Cyber Security for Smart Grid: A Human-Automation Interaction Framework

F. Boroomand, A. Fereidunian, M.A. Zamani, M. Amozegar, H.R. Jamalabadi, H. Nasrollahi, M. Moghimi, H. Lesani, C. Lucas

***Abstract*-- Power grid cyber security is turning into a vital concern, while we are moving from the traditional power grid toward modern Smart Grid (SG). To achieve the smart grid objectives, development of Information Technology (IT) infrastructure and computer based automation is necessary. This development makes the smart grid more prone to the cyber attacks. This paper presents a cyber security strategy for the smart grid based on Human Automation Interaction (HAI) theory and especially Adaptive Autonomy (AA) concept. We scheme an adaptive Level of Automation (LOA) for Supervisory Control and Data Acquisition (SCADA) systems. This level of automation will be adapted to some environmental conditions which are presented in this paper. The paper presents a brief background, methodology (methodology design), implementation and discussions.**

***Index Terms*—smart grid, human automation interaction, adaptive autonomy, cyber security, performance shaping factor**

I. NOMENCLATURE

SG: Smart Grid
IT: Information Technology
HAI: Human Automation Interaction
AA: Adaptive Autonomy
SCADA: Supervisory Control and Data Acquisition
FEP: Firewall Enhancement Protocol
HMI: Human-Machine Interface
EWS: Early Warning System
HCA: Human-Centered Automation
LOA: Level of Automation
PSF: Performance Shaping Factor

F. Boroomand is with ECE Dep., Concordia University, Montreal, QC, CANADA (f.boroomand@ece.ut.ac.ir).

A. Fereidunian is with CIPCE, School of ECE, University College of Engg., University of Tehran, Tehran, IRAN and Power and Water University of Technology (PWUT), Tehran, Iran (fereidunian@iiau.ac.ir & arf@ece.ut.ac.ir).

M.A. Zamani is with CIPCE, School of ECE, University College of Engg., University of Tehran, Tehran, IRAN (maz.zamani@gmail.com & ma.zamani@ece.ut.ac.ir).

M. Amozegar is with CIPCE, School of ECE, University College of Engg., University of Tehran, Tehran, IRAN (mah.amouzegar@gmail.com).

H. R. Jamalabadi is with CIPCE, School of ECE, University College of Engg., University of Tehran, Tehran, IRAN (h.jamalabadi@ece.ut.ac.ir).

H. Nasrollahi is with CIPCE, School of ECE, University College of Engg, University of Tehran, Tehran, IRAN(h.nasrollahi@ece.ut.ac.ir)

M. Moghimi is with CIPCE, School of ECE, University College of Engg, University of Tehran, Tehran, IRAN(mmoghimi@ece.ut.ac.ir)

H. Lesani is with CIPCE, School of ECE, University College of Engg., University of Tehran, Tehran, IRAN (lesani@ut.ac.ir).

C. Lucas was with CIPCE, School of ECE, University College of Engg., University of Tehran, Tehran, IRAN.

IDS: Intrusion Detection Systems

II. INTRODUCTION

TECHNOLOGY has set a day-to-day progress in most industries; however, the power industry has gained less advantage from technology during the last decades [1]. This lack of technology investments resulted in inefficiency of the whole system; On the other hand, the increasing price of the primary fuels draws great attentions to even slight inefficiencies and energy losses.

Smart grid is introduced to apply new technologies to power grid, in order to make it "work far more efficiently" [2]. Computer based automation is one of the core technologies which plays an important role in the smart grid innovations where the SCADA is its neural system. Although this increase in the level of automation is for better service (e.g. reliability), it can be regarded as a threat for the system's cyber-security. Security and reliability are not always aligned; for example increase in the amount of data in the IT infrastructure is consequences some security challenges [3]. Since our modern society is exceedingly dependent on reliable electrical energy, it is essential to ensure the security of the smart grid against any cyber attacks. The cyber security of the SCADA system has been extensively studied in recent years to overcome this problem.

A cyber attack can be decomposed into three steps: first, attacker intends to have control over the SCADA system. Once the control is obtained, the attacker should identify the system to launch an intelligent and effective attack. At the third step, the attacker initiates the control of Firewall Enhancement Protocol (FEP), Application Server, HMI, Early Warning System (EWS), system's database, and even controllers directly [4].

To prevent the attackers from gaining control of the SCADA system, human-automation teams will be more prolific than either human or automation working alone [31]. We present our strategy in the HAI function allocation framework, which was first introduced by P.M. Fitts in 1951. Fitts considered two levels of automation in his primary HAI model: manual or automatic [5]; However, since this primary model was no longer successful in the HAI optimization, Sheridan and Verplank introduced their ten-degree LOA [5]-[10]. Further in 2000, Parasuraman, Sheridan and Wickens suggested the AA concept, which schemes an adaptive level of automation for optimizing the HAI, based on the environmental conditions [6], [8], [9], [11]. Further, Fereidunian et al introduced a model-based framework for the

realization of the AA concept in order to manage the HAI complexity [12]-[17].

The importance of automation in the smart grid, and the fact that the human manual performance cannot completely be replaced by the automation, raise the importance of illustrating Human-Centered Automation (HCA) and the HAI positioning in the smart grid innovations. This paper outlines an adaptive level of automation for the SCADA systems, based on the changing environmental conditions. These environmental conditions affect the system's security and its vulnerability to the cyber attacks.

The reminder of this paper is organized as follows: a brief background on the HAI and AA concepts are presented. Later, a framework is proposed for improving the cyber security based on the AA. Afterward, the concept has been implemented on sample situations, followed by a discussion in the final step. The paper is concluded at the end.

III. BACKGROUND

This section is intended to briefly introduce the main concepts of HAI, LOA, AA, and Performance Shaping Factor (PSF), in order to make this paper self-explanatory. However, to the readers who are less familiar with the concepts, we suggest [6], [10], [13] for further reading.

A. Human Automation Interaction

Interaction between human and automation is something more than being only a matter of using automation [10]. What we considered as human-automation interaction is bound to those who:

a) Determine limits for automation, that is, specify goals and avoidances for the automation.

b) Start or end automatic processes or improve tasks that do the automation.

c) Provide the automation with information, energy, physical objects (requirements) and materials.

B. Level of Automation

As stated, the concept of automation level was first introduced by P.M. Fitts, where two levels of automation were considered (manual or automate) [5]. Further this concept was extended by Sheridan and Verplank. They proposed a ten-degree autonomy level, which has been widely accepted by the researchers. The ten levels of automation proposed by Sheridan and Verplank are listed in Table 1 [6].

It has been approved that level of automation affects the efficiency, situation awareness and mental work load [18]. Inagaki et al suggested a level between six and seven [11], and Fereidunian et al suggested a level between levels zero and one [12], [13].

Table I: SHERIDAN'S TAXONOMY FOR LEVELS OF AUTOMATION

LOA	Description
10	The computer decides everything, acts autonomously, ignoring the human
9	informs the human only if it, the computer, decides to
8	informs the human only if asked, or
7	executes automatically, then necessarily informs the human, and
6	allows the human a restricted time to veto before automatic execution, or
5	executes that suggestion if the human approves, or
4	suggests one alternative
3	narrows the selection down to a few
2	The computer offers a complete set of decision / action alternatives, or
1	The computer offers no assistance: human must take all decisions and actions

C. Performance Shaping Factors

The Environmental conditions which affect the performance of human-automation systems are represented as PSFs. In fact, the LOA can be formulated as a function of PSFs. The weather condition, day-time or night-time and mental work-load are some instances of the PSFs [19]-[23].

D. Why Human-Centered Automation?

In order to optimize the LOA in the human-automation systems, performance of both human and automation in different environmental conditions should be assessed first. In our application, these environmental conditions are those related to the power grid cyber security, either directly or not.

Automation system is the most important prerequisite for achieving the smart grid objectives. Even we can say that automation is almost unavoidable from any industrial point of view; however, this increase in the level of automation must not lead to neglecting human's supervisory control role. Especially, in the instances in which human's tacit knowledge is necessary, this knowledge cannot be presented in terms of rules or data.

Furthermore, there are some reasons that reduce our reliance on the automation systems: First, there could be contingencies which have not been seen in the automation system design. In this research, these contingencies are referred to the automation system intrusiveness by the hackers. Second, the immaturity in the automated systems broadens vulnerabilities to the potential cyber attackers. This will result in situations, in which the human's tacit knowledge can be helpful.

IV. METHOD

A. Problem Statement

In this paper, the problem is to adapt the LOA of the smart grid to the changing environmental conditions, or mathematically:

$$LOA = f(\mathrm{PSF}) \qquad (1)$$

$$\mathrm{PSF} = (PSF_1, PSF_2, \dots, PSF_n) \qquad (2)$$

This paper differs to that of [15]-[17], in terms of its objective function: the objective in this paper is to mitigate the cyber security risks for the HAI (the smart grid); whereas, the aim in [15]-[17] is to optimize the performance/cost rate of the HAI system.

Until recently, the most common concept, regarding power grid cyber security, was isolating the SCADA network from

all other networks, preventing attackers from penetrating the network [24], [25]. However, increasing demands for connecting the consumers and producers, accompanied by the spreading IT infrastructure over the smart grid and increase in the number of automated operations made the physical isolation almost impossible [25]. As a consequence, cyber security of the smart grid has drawn great attentions in recent years. This paper presents its cyber security strategy in an HAI framework.

We customized a framework, presented by Fereidunian *et al* [13], [14], for the realization of the adaptive autonomy concept to improve the cyber security of the smart grid. The framework proposed a subjective approach, known as expert judgments, which assesses the human and automation systems' performances based on superior experts' judgments [13], [14].

B. Solution Methodology

Interactions between the two complex systems (human and automation system) emerge to a high level of complexity which prevent us from employing the objective (i.e. model based) approaches. Instead, we adopt a subjective approach to the proposed problem which employs the experts' judgments, whose superiority has been confirmed due to their involvement in the human-automation (SCADA) systems. After extracting the human experts' judgments, we utilize them for determining the appropriate LOAs, according to the changes in the environmental conditions, referred to as the PSFs. Figure 1 shows the proposed methodology for the realization of the presented concept, that has conceptually been taken from [13].

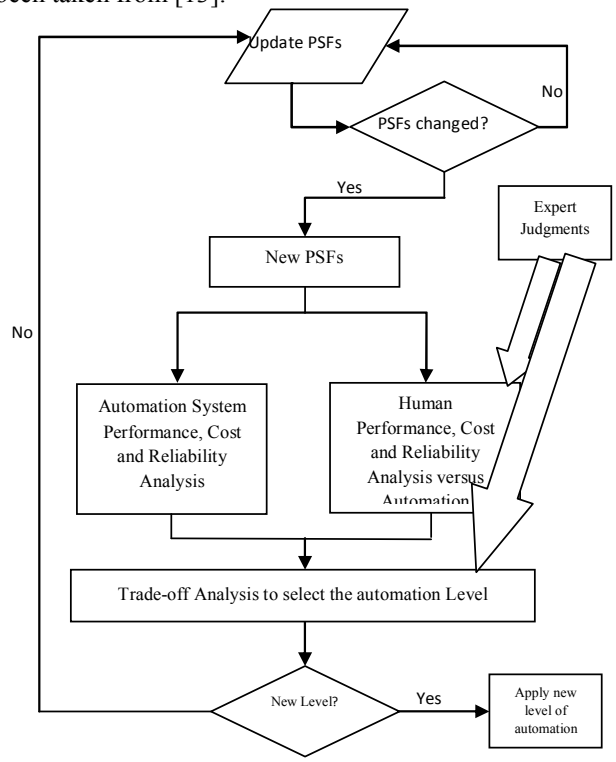


Figure 1: The proposed Methodology for Adaptive Autonomy Implementation [13]

C. Cyber Security Performance Shaping Factors

We classify the environmental conditions affecting the cyber security of the smart grid into the following three categories:

1) Environmental conditions which describe the power grid vulnerability at the time of the cyber attack:

PSF1: Number of weak points in the *power grid*

In August 2003, a generating plant went offline at the time of high electrical demand in Eastlake, Ohio. The imbalances between supply and demand resulted in chain reactions, which finally led to the second widespread electrical blackout in the history [26], [27]. Although it was not initiated with a cyber attack, but such a weak-point could be an ideal chance for a potential attacker.

The increase in the number of weak-points escalates the power grid vulnerability. Therefore, it broadens our potential attacker's choices; thus, one should be conservative in increasing the LOA in the grids with considerable number of weak points.

PSF 2: Power Grid Complexity

Power grid complexity is another parameter that affects its vulnerability. Complexity introduces new vulnerabilities and increasing exposures to potential attackers [28]. As a consequence, the attacker could find vulnerabilities that could hardly be understood. This will result in absolutely defenseless attacks which are very dangerous for the power grid security.

2) Environmental conditions which describe the ease of intrusion to the SCADA system

PSF 3: Number of Entry Points

Involvement of the smart grid with innovations has made the physical isolation of the SCADA system almost impossible. Even if we try to isolate the SCADA system, there always is a possibility of having a connection, through a phone line or an intranet, to the SCADA system, which is connected to a power plant [29]. Moreover, in online monitoring of demand—which is one of the smart grid objectives— it is essential to establish connections between the consumers and the SCADA system. This will increase the number of entry points in a great pace. The potential attacker could exploit any of these connections in order to access the SCADA network, and consequently gain control over the power grid.

PSF 4: Data flow in the *IT infrastructure*

Intrusion Detection Systems (IDS) and Firewalls are responsible for monitoring data flow into the SCADA system. However, if the amount of data flowing into the SCADA increases, it will be easier for an attacker to intrude the system with just a simple Virus, Trojan, Worm, and etc [30]. Increase in the data flow of the IT infrastructure increases system's reliability while decreases its security [3].

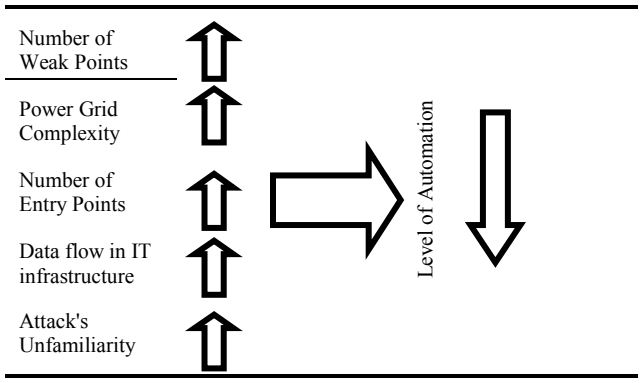
3) Environmental conditions which describe the ease of gaining control over the SCADA system

PSF 5: Anomalies vs. Signatures

When the defense system fails and an attacker intrudes to the SCADA system, the question will be the matter of what we should do to minimize and mitigate destructions caused by this attack. The destruction mitigation strategy differs if the

detected attack is an anomalies or a signature. If the detected attack is a signature (i.e. attack looks like prior ones), there will be no need to decrease the LOA considerably, because we know how to treat the threat. On the other hand, if the detected attack is an anomaly (i.e. attacks that we never seen before), it is recommended to decrease the LOA until more investigations, because we have no experience of such sort of events.

Table II: THE RELATION BETWEEN PSFs AND LOA



V. IMPLEMENTATION

Our implementation is based on the experts' judgments to determine the appropriate LOA for the SCADA system in different environmental conditions. For this purpose, first we define a PSF vector which describes the conditions of the SCADA system from cyber-security point of view.

A. The PSF Vector

We define a vector, entitled as a PSF vector, to represent the environmental conditions. This vector contains five elements; each of them describes one of the previously discussed PSFs. In the following, we describe each of these arrays:

1) PSF element for the number of weak points in the power grid (PSF_1): We define three different conditions for this PSF: few (represented by 0), more (represented by 1), and much more (represented by 2).

2) PSF element for the power grid complexity (PSF_2): Like the previous one, three conditions are considered for this PSF: little complexity, more complexity, and much more complexity. The element for this PSF is defined similar to that of the PSF_1.

3) PSF array for the number of entry points (PSF_3): Like the two previous PSF vectors, we define three states for this PSF. 0 for few entry points, 1 for more entry points, and much more entry points which will be presented by 2.

4) PSF element for the data flow in the IT infrastructure (PSF_4): Exactly like the previous ones this array is defined by three states. 0 describes little flow of data, while 1 depicts higher flow of data, and 2 stands for much higher data flow in the IT infrastructure.

5) PSF sub-vector for the anomalies and signatures (PSF_5): This sub-vector contains just an element, in which 0 stands for the signatures and 1 is for the anomalies.

Representing all of these sub-vectors in a vector as follows will result in our PSF vector which describes the SCADA system's condition from the cyber-security point of view.

$$PSF= [PSF_1, PSF_2, PSF_3, PSF_4, PSF_5] \quad (3)$$

B. Scenario Development and Results

In this research, only simple conditions are studied, this simplicity facilitates the human experts' judgments and, as a consequence, the result will be more reliable. Further studying simple conditions is the best way to explore the effects of each PSF on our human-automation system. For this reason six scenarios are developed, and asked from experts in interviews. Superior experts' judgments are employed to evaluate the appropriate LOA for each of these scenarios.

Scenario 1— Happy condition, PSF= [0, 0, 0, 0, 0]: In this condition there are few weak points in the power grid. Further, its complexity is low and it is possible to determine the grid's vulnerabilities. Moreover, the numbers of entry points are few and the flow of data in the IT infrastructure is low. In addition to these conditions there is no attack detected. As a consequence, this condition is the perfect candidate to have maximum LOA from the cyber security point of view.

Scenario 2— Vulnerable condition, PSF= [2, 0, 0, 0, 0]: In this condition all of the PSFs are in their normal state except PSF_1. This situation describes a vulnerable power grid with no deficiency other than this vulnerability; in our strategy believing that the increase in the number of weak points should be accompanied by a decrease in the LOA. Table 2 illustrates the relation between number of weak-points and the LOA.

Scenario 3— Complex condition, PSF= [0, 2, 0, 0, 0]: In this condition we are facing a complex power grid. This complexity concurs with non-identified vulnerabilities. Our strategy is to reduce the LOA while the complexity of the power grid increases. Table 2 shows the relation between power grid complexity and the level of automation.

Scenario 4— Accessible condition, PSF= [0, 0, 2, 0, 0]: In this condition we are facing a SCADA network which is accessible through many connections like internet connections, telephone lines, and etc. In order to increase the smart grid's cyber security, we suggest the reduction of the LOA, once the number of the entry points increases. Table 2 shows this relationship.

Scenario 5— Pervious condition, PSF= [0, 0, 0, 2, 0]: Once the data flow in the IT infrastructure is more than usual, it is easy for our potential attacker to intrude the SCADA system with just a simple Virus, Trojan, Worm, and etc [30]. In order to overcome this problem, our strategy is to reduce the LOA by increasing the data flow in the SCADA system. This relation has been demonstrated in Table2.

Scenario 6— Unexpected condition, PSF= [0, 0, 0, 0, 1]: In this condition, the IDS detects a cyber attack, even if there exists the possibility that the attacker has been intruded to the SCADA system. If we are facing a never seen attack (which means an anomaly), our strategy is to reduce the LOA for more investigations. Table 2 reports the relation between this PSF and the level of automation.

VI. DISCUSSIONS

This paper schemes an adaptive level of automation for improving the smart grid's cyber security. For this purpose, five PSFs were considered, and their effects on the LOAs were discussed from the cyber security point of view. Here we rank these PSFs, and determine which one has more influence on the appropriate LOA.

A typical attack can be decomposed into three steps: access, discovery, and control [4]. We classify our PSFs into three categories; these categories are related to the steps of a cyber attack. In the first step our potential attacker is going to intrude our system; so PSF_3 and PSF_4 are directly associated with this step. In the second step the attacker should discover the system. If the potential attackers have a candidate for their attacks (this should be a weak point) they should discover the system in order to realize how they can gain control over that point. PSF_1 and PSF_2 are directly involved in this step. At the final step the attackers should gain control of the candidate point where PSF_5 is generally related to this step.

When the attackers proceed through these three steps, it means failure in some defense strategies. This will result in the increase in the level of defenselessness; as a consequence the level of danger will increase.

We suppose that our PSFs could be ranked, based on the level of danger for these three steps. Figure 2 shows our PSF ranking for this research.

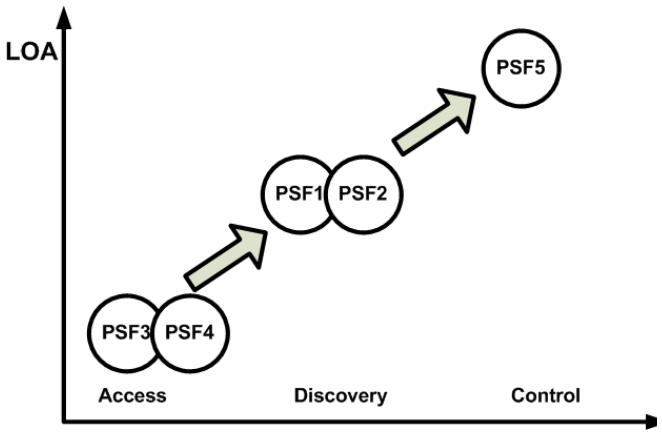


Figure 2: PSFs ranking

VII. CONCLUSIONS

This paper introduced a novel framework for the smart grid cyber security based on the human-automation interaction theory. Five different environmental conditions are presented as the system PSFs. Further, it studied that how these PSFs affect the cyber security of the smart grid. Afterward, the impacts of these PSFs on the level of automation were discussed (LOA decreaser or LOA increaser). Finally, these PSFs were ranked, based on their effect on the level of automation.

This research will continue with exploring the LOA in different environmental conditions, based on superior experts' judgments. This research group is working on introducing expert systems as a subjective approach for the determination of appropriate LOAs from the cyber security point of view.

VIII. REFERENCES

[1] C. Feisst ,D. Schlesinger, W. Frye, "Smart Grid: The Role of Electricity Infrastructure in Reducing Greenhouse Gas Emissions," Cisco Internet Business Solutions Group, October 2008

[2] The SMART GRID: an introduction, U.S. Department of Energy by Litos Strategic Communication under contract No.

[3] ABB Bulletin, "The Smart Grid Reliability Bulletin, from ABB". [Online]. Available: http://www.poweranswercenter.com/9

[4] Power Infrastructure Security: Fundamental Insights of Potential Cyber Attacks and Their Impacts on the Power Grid

[5] P. M. Fitts, "Some basic questions in designing an air-navigation and air-traffic control system", In *N. Moray* (Ed.), Ergonomics major writings (Vol. 4, pp. 367–383). London: Taylor & Francis., Reprinted from Human engineering for an effective air navigation and traffic control system, National Research Council, pp. 5–11, 1951.

[6] R. Parasuraman, T.B. Sheridan, and C.D. Wickens, "A model for types and levels of human interaction with automation," *IEEE kjfdgkrdjg Trans. On SMC– Part A*, Vol. 30, No.3, May 2000, pp. 286-297.

[7] R. Parasuraman, C.D. Wickens " Humans: Still Vital After All These Years of Automation", *Human Factors*, Vol. 50, No. 3, 511-520 (2008)

[8] M.R. Endsley, D. B. Kaber, "Level of automation affects on performance, situation awareness and workload in dynamic control task", *Ergonomics*, Vol. 42, No. 3, 1999, pp. 462-492

[9] D.B., Kaber, M. Endsley, "The effects of level of automation and adaptive automation on human performance, situation awareness and workload in a dynamic control task", Theoretical Issues in Ergonomics Science,Vol.5, 2004, pp. 113-153.

[10] T.B. Sheridan, and R. Parasunaman, "Human–Automation Interaction", in R.S. Nickerson's Review of Human Factors and Ergonomics, HFES Publications, 2006.

[11] T.Inagaki, , "Adaptive automation: Sharing and trading of control. In E. Hollnagel (Ed.), Handbook of cognitive task design. Mahwah, NJ: Erlbaum, 2003, pp. 46-89.

[12] A.Fereidunian, C.Lucas, H.Lesani, M. Lehtonen, M.M. Nordman, "Challenges in Implementation of the Human-Automation Interaction Models" Proceeding of 15th IEEE-MED'07 Conference, June 2007, Athens, Greece, pp 1-6

[13] A.Fereidunian, M. Lehtonen, H.Lesani, C.Lucas, M.M.Nordman" Adaptive Autonomy: Smart Cooperative Systems and Cybernetics for More Human Automation Solutions" *Proceeding of IEEE-SMC'07 Conference*, October 2007, Montreal, Canada, pp 202-207

[14] A.Fereidunian, H.Lesani, C.Lucas, M. Lehtonen, "A Framework for Implementation of Adaptive Autonomy for Intelligent Electronic Devices." *J. Applied Sci*. 2008, 8:3721-3726

[15] A. Fereidunian, M.A. Zamani, H.Lesani, C.Lucas, M. Lehtonen, "An Expert System Realization of Adaptive Autonomy in Electric Utility Management Automation" *J. Applied Sci*. 2009, No. 8, pp.1524-1530.

[16] A.Fereidunian, M.A.Zamani, H.Lesani, C.Lucas, M. Lehtonen, "AAFES: An Intelligent Fuzzy Expert System for Realization of Adaptive Autonomy Concept in Utility Management Automation" In *Proc. of IEEE-ISDA'09*, Pisa, Italy, 30 Nov.-2 Dec. 2009.

[17] A.Fereidunian, M.A.Zamani, F.boroomand, H.R. Jamalabadi, H.Lesani, C.Lucas, "AALRES: An Intelligent Expert System for Realization of Adaptive Autonomy Using Logistic Regression" To Appear in *Proc. of IEEE-MELECON 2010*, 28-30 April, 2010.

[18] M.R. Endsley and D.B. Kaber, "Level of automation affects on performance, situation awareness and workload in dynamic control task," *Ergonomics*, Vol. 42, No. 3, pp. 462-492, 1999

[19] J. Holmberg, K. Hukkib, L. Norros, U. Pulkkinen, P. Pyy, "An integrated approach to human reliability analysis – decision analytic dynamic reliability

model," *Reliability Engineering and System Safety*, Vol. 65, 1999, pp. 239–250.
[20] U. Pulkkinen, , "Programmable automation systems in PSA," *STUK YTOTR 127 Technical Report*, June 1996.
[21] T. Rosqvist," On the use of expert judgment in the qualification of risk assessment," Doctoral Dissertation, Helsinki University of Technology, VTT Publication 507, 2003.
[22] A.G. Sutcliffe and A. Gregoriades, "Automating scenario analysis of human and system reliability," *IEEE Trans. on SMC–A*, Vol. 37, No. 2, , pp. 249-261, 2007.
[23] Y.H.J. Chang, and A., Mosleh, "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents," *Reliability Engineering & System Safety*, Vol. 92, 2007, pp. 997-1013
[24] Carlson Rolf. "Sandia SCADA program – high-security SCADA LDRD final report," Sandia National Laboratories report, SAND2002-0729; April 2002.
[25] V. M. Igure, S. A. Laughter, R. D. Williams, "Security issues in SCADA networks", *Computers and Security*, Vol. 25, pp. 498-506 2006
[26] T. Albert, P. Palensky, T. Sauter, " SECURITY CONSIDERATIONS FOR ENERGY AUTOMATION NETWORKS", In *the proceeding of Fieldbus Systems and Their Applications Puebla*, Mexico, 2005, pp. 158-165
[27] "Interim Report on the August 14, 2003 Blackout", New York Independent System Operator. 2004-01-08. http://www.hks.harvard.edu/hepg/Papers/NYISO.blackout.report.8.Jan.04.pdf. Retrieved 2008-09-16
[28] National Institute of Standards and Technology, "Smart Grid Cyber Security Strategy and Requirements", September 2009,
[29] V. M. Igure, S. A. Laughter, R. D. Williams "Security issues in SCADA networks", *Computers and Security*, Vol. 25, pp. 498-506, 2006
[30] k. Tomsovic, D.Bakken, V. Venkatasubramanian, A. Bose "Designing the Next Generation of Real-Time Control, Communication, and Computations for Large Power Systems," *Proceedings of the IEEE,* Vol. 93**,** No.5, pp. 965-979, pp. 393 - 396, 2005.
[31] D.W. Corcoran, J.L. Dennett, A. Carpenter, "Cooperation of listener and computer in a recognition task: II effects of computer reliability and ''dependent'' versus ''independent'' conditions," *Journal of the Acoustical Society of America*, Vol. 52, pp. 1613–1619, 1972.

BIOGRAPHIES

Farzam Boroomand is a graduate student at Concordia University, Montreal, QC, Canada. He received his B.Sc. from School of Electrical and Computer Engineering, University of Tehran. His research interests include control systems, artificial intelligence, fault detection and diagnosis, power distribution system automation, decision-making, neural networks, fuzzy control, and human-automation interaction.

Alireza Fereidunian received his PhD and MSc from University of Tehran (CIPCE, School of ECE), in 2009 and 1997, where he is a Research Associate now. Dr. Fereidunian is a faculty member at the Power and Water University of Technology (PWUT), Tehran, Iran and serves as an independent consultant to GTEDC. His research interests include power systems automation, and application of intelligent systems, human-automation interaction, data mining, decision-support, decision-making, IT and signal processing in power systems. He is a member of IEEE (and IEEE Iran Section) and INCOSE (as INCOSE Iran point of contact).

Mohammd Ali Zamani is a Research Assistant at the Center of Excellence for Control and Intelligent Processing (CIPCE), School of Electrical and Computer Engineering, University of Tehran, Iran. He received his B.Sc. from School of Electrical and Computer Engineering, University of Tehran, Iran. His research interests include System Engineering, Artificial Intelligence, Smart Grid, and Adaptive Autonomy. He is currently working on implementation of system engineering approaches in smart grid.

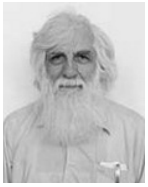
Mahdiyeh Amozegar is a B.Sc. Student at the Center of Excellence for Control and Intelligent Processing (CIPCE), School of Electrical and Computer Engineering, University of Tehran. Her major research interests include VLSI, integrated circuits, fuzzy electronics. She also works on artificial intelligence and cybernetics as her minor.

Hamid-Reza Jamalabadi is a graduate student at Amirkabir University of Technology, Tehran, Iran. He received his B.Sc. from School of Electrical and Computer Engineering, University of Tehran. His research interests include control systems, flight control, artificial intelligence, power distribution system automation, decision-making, neural networks, fuzzy logic, and human-automation interaction.

Hossein Nasrollahi is a B.Sc. Student at the Center of Excellence for Control and Intelligent Processing (CIPCE), School of Electrical and Computer Engineering, University of Tehran. His research interests include control systems, optimal control, robust control, power distribution system automation, and human-automation interaction.

Mojtaba Moghimi is a B.Sc. Student at the Center of Excellence for Control and Intelligent Processing (CIPCE), School of Electrical and Computer Engineering, University of Tehran. His research interests include control systems, optimal control, robust control, power distribution system automation, smart grid and human-automation interaction.

Hamid Lesani is a Professor at the Center of Excellence for Control and Intelligent Processing (CIPCE), School of Electrical and Computer Engineering, University of Tehran. He received the M.S. degree in electrical power engineering from the University of Tehran, Iran, in 1975, and the Ph.D. degree in electrical engineering from the University of Dundee, U.K., in 1987. Early in his career, he served as a Faculty Member with Mazandaran University. After obtaining the Ph.D. degree, he joined the Department of Electrical and Computer Engineering, Faulty of Engineering, University of Tehran. His teaching and research interests are design and modeling of electrical machines and power systems. Professor Lesani is a member of IEEE (PES) and IEEE Iran Section.



Caro Lucas was a Professor and a member (as well as the Founder- Director) of Center of Excellence for Control and Intelligent Processing (CIPCE), School of Electrical and Computer Engineering, University of Tehran, as well as a Researcher at the School of Cognitive Sciences (SCS), Institute for Studies in Theoretical Physics and Mathematics (IPM). His research interests included uncertain systems, intelligent control, multi-agent systems, data mining, business intelligence, financial modeling, biological computing, computational intelligence, neural networks, and knowledge management. He was the founder of the ISRF, IPM and has assisted in founding several new research organizations and engineering disciplines in Iran. He was the holder of the patent for Speaker Independent Farsi Isolated Word Neurorecognizer. Dr. Lucas has served as Chairman of the IEEE, Iran Section (1990-1992) and as the Chairman of several international conferences. Professor Lucas has been nominated as a member of Long-lasting Figures of Science and Culture Hall of Fame by the Iranian Academy of Engineering in 2006.
Regretfully, the late Professor Caro Lucas passed away on July 8, 2010.