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

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

Proc. IEEE Conference on Innovative Smart Grid Technologies Europe, Geothenburg, October 2010.

Presenter: Fred A. Ituzaro

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

- Introduction
- Literature Review
- Problem Formulation
- Solution Methodology
- Implementation
- Personal Assessment
- Suggested Future Work
- Conclusion

TEXAS A&M UNIVERSITY

Introduction

- Advancement in computer hardware and software has made possible automating human-machine systems
- Automation has the purpose to let machines do what formerly humans did equally or less effective.
- Computer based automation will play a critical role in smart grid innovations with SCADA as its neural system
- Question is what level of automation must be allowed in the smart grid?

Attack Process on the SCADA

- Typical attack on a SCADA system follow 3 main process
  - Access
    - Corporate to SCADA communication or external VPN
  - Discovery
    - Understanding of system mechanism
  - Control
    - FEP, Application server, HMI, Database systems

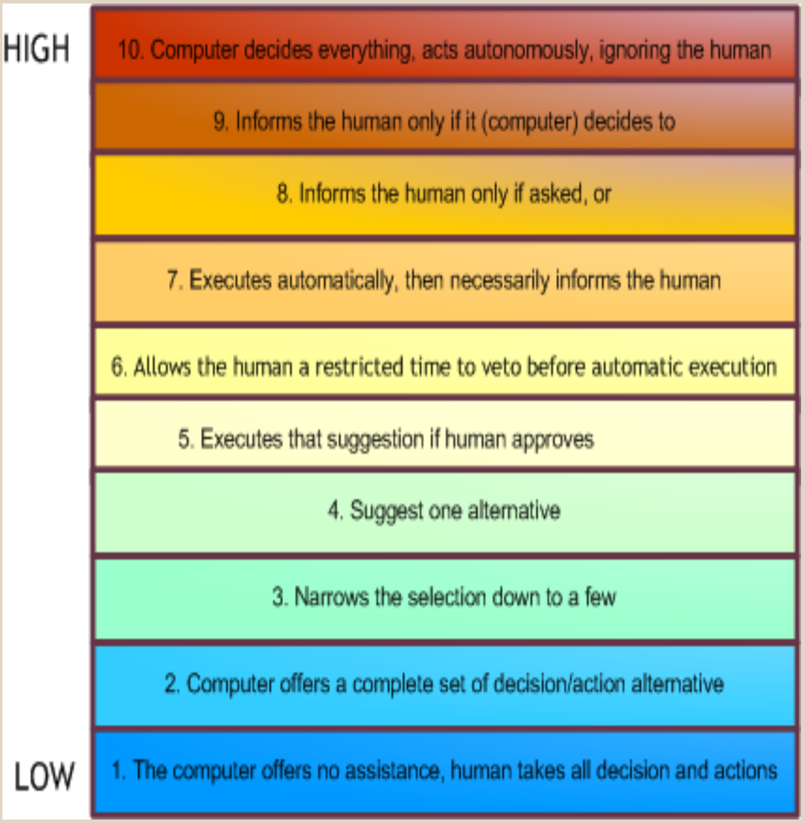
Human-Automation

- Full or partial replacement of a function previously carried out by a human operator [1]
- Automation can be applied across four classes [2]

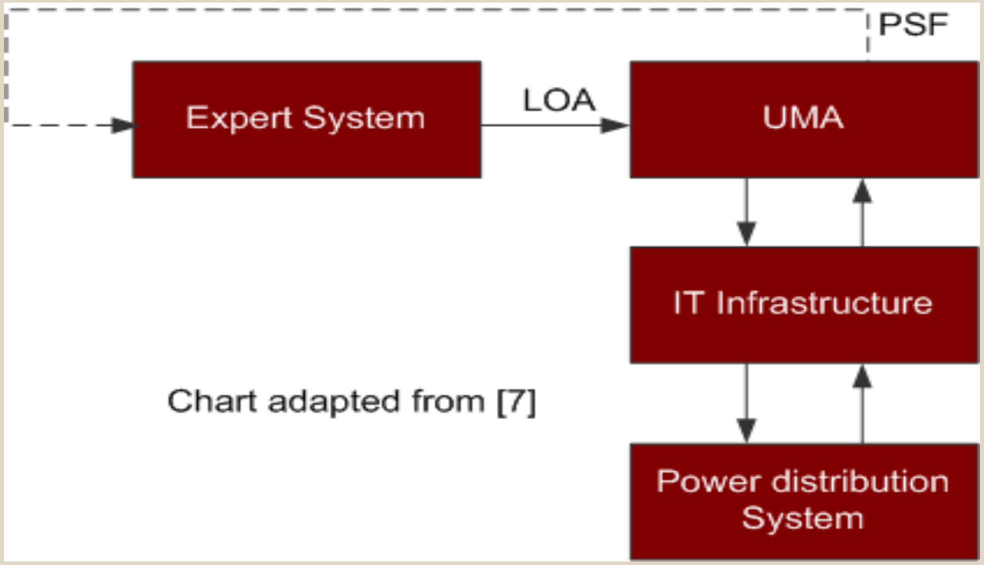
Literature Review

- P. M. Fitts – Proposed a fixed all or none automation philosophy [3]

- Sheridan & Verplant suggested automation can vary across a continuum of levels [4]



Adaptive Automation



- Adaptive automation has being proposed for used in utility management automation (UMA) as a core innovation for smart grid implementation [5-7]
- Changing the LOA in response to the PSF is what is called Adaptive Automation

Problem Formulation

- Level of automation LOA is formulated as a function of performance shaping factors PSF

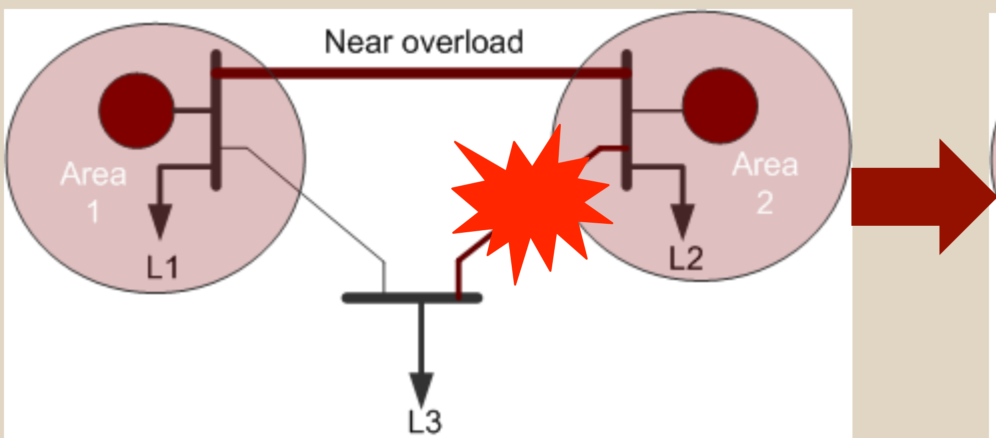
$$LOA = f(PSF)$$
$$PSF = [PSF_1, PSF_2, \ldots, PSF_n]$$

Performance Shaping Factors

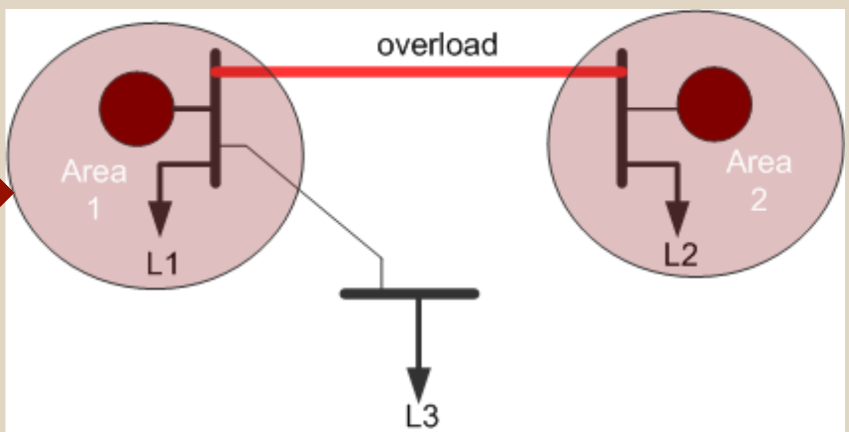
- PSF- Environmental conditions that affect performance of human-automation systems

Performance Shaping Factors

- Conditions describing power grid vulnerability at the time of attack
  - Number of weak points in the grid PSF1
  - Complexity of the power grid PSF2



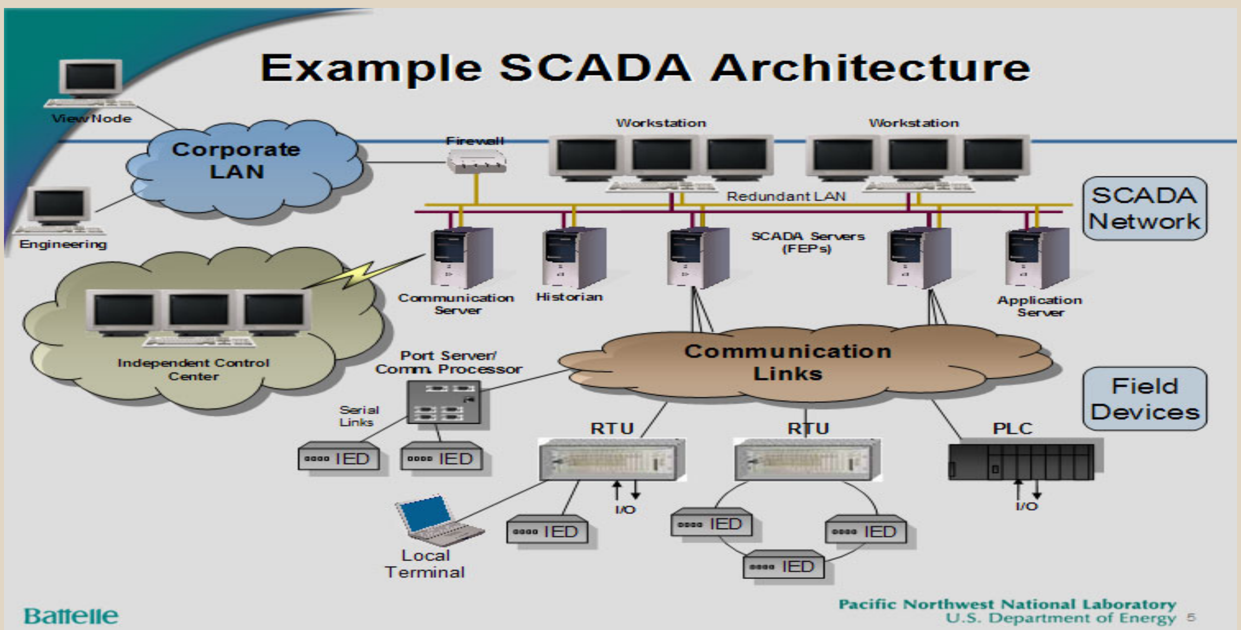
System with two transmission weak points



System condition when one weak point is attacked

PSF Cont'd

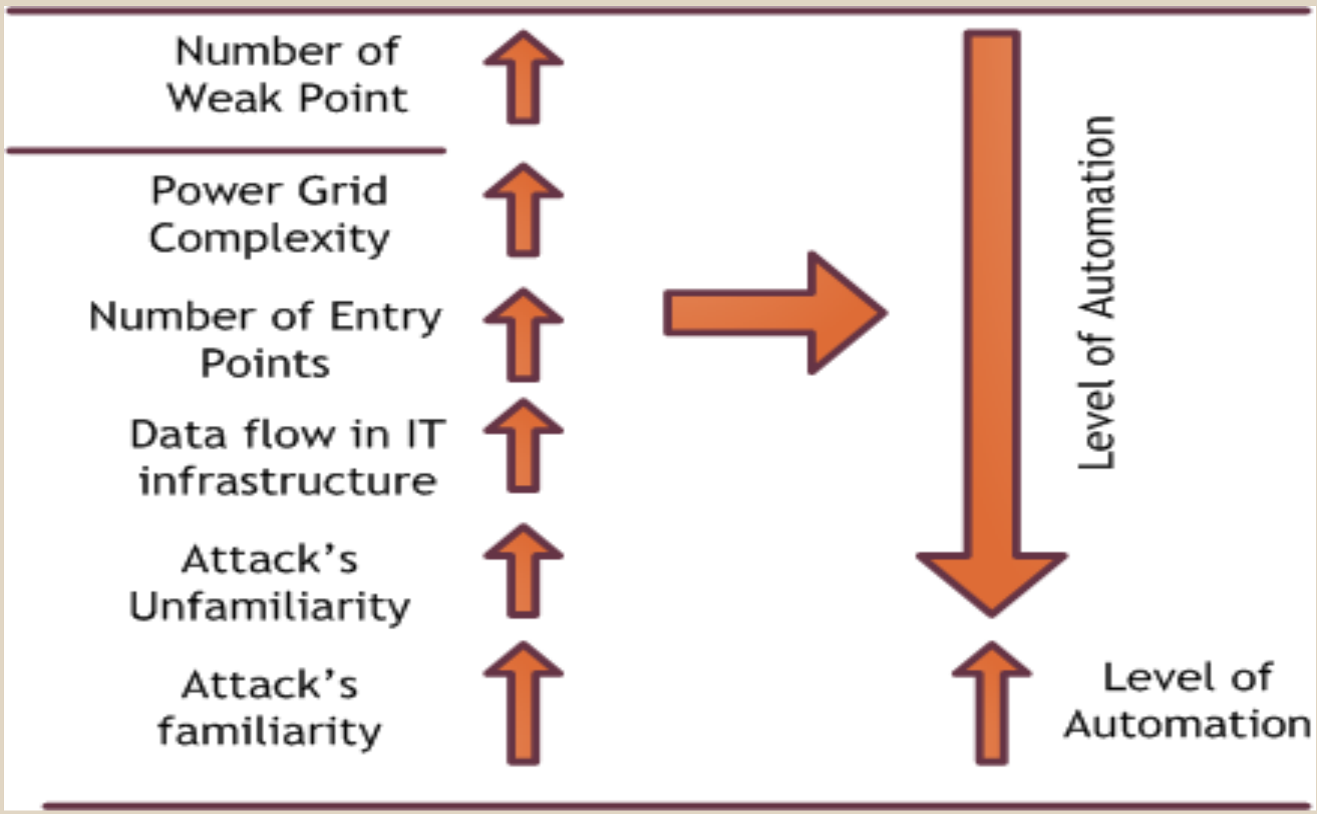
- Conditions describing ease of intrusions to the SCADA systems
  - Number of Entry Points PSF3
  - Data flow in the IT infrastructure PSF4



PSF Cont'd

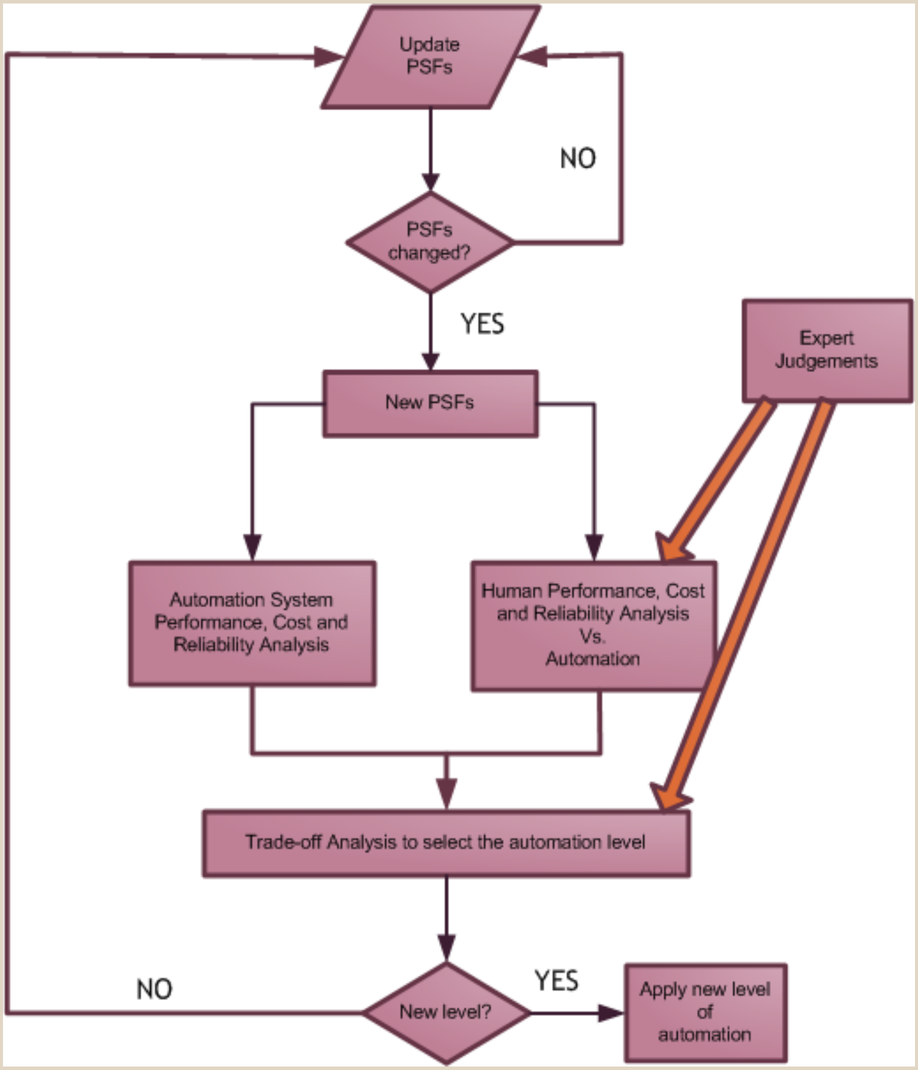
- Conditions describing ease of gaining control over the SCADA system
  - Anomalies vs. Signature PSF5

Relation Between PSFs and LOA



Solution Methodology

- Subjective approach based on experts judgments.



Implementation

- A PSF vector representing all the five possible PSF is defined

$$PSF = [PSF_1, PSF_2, PSF_3, PSF_4, PSF_5]$$

- PSF1 - Number of weak points

$$PSF_1 = \begin{Bmatrix} 0, few \\ 1, more \\ 2, much\ more \end{Bmatrix}$$

- PSF2 – Power grid Complexity

$$PSF_2 = \begin{Bmatrix} 0, little \\ 1, more \\ 2, much\ more \end{Bmatrix}$$

Implementation

- PSF3 – Number of entry Points

$$PSF_3 = \begin{cases} 0, few\,entry \\ 1, more\,entry \\ 2, much\,more \end{cases}$$

- PSF4 – Data flow in IT network

$$PSF_4 = \begin{cases} 0, little\,flow \\ 1, higher\,flow \\ 2, much\,higher \end{cases}$$

- PSF5 – Anomalies or Signature

$$PSF_5 = \begin{cases} 0, signature \\ 1, anomalies \end{cases}$$

Scenario Development

- Scenario 1 – Happy Condition

$$PSF = [0,0,0,0,0]$$

- Scenario 2 – Vulnerable Condition

$$PSF = [2,0,0,0,0]$$

- Scenario 3 – Complex Condition

$$PSF = [0,2,0,0,0]$$

Scenario Cont'd

- Scenario 4 – Accessible Condition

$$PSF = [0,0,2,0,0]$$

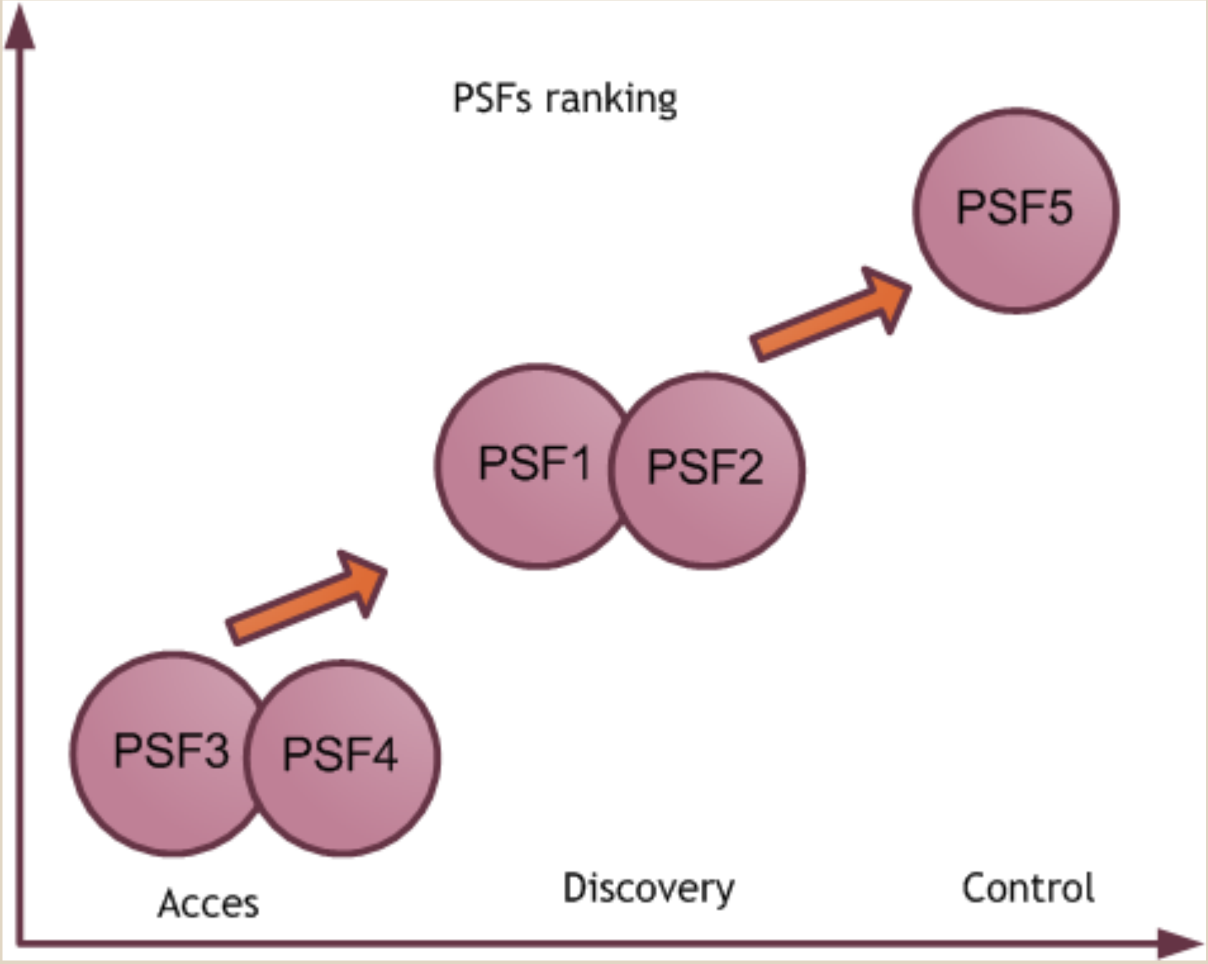
- Scenario 5 – Pervious Condition

$$PSF = [0,0,0,2,0]$$

- Scenario 6 – Unexpected Condition

$$PSF = [0,0,0,0,1]$$

PSFs Ranking



Critical Assessment

- Paper in my view forms the basis for further investigation of adaptive autonomy and its implication in smart grids
- The proper selection of the right experts is of significant importance to the approach as it affects the validity of the whole HAI.
- The author fails to present an approach that quantify what is more or less for a particular PSF. A framework for such quantification could be investigated in future works
- The relation between the PSFs and LOA was established by intuitive and has no quantitative approach.
- Simple scenarios are considered in this research and a prove of concept will be need for more complex situations such as PSF=[2 0 1 0 0]

Suggested Future Work

- Integrating the presented PSF into the four known states of the power system is something worth looking at.
- How does one measure "human in the loop"-ness and estimate its desired level?. A more objective approach from human reliability assessment in reliability engineering can provide some insights
- If subjective approach is to be followed, it will be appropriate to consider LOAs from the cyber security point of view as acknowledged by the author

Conclusion

- An approach for human-automation framework for a SCADA system based on adaptive automation using expert judgments has been presented
- The paper outlines 5 environmental conditions and their impact on cyber security of the smart grid
- The environment conditions are ranked based on their effect on the LOA

Reference

[1] R. Parasuraman and V. A. Riley, "Humans and automation: Use, misuse, disuse, abuse," *Human Factors, vol. 39, pp. 230–253.*

[2] Parasuraman, R.; Sheridan, T.B.; Wickens, C.D.; , "A model for types and levels of human interaction with automation ," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* , vol.30, no. 3, pp.286-297, May 2000

[3] 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.

[4] T.B. Sheridan and W. L. Verplank, " Human and Computer Control of undersea teleoperators, " MIT Man-Machine Systems Laboratory, Cambridge, MA., Tech., Rep., 1978.

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

[6] A.Fereidunian, H.Lesani, C.Lucas, M. Lehtonen, " A Framework for Implementation of adaptive autonomy for intelligent electronic devices" Journal of Applied Sci, No. 8 pp. 3721-3726, 2008

[7] Fereidunian, A.; Zamani, M.A.; Boroomand, F.; Jamalabadi, H.R.; Lesani, H.; Lucas, C.; Shariat-Torbaghan, S.; Meydani, M.; , "AAHES: A hybrid expert system realization of Adaptive Autonomy for smart grid," *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES* , vol., no., pp. 1-7, 11-13 Oct. 2010

Thank You!