IS OUR CONTAINMENT STRATEGY OVERDESIGNED?

Diagnostic Guide
GD-020

A technical diagnostic guide to accumulated conservatism, unnecessary complexity, maintainability, and lifecycle performance

A practical guide to distinguishing justified containment controls from accumulated design conservatism that increases cost, energy consumption, and operational fragility without clearly improving risk control.

DIAGNOSTIC GUIDE

HOW TO USE THIS GUIDE

MORE CONTAINMENT FEATURES DO NOT AUTOMATICALLY CREATE BETTER CONTAINMENT.

This guide was created for facilities where safety margins, inherited conventions, duplicated barriers, and elevated airflow requirements have accumulated over time without a clear relationship to the current risk basis.

Why we developed it

High-containment projects often grow conservatively. A requirement is added because another project used it, a second filtration stage is included "just in case," pressure differentials are increased, supply HEPA filtration is added, air-change rates rise, redundant systems multiply, and zoning becomes progressively more complex.

Each addition may appear prudent in isolation. Together they can produce a facility that is expensive to build, difficult to commission, energy intensive, complex to maintain, and increasingly dependent on sophisticated controls and specialized components.

The purpose of this guide is to identify controls justified by the accepted risk and operating basis and distinguish them from complexity that has no clear containment function.

Who can use it

The guide is intended for owners, project teams, architects, HVAC engineers, biosafety personnel, commissioning specialists, facility managers, and institutional decision-makers responsible for high-containment planning and lifecycle performance.

It may be used during conceptual design, value engineering, design review, renovation, energy optimization, or retrospective evaluation of an operating facility.

HOW TO USE IT IN PRACTICE

Trace each significant containment feature to a defined hazard, failure mode, operational need, regulatory requirement, or accepted institutional criterion. Then evaluate what it contributes to performance, what dependencies it creates, how it will be maintained, and whether a simpler control could achieve the same required function.

The objective is not to reduce containment. It is to eliminate unjustified complexity while preserving or improving the required level of risk control.

01 TRACE

02 QUESTION

03 SIMPLIFY

04 VERIFY

HOW THIS GUIDE MAY BE USED — AND WHAT IT DOES NOT AUTHORIZE

This guide is a general diagnostic-orientation tool. It is designed to help structure technical questions, organize evidence, and define what requires more specific evaluation.

Acceptable use

It may be used to:

- structure preliminary technical investigations;
- prepare internal reviews and multidisciplinary discussions;
- identify missing information, measurements, and documentation;
- support definition of the scope of a subsequent evaluation;
- serve as educational and internal technical reference material.

It does not constitute

This guide does not constitute authorization to remove or reduce containment controls, nor does it constitute redesign, value engineering, an acceptance criterion, certification, compliance determination, authorization to modify or operate, or a site-specific recommendation.

Technical and operational decisions

No accepted containment control should be removed, reduced, or modified solely on the basis of this guide. Any change should be justified through risk assessment, formal change control, and reverification proportionate to the affected function.

Applicable technical basis

The content should be interpreted together with the risk assessment, Basis of Design, applicable standards and regulatory requirements, institutional criteria, commissioning evidence, operating and maintenance performance, and other site-specific documentation.

Competent personnel

Rationalization or simplification of containment controls should be developed and reviewed by appropriately qualified personnel, with traceability between hazard, control function, failure consequence, and evidence that the revised solution maintains the required performance.

Responsibility

BioLab Solutions assumes no responsibility for decisions, modifications, interventions, or actions carried out outside a site-specific evaluation and without review by competent personnel.

First published: October 2026
Current version: October 2026 | v1.0

COPYRIGHT AND PERMITTED USE

© 2026 Biological Laboratory Solutions S.A.S. de C.V. All rights reserved.

This publication may be downloaded, retained, and used internally for educational, technical, and reference purposes.

It may not be reproduced, redistributed, modified, sold, or incorporated, in whole or in part, into commercial materials, courses, procedures, specifications, reports, or third-party publications without prior written authorization from BioLab Solutions.

Brief excerpts may be quoted with full attribution to BioLab Solutions and reference to the corresponding Diagnostic Guide.

01 Trace each significant control to a function

A design feature should have a reason that can be expressed technically.

Feature	Question to ask
High ACH	Is it driven by thermal load, dilution, recovery, equipment exhaust, a specific requirement, or simply convention?
High pressure differential	What additional containment function does the higher setpoint provide, and what consequences does it create for doors and control?
Supply HEPA	What hazard or process requires incoming-air filtration, and does that requirement remain valid?
Double exhaust HEPA	What failure scenario or release consequence is the second stage intended to control?
Redundant fans	What function must survive the failure, and is the redundancy genuinely independent and testable?
Multiple airlocks / change rooms	What personnel, contamination, or pressure function does each transition support?
Extensive zoning	What different risk or operating state requires separate control of each zone?

> **Design test:** if the project team cannot explain what a feature protects against, its basis should be reopened before it is treated as permanent.

02 Distinguish risk control from inherited convention

Some requirements persist because they were copied forward, not because the current project re-established their need.

Trace the origin

- risk assessment;
- regulation;
- standard;
- institutional requirement;
- previous project;
- consultant preference;
- manufacturer recommendation;
- historical operating practice.

Then ask whether the basis still applies

A previous project may have handled different agents, different activities, a different failure consequence, or a different regulatory environment.

Similarity of containment level does not make every engineering control transferable without review.

> **“WE ALWAYS DO IT THIS WAY” IS NOT A COMPLETE DESIGN BASIS.**

03 Look for stacked conservatism

Multiple individually conservative decisions can combine into a disproportionate system burden.

Overdesign often emerges through accumulation rather than through one obviously excessive feature.

High ACH + high pressure offset

These can simultaneously increase fan work, infiltration, door forces, and control effort.

Double filtration + oversized airflow

Higher system resistance is multiplied by greater airflow demand.

Multiple redundant systems

These can create shared controls, maintenance complexity, and commissioning burden without proportional resilience.

More rooms + more transitions

Each additional airlock, change room, or pressure zone adds doors, sensors, controls, and operating steps.

Tight tolerances + variable operation

Very tight setpoints can generate nuisance alarms and unstable control if the operating environment cannot sustain them.

Oversized systems + low-flow operation

Large terminals and fans may be more difficult to control efficiently under normal part-load conditions.

CONSERVATISM ACCUMULATES SYSTEM CONSEQUENCES EVEN WHEN EACH DECISION APPEARS REASONABLE IN ISOLATION.

04 Question unnecessary supply HEPA filtration

Supply filtration should address a defined function rather than being assumed automatically from containment level.

Possible legitimate reasons

- protection of highly sensitive processes or animals;
- specific product/environment requirement;
- defined contamination-control objective;
- applicable regulatory requirement or project/institutional criterion with a documented technical basis.

Potential consequences

- additional pressure drop;
- fan energy;
- filter maintenance;
- replacement cost;
- testing requirements;
- additional housings and access;
- greater fan-capacity demand.

Review principle: where supply HEPA is required, retain it and design its integration correctly. Where no function justifies it, question why that lifecycle burden is being added.

05 Review pressure differentials as performance requirements

More negative is not automatically better.

The required pressure relationship should establish reliable directional airflow without creating unnecessary operational or mechanical penalties.

Directional airflow

Does the selected differential reliably preserve the intended direction under normal conditions?

Door forces

A larger differential can make doors more difficult to operate and affect accessibility.

Leakage demand

A greater pressure differential drives more transfer air through the same leakage area.

Fan energy

Greater transfer/exhaust demand increases lifecycle energy consumption.

Control stability

Overly narrow control bands, insufficient deadbands, or aggressive control tuning can increase hunting and alarm frequency.

Failure state

The selected cascade should remain manageable during door events, filter loading, and equipment transitions.

SELECT THE PRESSURE NEEDED TO CONTROL AIRFLOW, NOT THE MOST NEGATIVE NUMBER THE FAN CAN PRODUCE.

06 Review ACH against its actual function

Excessive ventilation can become one of the largest consequences of inherited conservatism.

Ask what governs airflow

- pressure offset;
- thermal load;
- equipment exhaust;
- dilution requirement;
- recovery objective;
- applicable institutional/regulatory criteria.

If none justifies the current rate

The ACH may be an inherited convention rather than a current functional requirement.

Any reduction should still be treated as a controlled change and verified against pressure, thermal performance, airflow direction, and relevant recovery conditions.

HIGH AIRFLOW DOES NOT SUBSTITUTE FOR A CLEAR CONTAINMENT STRATEGY.

MORE BACKUP EQUIPMENT CAN CREATE MORE SHARED POINTS OF FAILURE

Redundancy should improve functional resilience, not simply duplicate components.

Shared controls

Two fans that depend on the same PLC or sensor may still be vulnerable to a single failure.

Shared filtration

Duplicated fans downstream of a single filter bank do not protect against every common-path failure.

Maintenance burden

More components require more testing, spares, access, intervention, and documentation.

Failure logic

Complex automatic transfer sequences can create additional modes that themselves require commissioning.

Space / access

Redundant equipment can compromise maintainability if mechanical rooms become overcrowded.

False resilience

A nominal N+1 architecture may create confidence not supported by functional failure testing.

> **REDUNDANCY SHOULD REDUCE THE CONSEQUENCE OF FAILURE, NOT JUST INCREASE THE NUMBER OF COMPONENTS.**

07 Ask what it costs to maintain complexity

A feature that cannot be maintained reliably can become a lifecycle weakness.

Specialized components

Are spare parts locally available, and can they be supported throughout the expected life of the facility?

Testing burden

How many additional integrity, alarm, interlock, or functional tests does the feature create?

Maintenance access

Can the component be serviced without compromising another containment function?

Training burden

Do operators and maintenance personnel understand the additional system states and failure modes?

Reserve capacity

Does the feature consume fan, electrical, or physical capacity needed elsewhere?

Documentation

Can the institution preserve the technical memory required to operate that complexity correctly?

> A design control that depends on a maintenance capability the institution cannot sustain may fail to deliver the intended risk reduction throughout the facility lifecycle.

COMPLEXITY OFTEN BECOMES A PERMANENT OPERATING BURDEN

Excessive airflow

Continuously drives fan, cooling, heating, and reheat energy consumption.

Additional filtration stages

Add resistance that fans must overcome throughout operation.

High pressure offsets

Increase transfer-air demand through the building envelope.

Over-zoning

Creates more controls, dampers, sensors, and minimum-airflow requirements.

Unnecessary 24/7 states

Keeping all spaces permanently in full operating condition may be unjustified where safe reduced modes are feasible.

Oversized plant

Large fans and AHUs may operate inefficiently when normal demand is well below the design peak.

> **A DESIGN DECISION MADE ONCE CAN BECOME AN ENERGY PENALTY PAID EVERY HOUR FOR DECADES.**

COMMON RATIONALIZATION ERRORS

SIMPLIFICATION CAN ALSO GO WRONG

“It costs too much, so remove it.”

Cost is not sufficient. First establish whether the feature is necessary for an accepted risk control.

“Other BSL-3 laboratories do not have it.”

Different facilities may legitimately use different controls.

“We have never had an incident.”

The absence of an observed failure does not demonstrate that the control is unnecessary.

“The guideline does not explicitly require it.”

Project-specific risk may justify controls above the minimum of a generic guideline.

“The energy savings justify the change.”

Optimization must preserve the required containment function.

“The system is too complicated.”

Complexity may be justified where it controls a high-consequence failure and can be maintained reliably.

THE OBJECTIVE IS A JUSTIFIED DESIGN, NOT A MINIMUM DESIGN.

08 Use a function-by-function rationalization review

Evaluate the purpose, consequence, and lifecycle burden of each significant control.

Review question	Decision test
What hazard/failure does it control?	The function should be explicit and traceable.
What requirement supports it?	Regulation, standard, institutional requirement, risk assessment, or documented design criterion.
What happens if it is absent?	Identify a realistic consequence rather than a generalized concern.
Is there a simpler control?	Compare equivalent risk control, not merely lower cost.
What dependencies does it create?	Power, controls, maintenance, testing, space, energy use, and specialized support.
Can the institution sustain it?	Evaluate maintenance capability, training, spare parts, and verification across the lifecycle.
How will any change be verified?	Define functional evidence before approving a simplification.

> A rationalization review should make both the retained control and any proposed simplification defensible.

BURDEN OF PROOF FOR SIMPLIFICATION

RATIONALIZATION IS A CONTROLLED CHANGE, NOT AN EXERCISE IN REMOVING FEATURES

A containment feature should not be removed solely because its justification is poorly documented. The review should determine whether the function is unnecessary, duplicated, or can be achieved through a simpler control without weakening the accepted risk strategy.

1 · Establish the current function

Identify the hazard, failure mode, operational need, or formal requirement the feature currently addresses, including functions that may have become implicit over time.

2 · Evaluate the proposed alternative

Determine whether the simplified configuration preserves the required containment function and whether removing one control creates a new dependency elsewhere.

3 · Define verification before the change

State which measurements, functional tests, and acceptance criteria will demonstrate that the simplified configuration performs as intended.

4 · Assign decision authority

Risk ownership, engineering review, biosafety participation, and institutional approval should be explicit before the change is implemented.

> The strongest case for simplification is not lower cost or lower energy use. It is equivalent or better control of the required risk with fewer unnecessary dependencies and a verification plan capable of demonstrating the result.

DIAGNOSTIC SEQUENCE

IS THE CONTAINMENT STRATEGY OVERDESIGNED?

01

Can each significant containment feature be traced to a current function or requirement?

No → determine whether the feature is an inherited convention or a current undocumented need.
Yes → continue.

02

Are multiple conservative controls accumulating around the same failure scenario?

Yes → examine whether the combination is proportionate and whether all controls are mutually necessary.
No → continue.

03

Does the feature materially improve containment performance or resilience?

No or unclear → reopen the design justification.
Yes → continue.

04

Can the institution reliably maintain, test, and operate the feature throughout its lifecycle?

No → the control may be creating a new failure vulnerability.
Yes → continue.

05

Could a simpler configuration achieve the same required level of risk control?

Yes → compare alternatives through formal technical review.
No → retain the justified complexity.

06

If simplified, has the revised containment function been reverified?

No → the new condition remains undemonstrated.
Yes → document the revised accepted basis.

WHAT SHOULD BE AVAILABLE?

Risk / requirement basis

- risk assessment;
- applicable standards;
- regulatory requirements;
- institutional criteria;
- failure assumptions.

Design basis

- airflow criteria;
- pressure cascade;
- filtration;
- redundancy;
- zoning;
- personnel/material transitions.

Lifecycle evidence

- energy data;
- maintenance history;
- alarm/failure history;
- spare-part availability;
- testing burden;
- operator workarounds.

Change evidence

- alternatives analysis;
- risk review;
- engineering calculations;
- change approval;
- verification plan;
- accepted revised baseline.

Review objective: distinguish controls that deliver real risk reduction from complexity that persists only because no one has challenged its original assumption.

LESS COMPLEX CAN SOMETIMES BE MORE RELIABLE

Simplification is technically valuable when it reduces points of failure while preserving the required control.

Potential benefits

- fewer sensors and control loops;
- fewer filter housings and penetrations;
- lower fan pressure and energy use;
- better maintenance access;
- simpler testing;
- clearer operating states;
- less dependence on spare parts.

But only when the function is preserved

The strongest simplification removes a dependency that does not provide meaningful risk control.

If simplification reduces a barrier, fault tolerance, or operational control that forms part of the required containment strategy, it is not rationalization: it is inadequate containment.

SIMPLIFICATION SUCCEEDS WHEN THE SYSTEM BECOMES EASIER TO OPERATE WITHOUT BECOMING EASIER TO FAIL.

BEFORE REMOVING A CONTROL, DEMONSTRATE WHAT FUNCTION IT SERVES AND HOW THAT FUNCTION WILL CONTINUE TO BE PROVIDED

Use this checklist as diagnostic support. A checked item does not constitute acceptance; each element should be interpreted against the risk basis, facility configuration, and applicable criteria.

□ Trace the existing feature or requirement to a current hazard, failure mode, operational need, or formal requirement.

□ Determine whether the control remains justified by the accepted risk and operating basis or is primarily an inherited convention.

□ Identify interactions with other conservative layers so that removing one feature does not expose a dependency that was previously masked.

□ Define the proposed alternative and demonstrate how it preserves the required containment function without creating a new unmanaged dependency.

□ Evaluate effects on commissioning, maintenance, controls complexity, spare parts, energy use, and lifecycle reliability.

□ Identify any change in fault tolerance, degraded operation, or recovery behavior created by the simplification.

□ Define the measurements, functional tests, and acceptance criteria that will be used to demonstrate the revised strategy.

□ Obtain appropriate risk, engineering, biosafety, and institutional approvals before implementing the change.

□ Update the Basis of Design, drawings, sequences, O&M information, and operating procedures to reflect the accepted configuration.

□ Treat rationalization as a controlled change: do not use cost or energy reduction alone as evidence that a containment feature is unnecessary.

> **Technical-use note:** This review checklist is a diagnostic-support tool. It does not establish site-specific acceptance criteria, replace risk assessment or professional judgment, constitute certification, or authorize operation or return to service.

If the review identifies a condition requiring site-specific evaluation, BioLab Solutions can support technical assessment, verification, and definition of the required evidence.

RELATED BIOLAB RESOURCES

EXPLORE RISK, AIRFLOW, REDUNDANCY, ENERGY, AND DECISION OWNERSHIP IN GREATER DEPTH

NT-012
ACH as a derived variable

NT-014–017
HVAC integration, exhaust authority, redundancy, and control hierarchy

NT-040–044
Risk assessment, classification, and incorrectly applied cleanroom logic

NT-045–048
Sustainability, Net Zero, energy recovery, and lifecycle energy demand

NT-049–051
Decision ownership, authority boundaries, and institutional interfaces

GD-004
Why does this high-containment laboratory use so much energy?

GD-010
Is our HVAC redundancy real or only nominal?

GD-017
Are we using ACH correctly?

BIOLAB DIAGNOSTIC GUIDES

Short technical resources organized around real containment problems rather than individual disciplines.

Series concept: symptom → system → evidence → restoration.

CLOSING DIAGNOSTIC PRINCIPLE

A GOOD CONTAINMENT STRATEGY IS NOT THE MOST COMPLEX ONE. IT IS THE ONE THAT RELIABLY CONTROLS THE RIGHT RISKS.

Containment design requires conservatism, but conservatism is most useful when it is explicit and proportionate to consequence.

When controls accumulate without a visible technical basis, the facility can become more difficult to commission, maintain, and operate while consuming more energy and creating additional failure dependencies.

Rationalization requires discipline in both directions: questioning complexity that does not provide meaningful risk control and retaining controls whose function remains justified. The result should be a system that is easier to understand and maintain because its architecture is more closely aligned with the actual containment requirement.

BIOLAB SOLUTIONS

Independent technical support for planning, design, commissioning, assessment, and lifecycle management of high-containment laboratories.

For site-specific evaluation, BioLab Solutions can support technical review, verification, and definition of evidence requirements.

RISK BASIS → REQUIRED CONTROL → ADDED COMPLEXITY → JUSTIFIED DESIGN