III. Conclusion

The ever increasing use of devices that are able to provide some kind of digital information regarding any aspect of our daily lives, such as sensors, has been the promoter of the development of new devices that are able to use this information in order to make our lives easier. Nowadays, with the boom of Internet of Things, controllers and such devices have been having a huge success, because of the facilities they provide to integrate so many different equipment into a single network where any user can have a quick overlook of the state of the network, facilitating the interaction with the information they provide and the interacting equipment. Also, it is necessary to consider that these controllers can be used in so many different environments (home applications, building application and industrial applications), so it can be said that they result so useful and purposeful. Hopefully, this investigation and development field will continue to excel in design and connectivity, so they can fulfill their role in the development of new technologies.

References

[1] A. Rezai, P. Keshavarzi, and Z. Moravej, "Advance hybrid key management architecture for SCADA network security," Secur. Commun. Networks, vol. 9, no. 17, 2016.

[2] K. Sayed and H. A. Gabbar, Scada and smart energy grid control automation. 2016.

[3] S. Misbahuddin, "Fault tolerant remote terminal units (RTUs) in SCADA systems," in 2010 International Symposium on Collaborative Technologies and Systems, CTS 2010, 2010.

[4] A. Rezai, P. Keshavarzi, and Z. Moravej, "Key Management Issue in SCADA Networks: A review," Eng. Sci. Technol. an Int. J., vol. 20, no. August, pp. 354–363, 2016.

[5] M. Caciotta, F. Leccese, G. S. Spagnolo, and L. Cozzella, "Automatic industrial electrical circuit firing prevention using infrared termography," in 20th IMEKO TC4 Symposium on Measurements of Electrical Quantities: Research on Electrical and Electronic Measurement for the Economic Upturn, Together with 18th TC4 International Workshop on ADC and DCA Modeling and Testing, IWADC 2014, 2014.

[6] D. Choi, H. Kim, D. Won, and S. Kim, "Advanced key-management architecture for secure SCADA communications," IEEE Trans. Power Deliv., vol. 24, no. 3, 2009.

[7] V. Mihic, B. Atlagic, and T. Maruna, "GAUS: An integrated SCADA/DCS control system," in Proceedings of the International Conference on Systems Science, 2001, vol. 3.

[8] C. Alcaraz, G. Fernandez, and F. Carvajal, Security aspects of SCADA and DCS environments, vol. 7130. 2012.

[9] S. Karnouskos and A. W. Colombo, "Architecting the next generation of service-based SCADA/DCS system of systems," in IECON Proceedings (Industrial Electronics Conference), 2011.

[10] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA Trans., vol. 46, no. 4, 2007.

[11] DeNoia, Lynn A. Data Communication: Fundamentals and Applications. Merrill Publishing Company, Columbus, Ohio, USA: 1987.

[12] L. Raman, Fundamentals of telecommunications network management. Wiley-IEEE Press, 1999.

[13] A. Rezai, P. Keshavarzi, and Z. Moravej, "Key management issue in SCADA networks: A review," Eng. Sci. Technol. an Int. J., vol. 20, no. 1, pp. 354–363, 2017.

[14] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," Comput. Commun., vol. 30, no. 7, 2007.

[15] LXGroup. Mango – the world's most popular open – source M2M platform, 2014 [Online]. Aviable: https://lx-group.com.au/mango-worlds-popular-open-source-m2m-platform/

[16] Tridium. Harness the power of the Internet of Things with Niagara, 2016. [Online]. Aviable: https://www.tridium.com/

[17] DGLogik. About DGLogik, Inc. | IoT Technology Company, 2016. [Online]. Aviable: http://www.dglogik.com/company/