

**Talk On “Integrated Security Management System Implementation Framework”**

by Alex Looi Tink Huey

Alex Looi Tink Huey is an electrical engineer and also a software engineer who is actively involved in renewable energy power plants, power system studies, and power quality analysis.

Critical infrastructures are vital as its incapacity or destruction have a debilitating impact on our country’s defense system, economy and national security. These infrastructures require more detailed attention in their protective security management strategy and implementation. Security intrusion incidents have dramatically risen over the last decades. Organisations are becoming more and more concern of the importance of safeguarding their critical infrastructure and information. To prevent dangerous security threats and to comply with to a variety of industry mandated standards, the organisation needs to deploy a proactive security strategy. The talk session provides the implementation framework for Integrated Security Management System as part of the protective security management strategy in critical infrastructures.

IEM Electrical Engineering Technical Division organised a talk on “Integrated Security Management System Implementation Framework” on 4th June 2016 at Wisma IEM, Petaling Jaya, Selangor. There were 50 participants comprising industry experts, engineering firms, plant owners, and academic institutions who attended the event. The speaker was Mr. Edmond Chin Kokyu, who has vast working experience for the past 18 years in Bosch Security System, Honeywell Security, General Electric Security and UTC Fire and Security. He is actively involved in the development of new fire and security system and specialises in critical infrastructure.

Various developments in the field of security have shown that the required action can best be taken based on a management system approach. It is important to identify security risks to ensure that effective controls are in place to protect people, product, and assets of an organisation. By identifying and evaluating potential risks, a risk profile can be created for each location. The risk profile provides and in-depth understanding of the site’s security needs that allows for optimal deployment of human and financial security resources. Many risks can be reduced or eliminated by proper security layout, system design and procedures.

There were several studies discussed on the positive impacts of using Integrated Security Management System for crime prevention and reduction. However, they were not without its flaws. The implementation framework helps designers and specifiers address the issues and challenges of integrated security system designs in critical infrastructure by incorporating elements from other security domains such as Policy, Physical, Personnel, Data, Document, and Devices.

A comprehensive security approach should also focus on: risk management; strong control measures; effective standards, policies, and procedures; and appropriate response to incidents. The development and implementation of these security practices will create a secure working environment for any organisations.

The talk ended with a token of appreciation presented by EETD to Mr. Edmond.



Figure 1: Participants listening intently to the speaker