SAIOH news

As part of our service to members, in this newsletter we provide feedback on the latest developments within the Southern African Institute for Occupational Hygiene (SAIOH). SAIOH exists for its members and is reliant on them to continue to serve this noble profession ethically. Therefore, we invite your inputs and feedback on any matters communicated below.

THE 'INTERNET OF THINGS' DEVICE CYBER VULNERABILITIES: ADDRESSING THE RISKS AND ENHANCING SECURITY IN OCCUPATIONAL HYGIENE

Naadiya Mundy: SAIOH President
e-mail: president@saioh.co.za

Naadiya Mundy
Photograph: courtesy of SAIOH

In the context of industrial hygiene management, the convergence of 'hygiene' and 'the internet of things' (IoT) presents both challenges and opportunities. Occupational hygiene focuses on identifying, evaluating, and controlling workplace hazards to protect the health and wellbeing of workers. IoT, on the other hand, involves the interconnection of devices and sensors, enabling data collection, analysis, and automation in various industries. Thus, the integration of IoT devices in occupational hygiene has revolutionised workplace safety and health monitoring.

In the realm of occupational hygiene, the integration of interconnected devices offers real-time data, empowering improved risk assessment and proactive safety measures for workers' protection. Nonetheless, the swift adoption of IoT in occupational hygiene also creates cyber vulnerabilities, posing risks to the confidentiality of sensitive health data and potentially compromising worker safety. Therefore, understanding the IoT device cyber vulnerabilities specific to occupational hygiene, and devising strategies to bolster security, become imperative to ensure the wellbeing of workers and safeguard their data.[2]

In simple terms, the IoT, in the context of occupational hygiene, begins with data-gathering sensors and monitors. The most common and useful of these, for occupational hygiene professionals, are mobile, wearable devices, which enable real-time monitoring of workers, even from remote locations. These devices are on the forefront of 'on the worker, on the job' technology that ushers in the 'sensing era' – a new era of information technology where the digital and physical worlds converge.

Gas detection is an exemplary application of this technology, where smartphone apps and sensors work together to warn workers about exposures to toxic substances, including otherwise undetectable gases. The potential applications of the IoT in occupational hygiene are vast and diverse, revolutionising safety practices by supplying real-time data for better risk assessment and proactive measures to protect workers' wellbeing. However, with the advantages of the IoT come inherent risks, particularly in terms of cyber vulnerabilities.

These potential vulnerabilities include:

1. Weak authentication and access controls: IoT devices may have weak authentication mechanisms or default credentials, making them susceptible to unauthorised access by cyber attackers.[1,2]
2. Lack of firmware and software updates: many IoT devices lack regular firmware and software updates to address known vulnerabilities, leaving them exposed to potential exploits.
3. Insecure communication: inadequate encryption or unsecured communication channels between IoT devices and central systems can expose sensitive health data to interception.
4. Data privacy and confidentiality: the collection of real-time health data raises concerns about data privacy and confidentiality. Improper data handling or storage can lead to unauthorised access or data breaches. As IoT devices collect and send sensitive health data, including exposure levels to hazardous substances and worker health parameters, ensuring the privacy and protection of this information is paramount to keeping the trust of workers and complying with data protection regulations.
5. Insider threats: malicious insiders or employees with access to IoT devices may exploit vulnerabilities or compromise sensitive data intentionally.
6. Lack of cybersecurity awareness: workers and personnel responsible for operating IoT devices may have limited cybersecurity awareness, leading to poor security practices and potential weaknesses.[2]
7. Interconnected networks: IoT devices may be connected to the organisation's network, creating potential pathways for attackers to gain access to critical systems.
8. Resource constraints: small and medium-sized organisations may lack the necessary resources and abilities to implement robust cybersecurity measures for IoT devices.

Enhancing IoT device security in occupational hygiene:

1. Implementing secure communication protocols, such as encrypted data transmission and strong authentication, ensures that data collected from IoT devices remain confidential and are accessible only by authorised personnel.
2. Device manufacturers and employers should ensure that IoT devices receive regular security updates and patches to address vulnerabilities and remain resilient against emerging cyber threats.
3. Adopting a multi-layered security approach with firewalls, intrusion detection systems, and secure authentication mechanisms strengthens the overall security of the IoT infrastructure.
4. Employing physical security measures, such as access controls, to prevent unauthorised physical access to IoT devices ensures that tampering attempts are minimised or detected promptly.
5. Organisations should conduct thorough audits to assess and find potential vulnerabilities.

In summary, the adoption of IoT devices in occupational hygiene offers significant benefits in enhancing workplace safety and health. However, it is essential to recognise and address the potential cyber vulnerabilities that these devices introduce. By implementing robust security measures, regular updates, and proactive risk management

strategies, employers can mitigate the risks associated with IoT device cyber vulnerabilities in occupational hygiene. Safeguarding the integrity and confidentiality of data collected by IoT devices ensures that occupational hygiene efforts continue to drive improved worker safety and wellbeing.

REFERENCES

1. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023; 12(6):1333. doi: 10.3390/electronics12061333.
2. Mupila FK, Gupta H, Bhardwaj A. An empirical study on cyber-crimes and cybersecurity awareness. Research Square; 2023 (preprint). doi: 10.21203/rs.3.rs-3037289/v1.

NATIONAL COUNCIL FEEDBACK

Naadiya Mundy: SAIOH President
e-mail: president@saioh.co.za
Deon Jansen van Vuuren: SAIOH General Manager
e-mail: deon.jvvuuren@gmail.com

Strategic plan and objectives

The targets within SAIOH's continuously evolving five-year strategy are consistently being met by our diligent management board. A signed-off strategy plan will be circulated to all our members and launched at the annual general meeting (AGM) in October.

Ethics

SAIOH's memorandum of incorporation (MoI), drafted by legal advisors NGO Law, is in the final stages of approval. NGO Law can now concentrate on the review of the SAIOH Ethics Policy and Procedure(s), which will empower the Ethics Committee to instil uncompromisable ethical behaviour in the industry.

> ***Note***
> Another Ethics PDC will be offered during the 2023 SAIOH Annual Conference.

SAIOH branch activities

The Western Cape branch hosted its second in-person meeting on 9 June 2023. Johan Coetzé discussed the use and application of Bayesian statistics in occupational hygiene. The Gauteng branch will hold its third hybrid meeting on 4 August 2023 at the National Institute for Occupational Health (NIOH) offices in Johannesburg. The Botswana branch, now registered in Botswana as the Botswana Association for Occupational Hygiene (BAOH), held its official launch on 25 May 2023 at the Debswana Training Centre in Gaborone. BAOH also signed a memorandum of understanding (MoU) with the Botswana Ministries of: Employment, Labour Productivity and Skills Development; Mineral Resources, Green Technology and Energy Securities; and Investment, Trade and Industry. Naadiya Mundy, the SAIOH President, attended this event.

International feedback

The Occupational Hygiene Training Association (OHTA) and the International Occupational Hygiene Association (IOHA) continue communicating with their members; relevant links are e-mailed to all SAIOH members and published on the SAIOH website. IOHA has informed us that they will no longer publish their *Global Exposure Manager* (GEM) newsletter.

Coinciding with the SAIOH 2023 Annual Conference, the IOHA Board of Directors will hold its autumn meeting in Cape Town – hosted by SAIOH on 22 October 2023. SAIOH will also host a formal dinner for the IOHA Board of Directors on 23 October 2023.

Disappointing news

Garth Hunter, the SAIOH representative on the International Occupational Hygiene Association (IOHA) Board and its National Accreditation Recognition Committee (NARC), and a very prominent member of the PCC and PCC Exco, resigned earlier this month. He and his family are emigrating to Ireland in mid-August. This is a huge loss, not only to SAIOH, but also to the occupation hygiene profession in South Africa. We take this opportunity to wish Garth and his family all the best in their new country.

The SAIOH PCC will nominate a new representative(s) on the IOHA Board and the NAR Committee.

SAIOH Technical Committee feedback

Our second technical committee is developing technical procedures and a SAIOH position paper on heat stress management, enabling SAIOH to provide comprehensive and relevant proposals to strengthen the newly launched Physical Agents Regulations (PAR) – the old Environmental Regulations for Workplaces.

Annual SAIOH Scientific Conference

The hybrid SAIOH 2023 Annual Scientific Conference will take place from 23 to 26 October this year, paired with the IOHA meeting. The theme of the conference is *Real-time monitoring revolutionising occupational hygiene for safer workplaces* and will take place at the Breakwater Lodge on the Victoria and Alfred Waterfront, Cape Town.

FROM THE PROFESSIONAL CERTIFICATION COMMITTEE (PCC)

Lee Doolan: SAIOH PCC Administrator
e-mail: lee@saioh.co.za
Deon Jansen van Vuuren: SAIOH General Manager
e-mail: deon.jvvuuren@gmail.com
Corlia Peens: PCC Chairperson
e-mail: corlia.peens@sasol.com

Certification assessments

A summary of results from the March to June 2023 assessments is provided in Table 1, which reflects the Q1 and Q2 written assessment results and the Q1 oral assessment results.

The second quarter (Q2) PCC written assessments took place on 23 June 2023; 23 virtual oral assessments were conducted from 21 to 31 July 2023 (Q2).

Oral assessment improvements

The PCC technical teams continue to revise the PCC oral assessment format and questions in line with the occupational hygiene self-assessment tool.

Table 1. SAIOH PCC certification assessment results (March–June 2023)

	Written assessments (Q1 and Q2)				Oral assessments (Q1)			
Certification category	**Assessed**	**Passed**	**Failed**	**Pass rate**	**Assessed**	**Passed**	**Failed**	**Pass rate**
	n	**n**	**n**	**%**	**n**	**n**	**n**	**%**
OH assistant	74	69	5	93.2	74	69	5	93.2
OH technologist	37	21	16	56.8	8	4	4	50.0
Occupational hygienist	34	19	15	55.9	15	13	2	86.7
Total	**145**	**109**	**36**	**75.2**	**97**	**86**	**11**	**88.7**

Two PCC technical teams are working in parallel. The first is updating the SAIOH self-assessment tool and revising the PCC oral assessment format, and the second is developing questions and the required answers. Improvements in the assessment format will encompass the growing field of occupational hygiene and ensure that the assessment format and tools are relevant and current.

Occupational Hygiene Skills Forum (OHSF)

The OHSF was instrumental in coordinating the development of a series of asbestos training courses. The most recent, 'Asbestos assessments in buildings, section 1: Introduction' is now available for use by OHSF-registered training providers. The assessments are administered by SAIOH for a certain fee per candidate. Please contact Lee Doolan for more info (lee@saioh.co.za).