SELECTING THE RIGHT EMBEDDED HARDWARE – A GUIDE FOR DEVELOPERS

How F&S and NXP Empower Developers for Scalable, Secure and Long-Life Design

F&S Elektronik Systeme GmbH has a long-standing and close technology partnership with NXP Semiconductors. As a certified **NXP Gold Partner**, F&S collaborates directly with NXP on both technical and strategic levels to deliver high-quality embedded solutions.

This partnership ensures early access to new NXP processor families, reference designs, and documentation, which enables F&S to provide its customers with state-of-the-art embedded platforms that are future-proof and production-ready.

F&S Elektronik Systeme NXP

Exclusive Use of NXP CPUs

F&S exclusively integrates NXP i.MX Applications Processors across its entire product portfolio, including the popular i.MX 6, i.MX 8, and the latest i.MX 9 series. This exclusive focus ensures:

- Deep technical expertise with NXP architectures
- Faster integration of new NXP features (e.g., **EdgeLock® Secure Enclave**)
- Long-term support and lifecycle stability
- Seamless scalability across CPU generations

Whether customers choose a ready-to-use Single Board Computer (SBC) or a highly customizable System-on-Module (SoM), they benefit from a hardware and software ecosystem that is fully aligned with NXP's roadmap.

By leveraging this close cooperation, F&S helps developers reduce development time, meet regulatory and security requirements faster, and bring robust embedded products to market more efficiently.

From UX to Security – Tackling the Key Challenges in Embedded Platform Selection

Modern embedded systems face diverse requirements: graphical user interfaces, wireless connectivity, energy-efficient 24/7 operation, real-time processing, and increasingly stringent IT security demands. The choice of hardware platform not only affects technical performance but also development effort, time-to-market, certification processes, and long-term maintainability. For embedded engineers, a central question arises: How can a well-founded, future-proof, and economically viable decision be made when selecting a CPU, module, and overall system? This article is aimed at developers and technical decision-makers facing a selection decision for an embedded platform. F&S, in close collaboration with NXP, delivers scalable, secure platforms that help developers bring industrial and commercial devices to market faster.

The goal is to present the most important technical, regulatory, and economic influencing factors—without focusing on specific manufacturers but illustrated with examples from common platforms, such as the NXP i.MX application processors..

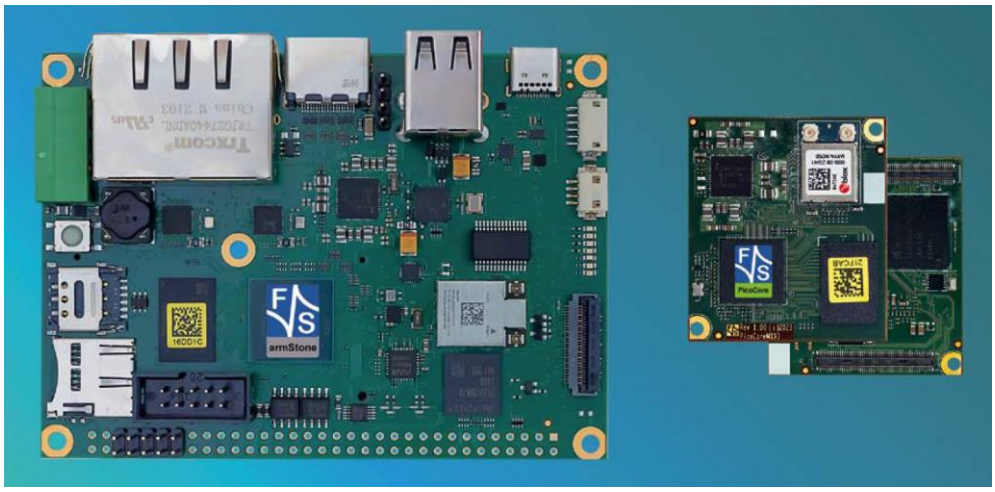

Figure 1 Size comparison of a single-board computer from the armStone series in Pico-ITX format and a pluggable computer-on-module from the PicoCore series measuring 35 mm x 40 mm, both by F&S. (Image: F&S)

Processor Selection as a Central Decision Criterion

The selection often begins with the processor. Nowadays, numerous platforms are available—with various architecture variants (e.g., ARM Cortex-A/M, RISC-V), performance levels, energy profiles, and supported interfaces. Processor families like NXP i.MX, are established in many embedded projects and offer scalable platforms for different application classes. Choosing within these families allows addressing various requirements (performance, security, energy) on a compatible platform level—e.g., through pin-compatible SoMs. From the example of the i.MX CPU families listed in Table 1, some typical questions can be derived: What are the application's requirements for graphics performance, peripheral integration, energy consumption, and security features? How can the design be maintained and expanded in the long term?

Table 1 Specific features and typical applications

CPU Series	Typical Applications	Special features
i.MX 6ULL / ULP	Ultra-low power devices, controllers, wearables	Mostly without GPU, very energy-efficient
i.MX 7 / 8M Nano / Mini	HMI systems with medium display requirements	MIPI/LVDS, Linux or RTOS capable
i.MX 8M More	Local AI applications (e.g. camera, speech recognition)	Integrated NPU, 3D GPU and VPU
i.MX8ULP	Battery-powered applications with good graphics performance	GPU und VPU, ULP, E-Paper Interface
i.MX 8X	Safety Applications, Automotive, Multi-Display Systems	Dual LVDS with different content possible
i.MX 9-Series	Security-by-Design Applications	EdgeLock® Secure Enclave, TrustZone, Cortex-A55, LPDDR4x

And how do software availability and ecosystem impact project success? Two typical application scenarios from the industry are outlined below: ➔Human-Machine Interfaces (HMI): Systems with touch displays and graphical interfaces. Here, graphics performance, response time, and usability are paramount—often complemented by requirements for design freedom and multimedia interfaces. ➔Industrial controls with displays (TFT or E-Paper): Devices where the display primarily serves status indication—e.g., in building automation, medical technology, or industry. Requirements like low energy consumption, robust communication, EMC compliance, or protection class often dominate. The hardware platform must not only be functional but also sustainable throughout the product lifecycle—technically and commercially. F&S offers a broad range of SoMs and SBCs all based on the NXP i.MX family, including i.MX 8M Plus, i.MX 93, and the i.MX 9 series, supporting everything from entry-level HMI to secure, AI-enabled industrial devices.

Choosing a processor family like NXP i.MX not only ensures technical scalability, but also benefits from NXP's proven long-term availability strategies, extensive ecosystem, and continued investment in embedded innovation.

Realistically Assessing System Requirements

When selecting a suitable embedded hardware platform, a systematic assessment of technical requirements is crucial. Wrong decisions often lead to oversized, inefficient, or poorly maintainable systems. The following outlines key technical factors.

A major decision driver is the required computing power. This depends not only on the application itself but also on hidden factors such as software architecture, real-time requirements, or multitasking capabilities.

Typical performance-related questions include:

- Will an operating system like Linux be needed, or is a bare-metal approach sufficient?
- Will multimedia content (video, audio) be processed?
- What latency and response times are essential?
- Is a separation of HMI and the core application logic required (e.g., Cortex-A + Cortex-M combinations)?

Modern processors offer a wide range: from energy-efficient single-core ARM Cortex-A7s with a few hundred MHz to multicore variants with several GHz, dedicated real-time cores, and integrated GPU/VPU.

However, benchmarks are not always the decisive factor. Power consumption in idle or partial load states is often more relevant, especially for battery-powered devices.

In some applications—e.g., image or speech recognition, predictive maintenance, or object detection—AI at the edge is playing an increasingly important role. Processors with an integrated NPU (Neural Processing Unit), such as the i.MX 8M Plus with 2.3 TOPS, or CPUs with optimized GPU architectures, offer advantages. However, integration is not trivial. Common stumbling blocks include:

- Support for frameworks (e.g., TensorFlow Lite, ONNX, PyTorch)
- Format and memory compatibility (e.g., INT8 quantization)
- Drivers and runtime environments for the target platform
- Toolchains for model conversion

An embedded system with AI support often requires close collaboration between hardware development, software engineering, and data science. Developers often feel pressured, as management, marketing, or sales demand AI features without a clear use case—similar to the multitouch hype a few years ago.

F&S's PicoCoreMX8MP, powered by the NXP i.MX 8M Plus, integrates an NPU and supports TensorFlow Lite and Yocto-based BSPs to simplify AI-at-the-edge deployment.

Display Interface Considerations

Display connection is another key factor. Depending on size, resolution, and colour depth, different requirements arise for the processor's graphics unit and physical interface. Common Hardware Interfaces include:

- Parallel RGB: inexpensive, simple, but resolution-limited
- LVDS: robust, noise-resistant point-to-point connection, common in industry
- MIPI-DSI: compact, high bandwidth – ideal for small, high-resolution displays
- HDMI/eDP: for large or external screens, but rare in embedded environments

Additional considerations include:

- Can the processor support multiple displays with different content simultaneously?
- Is capacitive touch integration required (USB, I2C, or SPI)?
- Are software libraries (e.g., LVGL) natively supported?

Display choice and interface impact power consumption, EMI (electromagnetic interference), and thermal design. A well-priced and long-term available display might not be compatible with the intended CPU due to interface mismatches.

Even seemingly trivial questions about display size and resolution have far-reaching consequences:

- RAM requirements: an 800x480 display needs ~1.5 MB per framebuffer at 24-bit color depth
- Graphics bandwidth: higher resolution increases internal bus load
- Touch precision: increases with larger displays
- User interaction: multitouch, gesture control, or on-screen keyboards affect usability

A too-small display hinders usability; too large a display may require oversized hardware, including power and thermal components.

Peripheral Interfaces and Connectivity

Standard industrial interfaces (UART, I2C, SPI, USB) are available on nearly all platforms. More critical are the number of interfaces and their pin configuration flexibility.

Key questions:

- Are multiple serial devices needed simultaneously?
- Are galvanic isolations required (e.g., RS-485)?
- Is CAN or CAN FD mandatory?
- Is 10/100 Mbps Ethernet sufficient, or is Gigabit Ethernet required?
- Is a PCIe slot needed for extensions?

Especially with SoM-based designs, it must be carefully checked whether all required interfaces are available on the carrier board or if limitations apply. Some

interfaces can be configured via device tree settings, but this may conflict with the chosen SoM form factor.

Wireless Communication and Integration

Many modern embedded systems require wireless communication: WLAN, Bluetooth, LTE, NB-IoT, LoRa, ZigBee, Thread, Matter—the list is long. Often, the decisive factor is not the technology but certification and integration capability.

What to check:

- Is a radio module with preconfigured drivers and certification used?
- Is an external antenna required (e.g., for medical devices)?
- How is antenna geometry integrated into the enclosure?
- Are OTA updates planned to close security gaps?

In most cases, an integrated and pre-certified wireless module is the safest choice—despite higher costs—as it already complies with CE, FCC, or IC, and saves development time.

F&S platforms combine NXP CPUs with pre-certified wireless modules tested for optimal coexistence, enabling faster integration of Wi-Fi, BLE, and cellular standards.

Security Requirements – Now Mandatory

Previously considered optional, security is now a legal requirement. Regulations such as the EU Cyber Resilience Act (CRA), RED require manufacturers to implement protection mechanisms at the hardware level. The Radio Equipment Directive (RED) is a European regulation that governs various aspects of radio equipment, including cybersecurity. Starting from August 2025, the cybersecurity-related provisions in Article 3.3 (d), (e), and (f) of RED become mandatory.

Compliance with these RED requirements can be demonstrated by applying harmonised standards—most notably the EN 18031 series. Thus, meeting EN 18031 effectively means fulfilling the cybersecurity obligations of RED Article 3.3.

Typical hardware security features supporting conformance claims include:

- Secure Boot and Chain-of-Trust
- Encrypted flash memory regions
- Secure key storage (e.g., TPM or Secure Enclave)

- Secure firmware updates (signed, fail-safe)

Modern processors often support such features, but correct implementation is complex. The key is integration into the entire system.

SoCs such as NXP's i.MX 9 series offer integrated security features like Secure Boot, Enclave, and the Edge Lock Secure Enclave, which supports tamper detection, key isolation, and cryptographic services—making regulatory compliance more attainable.

Real protection is possible only if properly configured and maintained. Here NXP and F&S collaborate closely.

Thermal Design and EMI

In fanless 24/7 systems, heat dissipation is a central issue. Even seemingly energy-efficient CPUs can consume 3–5 W under typical loads, which can be critical in small enclosures without active cooling.

Checklist:

- Is a heatsink, housing contact, or active cooling required?
- How is heat dissipated – heat spreader?
- Is temperature monitoring available on the CPU?
- What happens during thermal overload (throttling, shutdown)?

A solid thermal concept increases reliability, extends service life, and prevents late design changes.

EMI (electromagnetic interference) is a common hurdle in projects. The hardware platform choice already affects shielding and interference suppression options.

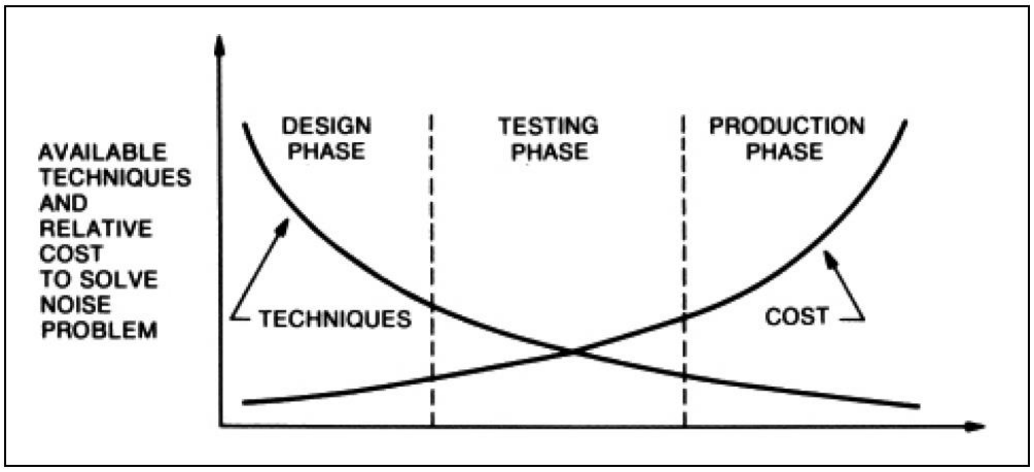

Figure 2 The earlier topics like EMC are considered in a project, the lower the cost of any necessary measures.

Key factors:

- SoM pin layout (e.g., twisted pairs, dedicated grounding)
- Display connection type (LVDS vs. parallel)
- Clock signal routing and decoupling capacitors
- USB, Ethernet, CAN layout—with or without magnetics
- Number and location of ground points

Addressing EMI early in the project is cheaper and more flexible, as illustrated by the "Ott graphic."

Comprehensive Hardware Evaluation Requires an Interdisciplinary Approach

Evaluating embedded hardware is a multidisciplinary task—it goes far beyond CPU benchmarks. Graphics performance, interfaces, wireless connectivity, security, and EMI all influence one another. A structured requirements analysis helps identify the optimal platform.

Especially in embedded systems, stability, maintainability, and feasibility often outweigh maximum performance or lowest cost.

Economics and Strategy – Between Time-to-Market and Total Cost of Ownership

While technical criteria define the feasibility of an embedded design, economic and strategic considerations determine the long-term viability of a project. In markets with long product life cycles, extensive approval procedures, or tight margins, planning security and flexibility are just as important as performance or energy efficiency.

In the security domain, the focus has traditionally been on acquisition cost. However, with emerging cybersecurity regulations like CRA, RED, and the US Cyber Trust Mark, it's increasingly clear that security must be maintained throughout the product lifecycle. As a result, total cost of ownership (TCO) is now shaped not only by initial cost but also by ongoing costs for vulnerability prevention, monitoring, and timely mitigation.

One of the most fundamental decisions is the architecture of the hardware design:

- Should a complete embedded platform as an SBC (Single Board Computer) be used,

- Or should a System-on-Module (SoM) combined with a custom carrier board be chosen?

Advantages of an SBC:

- Ready to use – ideal for prototypes and small series
- Often already certified (EMC, wireless)
- Minimal hardware development effort

Advantages of a SoM:

- Maximum design freedom for the carrier
- Better integration of customer-specific peripherals
- Lower risk during CPU changes (e.g., due to obsolescence)
- Often longer availability than complete SBCs

The strategic timeframe is decisive:
A SoM-based approach is more suitable for scalable, long-life products with multiple variants—despite the higher initial complexity.
For short-term market launches or proof-of-concepts, an SBC may be the more pragmatic choice.

Software Quality as a Success Factor

In practice, many platforms fail not due to CPU limitations but due to poorly maintained or immature Board Support Packages (BSPs). Even powerful CPUs become worthless without clean integration into embedded Linux or RTOS.

In this context, product quality is no longer defined solely by reliability. Compliance with cybersecurity regulations now requires products to be free from known vulnerabilities, making security an essential component of overall quality.

Key questions regarding the software base:

- Is the BSP actively maintained and patched for security?
- Which Yocto version underpins the Linux system?
- Are there long-term support (LTS) options for kernel and middleware?
- What about boot time, real-time capabilities, or OTA readiness?
- Is there a defined testing strategy for new releases?

A well-maintained BSP drastically reduces integration, testing, and maintenance efforts. Look for:

- Availability of device tree overlays
- Documentation quality
- Responsive support

Vendors who offer regular updates and maintain upstream compatibility enable long-term product stability—even across multiple CPU generations.

The Yocto-based BSPs provided by F&S are closely aligned with NXP's official releases and benefit from early access to patches and long-term kernel support.

Regulatory Requirements – From RED to CE to Industry-Specific Norms

Many embedded systems must comply with a wide range of regulatory requirements, including:

- CE marking in Europe
- FCC approval in the USA
- EU Machinery Directive
- MDR (Medical Device Regulation)
- Wireless certifications
- Medical standards (e.g., EN 60601)
- Railway standards (e.g., EN 50155)
- Automotive safety (e.g., ISO 26262)

The hardware platform has a significant impact on achieving compliance. Key aspects to consider include:

- Does the vendor have proven experience with regulatory and safety-critical markets?
- Are wireless modules pre-certified?
- Is there EMC-compliant layout support (e.g., reference designs)?
- How is the system protected from tampering and unauthorized access (Security by Design)?

Cyber-safety is an emerging focus: Regulatory frameworks like CE, FCC, ISO 26262, and MDR are increasingly requiring manufacturers to adopt a strong security posture to ensure the safety of their products throughout the lifecycle. Security is becoming inseparable from safety.

Note: Many certifications also demand full lifecycle documentation and control of all components and software versions. Hardware platforms with strong lifecycle and security management capabilities can significantly reduce both time and cost in achieving compliance.

Securing the Supply Chain

Recent years have highlighted how vulnerable embedded projects are to global supply chain disruptions, such as:

- Extended lead times for CPUs
- Shortages of power management ICs (PMICs)
- Limited availability of memory components

These disruptions carry not only commercial and operational risks, but also potential legal and reputational consequences—especially for safety- and security-critical products.

A secure and resilient supply chain is increasingly becoming a regulatory requirement. Frameworks such as the EU Cyber Resilience Act (CRA) and the US Cyber Trust Mark emphasize the importance of maintaining control over component sourcing and ensuring supply continuity throughout the product lifecycle.

To mitigate these risks, consider the following best practices:

- Choose platforms with long-term availability (10+ years)
- Select variants with flexible memory or package options
- Require transparent lifecycle and end-of-life (EOL) communication
- Ensure qualified second-source options, such as pin-compatible System-on-Modules (SoMs)

Also, prioritize processors used across multiple assemblies or product lines to improve flexibility and leverage in times of scarcity.

Total Cost of Ownership vs. Unit Price

The per-unit cost of a processor or module is visible—but not the decisive factor. Total Cost of Ownership (TCO) includes all effort across the entire product lifecycle.

Typical hidden costs:

- Software maintenance, patching, CVE monitoring
- Development time for custom carriers or BSP adaptation
- Certification costs (e.g., for Wi-Fi or LTE)
- Redesign due to obsolescence or performance issues
- Internal effort for security, logging, and OTA management

A system with a higher initial price, but with a robust toolchain, support structure, and update capabilities, can be more cost-effective in the long term than a cheaper platform with high integration and maintenance overhead.

Importantly, running costs must also be considered—especially in relation to patching and mitigating vulnerabilities. The ability to maintain a secure software supply chain throughout the product lifecycle has a direct impact on total cost of ownership and compliance.

Scalability and Platform Strategy

Many embedded projects begin with limited requirements but evolve over time—whether through feature upgrades, product variants, or entry-to-premium product lines. A scalable hardware platform enables this growth by offering a range of performance and feature levels within a consistent system architecture.

Examples of effective scalability include:

- Pin-compatible modules with different CPUs
- A shared carrier board supporting multiple performance classes
- A unified BSP (Board Support Package) across various platforms
- Variants with or without GPU, NPU, wireless connectivity, or scalable memory options

A strong platform strategy enhances reusability, reduces development effort for new variants, and supports a modular and cost-effective product approach. From a regulatory perspective, it also simplifies compliance: when multiple

products share a common hardware and software base, manufacturers can reuse evidence for conformance (e.g., test reports, risk assessments) across product variants—saving time and effort when demonstrating compliance for each model, from entry-level to premium.

F&S Elektroniksysteme supports this approach with both SBC families (e.g., armStone) and modular SoM solutions (e.g., PicoCore series), enabling scalable and future-ready embedded designs.

The Human Factor – Working with the Right Partner

The success of an embedded project depends not only on the hardware's quality but also on the quality of the collaboration with the vendor. Technical expertise, support availability, response times, and transparent communication are often more critical than datasheets or benchmarks.

Key factors:

- Are there direct technical contacts?
- Is the support workflow documented (e.g., ticketing system)?
- Are customizations supported (e.g., carrier boards, BSP tuning)?
- Are trainings or workshops available?

Some vendors actively support customers for years; others may be unresponsive or slow.
Embedded engineering is a team effort—including the hardware partner.

Strategic Outlook – Future-Proofing Embedded Projects

The business perspective on embedded hardware is just as important as the technical one.
Short-term thinking or focusing only on datasheet values can lead to long-term dead ends—whether in software maintenance, supply security, certification, or variant development.

Strategic foresight and careful platform selection always pay off, even if more effort is required upfront.

Real-World Examples – Lessons from Practice

Example 1: HMI Device with 7-Inch Capacitive Touch and Wi-Fi

Application:
Wall-mounted smart-home control panel with responsive UI, integrated Wi-Fi, and moderate cost.

Technical Requirements:

- 7" TFT with capacitive touch (1024 × 800)
- Local Wi-Fi (no cloud dependency)
- Wake-on-touch, energy-efficient standby
- User-friendly UI based on LVGL
- OTA update capability
- CE and wireless certification

Implementation:
Used an ARM Cortex-A55 SoM with RGB display and pre-certified Wi-Fi/BT module. BSP: Yocto LTS 5; touch via I2C. The decision to use the NXP i.MX 93 was driven by its optimal balance of performance, power-saving modes, and native support for RGB displays.

Focus: low heat generation and solid EMC design.

Lessons Learned:

- Pre-certified wireless module saved >8 weeks in testing.
- Native RGB support from i.MX 93 reduced EMC problems.
- CPU sleep modes worked reliably: >90% standby time.

Result:
Economically and technically successful. From kickoff to production: under 12 months.

Example 2: Control Unit with 2.7-Inch E-Paper, CAN, and 10-Year Lifetime

Application:
Control unit for decentralized sensor boxes with long battery life and CAN communication.

Technical Requirements:

- Ultra-low-power E-paper (128 × 296 px)
- i.MX 8ULP with Cortex-M33 and dual Cortex-A35
- Galvanically isolated RS-485, CAN, and digital I/Os
- Operating range: -30 °C to +85 °C

- No wireless or multimedia required

Implementation:
Selected i.MX 8ULP CPU capable of direct E-paper driving.
Boots minimal Linux for setup, then enters ultra-deep sleep.

Lessons Learned:

- Power consumption was initially underestimated (e.g., power LEDs, LDOs with high IQ).
- E-paper refresh caused unexpected EMC spikes—layout redesign was needed.
- Secure Boot was added late—caused significant extra effort.

Result:
Technically feasible but economically tight. Earlier power and security planning could have saved time.

Common Mistakes in Practice

1. Overdimensioned CPU
   "Better safe than sorry" often leads to oversized CPUs—more power, layout complexity, software load, and EMC risk.
2. Wireless integration without certification strategy
   Starting without CE/FCC planning leads to delays. Custom antennas often fail due to EMC or poor placement.
3. Underestimating software maintenance
   Initial BSPs are often snapshots. Later updates (e.g., CVEs, kernel changes) reveal gaps in maintenance.
4. EMC addressed too late
   First prototypes may pass by chance; second revision fails due to poor grounding, shielding, or signal routing.
5. No scalability plan
   When variants are needed, the SoM or carrier doesn't support extensions (PCIe, USB host, more GPIOs).

Regulatory Overview – RED, CRA, and EN 18031

Cybersecurity regulations are becoming a core requirement for embedded systems, with several major frameworks shaping the compliance landscape in the EU:

RED Directive & EN 18031

The Radio Equipment Directive (RED) applies to wireless-connected devices and introduces mandatory cybersecurity requirements under Article 3.3 (d), (e), and (f)—effective from August 2025. These include:

- Secure Boot to prevent unauthorized software
- Protection of personal data
- Prevention of unauthorized communication or manipulation

To demonstrate compliance, manufacturers are expected to follow the EN 18031 series of harmonised standards, which define the technical framework for:

- Cryptographic protections
- Role-based access controls
- Secure update mechanisms
- Hardware and software integrity protection

Cyber Resilience Act (CRA)

The CRA establishes EU-wide cybersecurity rules for all "digital products with elements of software." Key obligations include:

- End-to-end secure system architecture
- Regular security updates for a minimum of five years
- Vulnerability and CVE management processes
- A formal Declaration of Conformity by the manufacturer

Conclusion:
Cybersecurity is no longer optional—it is a matter of regulatory compliance and product liability. Manufacturers must adopt secure development practices, maintain lifecycle support, and ensure readiness for audits and conformity assessments.

Security Architecture Principles – Secure by Design

A secure embedded system begins with hardware architecture—not software.

Key Elements of a Secure Embedded System

Building a secure embedded platform requires not only design-time hardening, but also robust support for manufacturing, deployment, runtime protection, and incident recovery. NXP offers an integrated security approach that complements regulatory requirements such as RED, CRA, and EN 18031.

Secure Manufacturing and Provisioning

- Encrypted firmware and key installation at production stage
- Secure debug and configuration interfaces to prevent leakage or misuse
- Remote key provisioning for scalable, cloud-integrated deployments

Platform Integrity and Boot Chain

- Signed bootloader (Secure Boot) to verify firmware authenticity
- Measured boot and runtime software attestation to detect tampering
- Hardware Root of Trust (e.g., TPM, Secure Element, Secure Enclave)
- ARM TrustZone® and enclave isolation for trusted execution environments

Software Isolation and Minimal Footprint

- Separation of kernel and user-space domains
- Minimal software footprint by removing unused drivers and daemons
- SBOM reduction to simplify vulnerability management
- Disk and memory encryption, both internal and external

Secure Update Mechanism

- Signed OTA updates with rollback protection
- Fail-safe update handling to ensure recoverability
- Secure remote configuration and key management for lifecycle adaptability

Data Protection and Connectivity

- Encryption of sensitive configs, keys, and logs

- Secure key storage via HSM, SE, or SoC-integrated mechanisms
- Device attestation and origin verification
- Secure and accelerated networking with encrypted communication

Incident Response and Recovery (Cyber Resilience)

- Tamper detection and monitoring of critical regions
- Battery-backed security monitoring for post-breach analysis
- Cyber resilience and recovery mechanisms to restore system trust

By aligning embedded designs with both regulatory mandates and NXP's security capabilities, F&S can establish a secure foundation from development to field operation—covering compliance, lifecycle cost, and product liability.

Modern Embedded Security Features

Modern CPUs like the NXP i.MX 9 series with EdgeLock Secure Enclave include:

- Secure Boot
- Hardware Unique Key
- TrustZone®
- Secure Enclave (for crypto/keys)
- JTAG Lock
- eFuses/OTP (e.g., boot configuration)

Conclusion – Navigating the Embedded Jungle

Choosing the right embedded platform today is a complex, multi-dimensional task.
Engineers must balance technical needs, regulations, economics, and strategy.

What is required:

- Solid requirements analysis—early and thorough
- Processor selection based on system architecture—not gut feeling
- Early integration of security and EMC into design
- TCO thinking, not just price per unit
- Long-term thinking in Make-or-Buy decisions

- Robust lifecycle and supply chain strategies

Engineers today are no longer just developers. They are architects, security leads, integrators—and strategists.

Embedded systems are becoming smarter, more connected—and more vulnerable.
Expectations are rising for UX, performance, and OTA capabilities.

Trends Shaping the Future

- Security by Design becomes mandatory—regulatory and economic.
- Edge AI becomes more specialized—not every system needs an NPU, but many benefit from local inference.
- OTA becomes essential-software evolves, and so must the product.
- Platform strategies win-those with modular architectures and partner ecosystems will thrive.

With its forward-looking CPU roadmap, security-first architecture, and edge-ready platforms, NXP is a key enabler of embedded product evolution.

F&S Elektronik Systeme sees itself not just as a module vendor, but as a long-term engineering partner enabling customers to develop robust, scalable, and future-proof embedded products—from prototype to certified series. With F&S hardware and NXP processors, engineers gain a clear path through complexity—delivering smarter embedded products, faster.

Contact:

Dipl.- Ing. (TH) Andreas Kopietz

Sales Manager

F&S Elektronik Systeme GmbH

Untere Waldplätze 23

D-70569 Stuttgart
Mobile: +49 173 6407845
kopietz@fs-net.de