

the FOUNDATION FOR
INFRASTRUCTURE RESILIENCE

The Domains

An Introduction

Foundation for Infrastructure Resilience

November 2026

Foundation for Infrastructure Resilience, Inc. ("FIR"™), a non-profit 501(c) (3) Delaware Corporation.

Our Vision

A secure and prosperous future where resilient and sustainable critical infrastructure empowers communities and safeguards our nation.

Our Mission

Improve the quality of life and help ensure the continuity of the United States by facilitating sustainable communities and resilient critical infrastructures, fortified against threats and meeting the needs of the 21st century.

Legal Disclaimer: The Foundation for Infrastructure Resilience makes no representations or warranties of any kind, whether express, implied, statutory or otherwise regarding the content of this document, third party content or references to services or information referenced or available through links herein, and further disclaims all warranties regarding any information contained herein, including any implied or express warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, arising out of any course of dealing or usage of trade, that the third-party service will be uninterrupted, error free or free of harmful components.

© 2026 Foundation for Infrastructure Resilience
All Rights Reserved

Contents

FIR Book 5: The Domains — An Introduction 1
About this book set, and who it is for 1
About this book 2
How this book is organized 2
Chapter 1 — What hardening means 3
Readiness versus hardening 3
The survivable thresholds 3
The compliance domains 3
The human foundation 3
Chapter 2 — Energy 4
Islanded, not independent 4
What hardening looks like here 4
The hard line 4
Chapter 3 — Water and wastewater 5
The two halves 5
What hardening looks like here 5
Chapter 4 — Control systems and cybersecurity 6
What operational technology is 6
Why it is exposed, and what hardening looks like 6
The hard line 6
Chapter 5 — Communications 7
The layered plan 7
Hardening by vector 7
Chapter 6 — Food, agriculture, and the supply chain 8
The food system's legs, and local production 8
The supply chain as a domain 8
Chapter 7 — Putting the domains together 9
How domain hardening rolls up 9
Knowing your own domains 9
Where the work belongs 9
Appendices 10
Take the next step 10

FIR Book 5: The Domains — An Introduction

How each kind of infrastructure is actually hardened — sector by sector, and where the work belongs.

Foundation for Infrastructure Resilience — Book 5 of the FIR introductory set. Draft of November 3, 2026.

About this book set, and who it is for

The FIR introductory set is written for people who are new to all of this. It assumes no background in emergency management, infrastructure, the military, or finance — only an interest in why a long loss of the electric grid would be so dangerous, and what can be done about it. Each term is introduced in plain words the first time it matters, and the companion *FIR Field Handbook* holds the full glossary for anything you want to look up again.

These five short books are introductions, not the full course. Each one gives a clear overview of its part of the FIR method — enough to understand it, plan with it, and know where the detail lives — but it is not a substitute for the FIR courses, which remain the version of record for instruction. A later, more detailed textbook set will carry the complete student-guide content; these introductions are the on-ramp to it. The four Foundation courses (BSE 099–102) and the free member orientation (FIR 001) cost nothing to start — browse every course and enroll at the FIR course catalog.

The set is built to be read in order:

- **Book 1, Foundations** — the problem: what a Black Sky Event is, how a community is built, who and what threatens it, and what a household can do. Everyone starts here.
- **Book 2, The Assessment Method** — how a trained assessor measures a community's readiness and turns it into a plan that can be funded.
- **Book 3, The Resilient Community** — what a community that has done the work looks like in a prolonged event: how it governs, feeds, protects, and sustains itself.
- **Book 4, The Certification Path** — how that readiness is independently verified and credentialed.
- **Book 5, The Domains** — how each kind of infrastructure is actually hardened, sector by sector.

This is Book 5, the applied volume. It is written for the people who own or operate a piece of a community's infrastructure — a utility, a plant, a system — and for the assessors and planners who work alongside them. It assumes Books 1 and 2. One thing it is careful about: this book describes what hardening each domain means and why it matters, but the engineering itself in every domain belongs to the licensed and qualified professionals who run those systems. Where real work begins, this book points to them rather than attempting it.

About this book

The earlier books treated infrastructure mostly as a whole — a stack of tiers, a set of vectors, a community that holds together or does not. This book goes domain by domain: energy, water, control systems, communications, food and supply. For each, it answers the same practical questions a newcomer has. What does this domain do? Why is it exposed? And what does it mean to harden it against the three vectors — cyber, physical, and EMP/GMD?

A caution governs the whole book, and it is a safety matter, not a legal formality. Much of the work described here is genuinely dangerous to do wrong. Energizing electrical equipment, operating a water system, touching an industrial control network, or testing a system's security can injure people or break the very thing it was meant to protect. So this book stays at the level of what and why. The how — the actual engineering, operation, and security work — is reserved, every time, for the licensed utility, the qualified operator, the credentialed control-systems engineer, and, where law is involved, a community's attorney. When this book says "route it," it means exactly that.

How this book is organized

FIR prioritized certain infrastructure sectors as core contributors for local resilient communities. Those sectors are reflected in this version of this book, and additional sectors will be added over time. This version contains: Chapter 1 — what hardening means. Chapter 2 — energy. Chapter 3 — water and wastewater. Chapter 4 — control systems and cybersecurity. Chapter 5 — communications. Chapter 6 — food, agriculture, and the supply chain. Chapter 7 — putting the domains together.

Chapter 1 — What hardening means

Books 1 through 4 used two different words that are easy to confuse: readiness and hardening. They are not the same, and this book is about the second one.

Readiness versus hardening

Readiness, scored on the levels from Bronze to Diamond, measures whether a community has thought through, planned, resourced, and exercised a capability. Hardening measures something narrower and more physical: how well the actual equipment is protected against an attack or an event. FIR scores hardening on its own scale, the H-ladder, from H0 (no protection) to H4 (the strongest). A community can be well-organized and still under-hardened, or well-hardened in one spot and exposed everywhere else. Hardening is the work this book describes; readiness is the plan that directs it.

The survivable thresholds

Each vector has a level of hardening at which its infrastructure is credited as able to survive the event it is designed against. These survivable thresholds differ by vector: H4 for EMP/GMD, H3 for cyber, H3 for physical. They differ because the threats differ — an electromagnetic pulse is an all-or-nothing physical insult that demands the highest protection, while cyber and physical hardening reach their survivable standard a rung lower. A vector is only credited as truly hardened, and its days-of-supply figure only attaches, once it reaches its threshold.

The compliance domains

Hardening is measured against defined standards, grouped into six compliance domains: EMP/GMD, cybersecurity, physical security, process safety, supply chain, and governance. The list is worth noticing because it shows that hardening is broader than fences and firewalls. Process safety — running a plant so it fails safely — and supply chain — making sure the parts and materials a system needs will actually arrive — are as much a part of hardening as a hardened wall. The chapters that follow walk the infrastructure domains a community actually runs, and each one is hardened across all three vectors and judged against these standards.

The human foundation

The domains in this book are physical, but they all rest on the human foundation from Book 1 — Tier 0H, the workforce and households that run everything. Keeping people alive and able is its own hardening problem, and in a prolonged event its hardest part is health: infectious disease returning once sanitation and clean water falter, and chronic care interrupted when pharmacies and clinics close. FIR treats community health and the disease environment as a function to plan for, supported by its own course, BSE 113. It is the domain beneath the domains, and nothing above it holds for long without it.

Chapter 2 — Energy

Energy is the keystone. Book 1 placed it at the base of the built stack because almost everything else fails when it fails, and restoring it is the hardest problem in a Black Sky Event. Hardening energy is therefore where a community's work has the most leverage — and where the safety limits are strictest.

Islanded, not independent

The central idea in energy hardening is islanding: the ability of a community, or a critical facility within it, to disconnect from the larger grid and run on its own generation for a time. The phrase FIR uses is "islanded, not independent." The goal is not to leave the grid permanently; it is to keep critical loads — the water plant, the hospital, the emergency operations center — powered through an outage until the grid returns. This is the idea behind a community's planned local generation capability: generation, storage, and the controls to run a protected island, designed in advance and, crucially, exercised rather than merely installed.

What hardening looks like here

Across the three vectors, hardening energy means protecting the things the grid cannot quickly replace. Against physical attack, that means securing substations and the large transformers that take many months to replace. Against EMP and GMD, it means shielding control electronics and protecting long lines and transformers from the currents those events induce. Against cyber, it means protecting the control systems that run generation and distribution — the subject of Chapter 4. And underneath all of it sits fuel: a generator is only as resilient as its fuel supply, so fuel reserves and resupply are part of energy hardening, not an afterthought.

The hard line

Here the safety fence is absolute, and it is not FIR's invention — it is the law and practice of how power systems are run. No interconnection, islanding, or energization of electrical equipment happens outside licensed, utility-authorized work. A community plans for islanding; it does not wire it up on its own. Getting this wrong kills people and damages the grid. Every step from plan to reality runs through the utility and licensed engineers.

Chapter 3 — Water and wastewater

If energy is the keystone, water is the one whose loss is felt fastest. Pressure fails within hours of the pumps stopping, and the consequences — no drinking water, no sanitation, rising disease — arrive faster than almost anything else. Among the domains without a dedicated course yet, water and wastewater is the top priority, because the exposure is so immediate.

The two halves

A community's water domain has two halves that are easy to forget are connected. Clean water in — treatment, pumping, storage, and distribution — keeps people alive. Wastewater out — the sewers and treatment that carry waste away — keeps them from getting sick. Both run on electricity, both run on chemicals that have to be resupplied, and both are controlled by the same kind of industrial control systems that Chapter 4 covers. A water plan that secures the supply but forgets the sanitation has solved half the problem.

What hardening looks like here

Hardening water means keeping both halves running through an outage. Backup power for pumps and treatment is the first requirement, which ties the water domain directly to the energy domain. Stored, treated water and the chemicals treatment depends on provide a buffer. The control systems need the same cyber and EMP protection as the grid's. And the physical siting matters: Book 3's rule, Water Inside the Walls, puts treatment, distribution, and every critical node inside or against a community's protected perimeter rather than exposed outside it. As with energy, the operation of a public water system is the work of its qualified operators and the utility; this book describes the target, not the procedure.

Chapter 4 — Control systems and cybersecurity

Behind the grid, the water plant, and nearly every modern utility sits a layer most people never see: the industrial control systems that actually run the machinery. This domain is where the cyber vector does its damage, and it is the one that most needs its limits stated before anything else.

What operational technology is

The computers that run a pump, a valve, or a breaker are called operational technology, or OT, to distinguish them from the ordinary office information technology, or IT, that runs email and spreadsheets. The supervisory systems that monitor and control them across a utility are often called SCADA. The important thing for a newcomer is that OT is not just "computers at a utility" — it is the direct controls on physical equipment, where a wrong command does not corrupt a file but opens a valve or trips a line.

Why it is exposed, and what hardening looks like

OT was built, decades ago, for reliability and isolation, not for a world where it would be connected to the internet — and much of it now is. That exposure is what a patient cyber adversary looks for. Hardening it, at the level this book describes, means knowing what is connected and removing what should not be, separating the OT network from the IT network and from the internet, and keeping a way to monitor and operate the system that does not itself depend on the network under attack. One powerful and low-technology protection is the ability to run critical functions manually, out of band, when the automated system cannot be trusted.

The hard line

This domain carries the strictest conduct fence in the set, and it has three parts. Awareness, not access: a community and its assessors learn where the exposure is; they do not reach into live control systems. Report, don't respond: when something looks wrong, it is reported to the qualified people, not poked at. And no security testing, intrusion attempt, or incident response happens outside a qualified, authorized OT-security engagement. These are not cautious preferences. Testing a live control system can cause the exact failure it was meant to prevent, so the work belongs only to credentialed OT-security professionals operating under authorization.

Chapter 5 — Communications

A community that cannot talk to itself cannot coordinate anything — not repairs, not security, not the distribution of water. Communications is a lifeline sector, and hardening it is largely about having layers that fail in sequence rather than all at once.

The layered plan

The organizing idea, introduced in Book 1, is PACE: Primary, Alternate, Contingency, Emergency — a ranked set of ways to communicate, so that losing one is not losing all. For a community, the backbone beneath the public cell network is usually owned two-way radio, the land mobile radio that utilities and public safety already run, with push-to-talk channels that work when the cell network does not. Nonelectric alternatives must be included, such as church bells, sirens, even message couriers and runners.

Hardening by vector

Communications is the clearest example of why the vectors must be handled one at a time. Against cyber, physical, and ordinary weather, owned radio is a genuine strength — it outlasts the public network because the community controls it. Against EMP and GMD, that strength has a limit that is easy to over-claim: the repeaters, base stations, and trunking controllers that give radio its range are fixed electronics on towers and power lines, and they should be assumed degraded or down. What survives is the smallest, simplest gear — handheld radios used simplex, radio to radio, within line of sight, especially spares kept powered off in shielded Faraday containers. Hardening communications therefore means both strengthening the wide-area radio layer against the everyday vectors and keeping a simple, shielded, short-range fallback for the worst case. Hardening the sites themselves — shielding, surge protection on antenna and power leads, and protected backup power — is what buys the wide-area layer its best chance against EMP.

Chapter 6 — Food, agriculture, and the supply chain

A community can harden its power, water, and communications and still run out of food. This domain is about the one need that cannot be stored indefinitely and must, past a point, be produced.

The food system's legs, and local production

A local food system rests on a few legs: what comes in from outside, what can be stored, and what the community can produce itself. In a prolonged event the first leg fails — the trucks stop — so the other two carry the weight. Stored food buys the first stretch of time, measured in the household and community days-of-supply figures from earlier books. But stored food only ever buys time; the thing that turns a countdown into survival is local production, the gardens, livestock, and local water that let a community make more before the stores are gone. Hardening this domain is largely about shortening the distance between a community and its own food. Food and agriculture also has an animal half that is easy to overlook — the working animals, the livestock and herd biosecurity a community depends on, and the diseases that pass between animals and people. FIR covers the food side in its food-systems course (BSE 104) and the animal side in its veterinary and animal-health course (BSE 114).

The supply chain as a domain

Behind food sits the broader supply chain — the parts, fuel, chemicals, and materials that every other domain needs to keep running. Supply chain is one of the six compliance domains for a reason: a hardened system that cannot get a replacement part is not hardened for long. The strongest tool here is arranged before any crisis — contingent procurement, a pre-event agreement with a nearby supplier that sets its own triggers, priorities, payment, delivery, and duration. Because such an agreement is a contract, it is written and reviewed with counsel while everyone is calm, not negotiated once the trucks have already stopped.

Chapter 7 — Putting the domains together

The domains are described one at a time for clarity, but a community does not experience them one at a time. They fail together, and they have to be hardened together.

How domain hardening rolls up

Every piece of hardening in this book feeds the larger picture from Books 2 and 4. Hardening a substation or a control network raises a vector's position on the H-ladder; reaching a vector's survivable threshold is what lets it be credited as hardened and lets its days-of-supply figure attach. The domains are where the abstract vector scores touch real equipment. And the cross-cutting compliance domains — especially process safety and supply chain — run through every sector, because a system that cannot fail safely, or cannot get its materials, is not truly hardened no matter how strong its walls.

Knowing your own domains

Before a community can harden its domains, it has to know what it has — which systems it depends on, who owns them, and where they are exposed. FIR has a disciplined way of finding this out, covered in Book 2: it is desk research on what a community already makes public, done under a hard rule of observe and report, with consent before any access and never any trespass. A community maps its domains from the records, not by prowling its own facilities, and certainly not anyone else's.

Where the work belongs

The honest close to this book is the limit it began with. Knowing what a domain needs is within reach of any motivated community and its assessors. Doing the work — energizing a grid island, operating a water plant, securing a control network — is not, and should never be improvised. The value of this book is that it lets a community understand its own infrastructure well enough to plan, to fund, and to direct the qualified professionals who will do the hardening. That is the role these five books are written to prepare a reader for: to understand the whole clearly enough to lead the work, and to know exactly where to hand it to the people trained to carry it out.

Appendices

The reference material for this book — the glossary of record, the course field cards, and the sources — is gathered in the companion *FIR Field Handbook* rather than repeated here, so that one document stays the single source of record. The domain, hardening, and compliance terms used above are defined there in full, with the courses that own them (principally the energy, control-systems, and domain courses, and BSE 201's compliance standards). Where this book and the Handbook ever differ on a definition, the Handbook governs; where either differs from the online courses on instruction, the course governs, and the difference should be reported for correction.

Take the next step

This book is a free introduction. To learn the method in full — and to earn FIR's credentials — take the courses, which are the version of record for instruction. Each domain in this book has its own course — energy (BSE 103 and 105), food and agriculture (BSE 104 and 114), communications (BSE 111), logistics (BSE 112), critical-infrastructure research (BSE 106 and 110), and community health (BSE 113). Whatever your path, the four Foundation courses (BSE 099, 101, 102, and 100) and the free member orientation (FIR 001) are the place to start, and they cost nothing. Browse every course and enroll at the FIR course catalog, and learn more about FIR at fir.foundation.