Industry Paper

From Manufacturers to Manufacturers

Obligations and Opportunities for Technical Building Systems and Building Automation and Control Systems Manufacturers under the Cyber Resilience Act

Version 1 - June 2026

The current version of this digital document can be found at
https://doi.org/10.5281/zenodo.20506150

Audience, context, and disclaimer

This industry paper is addressed primarily to manufacturers of Technical Building Systems (TBS) and Building Automation and Control Systems (BACS), from SMEs to large enterprises. Its purpose is to provide high-level, practical, non-binding guidance and to support a common, association-backed interpretation of the Cyber Resilience Act (CRA) as it applies to TBS/BACS products. The paper is based on official European Commission materials and on the meeting minutes of the industry working roundtable held on 14 October 2025.

The information may become outdated, incomplete, or inaccurate over time, and the supporting associations do not guarantee its completeness, accuracy, or reliability. Readers should seek professional advice where needed.

The supporting associations and their members are not responsible for actions taken based on this document. Stakeholders in the TBS/BACS sector are not bound by its content, which does not constitute a commitment and has no binding effect.

This document is not binding for economic operators or other actors subject to the CRA, it is not legal advice and does not replace the CRA legal text or formal guidance; in case of doubt, the CRA and authoritative interpretations of the Court of Justice prevail. Each manufacturer remains responsible for its own compliance decisions and evidence.

A case-by-case assessment will always be necessary to account for the specifics of each individual case.

To improve readability, generative AI tools supported the editing and drafting process; however, the substance was reviewed, discussed, and agreed in collaboration with the participating associations. The associations listed on the cover page contributed in different ways to the formulation and drafting of this document, and we thank them for their commitment and constructive cooperation. These contributions were coordinated by Salvatore Cataldi (Liaison Officer between CEN/TC 247 and CEN-CENELEC/JTC 13 WG9, salvatore.cataldi[at]belimo.ch). For further clarifications or interpretations, readers are invited to contact the individual associations.

EXECUTIVE SUMMARY

Technical Building Systems (TBS) and Building Automation and Control Systems (BACS) are entering a new phase. Cybersecurity is becoming an essential part of product quality and resilience. The EU Cyber Resilience Act (CRA) accelerates this shift by setting clear, lifecycle-based requirements for all products with digital elements. For a sector built on long lifetimes, multi-vendor environments, and mixed-trust networks, the CRA is both a challenge and a significant opportunity. The regulation raises expectations across engineering: practical security-by-design, secure-by-default configurations, credible upgradeability strategies, and mature vulnerability handling throughout the support period. It also clarifies responsibilities within the supply chain, enabling component suppliers, OEMs, BACS manufacturers, integrators, and operators to exchange the information needed for proportionate, real-world risk management.

The transition requires discipline but is achievable. Long-lived building products need explicit lifecycle strategies, upgradeable devices designed for crypto agility, and resource-constrained devices paired with realistic support windows and clear migration paths. Legacy protocols will likely remain in installed bases; they therefore require compensating measures in the near term and a credible modernisation path toward more secure options over time. Fast reporting obligations for actively exploited vulnerabilities create new operational readiness, strengthening trust and coordination across Europe.

The good news is that the industry is already adapting. Manufacturers and associations are enhancing secure development processes, preparing coordinated vulnerability handling, improving operational security guidance, and contributing to realistic standardisation that reflects building environments.

With sustained collaboration between industry, authorities, and standards bodies, the CRA can act as a true catalyst, driving better product quality, stronger interoperability, and more trustworthy building technologies across Europe. We are at the beginning of an ambitious but promising path forward, offering a unique chance to modernise practices and deliver more resilient buildings for decades to come.

TABLE OF CONTENTS

1. WHY THE CRA MATTERS FOR TBS AND BACS

TBS products are embedded in buildings for long periods, often 10–20 years or more. They operate in mixed environments: multi-vendor systems, segmented networks, legacy protocols, and a wide range of operational maturity across building owners and operators. These characteristics create a cybersecurity context that differs from consumer IoT or short-lifecycle IT products. At the same time, TBS increasingly includes remote connectivity, software updates, cloud-connected services around devices, and data-driven features. This increases exposure and the need for systematic vulnerability handling, secure design, and clear support expectations. The CRA applies to "products with digital elements" and introduces lifecycle-oriented obligations, including vulnerability handling and reporting, and the use of CE marking as a conformity signal for cybersecurity requirements.

By using the CE marking, the CRA embeds cybersecurity compliance into the EU's established product-compliance and market-surveillance system, so the effect is felt across the whole procurement and distribution chain (placing on the market, declarations/technical documentation, checks by authorities), not only as an information cue for the end-user.

The CRA is not the only piece of the regulatory puzzle: frameworks such as the Data Act and NIS2 also shape expectations around data access, governance, and operational security in connected buildings. However, this paper focuses on the CRA because it directly targets the product lifecycle and the manufacturer's processes, thereby having the most immediate impact on how TBS products are designed, launched, supported, and improved over time.

2. CRA FOUNDATIONS THAT MATTER FOR OUR SECTOR

We align with several core CRA principles:

- **Lifecycle responsibility**: security is not a one-time feature. Products must be designed, maintained, and supported with vulnerability-handling practices throughout their expected support period.
- **Transparency and supply chain communication**: practical risk management requires that upstream and downstream actors can request and provide the cybersecurity information they need. This is particularly relevant in multi-tier TBS supply chains (component suppliers, device OEMs, system manufacturers, integrators, operators).
- **A clear timeline for readiness**: the CRA entered into force on 10 December 2024; the main obligations apply from 11 December 2027; reporting obligations apply from 11 September 2026.
- **Operational reporting infrastructure**: ENISA is tasked with establishing the Single Reporting Platform, expected to be operational by 11 September 2026, with testing before then.

3. A POSITIVE APPROACH: DEFINING BEST PRACTICES IN TBS

The industry does not view CRA compliance as a box-ticking exercise. In TBS, "meaningful, proportionate security" means:

a. security that is **fit for purpose** and risk-based across diverse building contexts

b. upgrades that **do not destabilise the safety and operational continuity** of installed building systems

c. clear, usable information for system integrators and operators (not only legal documentation)

d. a shift from implicit assumptions to explicit commitments: support periods, update policies, secure configuration guidance, and vulnerability management processes

For building owners and occupants, the outcome should be improved trust, resilience, and the continuity of essential building functions, as well as broader market availability of secure-by-design products and services.

4. WHERE WE SEE CRA-DRIVEN OPPORTUNITIES

4.1. Better product quality, not only "security features"

CRA encourages a quality mindset that integrates cybersecurity into engineering processes: requirements, architecture, testing, release, documentation, and post-market monitoring. This reduces avoidable rework and improves robustness in real deployments.

4.2. More transparent lifecycle and service offerings

Clearer commitments on support periods, security updates, and vulnerability handling create room for better service models across the supply chain, including professional maintenance offerings and security-relevant configuration support.

4.3. Stronger interoperability and modernisation momentum

The CRA creates incentives to modernise insecure or obsolete security mechanisms where technically feasible. This does not imply that all installed systems are inherently insecure, but that their security should be assessed in context. For TBS, this can accelerate migration paths from legacy practices toward secure protocols and architectures, while still managing installed-base realities.

4.4. A more professional supply chain security dialogue

TBS ecosystems depend on multi-party integration. The CRA pushes the market toward standardised "security information exchange" patterns: what information is needed, in what format, when it must be provided, and how it supports proportionate risk management.

5. WHAT THE TBS INDUSTRY IS DOING NOW

While the CRA introduces substantial new expectations for many TBS manufacturers, it also provides something the market has long needed: **a clear, common direction** for how cybersecurity should be engineered, maintained, and demonstrated over a product's lifecycle. This clarity allows the industry to plan investments with greater confidence and to build capabilities that remain valuable beyond compliance. In practice, the CRA can act as an accelerator for the broader digitalisation of the built environment: strengthening trust in connected products, improving lifecycle quality and transparency, and enabling secure services and data-driven innovations that support better buildings and better life outcomes.

Across manufacturers and associations, we commit to preparation in five areas:

1. **Security-by-design engineering practices**
Integration of secure development lifecycle practices, threat modelling, secure by default configurations, and secure update capabilities aligned with the product.

2. **Coordinated vulnerability handling**
Establishment or reinforcement of processes for intake, triage, remediation, disclosure coordination, and customer communication, anticipating CRA reporting obligations from September 2026.

3. **Clearer customer-facing security documentation**
Operationally useful guidance for secure installation, secure configuration, and operation, designed for integrators and operators, not only legal compliance.

4. **Supply chain transparency mechanisms**
Better upstream/downstream communication patterns about components, dependencies, and security-relevant properties to support risk assessment and remediation coordination.

5. **Standardisation engagement**
Active participation in developing practical standards that can support consistent implementation approaches in building contexts, including product-specific needs.

In addition to these technical preparation steps, we see an equally important capability gap at the ecosystem level.

Beyond product engineering, the industry also recognises a critical success factor: building a practical cybersecurity culture across the full TBS/BACS value network. In our domain, outcomes depend on many actors, building owners and operators, designers and specifiers, system integrators and service providers, component suppliers, OEMs, and system manufacturers, working with consistent assumptions on onboarding, credential handling, segmentation, remote access, patching discipline, and incident response. The industry is ready to support this shift by developing role-based training and courses tailored to technical building systems, and by collaborating with the European Commission and the existing competent bodies already active in awareness, guidance, and capacity-building, so that secure products are matched by secure commissioning and secure operation at scale.

6. LIFECYCLE CYBERSECURITY IS A PRODUCT REQUIREMENT

Manufacturers will need to be able to show secure-by-design/default practices, operate structured vulnerability handling, comply with the CRA's reporting obligations, and define credible support and refresh strategies that match the product context.

For TBS/BACS component manufacturers, the CRA represents a step change because it regulates not only what they place on the market, but also how they engineer it, produce, and support it over time.

In practice, this means cybersecurity stops being a "feature set" and becomes a demonstrable product discipline anchored in a documented risk assessment and in the essential requirements products must meet at design, release, and maintenance stages.

It also means manufacturers need a real vulnerability handling capability during a defined support period: a process to receive and triage reports, identify affected versions and third-party components, develop fixes or mitigations, inform users, and keep technical documentation up to date as risks evolve.

The reporting duties accelerate internal escalation and decision-making because when an actively exploited vulnerability is known, you may face deadlines such as early warning within 24 hours, a notification within 72 hours, and a final report no later than 14 days after a corrective or mitigating measure is available, which forces manufacturers to pre-build evidence collection, roles, and communication paths.

Finally, the CRA pushes manufacturers to be explicit and credible about lifecycle strategy in the building domain: where products are truly upgrade-capable (typically controllers and gateways), manufacturers must design for secure updates and crypto migration; where devices are constrained (many field devices), manufacturers must define a realistic support period and a practical migration or refresh path, because long installed life is normal but long secure software upgradeability on unchanged hardware cannot be guaranteed.

6.1. From Product Fixes to Ecosystem Recovery

In building automation, this lifecycle strategy also has a collective dimension that is easy to overlook. Many TBS/BMS products rely on standard interfaces for interoperability, and when a cybersecurity weakness is linked to how such an interface is commonly implemented or deployed, the durable fix is not always a single vendor patch in isolation. Often, manufacturers need a clearer profile, guidance, or an evolved version of the underlying standard to address the issue consistently across multi-vendor environments, while associations help translate that evolution into practical deployment recommendations and accelerated adoption. In that sense, the CRA turns vulnerability handling into a coordinated "system recovery" ecosystem: short-term mitigations can be issued quickly to reduce exposure in installed buildings, and longer-term improvements can be embedded into updated specifications and product generations, so that the system becomes secure again starting from the individual products that implement the standard protocols.

6.2. 10+ year installed life: plan upgradeability refresh paths

Building products often stay installed for 10–20 years. But it is rarely realistic to assume that the same device hardware will remain **secure, fully upgradable, and crypto-current** for that whole period. Security requirements and cryptography evolve, and software stacks typically grow in resource needs.

In fact, the concept of **intended use** already pushes manufacturers away from a "one device fits all forever" mindset. An actuator intended for HVAC in a standard office environment is not necessarily intended for HVAC in a clean room or a chemical laboratory, where the task, operating constraints, and impact of malfunction are different; this is not just a different risk level, but a different job, which shapes performance requirements and, in turn, the cybersecurity posture and lifecycle expectations.

For products embedded in buildings for long periods, a support-period strategy for TBS/BACS portfolios is needed. Manufacturers should define a support period for cybersecurity updates and mitigations that is credible for the expected time in use. A practical portfolio model is to combine a **5-year platform renewal cycle** (new hardware generation placed on the market) with a **10-year security support commitment per generation**, counted from the **last unit of that generation placed on the market.** This example approach aims to increase the likelihood that cryptography, libraries, and toolchains remain maintainable for the installed base, while keeping engineering effort predictable across multiple generations.

Even with a well-defined support horizon, some vulnerabilities may become impossible to remediate for a given hardware generation (e.g., due to a loss of supplier support, broken cryptographic assumptions, or hard platform constraints). This requires a Support-period strategy for TBS/BACS portfolios. The portfolio strategy may therefore include a **replacement offer**: if certain vulnerabilities cannot be remediated within the declared support period for a given hardware generation (for example due to supplier end-of-support or hard platform limits), the lifecycle plan should include a controlled replacement or migration path (compatibility where feasible, migration tooling, and clear guidance for integrators and building owners). This turns an unavoidable technical limit into a managed lifecycle transition rather than an ad-hoc field crisis.

A credible product lifetime approach is therefore:

1. Define product classes with different expectations

a. Controllers / gateways (software-rich, higher resources): design them to be upgrade-capable for many years (headroom in CPU/RAM/flash, secure update mechanism, certificate/key rotation, crypto agility).

b. Small field devices (resource-constrained): define a clear security support window and plan for secure operation through design limits plus system-level compensating controls after end of support.

2. Design upgrade-agility where you claim it

a. Secure boot and signed firmware updates.

b. Safe update operations (rollback/recovery, maintenance-friendly behaviour).

c. Ability to rotate credentials and migrate crypto suites over time.

3. Make refreshing a planned part of the lifecycle, not a failure

a. Provide a practical **evolution of products** (tooling, configuration transfer, compatibility plan) when the security baseline outgrows the hardware.

b. Publish end-of-support behaviour and recommended compensating controls for remaining installed devices.

A long installed life is normal; long-term secure upgradeability on unchanged hardware cannot always be guaranteed. A responsible manufacturer lifecycle strategy combines **upgrade-capable product classes** with a **planned evolution of products**.

7. "SECURITY BY DESIGN" IN THE TBS/BACS INDUSTRY

For Technical Building System (TBS) components and Building Automation and Control Systems (BACS), security by design means building cybersecurity into the product from the first concept decision to end-of-life, while acknowledging four realities of our domain: **multi-vendor integration, long operational lifetimes, mixed-trust environments with physical access, and strict availability/safety expectations.** Security must therefore be effective and usable at both commissioning and service scales; otherwise, it will be bypassed.

7.1. BACS realities that shape "security by design"

7.1.1. Multi-vendor integration is the default

A Building Management System (BMS) is not a closed IT stack. Devices, controllers, gateways, and tools from different manufacturers must interoperate. Security by design must not rely on "everyone uses our engineering tooling" or "single-vendor assumptions". It must work with standard roles, standard interfaces, and predictable onboarding and service flows.

7.1.2. Lifecycles are long, and upgrades are slow

TBS components often remain installed for 10–20 years or more. Security by design must include a realistic plan for updates, vulnerability handling, and secure end-of-support behaviour. "We will patch quickly" is not enough if the product cannot be updated safely in real buildings.

7.1.3. Physically accessible and mixed-trust operational environment

Building networks often include shared infrastructure, legacy segments, different interoperable protocols, temporary commissioning setups, and remote access paths. Many devices are reachable in plant rooms, ceilings, and cabinets. Manufacturer's risk analyses must assume that attackers may reach the network and sometimes the device, not only “the cloud”. In such mixed-trust environments, network segmentation into zones and conduits helps assess risk exposure and determine the need for security measures in both interoperable protocols and individual TBS components, based on their intended environment.

The practical IT/OT gap is that IT security assumes centrally managed identities and fast rotation, while OT must keep assets running for years in harsh, intermittently connected environments and often cannot “just renew everything” during business hours. A BMS network is therefore best treated as OT, because it directly influences physical outcomes (comfort, safety functions, energy), and its primary security objective is availability and safe operation. At the same time, modern BMS architectures are rarely “pure OT”: the field and automation layers behave like classic OT, while supervisory servers, remote access, analytics, and cloud connectors are IT-facing integration points that should be zoned (often via a DMZ/management zone) rather than merged into a flat network. This split makes certificate management (trust anchors, issuance, validation, renewal, revocation) a first-order operational risk: if certificates are not inventoried and monitored, expiry or compromise can cause outages and long recovery windows. NIST explicitly warns that organisations often deploy certificates without tracking ownership, private-key location, or validity, and that outages occur when certificates expire or must be revoked and replaced; it therefore recommends a certificate inventory and monitoring to enable proactive replacement. When disruption happens, NIST stresses that the corresponding certificate should be revoked as soon as possible, and relying parties must treat the binding as no longer trustworthy.

In parallel, the CRA implementation FAQs give a useful secure-by-default direction for our domain: security defaults may include enabling certificate validation by default and disabling deprecated algorithms (especially for crypto components), as part of a manufacturer’s risk-based analysis.

7.1.4. Availability and safe operation are hard constraints

A BMS supports comfort, energy, and sometimes safety-related functions. Updates, authentication, and protections must not cause uncontrolled downtime or unsafe states. Security by design must include safe failure modes, controlled recovery, and maintenance-friendly operation.

7.1.5. Product vs project: risk acceptance criteria in multi-vendor TBS/BMS

Risk acceptance criteria define the acceptable level of residual cybersecurity risk for a product in its intended context and, therefore, when additional mitigation is required. They are defined by the manufacturer as part of the product's security governance and documented decision-making.

For TBS/BACS products, risk acceptance criteria must therefore be set from the product context and re-validated over time as threats and state of the art evolve.
In building automation and, more broadly, in TBS, what people call "the BMS" or "the TBS" is often not delivered as one single product. It is typically a project-specific integrated solution assembled on site from multiple products (devices, controllers, gateways, servers, software tools, and sometimes cloud services) coming from one or more vendors. In those cases, the CRA does not add a separate "system-level product" for the overall project; instead, the CRA applies to each individual product with digital elements that is placed on the market on its own.
The acceptance criteria should explicitly differentiate between component products (field devices, controllers, gateways) and supervisory / platform products (for example, BMS software or an appliance, including any necessary remote data processing solution).

Component products often face strong pressure from multi-vendor interoperability and "embedded use" (a component integrated into another product), so acceptance criteria must reflect foreseeable deployments where professional actors can apply compensating controls (segmentation, controlled remote access, credential and certificate provisioning), while also acknowledging that security is sometimes constrained by legacy interoperability requirements. Compensating controls can reduce residual risk, but they do not replace the manufacturer's secure-by-design and secure-by-default obligations for the product placed on the market.

Supervisory- or Control-platforms, when placed on the market as products and not integrated solutions, concentrate higher-value functions (identity and access control, remote connectivity, fleet visibility), so acceptance criteria should be stricter for scalable impacts (one compromise affecting many devices or sites), availability of building functions, and exposure created by remote access and cloud dependencies.
In all cases, according to the intended use description, the acceptance criteria are aligned with different product users: some products may primarily be handled by OEMs, panel builders, and system integrators (professional users), while supervisory products may be operated by facility teams and service providers (operators), which directly affects what residual risk can be considered acceptable and what must be enforced by secure defaults versus addressed through clear installation and operational requirements.

7.1.6. Same Hardware, Multiple Contexts

Make the product context and the expected user explicit, because software-driven risk controls depend on them, even when the hardware is identical.

The same electronic device can reasonably ship with different software variants, because the "right" mitigation controls are not only a function of silicon or compute power, but of intended use, exposed interfaces, and who operates the product day to day. In building automation, a "component for integration" variant is typically engineered to fit cleanly into a larger system. It can be deliberately narrow: one well-scoped communication channel (e.g., BACnet/SC) and an onboarding flow designed for specialists (integrators, commissioning engineers), where it is realistic to assume governed environments (segmented networks, controlled credentials, defined patch discipline). The same hardware, marketed as a "direct-to-operator" product for facility managers, often needs a different software posture: adding a web UI and self-service workflows changes both the attack surface and the likely failure modes (sessions, role and user management, recovery, audit logging, safe defaults). In that context, controls must also protect against routine mistakes and support non-expert operation, not only defend against technical attacks.

This is why it is hard to just define the minimum set of controls. This minimum is not a universal checklist; it is the smallest coherent baseline that matches the declared context, user type, and interfaces. Once those assumptions change, the minimum changes. The scalable pattern is therefore to state the context explicitly and let the control baseline follow from it, rather than pretending one baseline fits every packaging of the same device.

At the same time, being explicit about context and intended user is not only a security practice, but it also enables more accurate product positioning and more credible offers. When a manufacturer clearly positions a device variant as "for integration by specialists" versus "for direct operation by facility staff" (or a hybrid with remote support and multi-site management), customers and integrators can select the right version, set realistic expectations on commissioning and support, and align procurement, deployment, and responsibility boundaries with the actual risk profile.

8. APPLYING CRA PRINCIPLES IN A RISK-BASED WAY

This section provides a practical interpretation for TBS manufacturers, aligned with the CRA's risk-based approach: **start from scope, anchor everything in a cybersecurity risk assessment, and translate the outcome into "Security by Design" and "Security by Default" choices.**

8.1. Secure by Default in Practice

For Technical Building Systems components, **secure-by-default must be achieved through a controlled commissioning and onboarding model**, not by assuming that "security will be switched on later". A secure by default commissioning means the product is not meaningfully exploitable when first powered on: it exposes only the minimum interfaces needed for onboarding, keeps non-essential services disabled, and blocks unauthenticated operational control. Trust between the products and the Building Management System is then established via a defined onboarding workflow that provisions credentials (certificates/keys), constrains commissioning access (time-limited and local or physically gated where appropriate), and documents the intended target secure state. Risk should be assessed in the context of both the product and its intended deployment environment. Where legacy protocols cannot provide interoperable encryption, manufacturers should still reduce attack surface by default and provide, within the boundaries of their responsibilities, examples or guidance on repeatable reference deployment patterns (for example, segmentation and secure gateways), together with clear residual-risk information.

CRA requires products to be placed on the market in a secure-by-default configuration, based on the risk assessment and the intended purpose and reasonably foreseeable use. For TBS supply chains, the key clarification is responsibility at the component level: if a component is placed on the market separately, secure-by-default applies to the delivered configuration; once integrated, the integrating manufacturer may reconfigure it, and the component supplier is not responsible for those later modifications. An exception to this requirement is possible for tailor-made products with explicit contractual terms agreed with a specific business user, and properly documented.

8.2. "Products with digital elements" are broadly in scope in TBS

The CRA applies to **products with digital elements** made available on the EU market whose intended purpose or reasonably foreseeable use includes a **direct or indirect logical or physical data connection** to a device or network.
For TBS, this typically captures not only controllers and gateways, but also many "small" connected components that can still become an attack vector in a larger system.

The CRA definition includes the product's **remote data processing** solutions when those are necessary for the product to perform a function (e.g., a manufacturer-operated remote service needed for a feature).

A standalone SaaS that is designed/developed outside the manufacturer's responsibility is not itself a product with digital elements; however, remote data processing under the manufacturer's responsibility can be in scope.

8.3. CRA scope, Security by Design, and Security by Default

Under the CRA, manufacturers must perform a cybersecurity risk assessment and take its outcome into account across the lifecycle: **planning, design, development, production, delivery, and maintenance**, with the objective of minimising cybersecurity risks, preventing incidents, and minimising impact (including health and safety).

The risk assessment must cover the **entire product** with digital elements, including remote data processing, where in scope, and supporting functions that form part of the product placed on the market.
The CRA does **not** mandate one specific risk assessment methodology; what matters is that the manufacturer can demonstrate how risks were identified, evaluated, and treated, and how this drove the implementation choices.

Manufacturers should first consider the horizontal CRA standards prEN 40000 series currently being developed by CEN-CLC/JTC 13/WG 9. These standards are being developed specifically to support the implementation of the CRA essential cybersecurity requirements for products with digital elements and therefore provide the most direct reference for CRA-oriented product compliance. Where the prEN 40000 series does not perfectly address the manufacturer's specific product, use case, operational environment, or risk treatment needs, manufacturers may consider product type standards such as EN IEC 62443 for the relevant aspects.

For example, EN IEC 62443-3-2 proposes a structured, repeatable workflow and set of outputs (scope/SUC, target security levels, and so on) that can be adopted as a risk-assessment method for TBS/BACS supervisory/platform products and, by extension, to derive and justify the security expectations for components.

The use of additional standards or security practices should not be interpreted as introducing obligations beyond the CRA; rather, they provide optional, structured approaches that manufacturers may adopt where appropriate to demonstrate compliance, depending on product complexity, deployment context, and business needs.

In many TBS projects, the manufacturer of a field component is not the same as the manufacturer of the supervisory platform, and both may differ from the system integrator or operator. In such multi-vendor scenarios, IEC 62443 concepts can be applied along product boundaries and deployment boundaries. Each manufacturer remains responsible under the CRA for the cybersecurity risk assessment, secure-by-design/default configuration, and vulnerability handling of the product it places on the market. By contrast, the project-specific deployment architecture, including zones and conduits, network segmentation, remote-access design, and account-management arrangements, is typically specified and implemented at system level by the system integrator and/or operator according to project requirements. In practice, this requires each product manufacturer to provide the security-relevant information and assumptions needed for secure integration, such as exposed interfaces, trust assumptions, hardening options, integration constraints, and residual-risk notes. This allows the system-level risk treatment to be assembled on an informed basis, without confusing the manufacturer's responsibility for its own product with the project-specific responsibility for system architecture and deployment choices.

8.4. "Intended Purpose" and "Reasonably Foreseeable Use"

The CRA explicitly ties both **scope** and **risk assessment** to the product's intended purpose and reasonably foreseeable use.

For TBS manufacturers, this is a practical lever to make cybersecurity expectations explicit: the more clearly the intended purpose and foreseeable use are defined, the more the professional will select the right product for the right security purpose.

This is also central for dual-purpose products. The guidance is: **state intended use clearly; if dual-purpose, the higher-risk level applies**, and sometimes a variant of the same product is better, as discussed in 7.1.6.

8.5. "Security by Design": properties *and* processes

For CRA, security is not only "features": the risk assessment must drive both (a) how the product is designed and (b) how the manufacturer's processes ensure security over time (including maintenance and vulnerability handling).

The Commission also frames CRA as pushing transparency and communication along the supply chain so that each actor can manage risk proportionately, and as introducing Secure Development Lifecycle concepts that can improve products.

8.6. Legacy protocols, compensating measures, and credible migration paths

Buildings have long lifecycles and installed-base constraints. The Commission's position, as reflected in today's draft guidance and in the minutes of our meeting in October 2025, is pragmatic but directional: where secure protocols are technically feasible, they are expected to be implemented.

In this context, "technically feasible" should not be understood as the device being able to support encryption alone. It also requires that the overall system remains operational and deployable in real conditions. In practice, this means that the product must be able to integrate into the intended system, interoperate with existing devices and protocols, and fit within current deployment environments. It should not become a "dead-end" product that cannot be integrated because the surrounding ecosystem, including legacy networks, gateways, supervisory platforms, tooling, and commissioning workflows, does not yet support the secure variant. Conversely, technical infeasibility may arise where the secure option cannot interoperate with the protocols used in the target system, or where the system architecture was not designed to support secure onboarding and trust establishment. In such cases, adopting secure protocols is not a simple substitution but may require broader system redesign.

Where this is the case, legacy solutions may be maintained, based on the outcome of the cyber risk analysis and supported by appropriate compensating measures if needed. However, manufacturers are still expected to aim to integrate secure protocol options in new designs to enable a gradual transition over time. In this document, "legacy" refers to systems already deployed and does not imply that such systems must necessarily be phased out.

In the same pragmatic spirit, DG GROW has also clarified that the CRA does not aim to force "throw-away" outcomes. It does not require recalling products from storage or replacing functioning installed systems by default, unless the product and system risk assessment justifies such measures. This is consistent with the Commission's emphasis on risk-based decision-making and with the clarification that products legally placed on the market before the CRA application date are not retroactively required to enter a replacement cycle.

8.7 Security maintenance as part of product quality and service

CRA expects manufacturers to ensure vulnerabilities can be addressed via security updates, distribute updates securely, disseminate them without delay, and keep users informed. Where applicable, automatic security updates should be enabled by default with an easy opt-out and the ability to postpone.

If a user opts out or does not install updates, the manufacturer is not responsible under CRA for that user's choice, provided the manufacturer has fulfilled its obligations to provide and communicate updates.

Many TBS components (room controllers, sensors, actuators) are not permanently connected to the Internet. They may be reachable only on a local network, via a supervisory controller, or via a temporary service connection (e.g., laptop, service tool, commissioning network). In these cases, "automatic updates by default" is often neither realistic nor expected among professional users, yet the CRA expectation still holds: vulnerabilities must be fixable, updates must be distributed securely, and users must be informed without delay. The practical approach is therefore to design *for secure updateability without continuous connectivity*: provide a signed, integrity-protected update package, a secure installation workflow (authenticated service role, local/physically controlled access where appropriate), and clear instructions for when and how to apply the update in operational buildings.

For intermittently connected products, TBS/BACS manufacturers intend "dissemination without delay" as *availability plus actionable communication:* publish the update and advisory promptly, and make it easy for integrators/operators to deploy it via the paths they actually use (BMS/edge controller rollout, maintenance windows, service tooling). Where a device cannot receive updates directly, a defined compensating pattern shall be documented (e.g., update via an upstream controller/gateway, segmentation and hardening guidance until the next service visit, or a managed migration/refresh path if the device is constrained). This aligns the CRA lifecycle intent with the OT reality of buildings: availability and safe operation remain hard constraints, but updateability is still engineered as a product capability rather than left to ad-hoc field practice.

8.8. Vulnerability handling and support period

CRA's core innovation is to enforce **transparency and communication along the supply chain**, so that every actor can conduct proportionate risk management, while the final manufacturer assumes overall responsibility for the final product placed on the market.

Operationally:

1. Vulnerability handling obligations apply **throughout the support period**, for the product in its entirety, including integrated components.

2. If an integrated component is no longer supported and vulnerabilities cannot be adequately mitigated, the product manufacturer must remediate via other means (disable functions, switch component, or develop a patch).

3. Products may sit in the distribution chain: the obligation to have no known exploitable vulnerabilities applies at placement on the market, but newly discovered issues must be handled under vulnerability handling once the product is in operation by the user.

4. Support period determination should reflect expected time in use and proportionality considerations, including the support period of core integrated components.

What to do:

Define a support policy that is realistic for TBS lifecycles (long-lived installations):

a. support period rationale and customer communication
b. coordinated vulnerability disclosure process
c. update and mitigation delivery model (incl. what happens when updates require functionality change)

8.8.1. CRA security-related support and warranty / commercial support

Security-related support under the CRA (vulnerability handling, security updates, and related user information) is a **time-bound lifecycle commitment** distinct from warranty and commercial maintenance/support contracts. Warranty typically covers defects and workmanship for a limited period, while CRA security-related support addresses newly discovered vulnerabilities and enables remediation over time. These timelines may differ in length, but they must be **made explicit** to avoid misaligned expectations across the supply chain.

In practice, three misunderstandings commonly arise and should be prevented through clear communication:

a. **Warranty expired, so security updates stopped.** Not necessarily: the declared CRA security support period may extend beyond the warranty period.

b. **Security support ended, so I'm entitled to free replacement.** Not necessarily: end of security support means the product is no longer maintained for newly discovered vulnerabilities; it does not automatically create a warranty claim. It does require guidance on residual risk, compensating measures, and upgrade paths.

c. **The device still works, so it must remain security-supported indefinitely.** Not necessarily: long-lived TBS installations can outlast feasible security maintenance, especially if core integrated components reach the end of support. Manufacturers should therefore define and communicate what happens at the end of security support (e.g., final update, mitigation guidance, secure configuration hardening, segmentation/gateway patterns, and new generation products).

8.8.2. Security updates in operation: roles and cost allocation

Cybersecurity maintenance for components used in Building Automation Systems introduces recurring operational work in the field (planning, testing, scheduling downtime, deployment, rollback).

Under the CRA, manufacturers of those components are expected to provide vulnerability handling and, where applicable, make security updates available throughout the component's declared support period.

However, the CRA does not set contractual or commercial rules on who performs and funds the operational deployment of updates in live Building Automation Systems. To avoid conflicts, it is useful to clearly distinguish between (i) product warranty (e.g., defects and non-conformities) and (ii) security support period (availability of security fixes and security guidance). In practice, the manufacturer makes the security update available (and communicates the necessary information and instructions), while building owners and their contracted operators or integrators typically plan and execute deployment as part of maintenance activities, unless specific service agreements define otherwise.

Clear contractual clauses on responsibilities, response times, and cost allocation (during and after warranty) help prevent disputes where necessary security updates are treated as "product faults" with charge-back expectations.

8.9. Manage the installed base and change responsibly

For products placed on the market before the CRA fully applies, CRA requirements generally apply only if the product is **substantially modified** after the application date; however, some reporting obligations apply broadly.

A functionally equivalent spare part that does not alter the intended purpose, cybersecurity-relevant behaviour, or underlying risk assessment of the product in which it is integrated does not constitute a substantial modification of that product. Its use for the maintenance or repair of a product already installed in the field therefore does not change the CRA compliance position of that product.

This is particularly relevant in TBS where:

- protocols, interfaces, and remote capabilities often evolve over time
- updates may add new functions that alter the security posture significantly

What to do:

- Put in place an internal "change classification rule":
  - security fix vs feature enhancement vs substantial modification
  - documentation updates and customer communication
  - decision record linked to the risk assessment

8.10. From horizontal to vertical

The CRA is a horizontal framework: it defines cybersecurity obligations (risk assessment, secure-by-design/default, vulnerability handling, lifecycle support) but remains technology-neutral and does not provide an OT-grade blueprint for engineering, documenting, and operating security in building automation.

In TBS/BACS, deciding whether "CRA-only" is sufficient depends on product context: the intended use, deployment environment, exposure (local network vs. remote access/cloud), the role in the system (leaf device vs. trust-terminating gateway/control plane), and the expected threat level. Horizontal standards from EN 40000 series are developed to address CRA. However, compliance with the CRA is a minimum required to put a product on the market and may not assure a sufficient level of security when the product is deployed in long-lived, multi-vendor, OT-like environments, is security-relevant by function, or must meet procurement expectations for auditable "state of the art" measures. The application of additional standards such as EN IEC 62443 addresses this.

For component products (actuators, controllers, gateways), EN IEC 62443 can drive minimum credible security capabilities and integration-safe behaviour: clear trust boundaries, secure defaults, identity and access control, authenticated update and recovery, hardening guidance, plus disciplined secure development and vulnerability handling, with stronger relevance as the component routes traffic, translates protocols, terminates trust, or enables remote access.

For supervisory/platform products (BMS software, edge platforms, supervisory controllers), EN IEC 62443 can be central because these products act as the security and operational control plane: segmentation concepts, robust IAM and role separation, secure remote access, audit logging and monitoring, secure APIs, resilience and recovery, and a full secure SDLC with systematic security testing, dependency risk control, release governance, and clear support and patch policies.

Importantly, the EN IEC 62443 mindset can be adopted even without pursuing certification: treat security requirements as engineered features, use threat modeling and "zones/conduits" thinking to structure the architecture, embed security gates and evidence generation in the SDLC, and run vulnerability handling and support as a disciplined lifecycle process.

The CRA sets the "what"; product context determines whether that baseline is sufficient; and as a complement to EN 40000, EN IEC 62443 can provide an OT-credible "how" and the evidence package, with components focusing on capabilities and safe integration, and platforms focusing on architecture, process discipline, and operational security.

9. ACTIVELY EXPLOITED VULNERABILITIES UNDER THE CRA

What gets reported, what may become public, and what TBS/BACS manufacturers should plan for.

For manufacturers of Technical Building Systems and BMS components, the CRA introduces a new operational reality: **very fast reporting deadlines** exist for actively exploited vulnerabilities, but **public disclosure is not automatic** and follows a different logic. Mixing these two tracks leads to wrong assumptions, unnecessary reputational risk, and poor coordination with integrators and CSIRTs.

9.1. Reporting as a regulatory channel, not a public announcement

When a manufacturer becomes aware of an **actively exploited vulnerability**, the CRA requires reporting to the **CSIRT coordinator and ENISA** via the single reporting platform. The reporting sequence includes:

- an **early warning within 24 hours** after becoming aware, meaning after an initial assessment shows that the vulnerability is actively exploited and affects the manufacturer's product,
- a **vulnerability notification within 72 hours**, and
- a **final report** no later than **14 days after a corrective or mitigating measure is available.**

These deadlines are designed to enable fast situational awareness and coordinated response. Importantly, the CRA provisions that create these deadlines **do not say that the vulnerability will be published X hours/days after the report**. They define how fast the manufacturer must notify authorities, not when the public will learn about it.

9.2. Confidentiality is the default for the report itself

The CRA framework expects that information submitted in notifications is handled with **confidentiality and appropriate protection** by the receiving actors (CSIRTs and ENISA). This is a critical point for TBS/BACS manufacturers: the 24h/72h report should be treated internally as **regulatory intelligence sharing**, not as a public communication. In practice, this supports coordinated disclosure, prevents unnecessary panic, and reduces the risk of giving attackers actionable detail before mitigations exist.

9.3. "Publication" can happen through different channels, with different owners

In a building automation context, there are two distinct "visibility" pathways that can follow an actively exploited vulnerability.

9.3.1. User communication (manufacturer-led, operational disclosure)

The CRA expects the manufacturer to **inform impacted users**, and where appropriate, broader users, with practical guidance that helps reduce risk (mitigations, configuration changes, updates). If the manufacturer does not do so in a timely manner, **CSIRTs may inform users directly** where this is proportionate and necessary to prevent or mitigate impact.

This is not "public vulnerability publication" in the classic sense. It is a duty to ensure that users can act.

9.3.2. EU-level database visibility (ENISA-led, structured publication)

The CRA links broader, structured visibility to the **European Vulnerability Database (EUVD)** operated by **ENISA**. The logic is not "report then publish". Instead, the CRA frames EUVD insertion around conditions such as:

- a **security update or other corrective/mitigating measure is available**, and
- the **vulnerability is publicly known**, and
- ENISA adds the entry **in agreement with the manufacturer**.

For manufacturers, this means there is **no fixed** time between the 24-hour early warning and any EUVD appearance. EUVD is meant to catalogue "publicly known vulnerabilities" with actionable context (affected products, severity, patches/mitigations). The practical sequence is typically: **report quickly, coordinate mitigations, communicate to users,** and then expect a structured publication when disclosure is appropriate and useful.

9.4. A conditional "public disclosure" lever exists

The CRA also provides a conditional mechanism under which a CSIRT may, after consultation (and, where appropriate, with ENISA), **inform the public** or **require the manufacturer to do so** if public awareness is necessary to prevent or manage harm. This is not an automatic outcome of the 24-hour report. It is an escalation tool used when risk management demands broader awareness.

9.5. In practice for the TBS/BACS industry

TBS/BACS manufacturers should plan their vulnerability handling at least as a **two-output process:**

1. **Regulatory reporting package (24h/72h discipline):**
   A prepared capability to assess whether exploitation is active, capture the minimum required facts, and notify the correct EU endpoints fast, even when information is incomplete.

2. **User-facing advisory (actionable, timely):**
   A customer communication path that prioritises operational guidance (what to change now, what to disable, what to patch, compensating controls, and deployment notes for real building networks).

3. **Global Triage and 'Becoming Aware' (internal alignment):**
   Multinational manufacturers should plan to establish global procedures that clearly distinguish between the initial reporting of a potential vulnerability and the point at which active exploitation is technically confirmed. In practice, this internal triage by the relevant PSIRT/CSIRT supports a consistent and proportionate understanding of when the manufacturer can be considered to have become aware, while helping to avoid false alarms and to manage coordination across global time zones.

This separation is particularly important in multi-actor building projects where integrators, BMS vendors, OEMs, and service providers share responsibility for deployment and remote connectivity. Manufacturers should not assume that "reporting" equals "public disclosure", nor that "publication" will happen on a predictable clock. Instead, they should design governance and playbooks for coordinated handling, aligned messaging, and evidence retention that supports both compliance and customer trust.

10. CONSISTENCY WITH ADJACENT EU POLICIES: DATA ACT

TBS and BACS are also impacted by horizontal EU digital regulation beyond the CRA. The Data Act, applicable from 12 September 2025, shapes access to and use of data generated by connected products and related services and is part of the broader EU data strategy.

For TBS and BACS, the combination of CRA and Data Act reinforces the direction of travel: more transparency, clearer responsibilities, and better-defined operational practices across complex ecosystems. We encourage consistent guidance so that cybersecurity obligations and data access obligations reinforce, rather than conflict with, each other in real building deployments.

10.1. Companion app: convenience without security dependency

Keep provisioning and data access available through documented interfaces so users can get their data (Data Act) without your app becoming a single point of failure or lock-in (CRA mindset).

A manufacturer's "companion app" can be genuinely useful in building automation, but it must be positioned carefully so it does **not** become a security single point of failure for the device, while still serving as a **user-friendly window** on device data that aligns with Data Act expectations. From a CRA mindset, the moment the app is the only practical way to onboard trust (e.g., loading certificates, enrolling into encrypted transport, setting credentials), the app becomes part of the product's effective security boundary: its authentication, update discipline, hardening, and compromise impact start to matter as much as the device firmware itself. That is avoidable. The scalable pattern is to keep **security-critical provisioning** possible through **documented, vendor-neutral interfaces** exposed by the device (e.g., BACnet/SC, KNX, a local web UI with mutual TLS, a standard API, or standardised enrollment mechanisms when feasible). Your app then becomes a *convenience layer* that uses the same documented interfaces as everyone else, rather than a privileged "magic tool". This reduces lock-in, makes integrators' tooling viable, and prevents a fragile dependency in which the loss of the app (or its ecosystem, accounts, mobile OS changes, or store policies) blocks commissioning or recovery.

At the same time, the Data Act pushes the market toward **practical user access** to data generated by connected products and toward **expectations of portability/switching for** related services. A companion app can help here precisely when it is treated as a **non-exclusive, user-centric interface**: it can present data in readable form, allow export in standard formats, provide clear metadata (time, units, context), and guide users to share data with third parties where applicable, without forcing them into a proprietary cloud workflow. The key is symmetry: whatever the app can see or export should also be available through **open, documented and**, where available, **standardised mechanisms** so that users, integrators and authorised third-party service providers can access the same data without relying on the app. This supports interoperability and facilitates switching between service providers, while preserving clear governance and avoiding the creation of de facto gated channels that could be perceived as lock-in by customers or regulators. In practice, it can be explicitly stated in product documentation: "The app is optional: it provides a user-friendly interface for commissioning and data viewing, but essential security, operational and data-access functions remain available through documented and interoperable interfaces, subject to appropriate cybersecurity safeguards." That single sentence avoids hidden dependencies and supports both secure operation and effective data access for users, integrators, and services.

10.2. Cloud dependency as a design decision across the lifecycle

Where and under whose control your cloud runs can determine whether customers accept your solution and whether the product still works when the cloud is unavailable or jurisdictionally constrained.

When a TBS/BACS manufacturer integrates a cloud service into a product at any point in the lifecycle (e.g., commissioning, normal operation, reconfiguration, analytics, remote maintenance), the cloud becomes part of the product's security and availability assumptions and must be treated as a design-time dependency, not a "deploy later" detail: the manufacturer should explicitly decide where the cloud service is operated (region), under which legal jurisdiction and governance it falls (who controls operations, who administers, who holds keys, which subcontractors exist), and how those choices affect data sovereignty (applicable law, access requests, and control over data and metadata) and service availability (continuity, resiliency, and the ability to keep essential functions running if the cloud is degraded or unreachable).

The European Commission's Cloud Sovereignty Framework is useful here because it translates "sovereignty" into concrete objectives spanning legal and operational control, supply-chain transparency, openness, security, and compliance. These aspects are increasingly reflected in customer expectations and public procurement approaches, meaning that manufacturers may be asked to provide evidence against such objectives. From a regulatory-readiness perspective, cloud contracts and architectures are likely to be scrutinized not only for cybersecurity controls, but also for governance clarity (roles and responsibilities, auditability, incident handling, subcontractor visibility and service continuity), as these elements are often critical in real cloud deployments and of interest to both customers and regulators. In parallel, the Data Act promotes switching and portability between data processing services and reinforces expectations that users should be able to access, transfer and continue using their data without unnecessary technical or contractual barriers. This makes exit readiness, interoperability and governance clarity increasingly important, including where cloud-based functionalities are introduced after market placement (e.g., via new commissioning workflows or added remote services).

Practically, this means the manufacturer should (i) define which functions must remain safe and usable without cloud connectivity (graceful degradation and local fallback), (ii) design commissioning and reconfiguration so that loss of cloud access cannot brick devices or prevent safe operation, (iii) implement a documented portability/exit plan for data, configurations, and logs (including formats, timelines, and responsibilities), and (iv) ensure operational controls for continuity (monitoring, redundancy, incident response, and clear recovery objectives) are aligned with the product's intended operational environment; ENISA's cloud security framework is a good reference because it explicitly covers the lifecycle from pre-procurement to contract finalization and exit, including migration planning and security/privacy considerations. The intent of this paragraph is simple: cloud location and control are not neutral implementation details; they are architecture choices that directly influence legal exposure (sovereignty), customer acceptance, and whether the product can continue delivering its essential building function under foreseeable connectivity or provider disruptions.

11. COMMITMENTS AND CALLS TO ACTION

Our commitments as an industry

- Treat cybersecurity as a core dimension of product quality and lifecycle responsibility
- Invest in vulnerability handling maturity and coordinated disclosure practices
- Improve supply chain transparency so actors can manage risk proportionately
- Engage in standardisation and guidance development to make implementation consistent and practical
- Support customers and integrators with usable operational guidance, not only compliance statements

What we ask from institutions and partners

- Continue structured dialogue with sector associations and representative industry groups
- Provide scenario-based guidance tailored to long lifecycle, multi-vendor "system-of-systems" realities
- Align reporting platform onboarding, templates, and processes with practical manufacturer workflows ahead of September 2026
- Encourage harmonized approaches across Member State market surveillance to avoid fragmentation
- Support SME enablement through training, examples, and facilitation mechanisms
- Ensure that regulatory and reporting expectations remain clear, simple and proportionate

SIGNATORIES

https://arge.org/

Founded in 1956 ARGE is the European umbrella association of locks and hardware manufacturers. It represents 12 National Associations within Europe, which serve over 200 manufacturers across the whole of Europe and Scandinavia. It aims to represent the interests of its National Associations, manufacturers and users of locks and hardware, and works on technical issues for the European Committee of Standardisation (C.E.N.).

https://www.edsf.com/

The E.D.S.F. European Door and Shutter Federation e.V. is the umbrella organisation for Europe's associations and manufacturers of doors, gates, shutters and components (operators). Founded in 1985 with members from several European countries E.D.S.F. stands for over 1,000 manufacturers and installers.

https://ehpa.org/

The European Heat Pump Association (EHPA) is the voice of the European heat pump sector in Brussels. Our vision is to be the leading authority and trusted partner in the path to fully enable the decarbonisation of buildings and industry in Europe.

https://epeeglobal.org/

The European Partnership for Energy and the Environment (EPEE) represents the refrigeration, air-conditioning and heat pump industry in Europe. Founded in the year 2000, EPEE's membership is composed of over 50 member companies, national and international associations.

https://eubac.org/

European Building Automation and Controls Association is the European "go-to" association on building automation and controls. We represent 85% of the European building automation and control sector. Our vision is a world where everyone lives in buildings that are smart, decarbonised and efficient

https://www.eurovent.eu/

Eurovent is the voice of the European HVACR industry, representing over 100 companies directly and more than 1.000 indirectly through our 16 national associations. The majority are small and medium-sized companies that manufacture indoor climate, process cooling, and cold chain technologies across more than 350 manufacturing sites in Europe. They generate a combined annual turnover of more than 30 billion EUR and employ over 150.000 Europeans in good quality tech jobs.

https://evha.eu/

EVHA is an independent European professional association bringing together companies involved in the cleaning and inspection of ventilation systems.
Our goal is to improve the quality and safety of indoor environments through certification, education, knowledge sharing, and support for legislative changes. We stand behind professional standards that shape the future of ventilation hygiene.

www.enocean-alliance.org

The EnOcean Alliance is a coalition of close to 400 companies in the building and IT sectors formed in 2008. They focus on improving Smart Homes, Smart Buildings, and Smart Spaces using the wireless EnOcean Radio Standard, developed for ultra-lowest power consumption enabling wireless sensors and switches to run off energy harvesting power, eliminating the need for batteries and battery maintenance as well as having to pull cables to power them.

https://www.evia.eu/

The European Ventilation Industry Association (EVIA) was established in Brussels in July 2010. EVIA's mission is to represent the views and interests of the ventilation industry and serve as a platform between all the relevant European stakeholders involved in the ventilation sector, such as decision-makers at the EU level as well as our partners in EU Member States. Our membership is composed of 40 member companies and 6 national associations across Europe.

https://smarten.eu/

smartEn is the European business association of the Flexible Demand Management Industry. We integrate consumer-driven solutions in the clean energy system by unlocking demand-side flexibility. Our mission is to create opportunities for every company, building, and vehicle to support an increasingly renewable energy system.

https://www.vdma.eu/en/building-automation-controls

VDMA Building Automation and Controls is the association of around 70 manufacturers of measuring, control, and regulating equipment for heating, ventilation and air-conditioning needs as well as building automation systems and providers of building management services.