Jansta Associates
LIMITED

IMPLEMENTING TECHNOLOGY TRENDS

THERMAL CAMERA SCREENING

RISKS, ISSUES, FALSE CLAIMS

GUIDE NOTE

+44 (0) 789 685 92 44
www.janstaassociateslimited.com
twitter.com/peter jansta
UK, Europe, Middle East & Asia

Table of Contents

1. INTRODUCTION

This document is part of the *Implementing Technology Trends Guide Note series,* focusing on physical security, project management, electrical, control engineering, and telecoms sectors.

As the world is becoming interconnected, the interdisciplinary approach is a standard. It is also clear that a simple application can be the best value on many occasions. The intent is to provide solutions that fit the purpose and simplify even the most complex systems.

The boundaries between physical security and cyber security are becoming ever so thin. Understanding current industry developments help to deliver practical solutions.

This document will focus on the rise of cameras detecting elevated skin-surface temperatures. Since 2020 we have seen a rapid deployment across many industries providing preliminary checks in office buildings, factories, stations, airports, and other public spaces. This note will outline technology and risks.

It is paramount to emphasise that the full benefits of deploying new technology can be achieved by following the deployment process (see Fig.1 below).

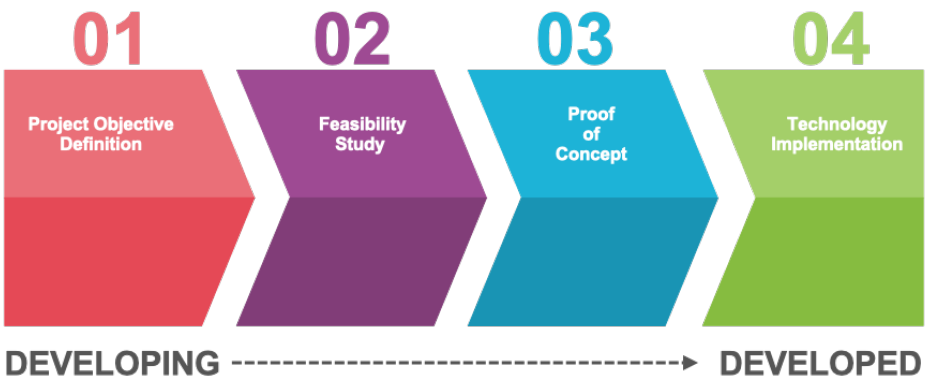

Fig.1 Deployment project cycle

The process will be tailor-made to suit each solution. The bellow flowchart chart (© JAL) shows the typical approach in the project management control environment when deploying technology into integrated security solutions.

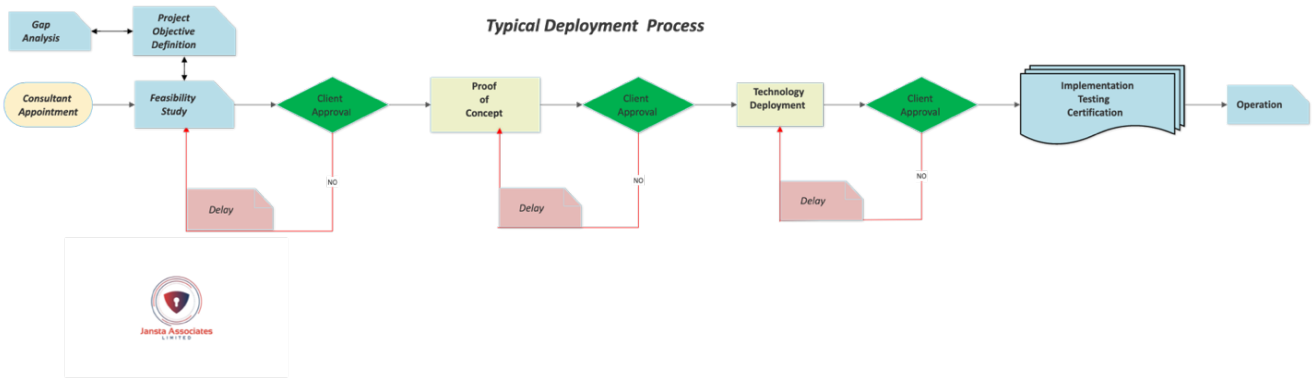

Fig.2 Typical deployment process

2. TECHNOLOGY TRENDS

The 2020 pandemic accelerated the growth of intelligent security technologies, often embedded in governance and politics. Particularly interests around contract tracing systems, people counting, touchless access control. While giving the operators and customer confidence, some of those technologies are ineffective, impractical, and increased government surveillance powers. Furthermore, raising more ethical questions about the deployment.

The sharp rise in thermal cameras detecting elevated skin-surface temperatures witnessed some stunning profits for many companies. This note will discuss:

- Concept
- Terminology
- Is deployment justifiable and legal?
- Is the system fit for the purpose and worth of the investment?

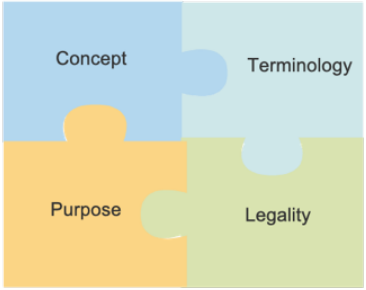

Fig.3 Technology trends

In the context of the processes as set out in Section 1. above, this note would form a part of the Feasibility Study. By outlining how we will manage the process, we can control the effective deployment, measure progress, and identify whether the system/technology fits the purpose.

2.1 Thermal Measurement

The elevated body temperature detection camera market has exploded over the past two years, with some manufacturers offering dubious solutions. Such as self-adjusting algorithms[1], in effect systematically manipulating temperature readings.

Numerous studies prove ineffective readings[2], concluding that these devices are utilised for sentinel detection of possible infectious disease transmission; now globally employed. The implications for reduced detection of febrility are a widespread false sense of security.

2.2 Regulations

Thermology science has been around for a long time. It covers all thermal imaging medical applications, including fever screening. The implementation and deployment[3] of the fever technology are governed by international standards, for example, Medical Equipment, safety, and essential performance[4].

The standards stipulate core guidelines, such as the measurement focus area shall be the inner eye (others are unreliable) and remove all obstructions (sunglasses, hair). The temperature laboratory accuracy of a screening thermograph, including the measurement uncertainty, shall be less than or equal to an offset error of ±0,5°C over the range of at least 34°- 39°C. Furthermore, the face shall be parallel to the camera to ensure sufficient image pixels.

Individuals suspected of being febrile with screening thermographs shall be confirmed with a secondary measurement using a clinical thermometer. Screening shall be used under indoor environment conditions, avoiding lighting and Indoor heating or cooling nearby.

For example, most shopping malls in the Middle East installed thermal cameras in the indoor locations, at the point of entry below cool air curtains situated in the ceilings. When accessing facilities from high ambient temperature (often 50C+), it is clear that accurate readings are unlikely.

With questionable self-adjusting algorithms, the guidelines mentioned above are often dismissed or violated by many manufacturers, false marketing, incorrect locations; we can see this technology is problematic.

1 https://www.washingtonpost.com/technology/2021/03/05/fever-scanner-flaws-covid/

2 https://www.nature.com/articles/s41598-021-91361-6

3 https://www.iso.org/standard/69347.html

4 https://www.iso.org/standard/69346.html

2.3 Legal Implications

General Data Protection Regulations (GDPR) regulates data processing in the EU. The UK GDPR stipulates general data protection regimes for most UK businesses and organisations.

2.3.1 Data Controller

The end-users: a shopping mall equipped with a security camera system is the controller of the video surveillance data it collects (companies that keep personal data on their employees are considered data controllers).

2.3.2 Data processors

Cloud providers store personal data on behalf of an end-user; these can be integrators and manufacturers that directly handle video recording data.

2.3.3 Data subjects

The people being recorded on camera.

2.3.4 Biometric data

They are defined as any technique which uniquely identifies a person, such as a video analytics technique - facial or age recognition.

2.3.5 Impact and Considerations

The consultant may advise the end-user to erect signs indicating video surveillance in use. The regulator goes further.

- The identity and contact details of the data controller
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- Informing data subjects of their right to lodge a complaint with a supervisory authority
- The existence of the right to request access, rectification, and removal of the Data
- The contact details of DPO, if you have one
- If the data will be transferred to another country, the relevant safeguards in place
- Recipients of the personal data (if other than the end-user)
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (facial recognition and biometric techniques)

GDPR legislation stipulates a Data Protection Impact Assessment (DPIA) to be conducted before any system is installed.

- systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- assessment of the necessity and proportionality of the processing operations concerning the purposes
- evaluation of the risks to the rights and freedoms of data subjects
- measures envisaged addressing the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation considering the rights and legitimate interests of data subjects and other persons concerned

The GDPR allows more extended storage periods for public interest, scientific, or historical research purposes. An end-user that indefinitely stores its video recordings is likely to violate the GDPR unless it can prove it is acting according to these reasons.

Under Art.9[5], processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

However, the GDPR recognises several exceptions to this prohibition. For video surveillance, the relevant exception is the vaguely termed (reasons of substantial public interest).

Individual EU member states are currently defining these public interest reasons, mostly related to law enforcement and crime prevention.

2.3.6 Temperature Screening

The GDPR doesn't mention video surveillance. However, fever screening with cameras is directly impacted by the GDPR; Art. 9 states that processing personal data concerning health shall be prohibited, while Art.22[6] states that people shall have the right not to be subject to a decision based solely on automated processing. However, these articles have significant exemptions, such as consent or substantial public interest.

In 2020 UK Medicine and Healthcare product Regulatory Agency (MHRD)[7] stated that most products were initially designed for a non-medical purpose. Furthermore, there is no evidence to support an accurate medical diagnosis. The agency also advised that anyone selling the hardware and claiming a direct link to the virus diagnosis will be prosecuted. In 2021 FDA also issued a public alert about improper use of thermal imaging devices.[8]

Note: There is no scientific evidence to support temperature screening as a reliable method.

[5] https://gdpr-info.eu/art-9-gdpr/

[6] https://gdpr-info.eu/art-22-gdpr/

[7] https://www.gov.uk/government/news/dont-rely-on-temperature-screening-products-for-detection-of-coronavirus-covid-19-says-mhra

[8] https://www.fda.gov/news-events/press-announcements/fda-alerts-public-about-improper-use-thermal-imaging-devices-warns-firms-illegally-offering-thermal

3. DEPLOYMENT

As mentioned above, this guide note would be part of the feasibility study stage as defined in the typical deployment process (see Fig.2). A simple assessment of the practicability of a proposed project plan or method. We can analyse technical, commercial, legal, and operational elements for each subject.

For example, in this case, the technical feasibility determines whether the technology fits the purpose. Economic feasibility should assess financial viability, such as cost benefits.

Legal: Your project meets legal requirements, such as the law that applies. Operational: planning, strategy goals, resource, business objective (see fig.4 below).

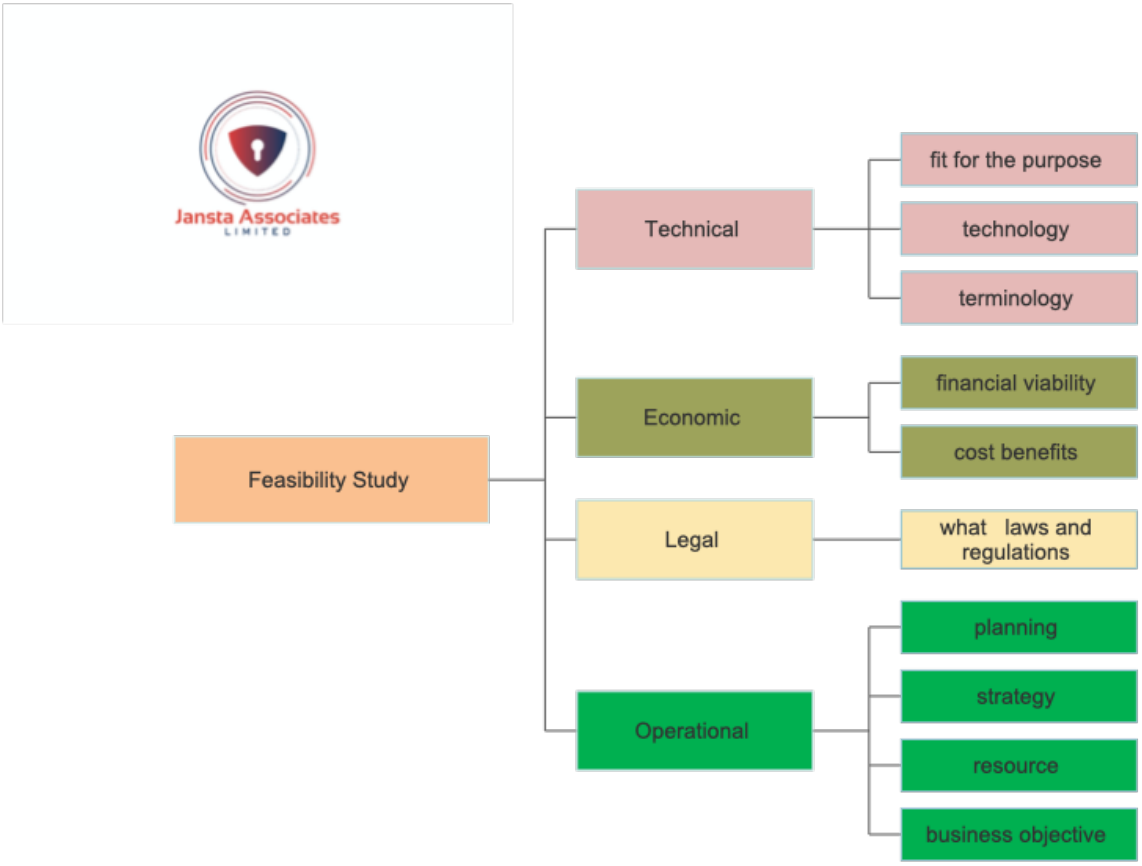

Fig.4 Feasibility study types

4. CONCLUSION

The key to successful transformation is managing the stages and simplifying complex solutions. To achieve the desired output, a clear objective and planning are essential.

In November 2020, CDC issued a detailed study that concluded that symptom screening is ineffective, creates false alerts, and is expensive. [9]

The main concerns with the technology are that there are no clear standards no independent tests. Such vacuum allowed camera manufacturers to market products that are, in fact, not medical devices, often promoted as cutting edge with dubious self-adjusting algorithms and AI. Based on all data available and formal statements issued by the official channels, this technology is not suitable for the purpose.

I would encourage operators and facility owners who consider deploying this technology to evaluate the investment with care. The only outcome is that the technology offers a false sense of comfort and security.

The technology that may seem attractive is not always the best solution, primarily based on the corporate junk science driven by profits.

Jansta Associates
LIMITED

*At **Jansta Associates Limited**, we serve our clients with a vast array of engineering consulting services. So, if you are thinking of deploying new technology, designing, or updating the system, we can help you navigate this complex subject.*

[9] https://www.cdc.gov/mmwr/volumes/69/wr/mm6945a4.htm?s_cid=mm6945a4_x