Smart Work-Assisting Gear

Chirag Mahaveer Parmar, *Member, IEEE,* Projjal Gupta, *Member, IEEE,*
K Shashank Bharadwaj, *Member, IEEE,* Swaroop Sudhanva Belur, *Member, IEEE*
Next Tech Lab (IoT Division)
SRM University, Kattankulathur

***Abstract*—This paper describes the use of IoT hardware and protocols to build a smart device which assists factory workers and other employees. This gear is a wearable glove device which can be used in various work spaces where power tools are being constantly used. This proposed system is built around a micro-processor acting as the central server, while many sensors are interfaced with microcontrollers, which act as the link for data transmission and perform various tasks. One of the microcontrollers acts as the master, which controls the other microcontrollers attached to various sensors. The master contains an LCD screen and few buttons, which can control the menu being shown on the screen. This can control the other sensors, and read the data in real time. The gloves contain safety features so that the workers are unable to use any dangerous power tools without wearing proper equipment. The glove will act as a security measure in such a way that each tool will have restricted access, according to the level of expertise of the worker. The glove can also restrict the access to the tools which are being used actively during a particular time-frame. The entire data is actively logged by the central server and various other sensors such as heat sensor, temperature sensor and vibration sensors can be attached and monitored by the master glove. The system also has an extra capability of analyzing tone of the workers so that whenever the user gets hurt and shouts in pain, the analysis function can classify the pain and call for medical help accordingly. A simple sweep based camera module is used alongside the central server to record and live-stream the captured video whenever any power tool is switched On. This system proliferates the value of safety of a worker in a factory floor.**

***Keywords*—Internet of Things, Industry 4.0, MQTT, Node, Wireless Communications, Factory.**

I. Introduction

With the start of industrial revolution, power tools became a very important part of the factory floor. Everyday, millions of people go to work and operate potentially life threatening machines[1] . According to publicly available statistics, more than a hundred thousand people are injured in power tool related accidents every year[3]. This results in a huge loss of precious work-force and other resources[2].

The idea of Connected Machines is an appealing one and it can be applied to the large as well as small scale machinery to improve the efficiency and thus, the productivity in factories. It is believed that both the aforementioned ideas can go hand in hand and that we can create a solution that would help with the safety in factories and improve efficiency that would be provided by the Internet-of-Things.

II. Problem Statement

Multiple hardware solutions exist to protect and incraease the level of safety in any power tool or machinery. A set of safety and hazard rules are placed in workspsace to limit such issues. But the current technology only aims at securing the machines and devices, but does not factor-in on human errors which is one of the major issues in this case. The tools are not access-locked and any user, irrespective of skillset, can use them. If proper protective measures are not taken seriously, they can lead to serious injuries.

The proposed solution is an IoT based system that implements a wearable that connects to any type of machinery and permits access based on whether proper safety equipment has been worn. We will use sensors on these equipment and send this data to a Raspberry Pi. On the Raspberry Pi, we will check if the machine, for which access is being requested for, is free to be used and if all the proper gear is being used by the person requesting access and based on this information, the Raspberry Pi will control a relay that will power the machine.

III. MQTT

MQTT or Message Queue Telemetry Transport is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based ”lightweight” messaging protocol for use on top of the TCP/IP protocol[7]. It is designed for connections with remote locations where a ”small code footprint” is required or the network bandwidth is limited. The publish-subscribe messaging pattern requires a message broker[10]. The broker is responsible for distributing messages to interested clients based on the topic of a message.

MQTT is a highly secure IoT protocol which is being used to implement the smart device. This requires a ”Broker” or a centralized server to act as a communication link between all the connected devices in the system. The Raspberry Pi is a micro-processor which can run as a broker. MQTT has a very small footprint due to which the data packet sizes are smaller and the transmission of data takes lower time than other IoT protocols and consumes much less power during operations. While HTTP on a gigabit network requires approximately 5,100ms per request[6], MQTT’s average publish-subscribe latency is 120ms per loopback request[8]. However, it is dependent on the availability of Wifi or plugged internet, due to which it has a low range, and can only be used in a local

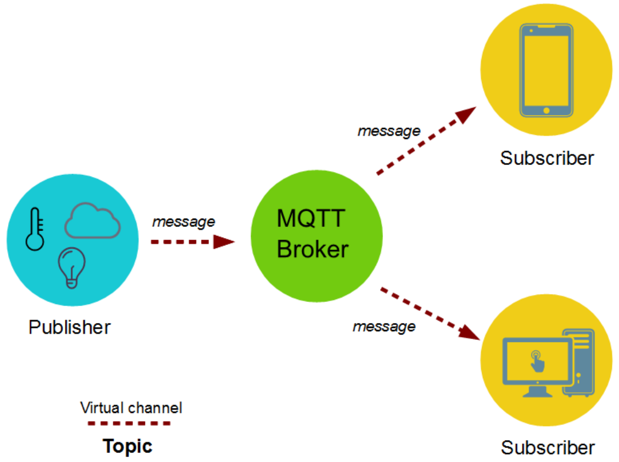

Fig. 1. MQTT broker-client working

network in one isolated institution. This kind of backdrop is actually more favourable in this very scenario where the operations of the power tools are not going to be shared outside of the work space.

It has several modes of usage. It uses the PUBLISH function to send data to one of the channels and uses the SUBSCRIBE function to listen to the channel and receive the transmitted data. It consumes less power and as it is being used in QoS 2 mode, the data received is highly secure and not damaged in any possible way. QoS 2 mode increases the overall time of operations, but increases the safety of the system. Due to the small size of the data, the overall increase in time is very low and the quality of the system is not hampered. MQTT is one of the most secure and useful protocols, which enhances the quality and the simplicity of the system[9,10].

IV. Method

The wearable can be included in any type of protective gear. A screen on the wearable and physical buttons allows the worker to select which machine he wants to work with. This data and the data from sensors on the protective gear allows the Raspberry Pi to make decisions. A self-built capacitive sensor placed on the gear allows us to monitor if it is worn or not. The wearable is provided on one piece of protective gear. Any additional pieces of protective gear required to be worn for a specific machine will have just the capacitive sensor. This data is analyzed by a microcontroller which acts as an MQTT Client. The client then sends this information to the server on the Raspberry Pi which is an MQTT Broker.

Simultaneously, all the machines in the factory also have various sensors including temperature, pressure, humidity etc, which will also regularly send data to the broker. This data can be used by the company for analysis and can be used by the company to improve the efficiency of its factory-floor. Depending on the availability of the required machines, the broker publishes this information to the wearable. If all the required conditions are met, the broker authorizes the microcontroller inside the machine to turn on the device.

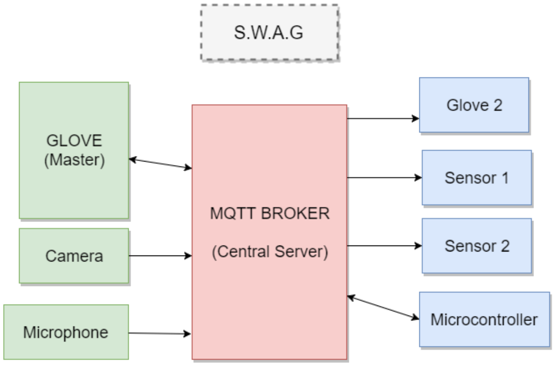

Fig. 2. Block diagram for SWAG

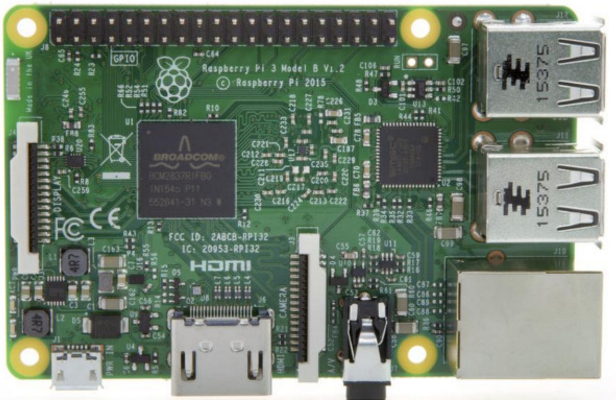

Fig. 3. A Raspberry Pi 3 model B

This way, the system ensures that the person working with the machine has the proper equipment on. Additionally, the machines have RFID readers placed in them. We will use these and RFID stickers to ensure that no tool is running while unattended. This is an extra dimension of security that will ensure safety in the workplace.

V. Hardware Resources and Features

A. *Raspberry Pi 3*

Raspberry Pi is a credit card sized microprocessor, which is based on ARM7 architecture. It has a BroadCOM SOC and can perform tasks which basic microcontrollers cannot perform due to speed or storage issues.The 3rd generation of Raspberry Pi supports in-built Bluetooth and WiFi chip, and doesn't require extra hardware. The wifi connects all the components of this system in a Local Area Network or LAN.

The Pi hosts the MQTT broker at all times, and the IP address of the RPi is used as the central host address. It

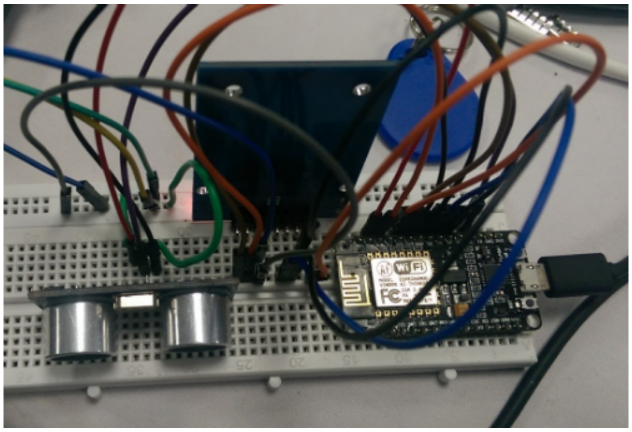

Fig. 4. The NodeMCU with the ultrasonic sensor and RFID scanner

also connects a servo motor via its GPIO pins and a Pi-Cam Module, to record video on every user trigger.

B. ESP 8266-01

ESP8266 is a low powered microcontroller developed by Espressif System, which specializes in building low power communication devices such as the Bluetooth and WiFi chipsets. It is a very low powered device, which has an in-built wifi chip, which is beneficial to get connected to the LAN. The 01 version of this microcontroller has only 2 usable GPIO pins on board and it can be used to create standalone sensor-transmitter pairs.

The ESP-8266 requires a 3.3v input and has a low current draw, due to which it can be deployed easily and can work for a long time at a stretch. The Low number of GPIO can be interfaced with a shift register to accommodate more number of sensors. This setup is very cost-friendly and its implementation decrease the overall power consumption.

C. NodeMCU

NodeMCU is microcontroller Unit based on the 12E version of the Esp-8266. It has an extended number of GPIO pins and features an on-board digital-analog converter (DAC) so that it can read analog sensor values. Unlike the 01 version of the ESP board, the NodeMCU can run at a higher processing frequency, and support multiple modules and sensor integration. In S.W.A.G, each microcontroller unit is connected to the broker, but it is also connected to multiple sensors and switches that can control the system [Fig 2.].

VI. Innovation and Related Work

The system brings Connected Machines to a whole new level. Safety at the work-place is the topmost priority for any company. Using the power of Internet of Things and the standard protocol MQTT, a product is developed, that not only ensures safety of personnel working with large machines, but also the machines themselves. This aims to bring innovation to the everyday lives of people.

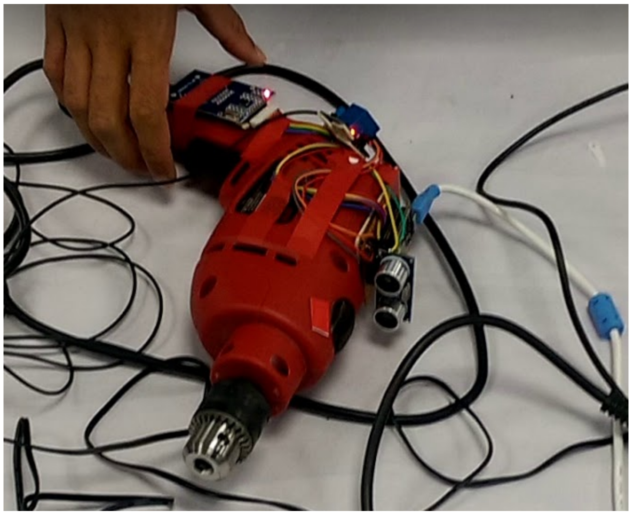

Fig. 5. The drill

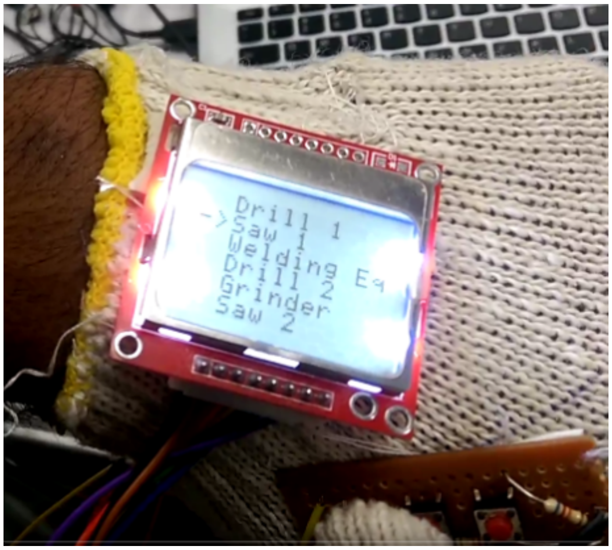

Fig. 6. The smart watch with various machine options to choose from

There is a huge demand for safety products and good ones at that. The manufacturing industry faces a large number of accidents and fatalities every year[3]. This is a revolutionary product for the manufacturing industry. This product is aimed to cut down accidents due to improper protective gear.

VII. Emotional Analysis using Machine Learning

Another dimension of safety is provided by looking for markers indicating that the user is injured or in pain. For this, the system captures sounds in the surrounding using a microphone connected to the existing raspberry pi. The sounds are captured every 5 seconds to reduce the load on the raspberry pi. This sound is then send to a Google speech-to-text service using a simple API call. The API returns the text of the words spoken in the surroundings.

This sentiment of this text is then acquired using another API. This is the IBM Watson API called the Tone Analyzer which returns various sentiments like happiness, sadness, anger etc. and a score associated with each one of them. This is then finally used by our own logistic regression machine learning algorithm to determine if the factory worker is in pain and requires some kind of immediate assistance[13].

Lastly, if the algorithm predicts that the worker is in pain, the system calls an ambulance and informs a predefined user(meant to be the factory floor manager) and this person is meant to rush to the assistance of the injured worker. This is done through the Twilio API.

VIII. Existing Technologies

There have been a fewf attempts at building devices for factory workers like the Australian SmartCap, which measures brain activity to detect fatigue. AIG, meanwhile, reportedly invested in Human Condition Safety(HCS), a company which makes wearable devices that monitor the workers in a factory. However, there has been no significant product that directly monitors the physical safety of the factory floor workers by checking if proper safety equipment has been donned.

IX. Enhanced Security

Since MQTT is a TCP based protocol, by default, it does not utilize an encrypted communication. To add a layer of security, we can use TLS(Transport Layer Security). TLS and SSL provide an encrypted communication channel between client and the broker[16]. Both being cryptographic protocols which use a handshake mechanism to negotiate various parameters, they set up a communication channel and no attacker can eavesdrop any part of the communication. Servers provide a X509 certificate, typically issued by a trusted authority, which clients use to identify the server. Port 8883 is a special port just for secure MQTT connections.

This security comes at a price, however. Clients and brokers must have hardware capabilities for the extra processing. This is especially difficult for the client, since they are normally small, low powered microcontrollers[17].

X. Conclusion

There is a large market for a product like this. Companies are looking for ways to ensure a greater sense of security at their factories. A safe, cheap alternate is exactly what they are looking for. However, the manufacturing industry is not the only place of use for Smart Work-Assisting Gear. Anyone who uses any type of power tool that requires protective gear to be worn can use this product.Thus, this product is aimed at large industries as well as the everyday consumer. Being fairly simple to use and cost-effective, it is ensured that its adoption rate is high.

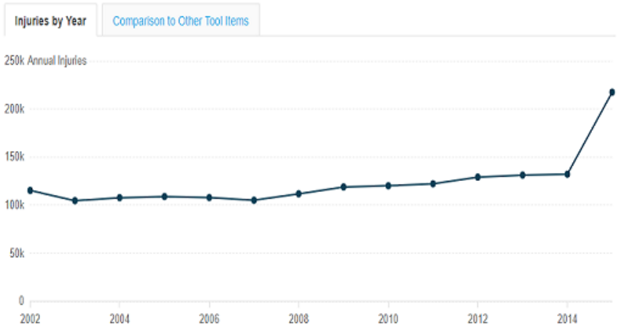

Fig. 7. The number of deaths recently due to machine related accidents

Smart Work-Assisting Gear is an innovative product that will definitely revolutionize safety at the workplace. By using technologies like the Internet of Things, data analytics and RFID, we have ensured that the product will improve the standard of the factory-floor.

Appendix A
Injury and Cost Estimation

Each year, it is estimated that a whopping 124,000 accidents related to power tools take place and it has been noted that the maximum injuries take place for adults of age between 35-44 years[3]. Since the year 2002, the number of power tools related injuries have increased by nearly double, and it has surged by at least 84% during the year 2014-15.[3,4] S.W.A.G aims to control this number by reducing the human error and reducing the chances of accidents. It is claimed that with the rise of industry 4.0, more amount of people will be working with power tools due to increase in consumer markets and a population boom. Implementation of a successful anti-injury system in a work eco-system can certainly decrease the overall injuries and save companies millions of dollars on employee insurance.

This number directly points towards a huge market of power tools that is in circulation today. It is predicted that, by 2020, the Power tools market will be at 34 Billion Dollars globally[15]. This prediction just goes to show how the costs related to injuries will drastically increase. This is a huge drawback for power tool industries and factory work spaces.

Acknowledgment

The authors would like to thank Next Tech Lab for its continued support and the Consumer Product Safety Commission for providing datasets, which was an integral part of the viability study.

References

[1] CPSC : 16 CFR Chapter 2

[2] Hazard Screening Report, 2003 Author : Natalie Marcy, George Rutherford & Alberta Mills .

[3] Consumer Product Safety Commision. Power tools Injury Report: http://product-injuries.healthgrove.com/l/126/Power-Tools” [Oct. 29, 2017].

[4] NEISS Search Query Tool

[5] U.S. Consumer Product Safety Commission [Docket No. CPSC-2011-0074]

[6] Analysis of HTTP Performance problems, [Online]. Available: https://www.w3.org/Protocols/HTTP-NG/http-prob.html. [Accessed: 22-Sep-2017].

[7] ”Transmission Control Protocol,” J. Postel, RFC-793, September 1981.

[8] Measuring Publish-Subscribe latency of MQTT, IOTIFY. [Online]. Available: https://iotify.help/network/latency/mqtt.html. [Accessed: 09-Sep-2017].

[9] Tomasz Szydlo, Piotr Nawrocki, Robert Brzoza-Woch, Krzysztof Zielinski, Advances in Intelligent Systems and Computing, vol. 461, pp. 279, 2017, ISSN 2194-5357, ISBN 978-3-319-44352-2.

[10] Brunno Vanelli, Mariana Rodrigues, Madalena Pereira da Silva, Alex Pinto, M. A. R. Dantas, Communications in Computer and Information Science, vol. 702, pp. 117, 2017, ISSN 1865-0929, ISBN 978-3-319-61402-1.

[11] Walaa Medhat, Ahmed Hassan, Hoda Korashy, Sentiment analysis algorithms and applications: A survey, In Ain Shams Engineering Journal, Volume 5, Issue 4, 2014, Pages 1093-1113, ISSN 2090-4479, https://doi.org/10.1016/j.asej.2014.04.011.

[12] The Fingerprints of Pain in Human Voice. (2017). [E-Book] Isreal: Yaniv Oshrat, The Open University of Israel. Available at [Shortened]: https://goo.gl/HAvVMC [Accessed 22 Nov. 2017].

[13] Acoustical Analysis of Pain Cries in Neonates: Fundamental Frequency. (2017). [ebook] Pune, Maharashtra, India: Raina P. Daga and Anagha M. Panditrao. Available at [Shortened]: https://goo.gl/5tD9vR [Accessed 22 Nov. 2017].

[14] Hand and Power Tools Safety [PDF]. Dallas, Texas: Environmental Health and Safety Department, 2012. Available at [Shortened]: https://goo.gl/9oTNGv [Accessed 22 Nov. 2017].

[15] TechNavio Reports, ”Global Power Tools Market 2016-2020”, August, 2016. Available at [Shortened]: https://goo.gl/8XjsjN [Accessed 11 Dec. 2017].

[16] ”MQTT Security Fundamentals: TLS / SSL”, HiveMQ, 2017. [Online]. Available: https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl. [Accessed: 15- Dec- 2017].

[17] W. Wong, ”Secure That Microcontroller”, Electronic Design, 2017. [Online]. Available: http://www.electronicdesign.com/boards/secure-microcontroller. [Accessed: 15- Dec- 2017].