When people talk about safety in a building, they often split the conversation into two neat buckets: secure entry for control, and emergency egress for escape. In practice, those buckets collide. A security change gets installed to prevent unwanted access, and suddenly the building's evacuation routes feel harder to use, slower to understand, or less reliable under stress. Or the other way around, an "always open" approach to convenience turns into a liability because it defeats the very controls the building needs.

The truth is less dramatic and more technical: emergency egress and secure entry are not competing goals. They are two parts of the same safety system. The difference is how they are designed, how they behave during normal conditions, and how they fail during emergencies.

I have worked with teams that built protocols beautifully on paper, then watched real occupants struggle in drills because a door behaved differently than people expected. That gap between design intent and lived behavior is where most failures happen. The best solutions protect both priorities without relying on perfect compliance or calm thinking.

What "secure entry" really means on the ground

Secure entry sounds simple, but in a functioning facility it usually includes at least three layers of intent:

First, access control. A building wants to allow the right people in and keep others out. That can mean keyed doors, access badges, keypad codes, managed unlock schedules, and sometimes guard presence.

Second, behavior management. Security is also about preventing tailgating, discouraging propping, and reducing the chance someone wanders into restricted areas because "it looks open."

Third, accountability. Logs, audit trails, and monitoring matter when you need to investigate incidents, verify who accessed a room, or prove a control was active at a given time.

Those layers often translate into hardware choices like electromagnetic locks, maglocks, magnetic strikes, motorized doors, controlled doors that remain latched until an unlock signal arrives, and turnstiles or gates in entry vestibules. None of those are inherently unsafe. Problems surface when the door is treated as if it only has one job.

A door is not just an interface. It is a direction decision for an occupant's body under stress, and it is a flow constraint for firefighters and rescue operations. The door's behavior during emergencies is not optional. It has to be predictable, fast, and compliant.

Emergency egress is not "leaving quickly," it is "leaving reliably"

Emergency egress is often described as a matter of speed, but reliability is the real metric. When smoke fills a corridor or a fire alarm forces movement, people do not navigate like they do during normal life. They look for familiar patterns, they follow visual cues, and they copy the nearest person. If a route requires an unfamiliar action, or if a door's lock behavior is ambiguous, movement slows or stops.

Egress design usually aims to ensure:

- Exit access stays usable under the expected conditions.
- Doors open in the right direction and with appropriate hardware behavior.
- People can move from their location to an exit without encountering "dead ends" created by security controls.

- The system maintains functionality during power loss, alarm events, or other abnormal states.

A critical detail is that security hardware frequently depends on power and control signals. If you lock something with a maglock that depends on an energized state, you must also be sure you are defining what “safe” means when power drops. Many door systems “fail safe” by unlocking when power is removed, but not all installations do that correctly or consistently.

I have seen door schedules that look correct on Monday, but during a holiday shutdown they switch to a maintenance mode and behave differently. An egress route that depends on an access control override can become a surprise during an actual event.

Where the two goals collide: common failure points

The overlap between secure entry and emergency egress is not theoretical. It shows up in real issues that facilities teams wrestle with during inspections, drills, and incident reviews.

One common failure point is the tendency to use the same control logic for normal security and emergency behavior. In a secure building, it can make sense to keep doors locked until someone is authenticated. During an emergency, authentication is irrelevant. A person’s identity does not change the physics of smoke, or the time it takes to travel.

If the security control does not switch to egress-appropriate behavior when alarms activate, evacuation becomes a problem. That can occur when the controller is not integrated with the fire alarm system, when the wiring is incomplete, or when someone later changes the fire alarm programming but forgets the door strategy.

Another failure point is “convenience customization.” Facilities sometimes override hardware to improve day-to-day usability. The override might disable alarms on the door, change how a latch engages, or introduce a delay for an electric strike. The result can be a door that sometimes behaves like a free egress door and sometimes behaves like a locked access door, depending on time of day, occupancy schedules, or maintenance states.

Then there is the human side. People will prop doors that are inconvenient or slow. Security teams sometimes add additional latching features to prevent propping, but those changes can make doors heavier, harder to open, or less intuitive for the next person. Propping is a symptom, not the disease. If a door system creates friction, occupants will find workarounds, and those workarounds can defeat both security and fire separation intent.

The design principle that prevents most trouble: define two states and test the transitions

The simplest way I have seen teams solve the conflict is to treat the door system as having distinct, intentionally designed states.

During normal operation, secure entry can do its job. During an emergency, the system shifts behavior to prioritize occupant egress. The most important part is the transition between those states.

That transition should be deterministic. If the fire alarm activates, doors should move into an egress-friendly behavior without requiring someone to badge, press a hidden request switch, or guess whether a keypad is still active. If power fails, the behavior should follow the intended fail mode, not a side effect of how the hardware was installed.

Even when a facility is technically compliant, inconsistent behavior undermines trust. A building’s safety is not just code. It is also how people perceive and react under stress. If an occupant has learned that a door sometimes

needs a badge, then during an alarm they may try the same action. The system must make the correct action obvious.

Design and test like you are dealing with a person who is confused, moving quickly, and wearing low visibility.

Hardware categories and how intent gets expressed

Without getting lost in manufacturer-specific details, it helps to understand the broad categories of door hardware used in controlled entrances and secure areas.

Some doors are controlled with electromagnetic locking devices that release when power is removed, which is commonly described as “fail safe” for egress. Others use electrically powered latches or strikes that may be configured to stay locked unless the controller sends a release command. Some systems include delayed egress functions, which can be appropriate in specialized settings but require careful coordination so they do not trap occupants.

Motorized doors add another layer, because an automation controller can introduce delay, sensor misreads, or “stuck door” behavior if power or network connectivity fails.

The practical insight is that integration matters as much as hardware selection. A maglock wired incorrectly might not release as intended. A strike might be powered in a way that behaves opposite of what the drawings claim. A door that is set up for controlled access in one state can become unpredictable if the fire alarm inputs are not mapped correctly.

This is why field verification is essential. Documentation is not a replacement for watching the door operate during alarm activation and power interruption. You want to see the sequence: who gets a release, what signals are used, how long any delay lasts, and whether the door returns to normal operation after the event.

A short checklist you can use to sanity-check an existing facility

You do not need to be an engineer to notice whether a facility is at risk. The goal of this checklist is not to prove compliance, but to surface obvious gaps that often correlate with real problems.

1. During a drill, do exit route doors unlock or open immediately when the alarm activates, without requiring badges or keycodes?
2. If power is interrupted in a controlled test, do the doors on the egress route revert to their expected fail-safe behavior?
3. Are doors clearly operable by pushing in the expected direction, without unusual force, weird latch points, or intermittent “sticking”?
4. Are security features such as vestibules, gates, or interlocks designed so that exiting does not require someone to “wait for access” logic?
5. Do signage and occupant education match what people experience, not what the control panel suggests?

If you can’t answer those confidently, the risk is real, even if the system looks “locked” on inspections.

Vestibules, gates, and the trap of conditional movement

Secure entry design often uses vestibules to add an extra layer between the public and the restricted interior. That can be appropriate, especially for government buildings, data centers, healthcare facilities, or any site with sensitive assets.

But vestibules and gated entries create a behavioral problem during egress if the exit path is not simple. For instance, if the vestibule door uses a controlled unlock method that requires a credential, occupants might instinctively attempt to authenticate while the alarm is sounding. If there is a second door in the vestibule that is also controlled, you can accidentally create a two-step exit process that adds time and confusion.

Another trap is interlocked systems. Interlocks are often intended to prevent both doors of a vestibule from being open at once, improving security and sometimes supporting environmental control. During an emergency, interlocks need to be overridden. Otherwise, one door may remain locked because the system is still enforcing the "both closed" or "one at a time" logic.

Gated entries add similar risks. Turnstiles and security gates might be excellent for access control, but if they do not provide a straightforward bypass or are not designed to free movement during alarm events, they can become bottlenecks. In emergencies, bottlenecks are not just uncomfortable. They become a measurable impact on egress performance and congestion.

The key is to design egress routes that do not require coordinated movement through security layers. If you must have controlled spaces, you need a clear and immediate escape path that treats security as subordinate to life safety.

Delayed egress: useful in the right context, dangerous when misunderstood

Delayed egress is one of those ideas that sounds reasonable to stakeholders until the details matter. The intent of delayed egress is to slow down movement to prevent harmful behavior or to manage certain security scenarios. It can be used in specific settings where the building is engineered and staffed to handle occupant behavior and where the door strategy aligns with life safety requirements.

The risk comes when delayed egress logic is applied without a strong operational understanding. Occupants may not realize that "exiting" means waiting through a delay. In a crisis, waiting feels like getting blocked, which can prompt panic and force people to look for alternative exits. Alternative exits may be longer, less direct, or blocked by other security decisions.

From a facilities perspective, delayed egress can also complicate drills. In a drill, you can tell people to disregard the delay. In a real emergency, you cannot. So the delayed behavior must still comply with the intent of life safety and should only be used where the design is justified.

If your building has delayed egress features, make sure your training and signage reflect what actually happens, and that your fire safety team reviews how it performs during smoke, alarms, and power interruptions.

Power failure scenarios: the practical difference between "designed" and "installed"

People often talk about emergency behavior as if it is purely a design feature. In real buildings, the installation and wiring details determine what the device does when the world changes.

Consider a controlled door that is meant to unlock when the fire alarm activates. If the integration depends on an auxiliary relay, that relay coil might be wired incorrectly, or might fail intermittently. If it depends on a door controller that loses network connectivity or is configured to ignore certain alarm classes, then the door might not receive the release signal.

Power failure is where these issues surface quickly. Even when a system is described as fail safe, the facility may have configured standby power in an unexpected way, or the device may have a dependency on a power distribution board that trips during an event.

This is why testing needs to cover more than “push to exit.” For egress routes, you want to confirm:

- What happens during a fire alarm event.
- What happens during loss of normal power.
- What happens during loss of control signal.
- How the system behaves afterward, during reset.

In my experience, the last part is often overlooked. A building might behave correctly during the first activation, then revert incorrectly after a reset. That can matter for multi-stage evacuations or reentry decisions.

Integration with fire alarm systems: don’t treat it as a checkbox

A secure entry strategy often lives with an access control system, while emergency functions live with the fire alarm and life safety system. The integration between them is where misunderstandings happen.

Teams sometimes assume that “the fire alarm will unlock doors” because there is a general statement in a specification, or because a vendor claims integration is standard. But standard integration still requires mapping: which doors, which alarm zones, which alarm conditions, and what delay or override logic is applied.

There is also a subtle but important point. Fire alarm systems can produce multiple states, including pre-alarm, alarm, trouble, and supervisory signals. You need to understand which of those states are intended to unlock which doors. If the door unlocks on the wrong state, you can defeat security too early or allow movement that should remain controlled. If it does not unlock on the correct state, you can trap occupants.

This is where collaboration matters between the stakeholders who care about security and those who care about life safety. You want shared language. You want test procedures that both teams recognize as meaningful. And you want an owner’s acceptance process that includes door operations, not just panel status.

When security is in restricted areas, not just at entrances

Some facilities treat security as an exterior boundary. Others secure internal spaces heavily, using controlled doors between departments, storage rooms, labs, data areas, or office suites.

Internal secure doors can still intersect with egress if those spaces have occupancy and if the doors are on the route to an exit. If a secure door is not on the primary exit route, you still need to ensure occupants can leave that space without being forced into a controlled access decision.

That may mean ensuring that egress from those spaces uses free egress hardware like panic bars or equivalent unlatching mechanisms, even if the door remains locked in normal operation. It may mean making sure that door locks do not prevent opening in the egress direction.

The judgment call here is location-dependent. A door that is perfectly safe for security might still be unsafe for egress if it is located on a path a confused occupant will take. The solution is to map likely occupant movement, not just code-defined paths. If people routinely walk through a secure corridor to reach a stairwell, then that corridor door is part of real egress behavior.

Training, drills, and the difference between “paper compliance” and “muscle memory”

A building can meet requirements and still fail people. That failure is often a training and familiarity problem.

During drills, I often ask occupants to point out their exit routes, then watch them walk without instructions. If they hesitate at a controlled door, that is the building telling you something. If they try to badge or key in where they shouldn’t, that is the building contradicting their learning. If they look for a staff member to open the door because the hardware feels wrong, that is a cue that the door is too ambiguous for real emergencies.

Muscle memory can be built in normal time too. If doors behave differently by time schedule, people will naturally learn those patterns, and those patterns can become dangerous when the alarm changes everything. The safest goal is that, during an alarm, the building behaves in a way that people can interpret without instruction.

Training should also cover what staff should do beyond “pull the alarm.” In a well-run facility, staff know which doors unlock, which doors must remain closed, and which doors should be directed to avoid. They also understand who has authority to manage security systems after an event while preserving life safety.

A practical incident example that shows why details matter

In one facility review I supported, the building had done a security upgrade across a set of office suites. The entrance doors were controlled, and internal secure doors were also upgraded to improve restriction enforcement.

On the first alarm drill after the upgrade, the exit route doors behaved as expected for some areas, but not for others. A subset of internal doors did not release until a specific alarm class was triggered, not the alarm event that was being simulated in the drill. The occupants did not attempt to badge, but they did hesitate and look around for assistance. Movement slowed enough to create crowding at the stairwell landing, even though the building was otherwise capable of clearing.

The fix was not to remove security. The fix was to align the alarm integration logic so that the correct alarm state caused the right doors to release during egress. After the change, we retested the exact alarm conditions used in drills and verified behavior across all door types, including those that depended on a local controller.

The lesson was simple. You can have the right hardware and still get the wrong outcome due to integration timing and alarm state mapping. That is why “getting it right” means validating the system under real sequences, not just trusting the plan.

Checklist for the alarm and egress transition test (keep it tight)

Here is a compact way to approach testing transitions without turning the effort into a project. Use this when you are verifying that secure entry and emergency egress work together.

1. Activate an alarm scenario that matches the fire alarm system’s behavior in real events, then observe every door on the primary egress paths.
2. Simulate loss of normal power, and confirm the egress route doors follow the intended fail-safe behavior.
3. Verify occupant operation, not just door operation, by having a small group attempt to exit as if they were under time pressure.
4. After the test, confirm the system returns to normal security behavior without leaving doors unlocked longer than intended.

This kind of test pays for itself quickly. It finds ambiguity, delay, and “it works when we tested it the day we tested it” problems.

Getting the balance right: decision guidelines that help stakeholders agree

When security and life safety teams disagree, the disagreement usually comes from different risk models. Security teams fear unauthorized access and tailgating. Life safety teams fear delayed egress, trapped occupants, and confusing door behavior under smoke.

The way to resolve that is to make trade-offs explicit. In most buildings, you can preserve secure entry during normal times without compromising egress. But you might need to accept that security mechanisms will behave differently during alarm and power loss.

A good decision framework is to ask, for every controlled door and every access feature, three questions:

- What should happen to this door during a fire alarm state?
- What should happen during power loss and control failure?
- How will an occupant interpret the door’s behavior in the first 10 seconds of confusion?

If the answers are clear and consistent across the building, you reduce both legal risk and human risk. If they differ by time schedule, alarm zone, or controller state, you increase the chance of failure at the worst possible moment.

What “good” looks like in real buildings

When emergency egress and secure entry are aligned, a building feels calm in the way it handles movement. During normal operations, access control does not obstruct legitimate entry or create friction that people circumvent. During emergencies, doors behave predictably, releasing or opening without requiring credentials.

Occupants still might be scared, but they are not trapped by doors that ask for permission when permission no longer matters. Staff are not scrambling to interpret which door logic is active. Inspectors and auditors see documentation that matches field behavior.

That alignment is rarely accidental. It comes from integration discipline, testing that covers *access control systems installation* alarm and power scenarios, and a willingness to revise designs when the building’s real behavior diverges from the intended behavior.

If you are responsible for security and life safety in the same environment, your job is not to choose between control and escape. Your job is to engineer the moments where control stops and escape starts, then prove that it happens the way people need it to happen.