation board is connected to a PC, for which a special software to collect the information on the attack, estimate the source location and type, and control and tune the device operation is developed. The system is currently under test.

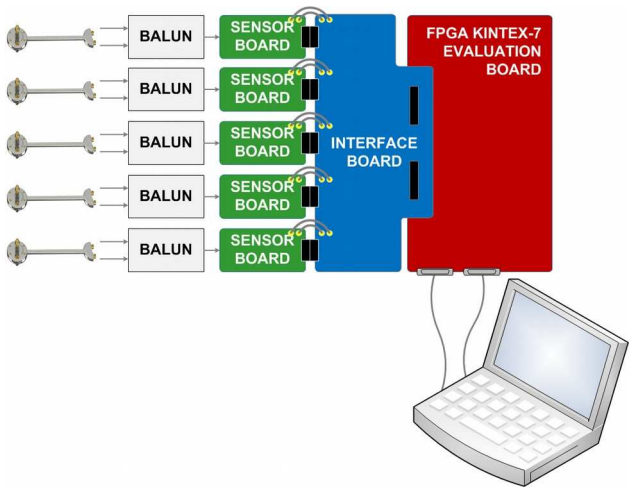

Fig. 6. The IEMI location and identification system block diagram. The device is modular, composed of a set of sensor boards, an interface board, and a high-speed signal-processing FPGA board. The control and the monitoring of the device operation is done via a PC. Additionally, the PC is used for displaying the location of the source and the estimated waveforms of the attack signals.

IV. Phase III

A. Guidelines and methodologies for IEMI protection

WP 10 will use the outputs and results of the previous work packages to provide a set of documents targeted at different audiences. The first document will be aimed at policy makers and standards bodies. It will recommend an assessment system which is based on a standard safety risk assessment approach to IEMI. The issues considered will include:

- Likelihood and severity of adverse consequences.
- Application of a suitably calibrated matrix and severity scale.
- Assessment of risk tolerability.
- Assessment of accessibility.
- Any other factors that may affect the vulnerability of the infrastructure.

The companion disciplines of and standards for CI protection such as the "Business Continuity Management" approach, the ICT standards for Security Techniques, etc., will be considered to situate the guidelines in a larger existing framework regarding CIs. Non-technical mitigation actions will be included as will a consolidated summary of applicable standards together with an assessment of the standards and recommendations for standards bodies. The second document will give guidelines and recommendations for the detection of IEMI for an au-

dience of engineers and policy makers based on the outputs from WP 9. The third document will be a technical summary of protection methods for engineers and standards bodies and will provide advice on where improvements to these could be made. The final document will include information on computational and experimental methods which may be used to provide some of the information used as input to the risk assessment. Guidance on how to use the data obtained from any modeling and experiments will be included, as will some examples of coupling data. The audience for this document is expected to be engineers charged with providing the input to the risk assessment. It may also be of interest to standards making bodies for the measurement techniques.

V. Conclusion

A brief account of the European project STRUCTURES is given. With the aim of investigating the emerging threats of high-power electromagnetic interference against critical infrastructures at the base of our way of living, the partners of the project have developed a cross-disciplinary approach, facing different aspects of the problem.

Acknowledgment

This work has been partially supported by the European Union Seventh Framework Programme under grant agreement number FP7-SEC-2011-285257.

References

[1] F. Sabath, "What can be learned from documented intentional electromagnetic interference (IEMI) attacks?" in *General Assembly and Scientific Symposium, 2011 XXXth URSI*, Aug 2011, pp. 1–4.

[2] G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein, and R. Cherkaoui, "Overview of IEMI conducted and radiated sources: Characteristics and trends," in *Electromagnetic Compatibility (EMC EUROPE), 2013 International Symposium on*, Sept 2013, pp. 24–28.

[3] Website: structures-project.eu.

[4] S. van de Beek and F. Leferink, "Current intentional EMI studies in europe with a focus on STRUCTURES," in *EMC Tokyo 2014*, May 2014.

[5] S. van de Beek, J. Dawson, I. Flintoft, F. Leferink, N. Mora, F. Rachidi, and M. Righero, "Overview of the european project STRUCTURES," *IEEE EMC Magazine*, 2015, accepeted.

[6] *Electromagnetic compatibility (EMC) Part 1-5: General High power electromagnetic (HPEM) effects on civil system*, IEC TR 61000-1-5, 2004.

[7] D. Giri and F. Tesche, "Classification of intentional electromagnetic environments (ieme)," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 46, no. 3, pp. 322–328, Aug 2004.

[8] F. Sabath and H. Garbe, "Risk potential of radiated hpem environments," in *Electromagnetic Compatibility, 2009. EMC 2009. IEEE International Symposium on*, Aug 2009, pp. 226–231.

[9] *Electromagnetic compatibility (EMC) Part 2-13: Environment High power electromagnetic (HPEM) environments Radiated and conducted*, IEC Standards 61000-2-13, 2005.

[10] *Series K: Protection against Interference. High-power electromagnetic immunity guide for telecommunication systems*, ITU-T K.81, 2009.

[11] B. Menssen, M. Mleczko, H. Garbe, K.-U. Rathjen, S. Dickmann, S. van de Beek, and F. Leferink, "Reference configurations for the characterization of critical infrastructures," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1218–1223.

[12] "Societal security – Business continuity management systems — Requirements," *ISO 22301*, 2012.

[13] J. P. Parmanier, J. C. Alliot, G. Labaune, and P. Degauque, "Electromagnetic coupling on complex systems: Topological approach," *Interaction Note*, 1990, 0488.

[14] J. P. Parmanier, "Numerical coupling models for complex systems and results," *Electromagnetic Compatibility, IEEE Transaction on*, vol. 46, pp. 359–367, 2004.

[15] S. Arianos, M. Francavilla, M. Righero, F. Vipiana, P. Savi, S. Bertuol, M. Ridel, J.-P. Parmantier, L. Pisu, M. Bozzetti, and G. Vecchi, "Evaluation of the modeling of an EM illumination on an aircraft cable harness," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 56, no. 4, pp. 844–853, Aug 2014.

[16] F. M. Tesche, M. V. Ianoz, and T. Karlsson, *EMC analysis methods and computational models*. New York: Wiley, 1997.

[17] S. Runke, V. Hansen, J. Streckert, and M. Clemens, "A coupled multi-method approach for the numerical simulation of intentional electromagnetic interference into critical infrastructure," in *Electromagnetics in Advanced Applications (ICEAA), 2013 International Conference on*, Sept 2013, pp. 875–879.

[18] M. Antonelli, F. Milani, and M. Bandinelli, "A methodology for modeling IEMI problems on complex scenarios," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1232–1237.

[19] S. Runke, V. Hansen, J. Streckert, M. Clemens, K.-U. Rathjen, and S. Dickmann, "IEMI analysis of critical infrastructures by simulations using a multi-method coupling strategy," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1238–1241.

[20] M. Francavilla, M. Righero, G. Vecchi, and F. Vipiana, "On dealing with low frequency problems using mom and dielectrics in a simplified IEMI scenario," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1228–1231.

[21] M. Francavilla, G. Giordanengo, M. Righero, G. Vecchi, and F. Vipiana, "Parametric interpolation of IEMI effects in a simplified scenario," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1224–1227.

[22] N. Mora, C. Kasmi, F. Rachidi, M. Darces, M. Hélier, and M. Rubinstein, "Analysis of the propagation of high frequency disturbances along low-voltage test raceway," in *AMEREM 2014*, August 2014.

[23] N. Mora, M. Salvatierra, C. Romero, F. Rachidi, and M. Rubinstein, "Critical equipment input impedance measurement for IEMI calculations," in *Electromagnetic Compatibility (EMC), 2013 IEEE International Symposium on*, Aug 2013, pp. 416–422.

[24] J. Schmitz, M. Camp, and M. Jung, "IEMI effects of a tetra base station as an example of a critical infrastructure," in *8th Future Security Conference*, 2013.

[25] S. van de Beek, R. Vogt-Ardatjew, and F. Leferink, "Robustness of remote keyless entry systems to intentional electromagnetic interference," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1242–1245.

[26] S. van de Beek and F. Leferink, "Robustness of a TETRA base station receiver against intentional EMI," *Electromagnetic Compatibility, IEEE Transactions on*, 2015, in press.

[27] J. Dawson, I. Flintoft, P. Kortoci, L. Dawson, A. Marvin, M. Robinson, M. Stojilović, M. Rubinstein, B. Menssen, H. Garbe, W. Hirschi, and L. Rouiller, "A cost-efficient system for detecting an intentional electromagnetic interference (IEMI) attack," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1252–1256.

[28] J. Dawson, I. Flintoft, L. Rebers, M. Camp, J. Schmitz, and M. Jung, "Circuit and electromagnetic modelling of a low cost IEMI sensor," in *Proceedings of EMCUK 2014*, 2014.

[29] M. Stojilović, B. Menssen, I. Flintoft, H. Garbe, J. Dawson, and M. Rubinstein, "TDoA-based localisation of radiated IEMI sources," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1263–1268.

[30] D. Recordon, M. Rubinstein, M. Stojilović, N. Mora, G. Lugrin, F. Rachidi, L. Rouiller, W. Hirschi, and S. Sliman, "A comparator-based technique for identification of intentional electromagnetic interference attacks," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, Sept 2014, pp. 1257–1262.