Since 2006, the LUSAX research program at Lund University in Sweden has investigated the effects of digitisation on the physical security industry. This article will look into the forces driving digitisation, and how those forces broadly translate and impacts the physical security industry.

Historically, physical security systems have moved from purely mechanical systems into systems holding both mechanical and electronic low-voltage circuit-based components. Development was pushed further forward when digital components emerged in the late 1980’s with the introduction of Digital Video Recorders (DVRs). And from 1996, when Sweden-based Axis Communications claims to have introduced the first network-enabled surveillance camera, digital components were further introduced into physical security systems. From a strategic business point of view, the digital shift most importantly brought with it new ways of doing business. Currently it is more common to observe novel and potentially more efficient business models challenging the proprietary and integrated one-brand manufacturer-distributor-integrator model historically associated with the industry.

However, from an end-user point of view, the primary objective of a security system is still to protect organisational assets from harmful action. Preferably this is achieved by means of pro-
active deterrence, and secondarily by direct prevention. Any change in the underlying technology – mechanical or digital – needs to be evaluated against these objectives. In order for technological advancements to be value adding, it needs to either strengthen the overall performance – both in terms of functional and non-functional requirements – of the current system, or lower costs for the same performance.

In the case of a video surveillance system, the purpose of the system could be to decrease the number of shoplifting incidents at a store by means of temporarily storing the snapshots or shorter video sequences of customers visiting the store. Two examples of advancements associated with digital surveillance cameras may for example be superior performance in terms of picture quality and ease of access to the recorded material compared to previous generations of surveillance cameras. But, it could also be to protect assets against unintended harmful actions, for example in protecting co-workers from exiting areas with sensitive business information. Furthermore, digital systems have been suggested to have potential value in improving core value-adding operations. A prime example of this feature is the track-and-trace functionality in parcel shipment. Finally, the potential of pre-programmed self-diagnostics is another example of feature associated with future digital systems.

Why digitisation happens

When Sweden-based Axis Communications claims to have introduced the first network-enabled surveillance camera, digital components were further introduced into physical security systems.

More broadly, digitisation is tightly coupled to what is referred to as Moore’s Law within the computing industry. First formulated by Gordon Moore at Intel in the early 1960’s, it proposed that computing capacity doubles every 12 months. Put in other terms, if we enter a computer store to buy computing power in June 2013 for one dollar, we would receive double the amount of computing power in June 2014 for the same amount of dollar. Gordon Moore was proven right, although slight modifications to the law have been added. The current doubling-speed in terms of computing power happens every 24 months. While this is merely a computational law, the business-consequences are important. Assuming a doubling of computing power every 24
months creates business opportunities for entrepreneurs that can translate the computing power into business-serving concepts at a low cost. This creates a strong cost-pressure on firms to consider digitising and even automating parts of the value-adding process. Examples of professional categories that have been affected by automation are for example secretaries, travel agents and bank tellers.

Moore’s law may impact industries in mainly two distinct manners: The first being digitisation that enhances the physical and manual activities – referred to as a kind of digital overlay to the current activities. The second one having more fundamental impact on an industry in the form of automation – simply substituting manual labour with (digital) machines, like in the case of the professions mentioned earlier.

**Reasons for a slower pace of digitisation**

Consequently, the key decision is not to ignore digitisation as a mere ‘gadget shift’, but rather to ask the question - in what way will Moore´s law impact my industry sector? Will Moore’s Law digitally reinforce and complement current work-practices according to the digital overlay-scenario, or will it simply substitute manual security labour gradually? The evidence the LUSAX-team has collected the past 9 years suggests a slower than expected, gradual and complementary development compared to other industries. We see three main reasons to a slower development speed.

The first (1) being the nature of security systems, they are to deter harmful action that is based on non-standardised behaviour. The intruder is actively attempting to outsmart the system. Routine business tasks, like registering invoices is a routine that once established may easily be duplicated and lends itself easily to digitisation and automation. Quite the opposite – and due to the variation in the intruder’s behaviour –duplication of the external qualities of a security system across an organisation would represent a risk in itself.

> In the case of the physical security industry, the evidence collected by the LUSAX group suggests a more slow-moving digitisation more associated with the digitally enhancing scenario
Secondly (2), the service-level of security systems should be near fail-safe. Everyday use of IT-based services is associated with a higher degree of acceptance to operational disruptions, meaning users and organisations tolerate a lower than fail-safe performance-level compared to security systems. This is sometimes refereed to as the Beta-culture of the IT-industry. In turn, this generates a more conservative approach to experimentation with new technologies among security practitioners that makes digitisation a slower-moving process compared to other sectors.

Third (3) and finally, while it is true that security management has increased in importance from a corporate point of view the past decades, security management still is redundancy and contingency-centric. This in turn hampers a rapid diffusion of digital security innovations. On the other hand, strategic management more generally concerns itself with achieving organisational goals by actively taking risks in a lean and non-redundancy direction. This orientation lends itself more compatible with the automation scenario, for example reducing the need to keep parts of the corporate accounting, marketing or R&D staff internally.

**Summary**

In this article we have briefly introduced Moore’s Law as a broad driver of digitisation. The effects of digitisation may impact industries differently. Either disruptively - basically gradually reducing the need for manual execution of current work practices, or enhance activities by means of digitisation. In the case of the physical security industry, the evidence collected by the LUSAX group suggests a more slow-moving digitisation more associated with the digitally enhancing scenario.

**Author Profile**
Markus Lahtinen holds a Master's degree in Informatics (2001) and a Bachelor's degree in Business Administration and Economics (2006). The past ten years he has been active as lecturer at the Department of Informatics at the School of Economics and Management, teaching mainly Interaction Design but also given classes on Decision Support Systems, UML, IT and organisation, and supervising theses work for students at Bachelor and Master level.