

N9LYA TECHNICAL GUIDES

Security Systems A to Z

Intrusion, Video, Access Control

Jerome M. Kutche

N9LYA

Second Edition · September 2026

About This Book

Security systems occupy an awkward gap in the technical literature.

The manufacturer documentation tells you how to wire their panel. The trade magazines tell you what's new. The certification material tells you what's on the exam. And almost nothing tells you how to think about the whole thing — how the pieces fit, what actually matters, and where the decisions get made that determine whether a system works or merely exists.

This book is that.

What It Covers

Intrusion detection, video surveillance, access control, and the infrastructure underneath all three — power, cabling, networking, and the increasingly unavoidable cybersecurity of devices that used to be isolated.

It covers residential, commercial, and industrial contexts, because the principles are shared and the constraints differ. Where they diverge, I say so.

The Perspective

I spent over three decades in industrial electrical and controls work. That shapes this book in several specific ways.

Power and infrastructure get proper treatment. A great many security system failures are power failures, grounding failures, or cabling failures wearing a costume. The chapters on those are longer than you'll find elsewhere, because in the field that's where the problems are.

Life safety is treated as the serious matter it is. Chapter 16 is the most important chapter in this book. Electrified locking hardware installed without understanding egress requirements has killed people, and it continues to be installed wrong by people who mean well. If you read one chapter, read that one.

Troubleshooting gets its own methodology, because diagnosing a system that worked yesterday is the actual job, and it's taught almost nowhere.

And there's honest treatment of what security systems don't do. A camera does not prevent a burglary. An alarm does not stop an intruder. Understanding what each element actually contributes — and what it doesn't — is the difference between a designed system and a collection of purchased equipment.

Who This Is For

Installers and technicians wanting the reasoning behind the practice.

Electricians and low-voltage contractors adding security work. Part I and Chapters 19 and 20 will feel familiar; Parts II through IV are the new material.

Facility and security managers specifying, buying, and living with these systems. You don't need to pull cable to benefit from knowing what to demand and what to reject.

IT people inheriting security systems, which happens constantly now that everything is on the network. Chapters 21 and 22 are yours specifically.

Homeowners and small business owners doing it themselves. Everything applies at smaller scale, and Chapter 16 applies to you too.

A Word on Scope

This book is not a substitute for code compliance, licensing, or authority having jurisdiction approval.

Security and life safety work is regulated. Requirements vary by jurisdiction, occupancy type, and building classification, and they change. Electrified locking, fire alarm interfaces, and anything affecting egress require design by qualified people and approval by the authority having jurisdiction — typically the fire marshal or building official.

Where this book states a requirement, verify it against your applicable code and your AHJ. I've been deliberate about flagging the areas where that matters most.

How to Use It

Each chapter ends with a **Field Check** — things to verify, measure, or test on a system you're responsible for. Do them. Reading a specification and confirming a specification are different activities, and the gap between design intent and installed reality is where most problems live.

About the Author

Jerome M. Kutche holds the amateur radio callsign N9LYA, first licensed in 1991. He spent over three decades in industrial electrical and controls work across manufacturing and heavy industry — Allen-Bradley and Siemens PLC systems, motor control centers, plant electrical maintenance and supervision — and holds NFPA 70E, lockout/tagout, arc flash, and thirty-nine other professional certifications.

From 1990 to 1996 he built RF test and measurement equipment for the telecommunications and cable television industries. He serves as Indiana's 44Net/AMPRNet coordinator and is trustee for two amateur radio clubs, and runs a segmented network with rather more cameras, sensors, and monitoring than is strictly necessary.

Most of the practical advice in this book comes from finding out the hard way.

Part I — Foundations

Chapter 1: What a Security System Does

Before any equipment decision, understand what you're actually trying to accomplish. Most bad systems are bad because nobody asked this.

The Four Functions

Every physical security measure performs one or more of four functions:

Deter — discourage the attempt. Visible cameras, lighting, signage, fencing, the appearance of occupancy. Cheap and it works on the opportunist and not on the determined.

Detect — notice that something is happening. Sensors, cameras, guards, and the people who work there.

Delay — slow the adversary down. Locks, doors, barriers, safes. **Delay is measured in time**, and its value is entirely relative to response time.

Respond — do something about it. Guards, police, staff, or automated action.

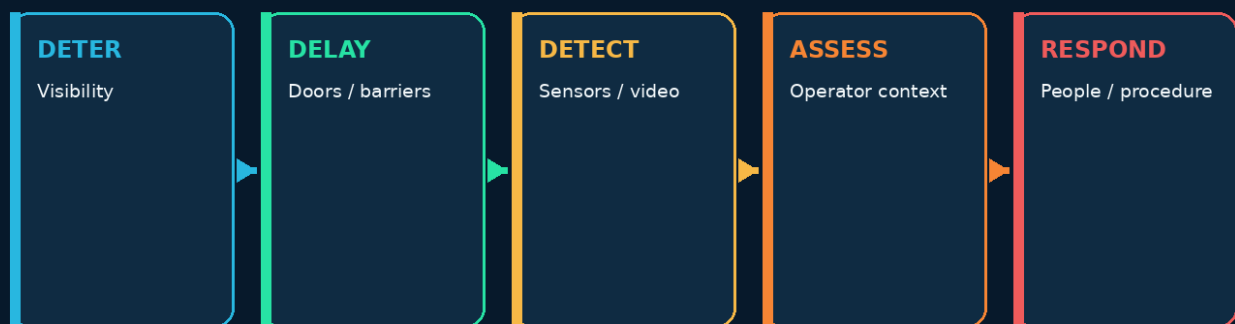
The critical relationship: delay must exceed response time, or detection accomplishes nothing.

A system that detects an intrusion and summons a response arriving in twelve minutes, protecting assets an intruder can take in four, has failed. Not because the detection failed — because the delay was insufficient.

This single relationship should drive your design, and it's the calculation almost nobody performs.

Security Is a Layered System

Detection without response is only information



N9LYA TECHNICAL GUIDES

Figure 1: Layered physical security

What Each Element Actually Contributes

Being clear-eyed here prevents a great deal of wasted money.

Cameras do not prevent crime. They deter marginally, they detect if someone is watching or analytics are working, and they provide evidence afterward. **A camera with nobody watching and no analytics contributes nothing until after the event.** That's a legitimate purpose — evidence and investigation have real value — and it should be understood as what you're buying.

Alarms do not stop intruders. They detect and they summon. If nothing responds, an alarm is a noise.

Locks do not prevent entry. They delay. Every lock can be defeated given time and tools; the question is how much time, with what tools, and whether that exceeds your response time.

Guards are the only element that does all four, which is why they're expensive and why they remain irreplaceable for high-value protection.

Lighting deters and enables detection — both by people and by cameras — and it's one of the highest value-per-dollar measures available.

Layers

Defense in depth — concentric rings, each requiring separate defeat.

Perimeter — property line. Fencing, gates, exterior lighting, perimeter detection.

Building exterior — walls, doors, windows, roof. Locks, contacts, glass break, exterior cameras.

Interior common areas — motion detection, interior cameras, access control on internal doors.

Restricted areas — server rooms, cash handling, controlled substances, hazardous materials. Higher-grade controls.

Assets themselves — safes, cabinets, cages, item-level tagging.

The design question is never “is this control sufficient?” It is **“when this control fails, what catches it?”** If the answer is nothing, you have a single point of failure regardless of how good that control is.

Threat Types

Different adversaries require different responses, and designing for the wrong one wastes money.

The opportunist — unplanned, low skill, deterred easily, defeated by basic measures. **The overwhelming majority of incidents.**

The determined amateur — some planning, some tools, will attempt to defeat obvious measures. Layered controls and prompt response handle this.

The professional — researched, equipped, patient, will circumvent controls. Requires detection depth, hardened delay, and fast response.

The insider — has legitimate access. **Bypasses your perimeter entirely by definition.** Addressed with least privilege, separation of duties, audit trails, and monitoring of access to sensitive areas rather than with better locks.

The unintentional — the employee propping a door, the contractor who was never escorted, the delivery driver who tailgated. **Frequently the largest actual risk** and addressed by procedure and culture rather than equipment.

Design against your realistic threat. Most facilities face opportunists and insiders. Systems designed against professionals while insider access goes unmonitored are protecting the wrong thing.

Common Design Failures

Buying equipment before defining requirements. The most common and most expensive error.

Cameras where they look good rather than where they see something useful.

Detection without response. An alarm nobody answers.

Delay insufficient for response time.

Ignoring the insider.

Ignoring the human factor — controls people bypass because they make the job impossible. A propped fire door defeats a hundred thousand dollars of access control, and the person propping it is solving a real problem you created.

No maintenance plan. Systems degrade. Cameras drift out of focus, sensors fail, batteries die, and nobody notices until it matters.

Field Check

1. For a facility you know: what's the actual response time, and what's the delay?
2. List every camera and state what it's actually for — deterrence, detection, or evidence.
3. Identify one control that people routinely bypass. Why?
4. Name the realistic threat. Is the system designed against it?

Chapter 2: Risk Assessment and Design



Figure 2: Risk-based security design

The process that turns a vague sense of insecurity into a specification.

The Method

1. Identify assets. What are you protecting? People first, always. Then property, information, operations, and reputation.

Be specific. “The building” is not an asset list. The server room, the pharmacy, the cash office, the chemical storage, the vehicles, and the people working the late shift are.

2. Identify threats. What could happen? Burglary, robbery, vandalism, theft by employees, workplace violence, unauthorized access, sabotage, and — frequently forgotten — accidents and natural events.

3. Assess vulnerability. How exposed is each asset to each threat? Walk the property. Look at it as an adversary would. **What’s the easiest way in, and what’s the easiest way out with something valuable?**

4. Assess consequence. What happens if it occurs? Financial loss, operational disruption, regulatory exposure, harm to people.

5. Calculate risk.

$$\text{Risk} = \text{Threat likelihood} \times \text{Vulnerability} \times \text{Consequence}$$

The numbers are estimates. **Their value is in forcing comparison and prioritization**, not in precision.

6. Choose treatments. Mitigate, transfer (insurance), avoid (stop doing the risky thing), or accept — deliberately and in writing, with a name attached.

Accepting risk is legitimate. What isn’t legitimate is accepting it implicitly, by never having assessed it.

Surveying a Site

Walk it at different times. A facility at 2 p.m. on a Tuesday and 2 a.m. on a Sunday are different places. Lighting, occupancy, visibility, and traffic all change.

Walk the perimeter completely. Look for gaps in fencing, gates that don’t latch, overgrowth providing concealment, and the informal path everyone actually uses.

Try the doors. All of them. You will find unlocked doors, doors that don’t latch, and doors propped for convenience.

Look up. Roof access, skylights, and second-story windows reachable from a dumpster, a truck, or an adjacent structure.

Look at the utilities. Where does power enter? Where does the telephone or fiber enter? Are they accessible from outside? **A system whose communication path is cuttable from outside the protected area has an obvious defeat.**

Note the lighting, and note where it doesn’t reach.

Talk to the people who work there. They know which door sticks, which alarm goes off for no reason, which area feels unsafe, and where the informal shortcuts are. **This is consistently the highest-value part of a survey** and it’s the part consultants skip.

Writing a Specification

A good specification states requirements, not products.

“Video coverage of the loading dock sufficient to identify a person’s face at the door” is a requirement. “One 4MP bullet camera” is a purchase order.

Requirements should specify:

- **What must be accomplished** — detect, observe, recognize, identify. Chapter 12.
- **Coverage areas**, precisely

- **Environmental conditions** — lighting, weather, temperature
- **Retention** requirements, and where they come from (policy, regulation, insurance)
- **Availability** — what happens during a power or network failure
- **Integration** requirements
- **Response** expectations
- **Compliance** requirements

Then evaluate proposals against the requirements. This is what makes competing bids comparable, and it's what prevents the outcome where you get exactly what you asked for and it doesn't do what you needed.

Documentation

What every system should have and most don't:

As-built drawings — actual device locations, actual cable routes, actual panel positions. **Not the design drawings.** They will differ.

Device schedule — every device, its location, its address or zone, what it covers, and its cable run.

Cable schedule — what runs where, what type, and which pair does what.

Programming record — zone assignments, user codes, schedules, access levels, camera settings.

Network documentation — addresses, VLANs, credentials location.

Test records — what was tested, when, by whom, with what result.

Contact list — who responds, who services, who authorizes.

Store it off-site as well as on. Documentation locked inside the building you can't get into is not documentation.

Field Check

1. Perform a walk-through of a facility at an unusual hour.
2. Try every exterior door. Record what you find.
3. Identify where power and communications enter, and whether they're accessible.
4. Ask three employees where they feel the security gaps are.
5. Locate the as-built documentation for a system you're responsible for. Does it exist?

Chapter 3: Codes, Standards, and Legal Constraints

The rules that constrain the design. Ignoring them produces systems that fail inspection, void insurance, or get people hurt.

The Authority Having Jurisdiction

The AHJ is the person or office empowered to approve and enforce. Typically the fire marshal, building official, or electrical inspector.

The AHJ's interpretation governs. Code language is subject to interpretation, and the AHJ's interpretation is the one that matters. **When in doubt, ask before installing.** A conversation is free; a re-installation is not.

Get approvals in writing where anything is unusual.

Codes That Apply

NFPA 101, Life Safety Code — egress requirements. **This is the code that governs electrified locking,** and Chapter 16 covers it. Its requirements are non-negotiable and they exist because people have died.

International Building Code (IBC) — parallel requirements, adopted in most US jurisdictions.

NFPA 72, National Fire Alarm and Signaling Code — fire alarm systems, and the interface between fire alarm and access control.

NFPA 70, the National Electrical Code — wiring. **Article 725 covers Class 2 and Class 3 power-limited circuits**, which is what most security wiring is. Article 800 covers communications circuits. **Requirements for cable listing, plenum rating, separation from power conductors, and support are all here.**

NFPA 70E — electrical safety in the workplace. Relevant whenever you're working near energized equipment.

Local amendments — jurisdictions modify model codes. Read yours.

Standards and Listings

UL listings — equipment tested to a standard. **UL 294** for access control, **UL 1076** for proprietary alarm units, **UL 681** for installation of burglar alarm systems, **UL 2050** for national industrial security. Insurance and some regulations require listed equipment and, sometimes, a certificate from a listed installation.

ANSI/BHMA grades for locking hardware — Grade 1 (heavy commercial), Grade 2, Grade 3 (residential). **Grade matters for delay time** and for durability.

IEC 62676 — video surveillance systems, including the image quality classifications in Chapter 12.

ONVIF — an interoperability standard for IP video and access control. **Its practical value is avoiding vendor lock-in**, and conformance is variable — “ONVIF compliant” covers a range of actual interoperability. Test before committing.

NIST and CISA guidance for anything touching federal work or critical infrastructure.

Privacy and Legal Constraints

This section is where installers get organizations in trouble.

Video recording of areas with a reasonable expectation of privacy is prohibited. Restrooms, changing areas, locker rooms, and medical treatment areas. **This is not a gray area.** Cameras have been installed in these locations by people who thought they had a good reason, and the consequences have been severe.

Audio recording is regulated separately and more strictly than video in most jurisdictions. Many US states require the consent of all parties to record a conversation. **Many IP cameras have microphones enabled by default**, which can make a lawful video installation an unlawful audio interception. **Check your state law and disable audio unless you have specific authorization.**

Notification requirements — many jurisdictions require signage where surveillance is in use. Some require it in specific language and placement.

Employee monitoring — subject to labor law, collective bargaining agreements, and in some jurisdictions specific notification requirements.

Data protection law — video of identifiable people is personal data under the GDPR and a growing number of state laws. That brings obligations around retention limits, access requests, security of the footage, and lawful basis for processing.

Retention — keep long enough to be useful, and no longer than policy or law permits. **Indefinite retention is a liability**, not a feature.

Facial recognition and biometrics are specifically regulated in a growing number of jurisdictions, some requiring explicit consent and imposing significant penalties. Several US states have biometric privacy laws with private rights of action. **Do not deploy biometric systems without legal review.**

Recording in another party's space — cameras pointed off your property at a neighbor's windows or a public sidewalk raise both legal and neighbor-relations problems. Aim them at what you own.

Procurement Restrictions

Certain equipment is restricted for government-funded and government-adjacent projects. US federal law restricts procurement of video surveillance and telecommunications equipment from specific named manufacturers for government use and for entities receiving certain federal funding.

The specifics change, and the practical guidance doesn't: **if the project involves government funding, a government customer, or critical infrastructure, verify the equipment's eligibility before specifying it.** Discovering this after installation is expensive.

Insurance

Insurance policies frequently specify security requirements — certified alarm systems, specific lock grades, monitoring, and testing. **A system that doesn't meet policy requirements can void coverage for a claim.**

Read the policy. Know what's required and document compliance.

Licensing

Most jurisdictions license alarm installation, and many license low-voltage contracting separately. Requirements vary widely — some require a licensed electrician, some a specific alarm license, some both.

Unlicensed installation can void insurance, fail inspection, create personal liability, and in some jurisdictions constitute a criminal offense.

Know what your jurisdiction requires before you take money for the work.

Field Check

1. Identify your AHJ and their contact information.
2. Determine what licensing your jurisdiction requires for the work you do.
3. Check whether any camera in a system you manage has audio enabled. Verify it's lawful.
4. Review the retention period on a video system against policy and applicable law.
5. Verify no camera covers an area with a reasonable expectation of privacy.

Chapter 4: Power

More security system failures trace to power than to any other cause. This chapter is the one my background makes me insist on.

Why It Matters

A security system that stops when the power does is not a security system. It's a convenience feature that works when nothing is wrong.

And an intruder who cuts the power — which requires no skill and no tools beyond what's in a truck — should not thereby defeat the system.

Backup power is not optional. It's the difference between a system and a decoration.

Supply Basics

Most security equipment runs on low-voltage DC — 12 V or 24 V — derived from a transformer or switching supply.

Voltage drop is the constraint that catches people. Over a long run of small conductor, voltage at the device is lower than at the supply.

Voltage drop = $2 \times \text{Length(ft)} \times \text{Current(A)} \times \text{Resistance per foot}$

The factor of two accounts for the return conductor.

Approximate resistance per 1,000 ft:

Gauge	Ohms per 1,000 ft
22 AWG	16.1
20 AWG	10.1
18 AWG	6.4
16 AWG	4.0
14 AWG	2.5

Worked example: a 500 mA device, 300 feet away, on 18 AWG.

Drop = $2 \times 300 \times 0.5 \times (6.4 / 1000) = 1.92 \text{ V}$

A 12 V supply delivers about 10.1 V at the device. **Many devices specify a minimum around 10.2 V**, so that's marginal — and it gets worse as the battery discharges and the supply voltage sags.

The fixes: heavier conductor, shorter run, a local power supply, or a higher supply voltage regulated down at the device. **Twenty-four volt systems tolerate roughly four times the voltage drop** for the same percentage, which is why longer runs use 24 V.

Calculate before you pull cable. Discovering a voltage drop problem after the walls are closed is expensive.

Maglocks deserve specific attention — they draw substantial current continuously, and a maglock at the end of a long undersized run will hold weakly or intermittently, which is a security failure that looks like a hardware defect.

Batteries

Sealed lead-acid is standard for alarm and access panels. Inexpensive, tolerant of float charging, and it degrades predictably.

Sizing:

Amp-hours = Total standby current (A) $\times$ Standby hours
+ Alarm current (A) $\times$ Alarm hours

Typical requirements: 4 hours standby for burglar alarm, 24 hours for fire alarm, both plus alarm-condition time. **Verify your specific code requirement**, since it varies by system type and jurisdiction.

Derate. A battery does not deliver its rated capacity in practice — cold reduces it, age reduces it, and high discharge rate reduces it. **Size at least 25% above the calculation.**

Batteries fail predictably and silently. A sealed lead-acid battery in float service typically lasts three to five years, and it fails by losing capacity rather than by dying outright. **A system with a three-year-old battery may run for eight minutes instead of four hours**, and nothing indicates this until the power fails.

Test under load, annually. A voltage reading on an unloaded battery tells you almost nothing — a nearly dead battery reads close to nominal until you draw current from it. **Disconnect AC and verify the system runs for its required duration.**

Replace on schedule, not on failure. Date them when installed.

Lithium chemistries are appearing in this space with longer life and better energy density. They require appropriate charging and protection circuitry, and they must not be substituted into a charger designed for lead-acid.

Grounding and Bonding

Two different things, and both matter.

Grounding connects to earth. **Bonding** connects metal parts together so they're at the same potential.

For security systems:

Bond equipment enclosures per the electrical code.

Ground shields at one end only for low-frequency signal cable, typically at the panel. **Grounding a shield at both ends creates a ground loop** — a circulating current driven by potential differences between the two points, which injects noise into the signal. This is a leading cause of video noise and unexplained sensor behavior.

Surge protection on anything entering the building from outside. Exterior cameras, gate operators, perimeter sensors, and any cable run between buildings.

And the point I insist on: a copper cable run between two buildings is a lightning path. Different structures have different ground potentials, and a conductor bonds them. This has destroyed a great deal of equipment and started fires.

Use fiber for inter-building runs. It's immune to this entire category of problem, it eliminates the ground potential difference issue completely, and it costs less than replacing a recorder, a switch, and eight cameras. If copper is unavoidable, use properly grounded surge protection at both ends and understand you've accepted a risk.

AC Supply

Know what circuit feeds the system, and what else is on it. Turn the breaker off and note what dies. Write it down.

Dedicated circuit for the head end where practical. A security system sharing a circuit with a copier or a space heater will experience nuisance trips.

Continuous loads should not exceed 80% of circuit rating — 1,440 W on a 15-amp, 120 V circuit. Security equipment runs continuously by definition.

Label the breaker so nobody turns it off during unrelated work. **And consider a lock-out device** on the breaker feeding the security head end, because someone will eventually shut it off to work on something else and not turn it back on.

UPS for the head end — recorders, servers, and network switches. Sized on the watt rating rather than the VA figure on the box, and signaled so shutdown is graceful. **Test it annually by pulling the plug deliberately.**

Never daisy-chain power strips. The failure mode is fire.

Power over Ethernet

Increasingly how cameras and some access control devices are powered. Appendix B tabulates the standards; two points belong here:

Budget the switch, not just the port. A switch with a 370 W PoE budget and 24 ports cannot deliver 30 W to all of them.

PoE devices need backup too. A PoE camera is powered by the switch, so **the switch needs to be on the UPS** or the cameras die with the lights.

End of the free sample

Security Systems A to Z — Second Edition · by Jerome M. Kutche

That was the first 12 of 70 pages. The full book continues with the practical detail, worked examples and recovery steps that don't fit in a sample.

Get the full book (\$8.99, PDF + EPUB):

<https://booksrus.biz/product/security-systems-a-to-z/>

Also on Gumroad:

<https://n9lya4.gumroad.com/l/whjehd>



All 17 Second Edition guides in one bundle for \$89.99:

booksrus.biz/product/n9lya-technical-guides-complete-bundle

This sample may be shared freely in unmodified form. © Jerome M. Kutche. Second Edition.