Reliable Connectivity & Cybersecurity for Alarm & Security Systems
Thales Portfolio Overview
MARKET CHALLENGES FOR SECURITY SYSTEM PROVIDERS

Producers of Alarms and Notification Systems, Intrusion Detection Systems (IDS), Access Control Systems (ACS) and Video Surveillance Systems (VSS) face ‘alarming’ challenges. They strive to continuously improve the reliability of their products, adapt to the very latest technologies and manage costs whilst simultaneously streamlining their production, rollout and logistics. Cybersecurity is essential for all technology providers, but it is uniquely crucial for security system providers.

With the need for secure digital communication coupled with the pitfalls of using ‘on-prem’ networks like Wi-Fi, cellular communication has become the primary connection method for security equipment. However, this evolution comes with its own challenges:

- Manufacturers need to address issues such as network availability, technology migration, fragmentation and network sundown whilst guaranteeing service levels, efficiency and secure communications. This is compounded by cost pressures across the lifecycle of the managed security device whilst still being futureproof, easy to install and simple to use.
- 2G and 3G cellular technology sunset announcements require smooth migration paths to advanced 4G and 5G cellular standards, specifically developed for IoT use cases.
- 24/7 connectivity is critical. A security system cannot be considered secure if the connectivity is unreliable or intermittent. Connectivity in advanced security systems needs to be continuously monitored and adapted, if necessary, to ensure maximum effectiveness.

Well-known brands in the IT industry have entered the home automation and security industry, using their mass market appeal to influence the market. Meanwhile, many start-up companies are also finding a niche in an already competitive marketplace. Creative technologies such as Artificial Intelligence (AI) or the use of biometric identification offer further opportunities to providers for differentiation.
Thales’ innovative security solution features help providers differentiate their products and address the challenges of IoT connectivity.

As a world leader in cellular connectivity and SIM technology, Thales has been serving the security industry by delivering industrial cellular module solutions for more than 25 years. Our unique combination of next generation 4G and 5G cellular connectivity solutions complemented by brand-new IoT eSIM technology offers a great opportunity to enable new services, streamline device manufacturing, ease installation, increase maintenance efficiency and shorten time to market.

### Thales solutions overview for security systems providers

<table>
<thead>
<tr>
<th>Reliable Cellular Connectivity Solutions</th>
<th>Seamless IoT Connectivity Activation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="5G LTE" /></td>
<td><img src="image" alt="eSIM" /></td>
</tr>
<tr>
<td>- Cinterion® wireless modules</td>
<td>- Remote subscription provisioning</td>
</tr>
<tr>
<td>- SIMs and eSIMs</td>
<td>- Easy connectivity management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advanced Biometrics &amp; System Integration</th>
<th>Comprehensive Cinterion® IoT Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Biometrics" /></td>
<td><img src="image" alt="IoT Suite" /></td>
</tr>
<tr>
<td>- Biometric authentication</td>
<td>- Trusted identity services</td>
</tr>
<tr>
<td>- Cinterion® SOM platform</td>
<td>- Remote diagnostics &amp; configuration</td>
</tr>
<tr>
<td></td>
<td>- Secure software updates</td>
</tr>
</tbody>
</table>

Thales offers a suite of tools to greatly simplify the management of connected security systems over their entire lifecycle through design, manufacturing, logistics, and rollout. Efficient ongoing maintenance of the installed base in the field helps ensure ongoing efficacy.

For ‘feature rich’ security products, the System on Module offers a platform to embed Thales’ own award-winning biometrics solutions, touchscreen, cameras and additional connectivity standards in a single package.
Thales offers innovation along the entire product lifecycle

- Manage your Devices Remotely
- Design for Advanced Security
- Benefit from Network Evolution
- Reduce your Time to Market
- Improve your Supply Chain and Delivery
- Streamline your Logistics and Roll-outs
- Thales Building a future we can all trust
Secure data transmission is crucial in today’s market and end-customers’ privacy concerns have increased. If ‘rogue parties’ were to discover a weakness in any IoT connected security system, they would have a huge advantage to remotely monitor and enter a location, cause continued false alarms or gain access to the identities of legitimate users. These breaches could cause damage, reputation loss and potential financial penalties to the security system provider.

At Thales, we know cybersecurity is a complex challenge, even for security companies. Recognised as a leader in digital security for decades, we offer end-to-end cybersecurity services, going from state-of-the-art consulting, penetration testing for system designers, secure device ID generation and credential management for security devices’ long years of operation.

Thales enhanced cybersecurity offering

Evolving networks and security standards are driving the need to design for secure and remote software updates. Thales ‘Cinterion IoT Suite’ platform includes a ‘Software Updates’ feature delivering an automated, secure, encrypted software update campaign, simultaneously, across large and globally distributed fleets. This helps enterprises proactively and cost effectively control the lifecycle of device firmware.

Thanks to Thales’ proven track record in serving the most demanding markets (banking, government and public sector), we provide the best security foundation for your business.

BENEFIT FROM NETWORK EVOLUTION

Whilst the sunset of 2G/3G was originally a source of concern for many device manufacturers, the rise of 4G and 5G cellular networks provides a world of new opportunities. From highly efficient low power standards to high-speed, low latency connections, 4G and 5G networks support new business opportunities for connected security system providers:

- Low power remote sensors
- Advanced video surveillance with smart video analytics
- Biometrics
- Advanced security levels
- New cloud interworking
But the plethora of new standards has caused a degree of uncertainty for security device manufacturers. When selecting a suitable cellular technology and module device, it is important to consider both current and future cellular standards, technology variances and support from network operators when planning your future roadmap. Today’s designs need to allow for a future transition to a 5G environment.

Thales partners with its customers to ease technology migration, ensuring a smooth transition to new technology as it becomes available. Our Cinterion cellular modules are delivered with a futureproof roadmap, a product family concept and footprint commitment, for ease of use with regional network standards or new variants.

Evolving network standards creating growth for the security IoT market

**High Data Speed**

- LTE
- 5G

**Mid-Speed IoT**

- Smart, Cloud based

**Low Bandwidth**

- Power Efficiency & Enhanced Coverage

- LTE-M
- NB-IoT

**Mission Critical IoT**

- Ultra Low Latency & Highest Reliability

- 5G

**REduce your time to market**

Choosing the right connectivity solution partner helps security system providers accelerate connectivity integration and reduce their time to market.

Thales’ unique expertise lessens the challenge of integrating communication into the security market, delivering the highest Supplier Lifetime Value to our customers.

We partner with key industry players to offer best-in-class, certified services to our customers:

- All major network operators globally
- Network and test equipment providers
- Standardisation IoT bodies

Furthermore, our global presence and local setup help shorten all your deployment steps from device design to production through:

- Dedicated teams of experts for value added support
- Precertified cellular solutions
- Comprehensive documentation and developer tools
- Thales flexible and unique Cinterion Embedded Processing
Advanced security solutions such as Thales Biometrics are pre-integrated in our cellular solutions (System on Module/SOM) to provide features like fingerprint-, facial- and voice recognition. We leverage the device OS, memory, processing power and GPU to host these applications directly on our cellular modules. All this shortens your development time and efforts whilst reducing costs.

IMPROVE YOUR SUPPLY CHAIN AND DELIVERY

At Thales, we understand the complexities and demands of an industrial marketplace. Short lead-times and continuous supply needs are increasingly gaining importance. Security device providers can benefit from Thales multi-factory and multi-sourcing strategies, ensuring a robust supply chain as well as long-term product availability.
Cellular connectivity offers inherent advantages for security systems when compared to alternative technologies such as Wi-Fi. A self-contained alarm panel, which operates outside on-prem networks, reduces the attack surface and simplifies the communication path.

However, the use of cellular networks means security device manufacturers need to handle SIM card logistics and cellular network registration during installation plus they must ensure the equipment remains connected throughout its active life.

### Simplified device manufacturing and connectivity deployment

Thales new Connectivity Activation solution is now available, revolutionising the way devices are manufactured, installed and remotely maintained during their operational lifetime.

![Seamless Connectivity Activation](image)

Thales has made this possible by creating the IoT eSIM, which is literally an empty shell into which you can easily inject your selected mobile network operator (MNO) subscription at any time – during manufacture, installation, or throughout the device lifetime. It can be changed automatically, at any time, under your control.

Technicians no longer need to test signal strength on-site while devices are deployed. At the time of installation, the powered-up device performs a network scan, reports the results to the Thales IoT Suite using Bootstrap Connectivity, and the most suitable MNO subscription is selected and downloaded automatically. This subscription selection can be based on signal quality measurements on site, remotely adjustable, individual parameters, or different contractual conditions with your MNOs. Each specific device in your fleet will automatically download the MNO profile that suits the device location best.

### Trusted enrolment to cloud platforms & credential management

If security devices require a trusted identity validation for secure enrolment in IoT clouds, such as Azure or AWS, the Thales Trusted Identity Services offer Device Identity lifecycle management. This includes the most secure pre-injection, remote rotation, transfer or revocation of keys and credentials through a single pane of glass. The strong security foundation ensures trusted enrolment of legitimate devices to private or public clouds whilst securing lifecycle updates performed remotely over-the-air. The requirement for onsite support by maintenance teams is greatly reduced, leading to significant cost savings, particularly for large, geographically dispersed fleets.

![Streamline your device logistics and roll-outs](image)

1. **Identity Generation**
   - Injection of unique trusted identities and IoT hub certificates (for the major clouds) during IoT module manufacturing

2. **Identity Provisioning**
   - Definition of business rules to automate and secure devices enrollment into targeted IoT cloud(s)

3. **Lifecycle Management**
   - Over-the-air credential management throughout the device lifecycle:
     - Certificates revocation / rotation / update
     - Application signing & verification
Whether you offer do-it-yourself installation or managed services for your customers, the hassle of repeated manual updates or unnecessary service trips by installation technicians needs to be avoided.

The Thales Device Performance Services provide improved visibility of your installed base of devices to help your operations team track status, performance and network-related information via automated notifications in real time.

Anomalies and connectivity issues can be detected, and corrective actions taken, before they impact your business. The Thales IoT Software Update Services provide remote configuration capability to optimise your device and communication settings in the field. The set of services is operated by an efficient update campaign manager, pushing secure software updates whenever needed. It also provides incremental software updates over-the-air (FOTA) to support longer device battery life, lower connectivity costs and faster updates.
THALES TO SUPPORT YOUR CONNECTED SECURITY DEVICES

Thales’ 24/7 cellular connectivity modules, IoT eSIMs, advanced security expertise, and device lifecycle management platform offer a comprehensive solution that helps security system providers ensure their customers are ready to leverage the innovations of today and the future.

Contact us today to learn how we can support your security devices’ connectivity and cybersecurity deployments for the following fields:

- Alarms and Notification Systems
  (cellular connected home & professional security solutions, supporting video, messaging and voice communications)
- Comprehensive Home Automation IoT Systems
- Smart Video Surveillance Systems
- Intrusion Detection Systems (IDS)
- Access Control Systems
  (biometrics identification, electronic locks, smart locks, control cameras, etc.)

For more information, visit our webpage.