New frontiers in security risk management

Luis Enrique Sánchez, ***University of Castilla-La Mancha, Spain***

Antonio Santos-Olmo, ***University of Castilla-La Mancha, Spain***

Haralambos Mouratidis, ***University of Essex, UK***

Eduardo Fernández-Medina, ***University of Castilla-La Mancha, Spain***

Abstract—Information and Communication Technologies (ICT) are fomenting a highly connected and modern society. This modernisation is making innumerable improvements to our daily lives (e.g. transport, health, communications, business, efficiency, entertainment, etc.). However, it is also creating a complex and interconnected ecosystem of security risks that threatens our privacy, honour, information, and other material resources. It can, therefore, clearly be seen that traditional Information Security Risk Analysis Methods (ISRAMs) are an insufficient means to protect citizens. Nevertheless, the emergence or evolution of advanced technologies (e.g. quantum computing, machine learning, semantic models, swarm intelligence or even blockchain) may push ISRAMs towards a new technological dimension that seeks a more connected and integrated awareness of security risks. In this paper, we present a vision of how these advanced technologies can be integrated in order to reduce risks in our daily lives and help us to make decisions regarding security risks.

The 20th century was the age of information, and the 21st century will be the age of connectivity and knowledge. These trends have been fomented by the emergence of disruptive technologies, such as quantum computing, machine learning, semantic models, swarm intelligence or even blockchain. They acquire a new dimension by being able to access large big data systems provided by the integral connectivity associated with IoT, Smart cities, Smart homes, Smart businesses, etc.

This new capacity to access large volumes of data has, along with total connectivity, enabled the development of an almost infinite potential to create intelligence around us, and to make information systems much more powerful, dynamic and intelligent. This has enabled connectivity and data to reach all aspects of our lives, from our work environment to our homes, cars, cities, and even our own bodies, and allow us to visualise, act and make decisions in real time as regards almost all these aspects of our lives.

However, it has also generated a paradigm shift. Organisations and citizens now confront a new type of risk derived from, among other things, five major social and technological transformations: i) Cloud Computing - Shared assets in the cloud: On the one hand, information assets have, in most cases, gone from being centralised and totally dedicated to the organisation to being in the cloud and shared by multiple organisations. This has been one of the paradigms derived from the implementation of microservices in organisations. The introduction of microservice architectures into organisations' information systems provides greater scalability at a lower cost, but in return requires a new vision of risk that is more global than the current one; ii) Teleworking: The emergence of COVID-19 brought about a major change in companies, bringing forward the decentralisation of work by several decades. During the pandemic, companies were forced to allow workers to work from home, which boosted the decentralisation of these companies; iii) IoT - Connectivity at all levels: Connectivity has not only appeared in organisations but has also spread to all aspects of our lives. We can now monitor biological signals from our bodies in real time. Homes have become fully connected, as has also occurred with other elements in our environment such as cars, or even cities themselves; iv) Industry 4.0 and IIoT - Increased automation and connectivity: The emergence of Industry 4.0 has, along with the IoT, allowed elements that were previously analogue and that relied on human intervention to now be digitalised, thus generating data and performing actions in an automated manner thanks to the total connectivity between systems. This is a great advance, but also implies the emergence of new risks that must be managed appropriately and by taking into account the connectivity of all these systems; and v) Machine Learning - Increased decision-making capacity: Greater access to data has, along with greater connectivity, allowed more intelligent and autonomous decisions to be made in information systems through the application of machine learning techniques. But it has also made organisations and individuals more vulnerable if this potential is used against them.

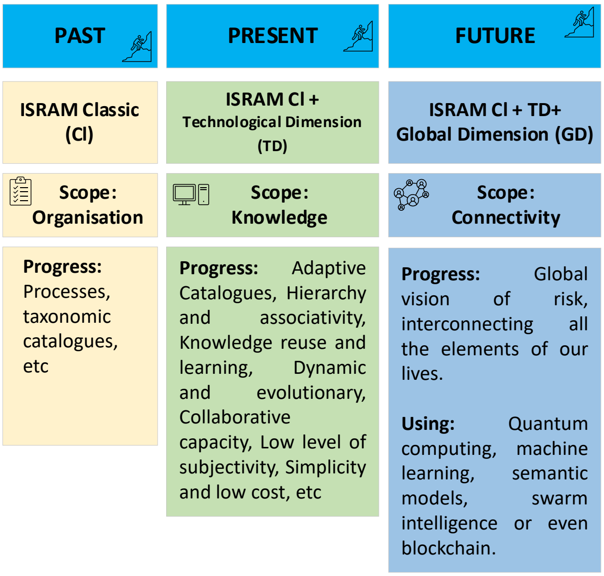
This new environment contains fully decentralised organisations with assets in the cloud, which is shared with many other organisations. Workers turn their homes into an extension of these organisations by teleworking, but these smart homes are simultaneously an information system in themselves. This system is joined by external elements, such as intelligent vehicles, and elements that take health data from our own bodies, such as smart watches.

This paradigm shift from a partly analogue and disconnected world to a fully digitalised and connected one has led to the emergence of unknown risks and vulnerabilities resulting from this delocalisation of information systems, and much of the effectiveness of traditional protection mechanisms has consequently deteriorated (Capodieci et al., 2020).

Risks in information systems have gone from being a problem with a limited scope to something global and much more difficult to control, and which can affect all aspects of our lives. This means that we have eventually moved from one scenario to another. The former comprised "islands of risk", in which risks associated with organisations and elements of our personal lives were compartmentalised and limited in scope. We are now, however, confronted with a scenario of global risk made up of interrelated elements in which we can, for example, use organisational mobiles for private use, or home networks to telework within organisations. This has, therefore, eliminated the borders that previously existed and has made the scope of the risk global.

Confronted with this new scenario, some researchers have already highlighted the need to develop new risk models that are capable of managing the new risks without increasing costs, and that can be adapted to any type of entity regardless of its size and sector (Govender et al., 2021). Other researchers stress the importance of being able to rely on risk systems that are more advanced than the current ones and have a greater capacity to generate knowledge (Affia et al., 2019, Genchev, 2021).

Part of this transformation has already taken place, and we have gone from a first generation of ISRAMs, which could be denominated as the "Classic ISRAMs" focused on procedural improvements, to a second generation focused on knowledge and the introduction of the technological dimension as a complement to the procedural dimension. But this is not sufficient, and a third generation of more advanced ISRAMs is now required. This will have the capacity to analyse risks from a global viewpoint and will enable the use of all the technological advances available to us to create models that are better adapted to the current technological situation (see Figure 1).



PAST	PRESENT	FUTURE
ISRAM Classic (CI)	ISRAM CI + Technological Dimension (TD)	ISRAM CI + TD+ Global Dimension (GD)
Scope: Organisation	Scope: Knowledge	Scope: Connectivity
Progress: Processes, taxonomic catalogues, etc	**Progress:** Adaptive Catalogues, Hierarchy and associativity, Knowledge reuse and learning, Dynamic and evolutionary, Collaborative capacity, Low level of subjectivity, Simplicity and low cost, etc	**Progress:** Global vision of risk, interconnecting all the elements of our lives. **Using:** Quantum computing, machine learning, semantic models, swarm intelligence or even blockchain.

FIGURE 1. Evolutions of ISRAM

This manuscript attempts to show the evolution of ISRAMs by starting from a perspective of their past and showing their previous limitations. However, some of the most relevant and valuable proposals that have led them to their current state by achieving very relevant improvements are also mentioned. We also analyse how recent technological and social developments have led to the need for further improvements in the way in which risks should be managed. These improvements will undoubtedly be achieved, thanks to the advances in information technologies themselves.

PAST

Several methodologies and frameworks were developed during the first generation of ISRAM (e.g. MAGERIT, OCTAVE, CRAMM, etc). Their orientation was more focused on improving the organisational capacity of the company from a formal point of view on the basis of procedures and taxonomic catalogues. This was valid in the environment in which they emerged, where organisations functioned as islands with centralised assets, and little information was exchanged with other organisations. With regard to the employees of these organisations, there was a clear differentiation between their working life and their personal life. In this context, the personal assets of their daily life outside work were completely unrelated to the resources of the job and consisted mainly of analogical elements, which were, therefore, separate islands with a low level of risk from an information systems point of view (see Figure 2).

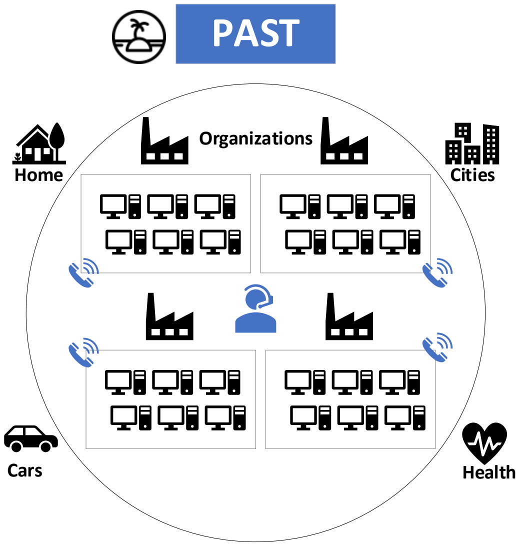


FIGURE 2. Classical society

The dawn of the so-called "Information Age" marked a shift in this paradigm of almost total isolation from information systems as the knowledge age and the Internet began to reach into all aspects of life. In this new context, in which information systems were increasingly interconnected (initially affecting principally the business domain), existing risk models quickly became obsolete. This was owing to the fact that they were not fully adapted and did not take advantage of the full potential offered by emerging technologies.

It was for this reason that, at the beginning of the 21st century, organisations began to believe that classic ISRAMs were insufficient as regards providing solutions to existing problems. These frameworks had significant deficiencies that limited their capacity to provide solutions, of which we can highlight the following: i) They were not capable of adapting to the casuistry of different sectors, as they lacked taxonomic catalogues of specialised controls, assets and threats; ii) They were not able to reuse the knowledge they acquired from different implementations in order to improve their analysis capacity; iii) They were static systems, often built on basic office tools, lacking a dynamic view of risk in a constantly changing world; iv) They were unable to take into account associative and hierarchical risks in a world in which companies were beginning to break down physical barriers, and finally, v) The results of the same risk analysis carried out by two consultants in the same scope were different owing to the level of subjectivity of many of the elements involved in these ISRAMs.

These problems required the development of a new generation of risk analysis that was more appropriate for the new reality.

PRESENT

The need for ISRAMs that were better adapted to the paradigm of the knowledge era led researchers to develop different proposals for risk analysis frameworks that sought to address the existing deficiencies from different points of view, with a common point in all of them: the improvement and reuse of knowledge.

An example of this new generation of ISRAMs, which sought to make systems more efficient by adding a technological dimension to the classic models, was the MARISMA framework.

This framework was developed in a real environment by using the action-research method throughout the research process. This framework was progressively refined and validated in dozens of companies in different countries, under different regulatory regimes, and in different sectors. This methodology can be adapted to any type of IT environment (Parra et al., 2016) and defines a new concept called a meta-pattern, which consists of the main elements of a risk analysis (controls, assets and threats), along with their interdependencies. This new framework allowed the reuse of artefacts and the definition of patterns for specific contexts. Moreover, the support provided by the eMARISMA tool makes the process and decision making agile and simple. MARISMA's adaptability to different contexts is owing principally to the definition of the pattern, e.g. for Big Data (Rosado et al., 2021) and CPS (Rosado et al., 2022). The pattern inherits the elements common to any ISRAM process defined in the meta-pattern, and then completes or adapts them to a specific context.

But the reality is that today's world does not merely concern better knowledge but can be defined as being a fully interconnected and decentralised world. Organisations have taken their assets to the cloud, where they share them with other organisations and citizens, and all elements of their lives are connected (see Figure 3).

The new generation of ISRAMs solved important shortcomings of classical risk analysis by introducing technology as a new dimension. But this was only a first step in the development of a new generation of ISRAMs.

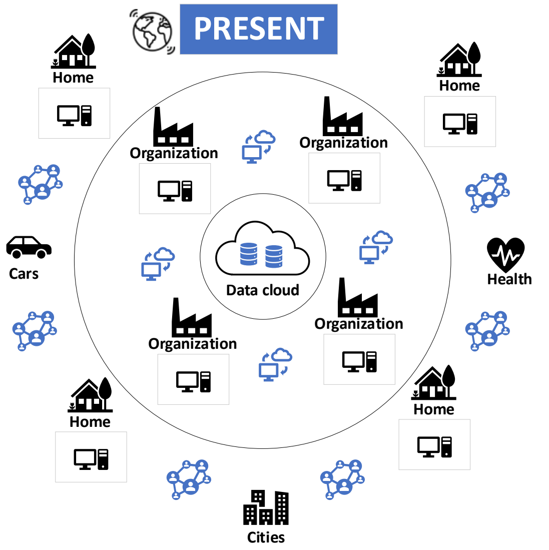


FIGURE 3. The world today

The unstoppable evolution of technology, and the way in which it affects more and more aspects of our lives, makes it necessary to re-advance and evolve existing frameworks. As we are now confronted with more global and connected systems that exchange data at a greater risk and at a greater speed, we need to be able to predict unwanted events earlier. It is here that the speed of computation will be a very important dimension.

FUTURE

This future generation of frameworks, denominated as AURORA (**A**dvanced and **U**nified **R**esearch **O**n**R**isk **A**nalysis of Information Systems), seeks to qualitatively improve the techniques currently used for the risk analysis of information systems, thus making scientific contributions of a different nature to the field of computer science. AURORA frameworks should seek to solve new ISRAM problems by using disruptive technologies.

One of these problems is that current models lack adequate **metadata and ontologies** (Liu et al., 2021). Being able to count on these ontology and taxonomy models is of great importance, because risk management and analysis systems increasingly rely on the use of data sets in order to integrate, train and improve their risk prevention and security decision support mechanisms (Figueira et al., 2020). The standardisation of these datasets through ontologies will allow not only better data quality and correlation, but also the attainment of **key risk indicators (KRIs)**, which do not currently exist (Siegel and Sweeney, 2020).

Another problem resulting from the technological evolution has been the emergence of networks of resources that are shared among organisations, thus creating decentralised networks among them (Mishra et al., 2021). But these networks can be seen as an opportunity for organisations to improve, as each node can collaborate in order to make the prevention of risks in the associated nodes more efficient, thus introducing the concept of **swarm intelligence**.

These new information models and decentralised networks similarly have some drawbacks, as they involve the constant exchange of information that is subject to risks, such as the loss of privacy, the alteration of data, or the dubious origin of the data, etc. (Xiao, 2020). Some of these problems are being addressed through the use of blockchain technologies and the smart contracts associated with them (Zou et al., 2019). However, very few researchers have attempted to bring together the concepts of **smart contracts** and **blockchain** in order to ensure the security dimensions of the data generated in risk management systems and guaranteeing agreements between nodes by means of smart contracts.

Once ISRAMs are able to unify these risk systems, a new objective can be achieved: that of analysing these data using advanced **machine learning** techniques in order to extract useful information with which to assist in the early detection of security risks.

The ability to rely on large heterogeneous information sources extracted from decentralised network nodes has led to a new problem, since the cross-referencing of all this information, even when formalised through the use of ontologies, will have a high algorithmic complexity. Moreover, response time is a critical dimension that must be taken into account during risk prevention. This problem is not easy to solve with current techniques, and a new vision with which to find an adequate solution is, therefore, required. The solution that some researchers are proposing is the use of **quantum computing** technologies (Griffin et al., 2021). Many researchers believe that for cybersecurity to work, this domain of knowledge must evolve, and some have even proposed the development of a quantum blockchain (Abd El-Latif et al., 2021). But the reality is that there are still very few scientific works that attempt to employ this new perspective in order to tackle the problems of high algorithmic complexity associated with risk analysis.

In other words, there are new problems, but also new technologies that provide solutions to these problems. The AURORA vision concerns the development of a new generation of ISRAMs by taking advantage of existing technological advances. Integrating all these elements and focusing them on not only information systems but also all aspects of life will make it possible to attain a more advanced and global concept of risk than exists at present (see Figure 4). This means the evolution from ISRAMs to ISRAM-AELs (All the Elements of our Life) and will give rise to a third generation of ISRAMs whose central point will be connectivity.

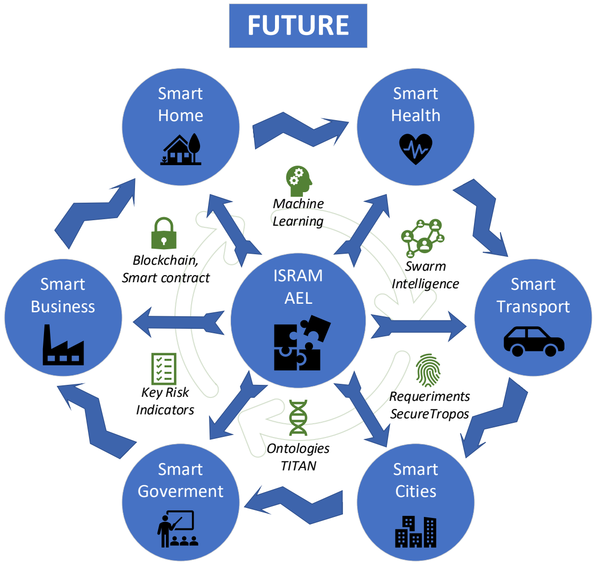


FIGURE 4. ISRAM-AEL

If this evolution is to be achieved, it will be necessary to incorporate all of the above elements on the basis of the second generation of ISRAMs and evolve them towards more complex ontological and taxonomic models with the capacity to support new technological evolutions.

Some of the advances included in the AURORA vision that can be highlighted are, therefore, the following: i) The construction of an ontology for the risk analysis: It is necessary to build an ontology for the context of risk analysis that will formalise and provide the risk analysis process with semantics. It will also characterise a multitude of datasets with large volumes of security data, such as vulnerabilities and exploits. This will help automate risk analysis processes, improve the semantic interpretation of security data that are currently very difficult to interpret, and prepare these data for the application of data analytics and knowledge extraction techniques. It will additionally enrich dashboards with key risk indicators; ii) The application of swarm intelligence in ISRAM: Research should be carried out into the application of swarm intelligence to distributed risk management in enterprises and organisations. There is an obvious connection between the inevitable evolution of the risk levels of these companies or organisations and the occurrence of certain security incidents. It will, therefore, be possible to visualise a global and decentralised risk analysis system as a swarm, in which each individual represents a specific instance of risk management corresponding to a specific entity; iii) The use of Blockchain in ISRAM: It is necessary to support the risk analysis and management process with Blockchain infrastructures, which are proving to be an appropriate solution by which to provide the information stored with immutability, while fully guaranteeing transparency and security. Having these guarantees is a key aspect in a global and distributed risk analysis and management infrastructure, in which decisions are made as regards risk levels and the execution of safeguards, and in which there may even be a propagation of information among different organisations with relevant effects on risk treatment; iv) The use of Machine Learning in ISRAM: It is necessary to research the application of machine learning techniques to datasets with large volumes of cybersecurity information with the aim of extracting valuable knowledge for risk analysis processes. These include the probabilities of the occurrence of attacks, attack patterns, relationships and dependencies among vulnerabilities, assets, attacks, etc; and v) The use of quantum computing in ISRAM: It is necessary to research and propose advances in quantum computing for the construction of algorithms applied to information security management system processes. These are unaffordable with classical computing because they require algorithms of an exponential complexity and are, therefore, unfeasible under certain conditions. They can, however, now be solved in polynomial time thanks to the characteristics of quantum computing.

The use of these disruptive technologies to develop this new generation of frameworks will make it possible to obtain valid risk models for a fully connected and decentralised world.

CONCLUSIONS

The current paradigm shift towards a fully interconnected world poses new challenges for ISRAMs, as risk is now a more globally interrelated concept than ever before, encompassing all aspects of our lives. Addressing these changes requires a new generation of ISRAMs that will utilise the full potential of emerging disruptive technologies.

These objectives are based on scientific and technological challenges that are, certainly in principle, far apart. This will make an integrated contribution to the improvement to various dimensions of risk analysis and the management of information systems in organisations and for individuals, households, etc. Ontologies and metadata will, therefore, contribute by facilitating the formalisation and semantisation required for the application of techniques with which to discover knowledge and carry out research into swarm intelligence. This will, together with the use of Blockchain technologies, contribute to building a global and distributed risk intelligence ecosystem that will be immutable, transparent and secure. Finally, research into quantum algorithms will provide the optimisation of certain risk management processes through the application of this emerging and promising discipline.

The integration of all these technologies into a common framework will generate a new field of research in the world of risk analysis and management. This will not only be applicable to the world of information systems security but can also be extended to all aspects of life and business sectors, thus helping to stabilise and advance them.

ACKNOWLEDGMENTS

This work has been developed within the AETHER-UCLM (PID2020-112540RB-C42) funded by MCIN/AEI/10.13039/501100011033, ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521) funded by the "Ministerio de Ciencia e Innovación", and in co-operation with the following companies: Sicaman NT S.L. and Marisma Shield S.L.

REFERENCES

1. Abd El-Latif AA, Abd-El-Atty B, Mehmood I, Muhammad K, Venegas-Andraca SE, Peng J. Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. Information Processing & Management 2021;58(4):102549.
2. Affia A-AO, Matulevičius R, Nolte A. Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review. Cham: Springer International Publishing; 2019. p. 282-300. 10.1007/978-3-030-33246-4_18.
3. Capodieci A, Mainetti L, Dipietrangelo F. Model-Driven approach to Cyber Risk Analysis in Industry 4.0. Proceedings of the 10th International Conference on Information Systems and Technologies: Association for Computing Machinery; 2020. p. Article 33. 10.1145/3447568.3448541.
4. Figueira PT, Bravo CL, López JLR. Improving information security risk analysis by including threat-occurrence predictive models. Computers & Security 2020;88:101609.
5. Genchev PG. Analysis of changes in the probability of an incident with information security. 2021 56th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)2021. p. 119-22. 10.1109/ICEST52640.2021.9483532.
6. Griffin PR, Boguslavsky M, Huang J, Kauffman RJ, Tan BR. 1 Quantum Computing. Data Science and Innovations for Intelligent Systems: Computational Excellence and Society 50 2021:1.
7. Liu W, Zhu S, Yang K, Qi L, Cong Z. RIShield: An Ontology Security Framework and Key Technologies for Power Industrial Control System. International Conference on Intelligent Automation and Soft Computing: Springer; 2021. p. 285-95.
8. Mishra S, Sagban R, Yakoob A, Gandhi N. Swarm intelligence in anomaly detection systems: an overview. International Journal of Computers and Applications 2021;43(2):109-18.
9. Parra ASO, Crespo LES, Alvarez E, Huerta M, Paton EFM. Methodology for Dynamic Analysis and Risk Management on ISO27001. IEEE Latin America Transactions 2016;14(6):2897-911. 10.1109/TLA.2016.7555273.
10. Rosado DG, Moreno J, Sánchez LE, Santos-Olmo A, Serrano MA, Fernández-Medina E. MARISMA-BiDa pattern: Integrated risk analysis for big data. Computers & Security 2021;102:102155. https://doi.org/10.1016/j.cose.2020.102155.
11. Rosado DG, Santos-Olmo A, Sánchez LE, Serrano MA, Blanco C, Mouratidis H, et al. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. Computers in Industry 2022;142:103715. https://doi.org/10.1016/j.compind.2022.103715.
12. Siegel CA, Sweeney M. Cyber Strategy: Risk-driven Security and Resiliency: CRC Press, 2020.
13. Xiao S. Research on the information security of sharing economy customers based on block chain technology. Information Systems and e-Business Management 2020;18(4):487-96.
14. Zou W, Lo D, Kochhar PS, Le X-BD, Xia X, Feng Y, et al. Smart contract development: Challenges and opportunities. IEEE Transactions on Software Engineering 2019.

LUIS ENRIQUE SÁNCHEZ (Phd) is a lecturer at the University of Castilla-La Mancha, C.Real, Spain, and is the co-founder of the Marisma startup. He is the corresponding author of this paper. Contact him at luise.sanchez@uclm.es

ANTONIO SANTOS-OLMO (Phd) is a lecturer at the University of Castilla-La Mancha, C.Real, Spain, and is the co-founder of the Sicaman startup. Contact him at antonio.santosolmo@uclm.es

HARALAMBOS MOURATIDIS (Phd) is a full professor at the University of Essex, Colchester, UK, and is a director of the IADS Institute. Contact him at h.mouratidis@essex.ac.uk

EDUARDO FERNÁNDEZ-MEDINA (Phd) is a full professor at the University of Castilla-La Mancha, C.Real, Spain, and is a director of the GSYA Research Group. Contact him at eduardo.fdezmedina@uclm.es