INTEGRATING TECHNOLOGY AND CONSTRUCTION:

A GUIDE TO ICT INSTALLATION WITHIN THE PRISON ESTATE

JOINTLY PRODUCED BY:

ICT EXPERT GROUP: PIA PUOLAKKA (FINLAND), MARJAN LUKAVECKI (CROATIA), HUBERT UNGER (AUSTRIA), JACQUES HENSEN (LUXEMBOURG).

REAL ESTATE EXPERT GROUP: TONY MCDONNELL (N. IRELAND), ERIC BESSON (FRANCE), MARK MCGOLDRICK (IRELAND), ENES SEDIC (CROATIA).

JULY 2025

Co-funded by the European Union

TABLE OF CONTENT

ACKNOWLEDGEMENTS

This paper is published by EuroPris – the European Organisation of Prison and Correctional Services. It was jointly developed and inspired by the insights of two EuroPris Expert Groups:

Real Estate and Logistics Expert Group:

- Tony McDonnell (Northern Ireland Prison Service, N. Ireland)
- Eric Besson (Ministry of Justice: Department of Prisons, France)
- Mark McGoldrick (Irish Prison Service, Ireland)
- Enes Sedic (Directorate for Prison System and Probation, Croatia)

Information, Communication and Technology in Prisons Expert Group:

- Pia Puolakka (Finnish Prison Service, Finland)
- Marjan Lukavečki (Specialist in the Head Office for the Prison System and Information Security Adviser at the Ministry of Justice and Public Administration, Croatia)
- Hubert Unger (Senior ICT Manager within the Austrian Ministry of Justice, Austria)
- Jacques Hensen (ICT Manager at the Administration Pénitentiaire, Luxembourg)

These Expert Groups are also coordinated by EuroPris' Deputy Director, Justina Dzienko.

1. INTRODUCTION

Digitalisation is advancing at a rapid pace in many aspects of today's modern world. This guidance note, jointly developed and inspired by the insights of two EuroPris expert groups **(Real Estate Expert Group and ICT Expert Group)**, focuses on the fundamental building blocks of establishing and operating ICT solutions within a prison environment. It brings together multidisciplinary knowledge and European experience from a diverse range of countries and prison systems related to infrastructure planning and digital integration. By drawing on this collective expertise, the document aims to support the wider European prison community in addressing common challenges and future-proof ICT solutions across national contexts.

Its aim is to offer a practical guide to the installation and operation of Information and Communication Technology (ICT) systems within prison real estate, whether in new buildings or retrofitting old buildings. Exploring the role that ICT plays in the operation of our prisons, the factors that need to be considered to ensure its effective operation, and the opportunities and challenges that ICT integration presents moving forward.

2. BACKGROUND

The use of Technology within prisons now sees the increasing use of digital solutions to enable the delivery of communication, security, education, inmate management and wider support services.

In the context of prisons it is important to understand that there is no single unified approach to the application or adoption of ICT solutions across the many jurisdictions operating across Europe. Levels of ICT integration and sophistication varies between different nations. These disparities in ICT adoption are due to a number of factors including differences in policies, access to financial resources and broader societal and socio-economic differences between nations.

Digital systems are continually evolving and advancements in these have moved forward at pace through the introduction of new Internet Protocol (IP) technologies and the increasing use of Artificial Intelligence (AI). IP has now become the dominant technology, gradually replacing the previous generation of 'analogue' technologies, with a focus on user interoperability and offering enhanced levels of functionality (as equipment has more processing power enabling devices to fulfil a broader range of complimentary functions).

This guidance note offers prison practitioners a clear commentary on the accepted practices of how to configure, manage and maintain ICT installations, as well as offering early insight into some of the new and emerging technologies that the prison community and individual prison systems need to carefully consider over the coming years.

3. APPROACH TO THE DELIVERY OF A DIGITAL STRATEGY

Investment in new technologies can be significant and, once installed, can quickly become embedded into the operational fabric of a Prison. It is therefore important to consider what you need and how best to configure and manage new technologies once installed. The effectiveness, ease of use, serviceability and long-term reliability of whatever products are selected and configured will have a long-lasting bearing on the functioning of the Prison and the whole life cost and maintainability of the systems installed.

It is extremely important to consider the best strategy to provide the most durable and effective digital solutions, which will support the long-term needs of the Prisons. IP systems are now commonplace. The installation of IP should deliver the benefits introduced by these new technologies whilst ensuring future resilience and affordable, accessible serviceability for the foreseeable future.

Whenever an ICT strategy is being developed, it should consider several key principles:

a. The plan should include a controlled methodology to allow systems to be upgraded in an affordable, timely manner whilst maintaining appropriate levels of security;
b. Transitioning from old to new – Clearly define your upgrade path, particularly within an operational prison, to ensure that appropriate levels of security are maintained and the operational integrity of the prison is preserved during the transition period;
c. New systems should be built from a secure platform which will facilitate the continuing integration between new and existing systems and ensure an appropriate level of resilience;
d. Individual systems should be reliable, affordable and maintainable – at acceptable levels of cost – for the foreseeable future;
e. (Training of Staff – ensure that Users are offered training and are competent and have familiarity with the systems if they are to be of benefit;
f. Human Interaction - maintaining an appropriate amount of human interaction is an essential consideration when determining the extent of automation that is to be introduced in the design of new IT systems.

Across Europe, the application of digital strategies varies between the different jurisdictions. This variance is reflected in the digital technologies in use. Importantly, every correctional system retains the autonomy to choose the path that best suits their operational environment and the priorities and resources available to them. One of the key indicators of digital maturity is how open a prison system is to embrace new technologies.

Whilst technology can introduce a range of opportunities, such as improved communications and easier access to education and rehabilitative programmes, it can also introduce potential risks and challenges with regard to security and data protection.

Attitudes to the use and application of technology within prisons can adapt over time. For example, the accepted norm was the widespread use of highly durable, tamper-resistant equipment within prisoner areas. Over time, attitudes have shifted, and we now see many prison systems moving to introduce standard consumer-grade devices (such as telephone handsets and tablets for use in their cells).

Importantly, the evolution of ICT does not negate the need for carefully considered solutions to prevent misuse. In particular, attention must be paid to **data confidentiality** and information security to ensure that sensitive information remains protected.

4. THE NATURE OF ICT SYSTEMS USED WITHIN PRISONS

There is a wide range of digital solutions available to and used with prisons to support both their operation and the rehabilitation of prisoners. These are achieved through the deployment of a number of separate networks (these can be either physically or virtually separated) which typically include:

Administrative (Office): The admin network will cover all the standard general office, administrative and communication services operating across government, as well as any video-conferencing (for court attendance) and telemedicine

Security Systems: A dedicated network to provide video surveillance, biometric access control, electronic locking, cell call systems, detection and intruder alarms, staff alarms, key management, telephone surveillance, transceivers, man-machine interfaces in protected workstations, intercom systems, jamming of unauthorised phone communications as well as fire alarm and fire detection systems.

Building / Facilities Management (IoT): A network to support energy and building management, power generation and back-up systems contributing to the efficient operation of critical infrastructure supporting the operation of a prison.

Prisoner Services: These are designed to improve the living conditions and rehabilitation opportunities offered to inmates, including supporting education through e-learning and training, prisoner television systems, tele-health services, booking internal appointments or placing menu orders and the like. These are often delivered through integrated software solutions accessed through special secure hardware (either in-cell devices or kiosks on landings) and include prisoner telephony services. Where there are heightened levels of communication options (electronic messaging between staff and prisoners as well as video calls and possibly email possibilities for prisoners), these are now being referred to as 'smart' prisons.

5. THE CHALLENGES OF OLD VERSUS NEW - INSTALLING ICT SOLUTIONS INTO PRISON STRUCTURES

A number of factors need to be considered whenever physically installing ICT solutions within prison buildings, whether in new or old ones. This is particularly challenging whenever retrofitting ICT installations within older prison structures. Both are examined below:

5.1 OLD STRUCTURES

Older existing structures were not designed with the needs of the modern world in mind. As such they are often incapable of easily accommodating the need for structured cable routes, temperature controlled equipment rooms and the installation of devices within inmate living areas. It can often be a struggle to incorporate ICT solutions within these older structures, particularly those which are of historical significance.

- Solid walls often need to be cored to provide cable routes, in most cases it becomes necessary to surface mount the majority of new cabling;

- Equipment rooms must be created to service any new ICT installation. This can be particularly challenging and either means the loss of accommodation (as an existing room must be used – which may not be the best size or shape – to house the racks and servers) or the creation of a space/room within a larger circulation space.

- Older prisons often have smaller circulation spaces as cell confinement was often a factor in earlier prison approaches. Light open spaces were less common which can present challenges in opening up structural elements to facilitate ICT wireless solutions.

- Modern cell doors – which often incorporate an increasing amount of technological features – are generally taller and wider than older cell doors. This presents a challenge whenever seeking to retrofit inside an older facility.

5.2 NEW STRUCTURES

Constructing a new purpose-built facility presents a valuable opportunity to deploy modern ICT solutions into a new prison. Items to be considered:

- Consider the category of prisoner for which you are designing as this will be of particular benefit in informing the in-cell ICT requirements. Training and resettlement prisons are likely to have a strong focus on education and learning which will suggest the promotion of in-cell digital solutions.

- Opportunity for full integration of structured cable routes throughout the fabric of the building (avoiding unsightly and cluttered cable runs) will enhance the level of security by mitigating the chance of cable damage.

- New prison developments take several years to complete. It is important to recognise that specific ICT solutions included in the original tender package may become obsolete or less relevant over the course of a 3- or 4-year construction phase. It will therefore be important to include for cabling solutions at the outset but allow flexibility to procure the final ICT system solution during the construction phase so that it offers the most appropriate solution once the facility is eventually opened.

6. DEVELOPING A ROUTE MAP FOR THE ROLLOUT OF ICT WITHIN PRISONS

A Prison estate often comprises large assortments of different building forms and structures that have been incrementally established over many years. Some may have been purpose built as prisons other buildings may have been repurposed. The vast majority of existing buildings were designed and built prior to the arrival of the digital revolution. Whilst newly designed structures are generally designed to incorporate new technologies this is not the case for the vast majority of the existing building stock.

It is therefore important when planning to incorporate new technologies into both new and existing buildings that a number of key steps are followed:

STEP 1 - ESTABLISH EQUIPMENT ROOMS

These need to be strategically positioned around the site to house the array of electronic equipment (servers, switches, head-end equipment, uninterruptible power supplies (UPS) etc. that make up each distinct system.

These rooms need to be clean and air quality and temperature need to be carefully controlled (electronic equipment generates heat and in order to both extend the life of the electronic components and optimise their performance the equipment rooms need to be operated with a defined temperature) to ensure the longevity of the devices and any back-up. Ideally rooms should contain raised access floors (creating sufficient space beneath the floor to lay and route cabling).

STEP 2 - CABLING INFRASTRUCTURE - SITE WIDE CONTAINMENT

Once the equipment rooms are created there will be a need to provide appropriate levels of physical inter-connectivity to establish the linkages between the different devices and the systems and the head-end servers with the equipment rooms.

The connectivity between the servers and the main switches within the equipment rooms and those switches distributed around the site is best achieved through redundant fibre rings (providing two separate routes for cabling) as this offers resilience in the event of one of the cables being subsequently damaged.

The diverse rings will enable multiple diverse connections between the planned equipment rooms. This will ensure a resilient physical infrastructure, limiting the likelihood of any single event disabling connectivity between systems.

STEP 3 - DEDICATED FIBRE OPTIC CABLE NETWORK

The enhanced functionality brought by IP is matched by increased requirements for data capacity across the networks on which the IP devices operate. A fundamental building block is the establishment of a solid network foundation that can easily handle the increased volume of data traffic introduced by a full IP solution.

The interconnections should be achieved using fibre optic cables in order to provide a suitable bandwidth on which to transmit the volumes of data traffic. However, for the final distance (up to 90 metres) to the device/desktop it is appropriate to use twisted pair copper cables (Cat 6 or higher) with RJ45 sockets.

STEP 4 - ESTABLISH THE PRISONS SEPERATE IT NETWORKS

The technologies and ICT systems operated within Prisons are different from those operating within other parts of the government. It is therefore advisable to establish a separate dedicated IT network on which you can run and operate those prison systems.

Establish Local Area Networks (LANs) incorporating the cabling and the network equipment (i.e. network switches, routers, firewalls, etc.) interconnected using the fibre optic cabling infrastructure. Whilst creating a LAN is cost-intensive, once established, it should be possible to share the hardware and cabling by creating a Virtual LAN (VLAN) using digital separation techniques, helping to reduce further costs. Both the physical and logical elements of the network must be secure, resilient and robust. The network must be capable of catering for a range of varied requirements and nuances of various protocols used by systems connected to it.

The network must be designed by a qualified IT network design expert and the appropriate design certifications provided to the prison administrations on completion.

STEP 5 - DETERMINE LEVEL OF INTEGRATION

Integration occurs when two or more different systems are designed to interact with each other to improve the overall ease of delivering/managing a task. An example could be where CCTV and alarm systems interact – so upon activation of an alarm the CCTV systems automatically select the most appropriate camera and displays the image on a designated monitor.

There are both advantages and disadvantages to integration. Whilst integration may offer some operational improvements these need to be balanced against the added complexity and additional ongoing servicing/maintenance costs of merging two or more systems (i.e. the introduction of a software update from one supplier or the simple expansion of one of the systems can introduce instability in both integrated systems and lead to unplanned outages. Systems that previously worked may no longer function). Necessary software updates or changes to one system often require each systems software developers to investigate and debug the systems to ensure both systems talk to each other. This can become extremely costly with any future glitches in a suppliers system being blamed on the other integrators system.

For the reasons outlined above integration is best avoided unless it can demonstrate real benefits from a prisons perspective which significantly outweighs any possible future disruption caused as a result of the integration. These also need to be considered alongside the ongoing additional costs of creating and maintaining integration on the two or more systems.

STEP 6 - SELECTION/PROCUREMENT OF DELIVERY PARTNER(S)

Whenever progressing the selection of a suitable ICT partner consideration should be given to the following considerations:

- Outcome based specifications – technology changes rapidly it is therefore advisable to procure IT systems based on the deliverables (rather than note a particular model of equipment – in some instances years may pass from the design phase to the inauguration date and the original concept may be subjected to concerns around scalability or economic restraints)

- Open Protocol solutions – whenever possible open protocol solutions should always be sought. These offer the maximum amount of flexibility to future-proof the installation by maximising the opportunities to integrate, communicate, service and maintain IT systems with future third party suppliers.

- Ensure that the long-term servicing and maintenance of the systems are built into the original award of contract – In order to ensure the enduring functionality of IT installations they should always come with a corresponding guarantee and service package (typically these need to be in place for the lifetime of the installed solution which typically can be 10 years or more)

- Consider using established pan-government IT contracts – IT solutions can be technically complex so before trying to develop a bespoke solution examination should be made to see if nationally procured contracts can be accessed

- Security Clearance for 3rd party ICT Staff – during both the initial system design phase and the ongoing servicing and updating of IT systems it will be important that the prison authorities have controls in place with 3rd party suppliers to ensure that only nominated staff are given access to the system/ network (and that these staff are both security cleared and are audited in their access to the systems)

STEP 7 - STRESS TESTING THE FINAL SOLUTION

To prove the capability of a system its often good practice to subject it to a targeted load test. This provides a controlled stress test to check how well a system can withstand extreme conditions. Typically, this would involve simulating how the system reacts to attacks, high data loads or technical failures. These tests can also include security audits to ensure that data protection and data security requirements are being met.

The aim is to identify any weaknesses at an early stage so that steps can be taken to improve resilience. Such tests are particularly important in security-critical areas such as IT infrastructures, video management systems or energy supply. Regular stress tests can guarantee the security and stability of a system in the long term. There are companies that specialise in carrying out stress tests who are able to provide advice and support.

7. DESIGN OF SYSTEM ELEMENTS

7.1 EQUIPMENT ROOMS

Location: Equipment rooms need to be conveniently located so that they are able to serve individual buildings with access to suitable power and cabling routes. Their location must enable connection of all network devices within those buildings using cables that are a maximum of 90 metres in length.

Raised access floors: These need to create a minimum of 150 mm of space below the floor to route cables.

Ceilings: Suspended ceiling are not required within Equipment rooms unless forming an integral part of the air conditioning system.

Environmental Control: The electronic equipment produces heat and in order to operate effectively the rooms must be clean and air quality and air temperature within the rooms need to be carefully controlled to optimise the performance and extend the lifespan of the electronic equipment and any back-up systems such as Uninterruptible Power Supplies (UPS) and their associated batteries housed within the rooms.

Electrical Power Supplies: These need to be protected from transient voltages.

Dual Power Supplies: Consideration of providing dual power from a source protected by a UPS and a separate independent power source (mains power) to negate potential failure of a UPS affecting the system. Both supplies should be protected by a standby generator.

Uninterruptible Power Supplies (UPS) Location: For added security it may be prudent to consider the separation of the UPS equipment from the Equipment rooms. As, although rare, it might be possible for the UPS batteries to overheat which presents a small risk of fire. This needs to be risk assessed to achieve a balanced and considered approach (there will be an additional cost and space needed to create separate equipment rooms for the UPS's and maintain the environmental conditions which may prove unrealistic).

Restrict Access: Access to the Equipment rooms – and the sensitive equipment within them – must be controlled and monitored. Only authorised personnel should have access to the equipment rooms. This could be on a key or access control system.

7.2 CABLING INFRASTRUCTURE

Once the equipment rooms are established, there will be a need to provide appropriate levels of physical interconnectivity to link the individual items of equipment. There will be a myriad of individual pieces of equipment (CCTV cameras, alarms, sensors, etc.) distributed throughout a building, and these all need to be cabled back to an equipment room. To handle the myriad of connections, a series of network switches will be used [each switch has either 24 or 48 ports, which individual items of equipment can be connected into. The switches are then connected to the IT network to communicate with the relevant head-end equipment.

In order to allow the efficient and timely transmission of data a vitally important component will be the capabilities of the cabling infrastructure. If the bandwidth/capacity of the cables is limited, then the entire system will suffer from time lag and the functionality of the devices will be compromised. It is therefore important to plan for a suitable cable infrastructure.

The cabling strategy is influenced by the distances over which an acceptable signal strength can be achieved. This is assessed as follows:

COPPER (CAT 5,6,7)

[Linking individual pieces of equipment back to the switches within the Equipment room]

90 m

FIBRE

[Linking switches located with the Equipment rooms dispersed around the site back to the head-end servers/ control room]

1,000 km

The following considerations should be made when planning the cable infrastructure:

The 90-metre rule: Cabling from the network switches to the individual pieces of equipment is limited to a maximum distance of 90 metres (these will be connected using Cat 5, 6 and 7 copper and communicate over the Ethernet). This limitation means that network switches need to be distributed around the campus (mainly in local equipment rooms but in exceptional circumstances the switches can also be placed at intermediary points in order to bridge longer distances).

Not all digital systems currently use the Ethernet protocol, and these will also need to be considered when designing the cable infrastructure (RS485 is also widely used by manufacturers).

Fibre Optic Cabling: Digital systems operate using transmission of binary data. The amount of data needed to be transmitted must be considered for current anticipated requirements and any foreseeable future requirements. As new IP systems are developed, there is an increasing need to provide additional capacity, or bandwidth, within the cabling to accommodate the free passage of higher amounts of digital traffic. For this reason, it is necessary to use fibre optic cabling throughout a site to link all the equipment rooms to the head-ends. There are different grades of fibre optic cables, single mode and multi-mode, each with variations and differing bandwidth capabilities, distance limitations and operational characteristics.

Two fibre optic methodologies are available to achieve this connectivity:

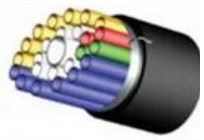
1) Standard multi-core cables; or
2) Blown fibre duct

The standard multi-core cables are installed to suit the existing requirements, but these would offer only limited provision for any spare capacity beyond the envisaged design requirements. Thus, limiting the opportunity for any future development of a system. This option is therefore considered too restrictive. A blown fibre duct would facilitate a number of tubes and would offer ample spare capacity to accommodate any future development of the network. This is the recommended solution.

Blown Fibre Micro-duct system: A blown fibre micro-duct solution enables multiple fibres to be laid in one duct. The blown fibre ducts are available in a range of formats, duct sizes, grades (internal and external as well as protection from attack by rodents) and can be laid directly into the ground.

Within each duct, there is a series of micro-ducts. Each micro-duct can accommodate a 12-core fibre optic cable (single mode or multi-mode). It is recommended that a blown-fibre micro-duct infrastructure be laid across the site.

In line with recent installations, it is recommended that a 24-micro duct tube be used (image on right).



It is envisaged that the initial installation would utilise 6 micro-ducts in each ring. This provides spare capacity in excess of any foreseeable future expansion of the fibre cabling infrastructure. To improve resilience two diverse routes should be laid, both around the site and within the buildings, thereby limiting the possibility of a single event removing connectivity between the systems.

7.3 NETWORK DESIGN

The design of the system should be undertaken by a certified network expert. The network should be established within each equipment room and connected to the network cabling infrastructure. The ongoing management of the network (which includes the resolution of any faults that may arise and the registering and programming of the individual items of IP equipment onto the network) is best undertaken by a certified network professional.

The network designers and network users (system providers) should work collaboratively throughout the design process to ensure that all the requirements for each system can be discussed reviewed and incorporated into the design.

Regular design workshops and performance testing of systems is of paramount importance to mitigate any potential performance issues that may be inherent in each system. In taking forward the design the following considerations should be made:

Consider each Systems bandwidth requirements: The network should be designed to cater for each system to be connected to it and control and limit the bandwidth consumed by the various security systems.

For instance, CCTV systems require substantial bandwidth as they stream large amounts of data from cameras continuously, 24 hours per day, 7 days per week. The bandwidth required for the systems is relatively consistent; however, various protocols and techniques are available to limit and control the bandwidth required. This is true of many IP systems, and the network must be designed to take account of all of the system's requirements.

Use of unicast and multicast protocols should be used as required.

Separate VLAN for Logical separation: Each system using the network should be allocated with a separate Virtual Lan (V-LAN) to provide logical segregation of the systems. Interconnection and integration should be controlled through layer 3 switches or routers to control and protect each system on the network.

Virtual Link Aggregation Protocols: Various protocols and techniques are available for connection of equipment on the network and are as diverse as the physical cabling topologies.

Virtual Link Aggregation protocols enable redundancy between equipment and connections in a network. Various manufacturers call their protocols different names with Dell using Virtual Link Trunk.

This can be used to provide maximum redundancy within the network without affecting efficiency of data transfer within the system. This form of deployment can help to improve network efficiency while providing protection against failure of equipment and connections.

Enterprise Level: All network equipment should be enterprise level to ensure its resilience manufactured by the same manufacturer to ensure their optimum inter-operability with the other devices on the system.

The system should be designed to provide maximum protection from cyber-attack and misuse.

8. STRUCTURED CABLING IN CORRECTIONAL FACILITIES

In modern correctional facilities, a reliable and well-organised IT infrastructure is of central importance. The demands for communication, surveillance, and management are constantly increasing. Structured cabling forms the backbone of this infrastructure and plays a crucial role in the efficiency and security of a correctional facility. But what exactly does "structured cabling" mean, and why is it especially important in correctional facilities? This article will explain the basics of structured cabling and highlight its advantages in correctional facilities.

8.1 WHAT IS STRUCTURED CABLING?

Structured cabling is a standardised system for network wiring that ensures a flexible, scalable, and cost-efficient infrastructure. It includes both the physical wiring and the components, as well as the structure that allows for easy maintenance and future network expansion. Key components include:

- **Cables:** Typically copper cables (Ethernet) or fiber optic cables.
- **Patch panels and outlet boxes:** These connect the cables to end devices.
- **Cable management systems:** Cable channels and conduits that ensure the organisation and management of the wiring.
- **Switches and routers:** These devices enable data transfer and network connections.

Structured cabling follows clear standards, such as **ISO/IEC 11801** and **DIN EN 50173**, ensuring that the entire infrastructure is built to a high standard and can easily accommodate future expansions.

8.2 SPECIFIC REQUIREMENTS FOR CORRECTIONAL FACILITIES

In correctional facilities, the IT infrastructure is not only a tool for daily operations but also a vital element for maintaining order, security, and communication. Special requirements apply in these environments:

1) Security Requirements: Due to the sensitive data processed in correctional facilities—such as prisoner records, legal documents, and surveillance information—the network infrastructure must meet the highest security standards. Encryption, firewalls, and physical security of the cabling are essential.

2) Availability and Reliability: In a correctional facility, systems must remain operational even during emergencies or technical failures. Structured cabling provides a redundant and fault-tolerant infrastructure, ensuring that communication and critical systems continue to function in case of a failure.

3) Scalability and Flexibility: The needs of a correctional facility can change over time. Structured cabling systems allow for easy expansion or modification of the infrastructure without the need for a complete overhaul of the cabling.

4) Surveillance and Control Systems: Correctional facilities increasingly rely on modern surveillance technologies, such as CCTV systems, motion detectors, and electronic access controls. These systems require a reliable and high-performance cabling infrastructure to operate around the clock.

5) Data Protection and Compliance: Correctional facilities must comply with specific legal requirements, such as the GDPR (General Data Protection Regulation). Structured cabling helps meet data protection requirements by enabling clear separation between different networks (e.g., administrative, security, and inmate communication systems).

8.3 ADVANTAGES OF STRUCTURED CABLING FOR CORRECTIONAL FACILITIES

Implementing structured cabling in correctional facilities offers numerous advantages:

1) Easy Maintenance and Management: The clear structure of the cabling allows for quick identification and resolution of issues. Network management is simplified since every component of the infrastructure can be clearly identified and traced.

2) Cost Savings: Standardising the cabling and using a modular setup avoids expensive renovations or expansions. If new technologies or devices need to be introduced, the infrastructure can be easily expanded or adapted.

3) Futureproofing: Structured cabling is not only suitable for current needs but also for future expansion. With proper planning, the infrastructure can handle increasing demands or new technologies without the need to replace the entire cabling system.

4) Enhanced Operational Security: Redundant systems and well-structured cabling minimise the risk of failures. Even during technical disruptions, alternative systems can be activated, ensuring the smooth operation of the correctional facility.

5) Higher Security Standards: In a correctional facility, the security of data and communication is of utmost importance. Structured cabling allows networks to be designed to meet the latest security requirements, and physical security measures (e.g., shielded cables) reduce the risk of tampering or eavesdropping.

8.4 SUMMARY

Structured cabling is a central element of the modern IT infrastructure in correctional facilities. It not only enables efficient communication and high data security but also ensures that the network remains flexible, scalable, and fault tolerant. Given the specific requirements for security, data protection, and reliability in correctional facilities, a well-planned and implemented structured cabling system is essential. With its many advantages, structured cabling significantly contributes to the efficient and secure operation of correctional facilities, while also preparing them for future challenges.

9. WIDER CONSIDERATIONS ON DEVELOPING ICT SYSTEMS WITHIN PRISON

Operating Prisons presents additional challenges that need to be considered in managing ICT. Some of these challenges are summarised below:

9.1 INFORMATION SECURITY

Information Security involves establishing safeguards to protect data that is processed, stored or transmitted to ensure it remains available and accessible only to authorised users.

To safeguard the information security considerations must be applied throughout the entire lifecycle of the information system – design, development, operation, maintenance and decommissioning. This includes the implementation of physical, technical and administrative controls in line with recognised information security standards.

Information security entails protecting data, minimising risk and ensuring system resilience in the face of potential issues. Key actions include incorporating security measures during system design and development, developing contingency and back-up plans, maintaining system logs and conducting threat analysis.
The application of best practice in information security is guided by ISO/IEC 27002 and 15408, and COBIT as well as recommendations from the European Union. Whilst prisons are generally exempt from formal certification it is recommended that these standards are adopted to ensure the delivery of a robust and secure environment.

9.2 AN IOT NETWORK INCLUDING REMOTE ACCESS WITHIN SECURE FACILITIES

The Internet of Things (IoT) has increasingly found its way into various sectors in recent years, including security-related facilities such as prisons, police stations, and other critical infrastructures. IoT technologies offer numerous benefits, particularly in surveillance, access control, and alarm systems. However, implementing IoT networks in security facilities also brings significant challenges, especially in terms of network stability, security, and remote access.

CHALLENGES IN IOT NETWORKS

1) Security Risks: One of the biggest issues with the adoption of IoT in security-sensitive areas is the risk of cyberattacks. Since IoT devices typically establish multiple connections and often communicate with each other, they can serve as potential attack vectors for hackers. This is especially true for devices like cameras, sensors, or access control systems, which are directly connected to sensitive data and systems. An insufficiently secured IoT network could lead to unauthorised access, data manipulation, or even a complete system failure in critical security areas.

2) Data Integrity and Privacy: Security facilities handle large volumes of sensitive data, whether it comes from surveillance cameras, motion detectors, or electronic access control systems. This data must not only be securely stored but also protected during transmission to ensure it cannot be intercepted or tampered with. The integration of IoT into these environments requires robust encryption mechanisms and regular security audits to safeguard data protection and comply with regulations like the General Data Protection Regulation (GDPR).

3) Network Stability and Scalability: IoT networks in security facilities must ensure high availability and stable performance. The numerous devices and sensors, which continuously collect and transmit data, put a significant load on network resources. It's not just about whether the network provides enough bandwidth, but also whether it can handle growing demands as more devices are added or existing systems are expanded. Poor network performance can lead to failures of critical security functions, such as real-time monitoring of surveillance systems or the immediate response to security alarms.

CHALLENGES OF REMOTE ACCESS

1) Access Permissions and Authentication: Remote access to IoT systems in security facilities presents an additional challenge. Only authorised personnel should be able to access devices and data, particularly in critical security systems. Reliable authentication and strong access control are essential to ensure that only authorised users can remotely access the network. Multi-factor authentication (MFA) and role-based access controls are common practices that restrict access to sensitive data and systems.

2) Secure Remote Access: As IT systems managed by Prison Real Estate Departments become ever more complex, so consideration needs to be given to providing some form of remote access to allow specialist engineers to log into their equipment within Prisons to diagnose/repair faults.

While remote access enhances flexibility and efficiency, it also introduces risks, especially when connecting through insecure networks. Unencrypted access to the IoT network can create numerous security vulnerabilities. Using Virtual Private Networks (VPNs) and secure access methods like TLS/SSL encryption is essential to ensure that remote maintenance and management tasks do not compromise security standards.

3) Real-Time Monitoring and Response Times: Security facilities rely on real-time monitoring to respond quickly when necessary. Remote access to IoT systems must, therefore, be fast and reliable. Delays or failures in accessing security-critical data can prolong response times and hinder the ability to react to threats promptly. The quality of the network infrastructure and software used plays a crucial role in ensuring continuous and rapid data transfer.

CONCLUSION

Integrating IoT technologies into security facilities brings numerous benefits but also imposes high demands on network architecture and security protocols. The challenges related to security, data privacy, network stability, and secure remote access must be carefully addressed to ensure the integrity and availability of systems. Only by employing robust security mechanisms, well-planned network infrastructures, and comprehensive control over remote access can the full potential of IoT in security-sensitive environments be realised.

10. NEW ICT CONSIDERATIONS

Technology and its use within prisons is constantly evolving and therefore this penultimate chapter provides a brief commentary on some of the relatively new and emerging ICT solutions which the broader prison community and individual prison systems needs to carefully consider over the coming years.

10.1 CONCEPT OF SMART PRISONS

This terminology relates to the provision of ICT systems which facilitate a range of interactive prisoner services.

'Smart' currently has different meanings depending on the context it is used across different jurisdictions. Some use the terminology to define digital services that are accessed directly from workstations within cells (using laptops, tablets, PC's or in-cell TV's). Others associate 'smart' with advanced security features to monitor and identify the location of prisoners (biometric solutions) which increasingly involve AI driven components.

Some jurisdictions are developing their own smart solutions focused around a prisoner's daily programme of activities in an effort to support rehabilitation and reintegration of offenders ahead of their release. A common criticism of adopting smart technologies is that they lessen traditional face-to-face contacts which can help support a healthy prison agenda. However, there are those who argue that on the contrary they make staff workflow faster and smoother and better prepare individuals for life after release (encouraging prisoners to independently gain essential skills and support their wider well-being by enabling them to make video calls, access the internet and use e-mail services).

Whatever solution is decided upon it will be important to clearly define and carefully assess what devices and services are appropriate for the environment in which they are to be set. This is particularly true whenever they are intended for use within closed prisons. Importantly, if 'smart' is to be adopted it will be important to ensure a balance between offering a digital solution rather than a face-to-face solution especially when working with vulnerable prisoners.

10.2 ARTIFICIAL INTELLIGENCE (AI)

The adoption and use of AI is still at an early stage. Whilst there may be real benefits in automating the delivery of digital solutions the use and understanding of AI within a prison setting has yet to be fully understood. The Council of Europe recently launched **Ethical and Organisational Aspects of the Use of Artificial Intelligence and related digital technologies by prison and probation services (CM/Rec(2024)5)**.

It encourages a proportionate and carefully considered approach on the use of AI so that it is only used when it can be demonstrated that it:

(1) Contributes to the rehabilitation and reintegration of prisoners; and
(2) Does not replace prison and probation staff (but assists them in their everyday work); and
(3) It helps the criminal justice system measure and reduce recidivism.

At present, the first tentative steps are being taken to use AI related solutions within a prison setting. Its wider adoption will continue to be assessed and evaluated over the coming years. One day it may be commonplace in all prisons, but at present its deployment is being more tightly controlled and introduced gradually on discrete solutions such as breathing control in cells, prisoners monitoring, translation systems, face recognition, scan perimeters and prisoner rehabilitation.

11. CONCLUSION

The seamless integration of ICT within prisons real estates is both a necessary and complex undertaking, driven by the broader digital transformation across society. That's why both EuroPris Expert Groups, ICT and Real Estate, decided to come together and jointly produce interdisciplinary guidelines for modern prisons – an approach to infrastructure planning and digital integration in prisons. Balancing innovation with practical constraints, particularly the physical limitations of older prison structures, can be challenging. While new builds offer opportunities for seamless ICT integration, retrofitting older prisons demands creative, secure, and resilient solutions.

This guide aims to offer a framework for prison authorities to strategically plan, install, and operate ICT systems that will enhance prison security, administration, rehabilitation and prisoners' welfare services. Embracing new innovations in prisons requires a thoughtful, balanced approach, ensuring that emerging technologies are introduced with clear purpose, the provision of ethical safeguards, and a focus on supporting positive outcomes for both prisoners and staff.

Ultimately, the rollout of ICT must be tailored to each national jurisdiction's unique legal, financial, and operational context. Through careful planning, phased implementation, and collaboration with experienced ICT partners, prison systems can harness the benefits of digital technologies while safeguarding institutional integrity. Central to a successful ICT infrastructure is the provision of high-capacity structured cabling, the use of enterprise-grade network equipment, logical separation via VLANs, and advanced protocols like virtual link aggregation. Configuring ICT infrastructure in different European prison systems in this way will ensure the systems long lasting efficiency, reliability, and security.

EuroPris
Bezuidenhoutseweg 20
2594 AV, The Hague
Netherlands
secretariat@europris.org

Co-funded by the European Union