River Refugium Project (RRP)

CERNUNNOS FOUNDATION

BRIGHT MEADOW GROUP

Systems Analysis and Solutions Consulting

Document Title:

RRP9 Risk, Failure Modes & Resilience Architecture

RRP Document Number:

RRP0002.10

Version by date time group:

01 APR 2026 0001

Cernunnos Foundation / Bright Meadow Group

Email: robert@brightmeadowgroup.com

Website: www.cernunnosfoundation.com

RIVER REFUGIUM PROJECT Cernunnos Foundation Bright Meadow Group	**RRP9 — Risk, Failure Modes ****&**** Resilience Architecture** Document No: RRP0002.10 │ Version: 2.0 │ 01 April 2026 Status: Published — Version 2.0 │ Supersedes: Version 1.0 (2025) *Contact: robert@brightmeadowgroup.com │ www.cernunnosfoundation.com*

Abstract Every infrastructure system has risks. Only resilient infrastructure systems have predictable, contained, non-catastrophic failure outcomes. The RRP was designed to fail safely — to default to a stable, non-hazardous state without operator intervention across hydraulic, biological, mechanical, thermochemical, electrical, and governance failure modes. This document identifies those failure modes and demonstrates the engineered resilience that prevents each from becoming a systemic threat. It is the chapter that tells permitting agencies, investors, and insurers: we already asked the scary questions and designed for the answers.

1. Core Risk Philosophy: Fail Small, Fail Slow, Fail Safe

The RRP contains zero failure paths that result in toxic releases, uncontrolled chemical reactions, hazardous air emissions, explosive conditions, wildlife kills, drinking-water contamination, or irreversible system loss.[1] Hydraulic, biological, and thermochemical systems are separated by design so that failure in one domain cannot cascade into another.

Every critical process has a passive safety state. If pumps fail, flow stops. If power fails, valves shut and the system isolates. If sensors fail, the PLC defaults to containment loops. If reactors fail, they depressurize into quench tanks. The system goes safe without operator intervention.[2]

2. Hydraulic Risks

Intake blockage is mitigated by triple-layered screens, bypass gates, automatic low-flow alarms, and manual access platforms. Result: reduced inflow, not contaminated outflow. Pump failure is mitigated by redundant pump trains (N+1 or N+2), VFD predictive diagnostics, passive gravity-fed backup, and isolation valves. Cistern overfill during storm surge is mitigated by automatic diversion to overflow wetlands and SCADA-controlled inflow throttling — controlled bypass through naturalized overflow, no discharge of untreated water.[3]

3. Biological Risks

Crop disease is contained by greenhouse segmentation — each house is a physically isolated subunit with clean-in/clean-out cycles, controlled humidity and airflow, and biochar substrate that reduces pathogen residency.[4] A disease event in one house does not spread to others. Algae culture crashes are mitigated by separate polishing algae houses, CO_2 injection control, automated pH buffering, redundant lighting, and the ability to reseed in under 12 hours.

4. Thermochemical Risks

HTC/HTL reactors operate at elevated temperature and pressure. Overpressure scenarios are mitigated by ASME-compliant pressure vessel design, automatic pressure relief to quench tanks, redundant temperature monitoring, and staged depressurization protocols.[5] All thermochemical processes are physically separated from greenhouse and biofiltration zones — no failure path connects reactor overpressure to the biological system.

5. Cybersecurity

SCADA/PLC systems controlling RRP operations present a cybersecurity attack surface that must be explicitly designed for. Industrial control system security follows NIST SP 800-82 guidelines for ICS security: network segmentation between business and control networks, encrypted communications for all sensor and actuator data, multi-factor authentication for remote access, regular penetration testing, and air-gapping of critical control functions from internet-accessible systems.[6] The open-data commitment applies to environmental output data — not to control system architecture, which remains protected.

6. Financial **&**** Market Risks**

The three-scenario financial model (RRP Economic Analysis, Version 2.0) explicitly models market failure conditions in the Stress Test scenario. The primary financial risk is nitrogen credit market inactivity — this single variable accounts for the difference between the operating model floor and profitability. Mitigation: the hub-and-spoke cluster architecture and the biomass revenue stream from Model B nodes provide operating revenue independent of credit markets. The system does not require credit markets to function — it requires them to be profitable at scale.[7]

Notes

Citations follow Chicago Notes-Bibliography style. Internal Bright Meadow Group / Cernunnos Foundation documents are cited by document title and year. Figures marked ⚑ are provisional academic proxies pending replacement by RRP pilot data per RRP8.

- **1. ***Bright Meadow Group, **"**RRP System Resilience **&** Safety Notes.**"** CF/BMG Internal, 2025.*

- **2. ***Passive Fail-Safe Architecture in Industrial Process Design. Chemical Engineering Manuals, print edition.*

- **3. ***USACE, Forebay **&** Intake Design Manuals. Engineering Manual EM 1110-2-1603, print edition.*

- **4. ***Bright Meadow Group, **"**Substrate Biosecurity **&** Plant Pathogen Control.**"** BMG Greenhouse Ops, 2025.*

- **5. ***ASME Boiler and Pressure Vessel Code, Section VIII — Pressure Vessels. Print edition.*

- **6. ***NIST Special Publication 800-82, **"**Guide to Industrial Control Systems (ICS) Security,**"** Rev. 2. National Institute of Standards and Technology, print edition.*

- **7. ***Bright Meadow Group, **"**RRP Economic Analysis — Three-Scenario Framework,**"** Version 2.0. CF/BMG, 01 April 2026.*