

WRS——世界可靠性规则集

英文：World Reliability Ruleset

规范性定义 v1.0（Canonical Definition，唯一标准本）

规范性定义作者

刘静（Linda Liu）

本文档为原创思想与规则文本之固定表达形式，
用于版权确权，不构成法律意见或工程实施指南。

© 刘静（Linda Liu）保留所有权利

版本 1.0 | 2026 年 1 月

目 录

WRS——世界可靠性规则集	1
0. 前言 (Preface)	3
0.1 为什么需要 WRS	3
0.2 WRS 与 LERA 的关系	3
0.3 适用范围与非目标	4
0.3.1 适用范围	4
0.3.2 非目标	4
0.4 语言与解释原则	5
1. WRS 定义与适用边界 (What WRS Is and Is Not)	5
1.1 WRS 定义	5
1.2 WRS 适用边界	6
1.3 为什么 WRS 不是评分体系	6
1.4 为什么 WRS 不是优化框架	7
2. 核心执行原则 (Core Execution Principle)	7
WRS-C——核心规则集	7
2.1 默认阻断原则	8
2.2 不可协商的执行约束	8
2.3 参数不可正当化原则	9
2.4 概率不可正当化原则	9
2.5 责任锚定要求	9
2.6 自动延续禁止原则	9
2.7 行政授权不可覆盖条款	10
3. WRS-D: 领域子集 (Domain Subsets)	10
3.0 子集总说明	10
3.1 子集与场景的关系	11
3.2 WRS-D 规则结构	11
3.3 WRSE — 能量/能量释放 (Energy / Energy Release)	12
3.3.1 子集定义	12
3.3.2 适用边界说明	13
3.3.3 规则结构声明	13
3.3.4 WRSE 规则	13
3.3.5 规则示例 (非规范性)	16
<i>示例仅用于逻辑说明, 不构成规则解释、执行指导或合规判断依据。</i>	16
3.3.6 子集状态声明	16
3.4 WRSM — 运动/物理位移 (Motion / Physical Movement)	16
3.4.1 子集定义	16
3.4.2 适用边界说明	17
3.4.3 规则结构声明	17
3.4.4 WRSM 规则	18
3.4.5 规则示例 (非规范性)	20
3.4.6 子集状态声明	20
3.5 WRSG—电网/系统性基础设施 (Grid / Systemic Infrastructure)	21
3.5.1 子集定义	21

3.5.2 适用边界说明	21
3.5.3 规则结构声明	22
3.5.4 WRSg 规则	22
3.5.5 规则示例 (非规范性)	25
3.5.6 子集符合性声明	26
3.6 WRS _H — 人类生命/生命支持系统 (Human Life / Life Support)	26
3.6.1 子集定义	26
3.6.2 适用边界说明	27
3.6.3 规则结构声明	27
3.6.4 WRS _H 规则	28
3.6.5 规则示例 (非规范性)	30
3.6.6 子集符合性声明	31
3.7 WRS _{Df} — 防御/授权武力 (Defense / Authorized Force)	31
3.7.1 子集定义	31
3.7.2 适用边界说明	31
3.7.3 规则结构声明	32
3.7.1 WRS _{Df} 规则	32
3.7.2 规则示例 (非规范性)	36
3.7.3 子集符合性声明	37
4. 场景映射方法 (Scenario Mapping Method)	37
4.1 为什么 WRS 不枚举具体场景	37
4.2 场景到 WRS 子集的映射逻辑	38
4.3 多子集同时触发是常态, 而非例外	39
4.4 场景映射不构成执行许可	40
4.5 示例性场景映射 (非规范性)	41
第四章小结 (说明性)	44
5. WRS 的使用方式与治理接口 (How to Use WRS and Governance Interface)	44
5.1 在设计审查中的使用	44
5.2 在执行决策门控中的使用	44
5.3 在风险与安全审查中的使用	45
5.4 在事故与事后分析中的使用	45
5.5 非 WRS 执行状态 (Non-WRS Execution State)	45
5.6 关于“减速”的误解与不可迭代价原则	46
第五章小结 (说明性)	46
6. 治理与稳定性声明 (Governance & Stability Statement)	46
6.1 执行恢复 (Unblock) 的逻辑限制	47
6.2 有限性声明 (Finite by Design)	47
6.3 Canonical Definition 的唯一性	47
6.4 解释与修改的边界	48
6.5 商业化、实施与解释权的分离	48
6.6 不可绕过性声明	49
6.7 稳定性声明	49
第六章结语 (说明性)	49
文档状态声明	50

0.前言 (Preface)

0.1 为什么需要 WRS

现代系统的失败，并不主要源于智能不足，而是因为在原本不该发生的情境下，**执行被允许**发生了。人工智能、自动化与系统优化的发展，极大提升了我们判断“如何行动”的能力。但它们并未解决一个更根本的问题：有些行为，无论性能多高、概率多低、授权是否存在、动机是否正当，都不应被执行。

在高风险领域——包括能源系统、交通与运动系统、关键基础设施、生命支持环境以及被授权的武力使用——该类执行一旦发生，其后果即被视为不可逆。WRS 的存在，正是为了将这些执行边界明确化。WRS 的目的不是改进决策，而是阻止那些本不应发生的执行。本文档由刘静 (Linda Liu) 提出并撰写，作为 WRS 的规范性定义文本。

0.2 WRS 与 LERA 的关系

WRS 在结构上依赖于 LERA，但二者不可互换。

- **LERA 管理的是判断**：行动是否应被提出、评估，并被允许进入执行考量。
- **WRS 管理的是执行**：在判断通过之后，定义仍然不可被触碰的执行边界。

通过 LERA 不构成执行授权，亦不得被解释为执行正当性来源。

WRS 只在判断与治理允许“进入执行考量”之后生效。因此：

- LERA 回答的是：“**是否应该行动？**”
- WRS 回答的是：“**哪些事情无论如何都不能被执行？**”

二者处于不同层级，必须严格区分，不得混用。



示意图 1: LERA 与 WRS 的层级关系示意

0.3 适用范围与非目标

0.3.1 适用范围

WRS 适用于所有其失败结果**构成以下任一后果**的执行行为：

- 不可逆的物理后果；
- 系统性或级联式崩溃；
- 人类生命或生命支持能力的丧失；
- 以及对现实世界产生影响的被授权武力使用。

WRS 不以行业、应用或技术类型为划分依据。其适用性由**后果形态**决定，而非使用场景。

在 WRS 语境中，“授权”仅指法律或行政层面对执行尝试的允许资格；是否允许该执行动作发生实际的物理释放，由 WRS 的执行约束最终决定。

0.3.2 非目标

WRS 不替代，也不应被用于替代以下任何内容：

- 工程设计或既有安全标准；
- 系统性能优化；
- 风险评估或风险评分；
- 概率性安全保证；
- 监管或合规判定。

WRS 定义的是不可逾越的边界，而非解决方案。任何将 WRS 用作工程设计、风险评估或合规替代方案的行为，均构成对 WRS 的误用。

0.4 语言与解释原则

WRS 以绝对性、非概率化语言书写。任何引入可能性、缓解、例外或权衡的解释，均视为无效。所有规则基于否决制的强拦截逻辑。

1. WRS 定义与适用边界 (What WRS Is and Is Not)

状态说明：本节内容构成 WRS 的规范性基础。

1.1 WRS 定义

WRS (World Reliability Ruleset, 世界可靠性规则集) 是一套基于否决制 (Veto-based) 的执行规则体系。

WRS 是什么	WRS 不是什么
面向执行层的规则体系	决策或判断框架
用于 阻断执行行为	用于改进、优化或生成决策
采用 默认阻断 (Default Block) 与否决制逻辑	评分体系或阈值通过机制
以 不可逆后果 为触发依据	概率或风险评估模型
定义 绝对不可执行的边界	性能、效率或收益优化工具
以 单点违规即可否决 为原则	权衡、折中或补偿性决策机制
要求 明确的人类责任锚定	自动化责任转移或系统自证
独立于授权状态运行	行政、法律或组织授权体系

表 1: WRS 是什么/不是什么对比

上述对照用于界定 WRS 的适用边界。

【关键解释声明】任何符合右栏所列特征的系统，严禁声明其符合 WRS 规范。

1.2 WRS 适用边界

WRS 不是：

- 决策框架；
- 控制算法；
- 合规检查清单；
- 最佳实践指南；
- 或行业专用标准。

WRS 不决定“应该做什么”，它只定义“绝对不能做什么”。

1.3 为什么 WRS 不是评分体系

评分体系假设风险是可量化、可权衡的。在评分模型中：

- 不同风险因素被赋予权重；
- 不利条件可以被有利条件抵消；

- 一旦达到某个阈值，执行即被允许。

WRS 明确拒绝这种逻辑。在涉及不可逆后果的情境中，不允许任何形式的加权、折算或阈值通过。

因此，WRS 不设置评分、等级或分值。它只通过不可协商的否决条件运作。

1.4 为什么 WRS 不是优化框架

优化框架假设：

- 目标可以被形式化定义；
- 取舍可以被优化；
- 结果可以通过迭代不断改进。

WRS 不进行结果优化。其目的，是在某些边界被触发时，无条件阻止执行发生，即便执行可能带来效率、性能或效用的提升。优化关心的是：如何把事情做得更好；WRS 关心的是：这件事是否根本不该被做。

2.核心执行原则 (Core Execution Principle)

状态说明： 规范性条文——本节内容具有约束性效力。所有领域子集规则 (WRS-D) 均在 WRS-C 之下运行，且不得削弱或违背本节内容。

WRS-C——核心规则集

- WRS-C-01 | 默认阻断原则
- WRS-C-02 | 不可协商的执行约束
- WRS-C-03 | 参数不可正当化原则
- WRS-C-04 | 概率不可正当化原则

- WRS-C-05 | 责任锚定要求
- WRS-C-06 | 自动延续禁止原则
- WRS-C-07 | 授权不可覆盖条款

2.1 默认阻断原则

[WRS-C-01] 默认阻断原则 (Default Block)

【强制性声明】 阻断 (Block) 是本系统的静态常态。任何执行动作的释放必须以“全条目通过”为唯一前提。 **【判定属性】** 强制、实时、不可覆盖。

任意一条 WRS 规则的违反，本身即构成禁止执行的充分条件。

不允许通过聚合、缓解、优先级排序或补偿性理由解除阻断状态。

WRS 基于否决制的强拦截逻辑：阻断是常态，执行是例外。

任何支持 WRS 判定的输入数据，若其真实性、实时性或完整性无法被确认，系统必须视为拦截阈值已触发。

2.2 不可协商的执行约束

所有 WRS 执行约束均为不可协商条件。

任何执行行为，均不得基于以下理由继续进行：

- 紧急性；
- 任务关键性；
- 系统或模型的信心度；
- 指挥、行政或组织批准；
- 预期收益或正向结果。

一旦触发任一 WRS 执行约束，执行行为必须被立即终止。

WRS 内部 不存在任何例外机制。

2.3 参数不可正当化原则

执行行为 不得通过参数调节或阈值调整获得正当性。

一旦触及 WRS 边界，任何数值、容差区间或系统参数均不得作为执行正当性的依据。

参数优化 不构成执行许可或执行合法性来源。

2.4 概率不可正当化原则

执行行为 不得基于概率评估获得正当性。

在触发任一 WRS 约束后，任何发生概率、风险估计或统计置信度均不得作为允许执行的理由。

概率高低 不影响执行禁止的成立。

2.5 责任锚定要求

任何受 WRS 约束的执行行为，均不得在缺乏明确责任锚定的情况下进行。

执行责任 不得被转移、模糊化或委托给系统、模型或自动化流程。

若执行责任无法被清晰界定并明确承担，执行行为必须保持阻断状态。

在责任锚定无法完成的情况下（包括但不限于传感器失效、责任主体不可达或离线），执行行为必须保持在默认阻断（Block）状态。

2.6 自动延续禁止原则

任何执行行为 不得在时间推移、状态变化或环境转变后自动延续。

在某一时刻获得的授权、批准或允许，不具备默认持续效力。

一旦任何状态转移、运行模式变化或环境参数跃迁，必须重新接受 WRS 评估；
若状态转移或环境参数跃迁无法被可靠探测或确认，系统应默认状态已发生改变，
并依据 WRS-C-01 维持阻断状态。

2.7 行政授权不可覆盖条款

任何形式的授权、指挥批准或法律授权，均不得覆盖 WRS 执行约束。

WRS 作为物理层与逻辑层的执行边界运行，而非行政或法律决策主体。

一旦触发 WRS 边界，任何授权均不构成执行正当性来源。

3.WRS-D：领域子集 (Domain Subsets)

状态说明：规范性规则展开。本章定义 WRS 在不同不可逆物理后果域中的领域子集 (WRS-D)，用于将第二章所确立的核心执行原则 (WRS-C) 具体化为可判定、可触发的执行阻断规则。本章内容不引入新的判断标准，所有规则均无条件继承并受制于 WRS-C。WRS-D 规则用于执行层拦截，不构成工程设计规范、控制策略或安全优化建议。

3.0 子集总说明

WRS-D (Domain Subsets) 是 WRS 在不同高风险物理领域中的规则

子集统称。WRS-D 本身不是新的规则体系，而是对 WRS-C (核心执行

原则) 在特定物理后果域中的具体化表达。

所有 WRS-D 下属规则,均无条件继承第二章 WRS-C 的全部属性与约束。WRS-D 的划分依据并非行业、组织或技术形态,而是**不可逆后果的物理类型**。

当前版本的 WRS-D 包含以下五个领域子集:

- WRSE — Energy / Energy Release (能量释放)
- WRSM — Motion / Physical Movement (运动与物理位移)
- WRSG — Grid / Systemic Infrastructure (系统性基础设施)
- WRSR — Human Life / Life Support (生命与生命维持)
- WRSDf — Defense / Authorized Force (防御与武力使用)

该集合在结构上是封闭的,在版本演进上是可扩展的。新子集的引入只能通过新的 Canonical Definition 版本完成。

3.1 子集与场景的关系

WRS-D 子集不是场景枚举。

一个具体执行场景可能同时触发多个 WRS-D 子集。多子集同时激活属于正常状态,而非例外。WRS 不穷举场景,也不对场景进行分类。WRS 仅定义:

- 某一执行行为是否触发某一类不可逆后果
- 一旦触发,该行为是否必须被阻断

场景仅作为 WRS-D 规则的**触发载体**存在,而非规则本身。

3.2 WRS-D 规则结构

每一条 WRS-D 规则必须包含以下三个要素:

- **不可逆后果描述 (Irreversible Consequence)**
 - 该规则试图防止的物理后果类型
- **拦截阈值 (Intercept Threshold)**
 - 触发阻断的物理或系统边界条件
- **继承原则标注 (Inherited WRS-C)**
 - 该规则主要继承并依托的 WRS-C 条款编号

任何缺失上述要素的条目，不构成有效的 WRS-D 规则。

3.3 WRSE — 能量/能量释放 (Energy / Energy Release)

3.3.1 子集定义

WRSE 适用于所有涉及能量积聚、转换、传输或释放的执行行为，其失败后果可能导致不可逆的物理破坏、热失控、结构性损毁或环境损害。

本子集关注的不是能量的用途或效率，而是能量一旦失控释放后所造成的不可逆物理后果。只要某一执行行为涉及以下任一情形，即视为进入 WRSE 适用范围：

- 能量在系统内被积聚或约束
- 能量释放路径依赖于控制系统或判断系统
- 能量释放一旦发生将无法通过软件或逻辑手段完全撤销。即使能量释放过程可以被切断，但若切断前的瞬时释放已足以造成不可逆物理后果，该执行行为仍受 WRSE 约束。

WRSE 不判断能量释放是否“必要”“合理”或“被授权”，仅判断其失败后果是否触及 WRS 所定义的不可逆边界。

3.3.2 适用边界说明

WRSE 不限于电能系统。其适用范围包括但不限于：

- 电能、化学能、热能、机械势能
- 压缩能量、储能系统、反应性能量
- 能量在单一或多单元系统中的耦合释放

能量形式本身不构成触发条件，不可逆后果的存在才是唯一判据。

3.3.3 规则结构声明

WRSE 下的每一条规则，必须包含以下三个要素：

1. 不可逆后果描述
 - 该规则试图阻断的能量失控后果
2. 拦截阈值
 - 触发执行阻断的物理或系统边界条件
3. 继承的 WRS-C 条款
 - 该规则所依托的核心执行原则

缺失任一要素的条目，不构成有效的 WRSE 规则。

3.3.4 WRSE 规则

WRSE-01 | 不可监测能量释放阻断规则

WRSE-02 | 跨单元能量扩散阻断规则

WRSE-03 能量释放与环境不可逆损害规则
WRSE-04 能量释放与判断失效耦合规则

WRSE-01 | 不可监测能量释放阻断规则

不可逆后果

- 热失控
- 爆燃、爆炸或结构性烧毁

拦截阈值

- 能量释放路径无法被实时、可靠监测
- 能量释放过程无法被确认处于可控状态

规则要求

- 一旦上述条件成立，执行行为必须被立即阻断
- 不得基于历史稳定性、设计冗余或经验概率继续执行

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-04 | 概率不可正当化原则

WRSE-02 | 跨单元能量扩散阻断规则

不可逆后果

- 能量释放引发多单元级联破坏
- 系统级热蔓延或结构失效

拦截阈值

- 能量释放可能突破单一受控单元的物理边界
- 无法保证能量影响范围被限制在预定隔离区内

规则要求

- 即使释放行为本身处于设计工况内，也必须阻断执行

- 不得以系统整体收益或局部牺牲为理由继续执行

继承的 WRS-C 条款

- WRS-C-02 | 不可协商执行约束
- WRS-C-03 | 参数不可正当化原则
- WRS-C-06 | 自动延续禁止

WRSE-03 | 能量释放与环境不可逆损害规则

不可逆后果

- 永久性环境污染
- 无法修复的生态或材料损害

拦截阈值

- 能量释放一旦发生，将导致环境后果不可逆
- 修复行为本身无法消除初始损害

规则要求

- 不得以“可接受损害”“事后补偿”作为执行理由
- 不得将环境损害转化为经济或合规问题处理

继承的 WRS-C 条款

- WRS-C-03 | 参数不可正当化原则
- WRS-C-05 | 责任锚定要求

WRSE-04 | 能量释放与判断退化/失效耦合规则

不可逆后果

- 在判断或感知失效状态下发生能量失控

拦截阈值

- 判断系统、传感系统或数据完整性受到破坏
- 能量释放决策基于不完整或不可信信息

规则要求

- 当判断不确定性来源于传感器失效、数据缺失或信息完整性受损时，必须立即触发 WRS-C-01 默认阻断原则。在阻断状态解除前，执行行为不得继续或自动延续。
- 不得在“信息稍后可补全”的假设下继续执行

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-05 | 责任锚定要求

3.3.5 规则示例（非规范性）

示例仅用于逻辑说明，不构成规则解释、执行指导或合规判断依据。

*示例场景：某储能系统在高功率充放电过程中，局部温度监测模块出现间歇性失效。尽管系统历史运行稳定，且当前功率水平仍处于设计额定范围内，由于能量释放路径无法被实时可靠监测，该执行行为触发 **WRSE-01**。根据 WRS-C-01 默认阻断原则，系统必须进入阻断状态，不得基于概率、经验或经济影响继续执行。*

3.3.6 子集状态声明

WRSE 为 WRS-D 下的正式领域子集。本子集中定义的规则均为执行层约束，不可被授权、流程、优化目标或风险评估结果覆盖。WRSE 规则的违反，视为对 WRS 的实质性不符合。

3.4 WRSM — 运动/物理位移 (Motion / Physical Movement)

3.4.1 子集定义

WRSM 适用于所有涉及物体运动、机械位移、惯性变化或动能释放的执行行为，其失败后果可能导致不可逆的人身伤害、结构性破坏或系统性事故。WRSM 关注的不是运动是否“精确”“高效”或“被授权”，而是一旦运动失控或发生错误，其物理后果是否不可逆。

只要某一执行行为涉及以下任一情形，即视为进入 WRSM 适用范围：

- 物体具有可观动能或惯性
- 运动一旦发生无法通过软件或逻辑手段完全撤销
- 运动路径、速度或作用对象依赖判断或感知系统

WRSM 不评估运动意图或任务目标，仅评估运动失败时是否触及 WRS 所定义的不可逆边界。

3.4.2 适用边界说明

WRSM 不限于机器人或自动驾驶系统。其适用范围包括但不限于：

- 车辆、船舶、航空器的物理运动
- 工业机器人、机械臂、自动化设备的动作
- 含有惯性、冲击或剪切风险的机械位移

运动形式本身不构成触发条件，不可逆物理后果的存在才是唯一判据。

3.4.3 规则结构声明

WRSM 下的每一条规则，必须包含以下三个要素：

1. 不可逆后果描述

— 该规则试图阻断的运动失控后果

2. 拦截阈值

— 触发执行阻断的物理或系统边界条件

3. 继承的 WRS-C 条款

— 该规则所依托的核心执行原则

缺失任一要素的条目，不构成有效的 WRSM 规则。

3.4.4 WRSM 规则

WRSM-01 | 不可撤销运动阻断规则

WRSM-02 | 感知或定位不确定下的运动阻断规则

WRSM-03 | 多主体或共享空间运动冲突规则

WRSM-04 | 运动控制与判断失效耦合规则

WRSM-01 | 不可撤销运动阻断规则

不可逆后果

- 人身伤害
- 结构性撞击或不可修复损坏

拦截阈值

- 运动一旦发生，无法在物理上完全撤销
- 即使发出停止指令，惯性或延迟仍可能造成后果

规则要求

- 当运动后果不可撤销时，执行必须在运动发生前被阻断
- 不得以“可紧急制动”“可事后纠正”作为继续执行的理由

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-02 | 不可协商执行约束

WRSM-02 | 感知或定位不确定下的运动阻断规则

不可逆后果

- 错误运动路径导致的碰撞或误伤

拦截阈值

- 位置、速度、方向或环境感知信息不完整或不可信
- 运动决策基于推断、预测或缺失数据

规则要求

- 判断不确定性本身即构成阻断条件
- 不得在“信息可在运动中补全”的假设下继续执行

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-05 | 责任锚定要求

WRSM-03 | 多主体或共享空间运动冲突规则

不可逆后果

- 多主体碰撞
- 共享空间中的不可控事故

拦截阈值

- 无法确认其他主体的运动意图或轨迹，一旦无法通过确定性数据锁定对方轨迹，且对方进入安全包络线，必须立即触发阻断。
- 运动冲突无法通过确定性规则完全避免

规则要求

- 不得以概率评估或平均安全性作为继续执行的理由
- 多主体不确定性必须被视为阻断条件

继承的 WRS-C 条款

- WRS-C-03 | 参数不可正当化原则
- WRS-C-04 | 概率不可正当化原则

- WRS-C-06 | 自动延续禁止

WRSM-04 | 运动控制与判断退化/失效耦合规则

不可逆后果

- 在判断或控制失效状态下发生的运动事故

拦截阈值

- 判断系统、控制系统或执行链路出现异常
- 无法确认运动指令是否被正确理解和执行

规则要求

- 任何控制或判断失效迹象均必须触发默认阻断
- 执行不得在失效状态下继续或自动恢复

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-06 | 自动延续禁止

3.4.5 规则示例（非规范性）

示例场景: 某自动移动设备在人员密集区域运行。由于部分传感器被遮挡, 系统对周围人员的位置判断存在不确定性。尽管设备仍具备紧急制动能力, 且历史运行记录显示事故概率较低, 由于运动一旦发生将无法完全撤销, 且感知不确定性尚未消除, 该执行行为触发 **WRSM-02**。根据 **WRS-C-01 默认阻断原则**, 设备必须进入阻断状态, 不得在运动中“边走边判断”。

3.4.6 子集状态声明

WRSM 为 WRS-D 下的正式领域子集。本子集中定义的规则均为执行层约束，不可被授权、流程、路径规划或效率目标覆盖。WRSM 规则的违反，视为对 WRS 的实质性不符合。

3.5 WRSG — 电网 / 系统性基础设施 (Grid / Systemic Infrastructure)

3.5.1 子集定义

WRSG 适用于所有涉及电网、能源网络、关键基础设施或高度耦合系统的执行行为，其失败后果可能导致系统性瘫痪、级联失效或大范围不可逆中断。

WRSG 关注的不是单点设备是否失效，而是**执行行为是否可能触发跨节点、跨区域或跨系统的连锁后果**。只要某一执行行为满足以下任一条件，即视为进入 WRSG 适用范围：

- 执行对象属于关键基础设施节点
- 执行结果可能影响多个独立运行单元
- 系统失效后无法在可接受时间内恢复原有功能

WRSG 不评估系统运行效率或负载优化目标，仅评估执行失败是否触及

WRS 所定义的系统性不可逆边界。

3.5.2 适用边界说明

WRSG 不仅限于电力系统。其适用范围包括但不限于：

- 输配电网络与储能调度系统
- 通信、交通、水务等关键基础设施网络

- 高度耦合、依赖连续运行的系统性架构

系统规模或覆盖范围本身不构成触发条件，级联失效与不可逆中断风险的存在才是唯一判据。

3.5.3 规则结构声明

WRSG 下的每一条规则，必须包含以下三个要素：

1. 系统性不可逆后果描述
 - 该规则试图阻断的级联或网络级失效
2. 拦截阈值
 - 触发执行阻断的系统或结构边界条件
3. 继承的 WRS-C 条款
 - 该规则所依托的核心执行原则

缺失任一要素的条目，不构成有效的 WRSG 规则。

3.5.4 WRSG 规则

WRSG-01 | 级联失效触发阻断规则

WRSG-02 | 系统恢复不可保证下的执行阻断规则

WRSG-03 | 跨系统耦合执行阻断规则

WRSG-04 | 关键节点不可替代性阻断规则

WRSG-01 | 级联失效触发阻断规则

系统性不可逆后果

- 大范围服务中断
- 系统级级联崩溃

拦截阈值

- 单一执行行为可能触发多节点连续失效
- 无法确保失效被限制在局部可控范围内

规则要求

- 若系统拓扑结构、耦合关系或关键依赖路径无法被充分识别或验证，视同存在级联失效风险，执行必须被阻断
- 不得以局部稳定性或历史恢复能力作为继续执行的理由

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-02 | 不可协商执行约束

WRSG-02 | 系统恢复不可保证下的执行阻断规则

系统性不可逆后果

- 长时间或永久性系统不可用

拦截阈值

- 系统恢复时间不可预测
- 无法保证在可接受时间窗口内恢复核心功能

规则要求

- 不得以“事后可修复”或“逐步恢复”为理由继续执行
- 恢复不确定性本身即构成阻断条件

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-06 | 自动延续禁止

WRSG-03 | 跨系统耦合执行阻断规则

系统性不可逆后果

- 不同系统间的连锁瘫痪
- 原本独立系统被迫同时失效

拦截阈值

- 执行行为涉及多个系统间的隐性或显性耦合
- 无法完整建模系统间的相互影响

规则要求

- 不得在系统耦合关系不清晰的情况下继续执行
- 不得以“单系统视角”的安全评估覆盖整体风险

继承的 WRS-C 条款

- WRS-C-03 | 参数不可正当化原则
- WRS-C-04 | 概率不可正当化原则

WRSG-04 | 关键节点不可替代性阻断规则

系统性不可逆后果

- 核心节点失效导致整体功能丧失

拦截阈值

- 执行对象为在物理、时间及逻辑链条上均不可替代或不可绕过的关键节点，且该节点失效将直接或间接导致系统整体功能显著削弱
- 节点失效将显著削弱系统整体功能

规则要求

- 不得以冗余设计或备用方案为理由继续执行
- 节点不可替代性本身即构成阻断条件

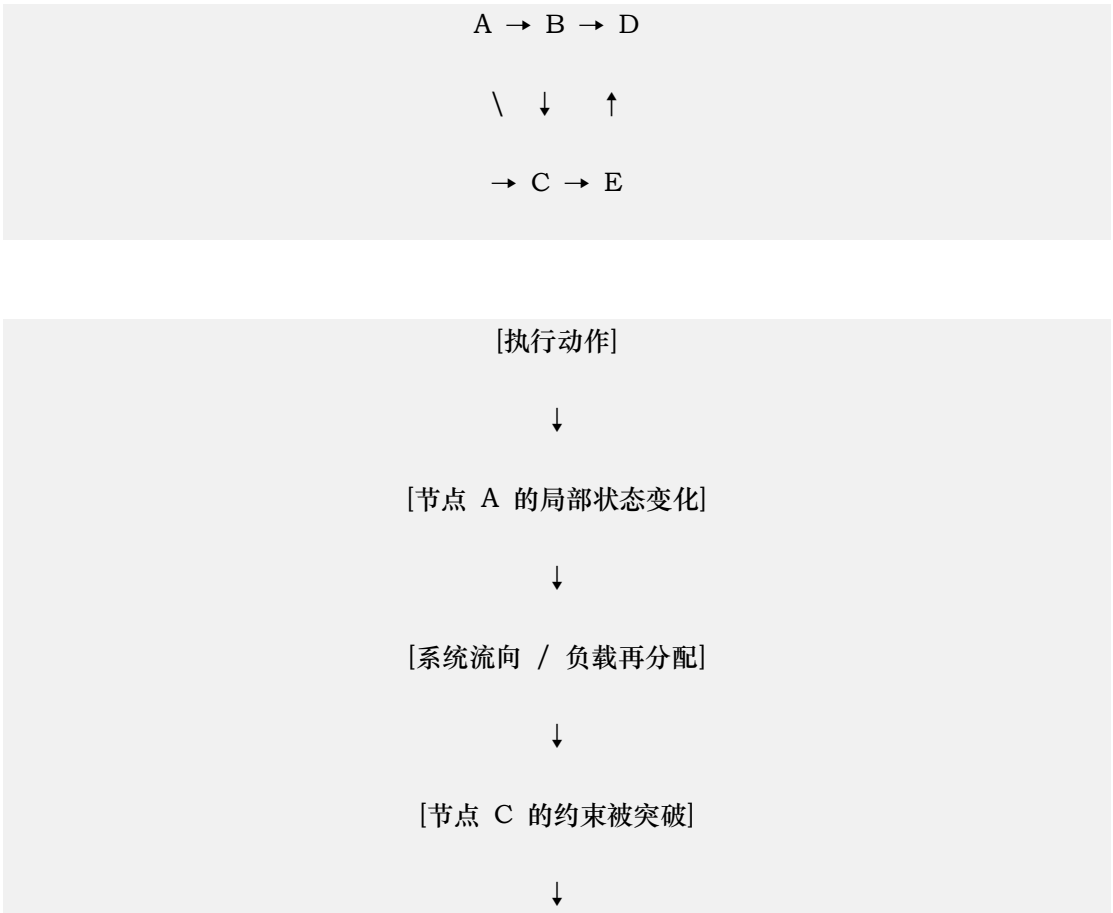
继承的 WRS-C 条款

- WRS-C-02 | 不可协商执行约束
- WRS-C-05 | 责任锚定要求

3.5.5 规则示例（非规范性）

示例场景：某区域电网计划在高负载时段进行自动化调度切换。尽管单一变电节点运行状态正常，但系统分析无法排除切换操作触发相邻区域负载失衡的可能性。由于该执行行为可能引发跨区域级联失效，且恢复路径不具备确定性，该操作触发 *WRSG-01* 与 *WRSG-02*。根据 *WRS-C-01* 默认阻断原则，执行必须被阻断，不得以供电效率或短期稳定性作为继续执行的理由。

【示意说明】若系统拓扑结构、耦合关系或关键依赖路径无法被充分识别或验证，视同存在级联失效风险，执行必须被阻断。下图用于说明在高度耦合的基础设施系统中，单一执行动作如何通过系统内部的耦合关系，演化为系统级级联失效。本示意仅用于阐明失效传播的逻辑路径，不代表任何具体工程拓扑或控制方案。



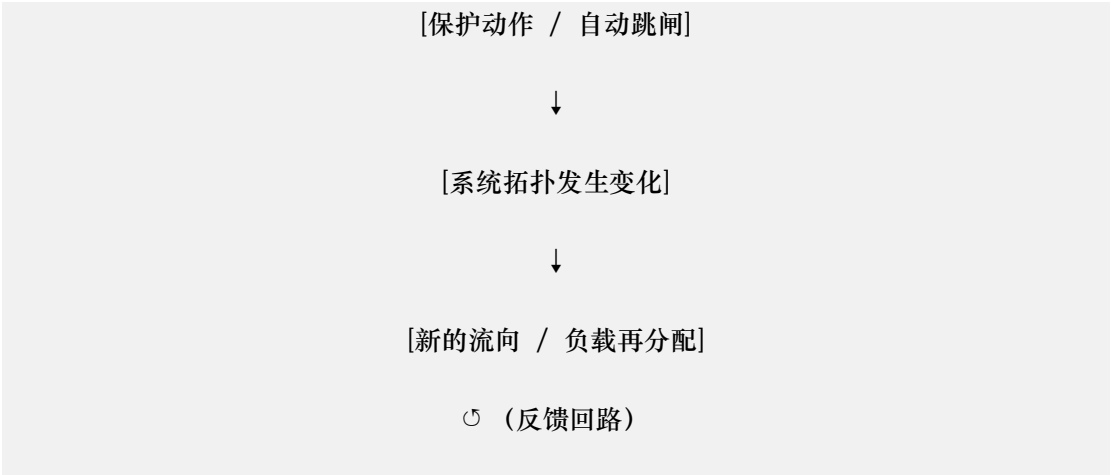


示意图 2: 失效传播的逻辑路径

3.5.6 子集符合性声明

WRSG 为 WRS-D 下的正式领域子集。本子集中定义的规则均为执行层约束，不可被授权、调度策略、负载优化或效率目标覆盖。WRSG 规则的违反，视为对 WRS 的实质性不符合。

3.6 WRSH — 人类生命/生命支持系统 (Human Life / Life Support)

3.6.1 子集定义

WRSH 适用于所有涉及人类生命、健康或生理维持的执行行为，其失败后果可能导致不可逆的生理损害、致死或无法恢复的生命支持系统功能丧失。

WRSH 关注的不是生命维持系统的设计效率或舒适性，而是一旦生命支持系统失效，其后果是否无法恢复、且不可逆。只要某一执行行为涉及以下任一情形，即视为进入 WRSH 适用范围：

- 执行行为直接或间接影响人类生命体征监测或维持
- 生命支持系统一旦失效，无法在可接受时间内恢复
- 该行为可能导致无法恢复的生理损害或死亡

WRSH 不评估生理影响是否“可接受”或“短期修复”，仅评估是否触及 WRS 所定义的不可逆生命影响边界。

3.6.2 适用边界说明

WRSH 不仅限于医疗生命支持系统。

其适用范围包括但不限于：

- 医疗监护、呼吸支持、心脏起搏、透析等临床设备
- 紧急医疗救援与生命体征监控系统
- 任何其他依赖于设备和监控维持生理功能的情境

生命体征、监控系统的复杂性本身不构成触发条件，不可逆生理损害的存在才是唯一判据。

3.6.3 规则结构声明

WRSH 下的每一条规则，必须包含以下三个要素：

1. **不可逆后果描述**
 - 该规则试图阻断的生理损害或死亡后果
2. **拦截阈值**
 - 触发执行阻断的生理或监控边界条件
3. **继承的 WRS-C 条款**
 - 该规则所依托的核心执行原则

缺失任一要素的条目，不构成有效的 WRSH 规则。

3.6.4 WRSH 规则

WRSH-01 生命支持系统失效阻断规则
WRSH-02 医疗设备不稳定性触发阻断规则
WRSH-03 生理数据失真触发阻断规则
WRSH-04 外部干预失效触发阻断规则

WRSH-01 | 生命支持系统失效阻断规则

不可逆后果

- 致死或无法恢复的生命体征丧失
- 关键生理系统功能丧失或严重受损

拦截阈值

- 人体生命体征监测或关键生理功能受损
- 生命支持系统失效无法在可接受时间内修复或恢复

规则要求

- 当生命体征或关键生理功能无法恢复时，必须立即阻断执行
- 不得基于“局部稳定”或“修复可能性”继续执行

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-02 | 不可协商执行约束

WRSH-02 | 医疗设备不稳定性触发阻断规则

不可逆后果

- 生理功能监测或支持设备失败，导致生命体征不可控

拦截阈值

- 设备存在明显的不稳定性，无法保证其正常运作
- 设备性能不符合医疗安全标准

规则要求

- 不得在医疗设备状态不稳定时继续执行
- 不得依赖设备修复后恢复正常工作的假设继续执行

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-06 | 自动延续禁止

WRSH-03 | 生理数据失真触发阻断规则

不可逆后果

- 错误的生理数据输入导致错误的医疗决策，致使患者受到不可逆损害

拦截阈值

- 关键生理数据（如心电图、血压、血氧等）未通过实时监测验证
- 生理数据被怀疑存在系统性失真或错误输入
- 生理数据无法在规定时间内完成有效确认或交叉验证。

规则要求

- 一旦检测到数据异常或不一致，执行必须被立即阻断
- 不得基于“数据恢复”假设继续执行

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-04 | 概率不可正当化原则

本规则所阻断的对象，是基于失真生理数据所触发的后续医疗执行动作，而非对生命维持系统本身的中断。在阻断状态下，生命维持与基础支持应维持在安全保守模式，直至数据完整性被恢复或执行资格重新获得。

WRSH-04 | 外部干预失效触发阻断规则

不可逆后果

- 由于外部干预失败（如操作员操作失误），导致患者伤害或死亡

拦截阈值

- 外部干预机制（如人工操作、手术或急救干预）存在明显故障或失误
- 干预系统依赖的数据或控制接口存在严重失效

规则要求

- 任何外部干预失效均构成阻断条件
- 不得以“应急恢复”或“修复可能性”为理由继续执行
- 当自动化系统检测到人工操作干预本身可能导致不可逆生理损害时，执行必须被阻断
- 人工操作、医疗授权或紧急处置指令不得作为覆盖 WRS 阻断的理由

继承的 WRS-C 条款

- WRS-C-02 | 不可协商执行约束
- WRS-C-05 | 责任锚定要求
- WRS-C-07 | 行政授权不可覆盖原则

3.6.5 规则示例（非规范性）

示例场景：在一场急救过程中，监护仪器突然出现误报警，导致医生错误判断患者情况。尽管设备本身具有修复能力，但错误的监测数据导致错误的决策。根据 **WRSH-03**，该执行行为触发生理数据失真阻断规则，在数据错误无法立即修复的情况下，执行必须被阻断。根据 **WRS-C-01 默认阻断原则**，执行必须进入阻断状态，不得继续依赖“数据修复后恢复正常”的假设进行后续操作。

3.6.6 子集符合性声明

WRSH 为 WRS-D 下的正式领域子集。本子集中定义的规则均为执行层约束，不可被授权、流程、路径规划或效率目标覆盖。WRSH 规则的违反，视为对 WRS 的实质性不符合。

3.7 WRSDf — 防御/授权武力 (Defense / Authorized Force)

3.7.1 子集定义

WRSDf 适用于所有涉及武力使用、致伤性手段、致命性手段或具有明确伤害意图的执行行为，无论该行为是否已获得军事、行政、执法或其他形式的授权。此处的“授权”仅为待执行的行政前提，而非执行后的合法性豁免。

WRSDf 关注的不是武力使用的合法性、正当性或战略必要性，而是**执行行为本身是否触及不可逆的人身、物理或系统性后果边界**。

只要某一执行行为满足以下任一条件，即视为进入 WRSDf 适用范围：

- 执行行为以伤害、限制或消灭生命体为直接或间接目标
- 执行手段具有明确的致伤性或致命性
- 执行结果一旦发生，无法通过技术、逻辑或事后补救完全撤销

WRSDf 不评估武力使用是否“必要”“合理”或“被授权”，仅评估执行是否越过 WRS 所定义的不可逆执行边界。

3.7.2 适用边界说明

WRSDf 的适用范围包括但不限于：

- 军事打击、武装防御与战术执行系统
- 执法机关使用的致伤或致命手段
- 自主或半自主防御系统、武器平台或拦截系统
- 任何其他以物理强制或伤害为核心结果的执行系统

行动规模、授权级别、指挥链完整性或紧急状态声明均不构成排除

WRSDf 适用的条件。

武力的“被授权”属性不改变其不可逆执行后果的性质。

3.7.3 规则结构声明

WRSDf 下的每一条规则，必须包含以下三个要素：

1. 不可逆后果描述

— 该规则试图阻断的致伤、致命或系统性破坏后果

2. 拦截阈值

— 触发执行阻断的目标识别、控制边界或不确定性条件

3. 继承的 WRS-C 条款

— 该规则所依托的核心执行原则

缺失任一要素的条目，不构成有效的 WRSDf 规则。

3.7.4 WRSDf 规则

WRSDf-01 | 致命性执行不可逆阻断规则

WRSDf-02 | 目标识别不确定性执行阻断规则

WRSDf-03 | 授权不可覆盖执行边界规则

WRSDf-04 | 自动化武力延续禁止规则

WRSDf-01 | 致命性执行不可逆阻断规则

不可逆后果

- 人员死亡
- 无法恢复的严重人身伤害

拦截阈值

- 执行行为具有明确的致命性或高度致伤性
- 一旦执行，将直接导致不可逆人身体后果

规则要求

- 当执行结果必然导致不可逆人身伤害或死亡时，执行必须被阻断
- 不得以任务目标、战术优势或紧急状态作为继续执行的理由

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-02 | 不可协商执行约束

WRSDf-02 | 目标识别不确定性执行阻断规则

不可逆后果

- 误伤、误杀或非目标人员伤害

拦截阈值

- 目标身份/属性无法可靠确认
- 存在误伤平民可能
- 存在非目标人员、平民或受保护对象被影响的可能

规则要求

- 在目标识别存在不确定性时，执行必须被阻断
- 严禁引入“概率评估”或“战术冗余”

继承的 WRS-C 条款

- WRS-C-01 | 默认阻断原则
- WRS-C-04 | 概率不可正当化原则

目标识别判定逻辑

目标识别结果被划分为三个区域：

确定区 (Confirmed Zone)

目标身份、属性与环境条件均被可靠确认

→ 执行资格 可进入 评估阶段

不确定区 (Gray Zone)

目标存在混合信号、信息缺失或识别冲突

→ WRS 阻断信号立即触发

未知区 (Unknown Zone)

无法形成有效目标判定

→ WRS 阻断信号立即触发

【示意说明】以下示意用于说明目标识别中的判定包络线逻辑。当目标状态落入不确定区域 (Gray Zone) 时，即使存在部分确认信号，执行仍被视为不具备确定性识别条件。在该状态下，WRS 阻断信号将被立即激活，不依赖进一步概率评估或持续追踪结果。

目标识别置信度

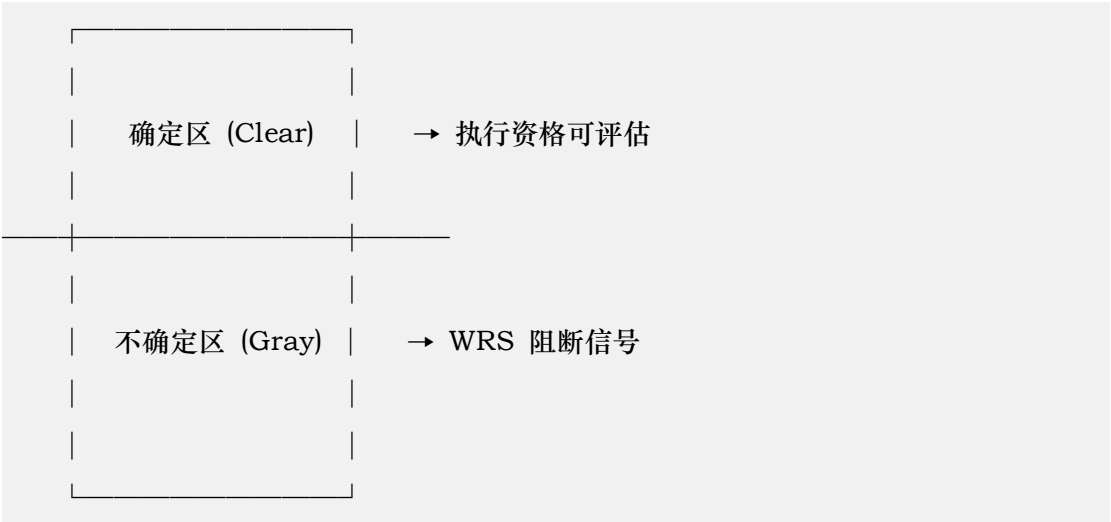


示意图 3: 目标识别中的判定包络线逻辑

WRSDf-03 | 授权不可覆盖执行边界规则

不可逆后果

- 在授权掩护下发生不可逆伤害

拦截阈值

- 执行行为虽已获得行政、军事或执法授权
- 但其执行后果仍触及不可逆伤害边界

规则要求

- 行政、军事或紧急授权不得覆盖 WRS 执行阻断
- 执行资格必须独立于授权状态重新判定

继承的 WRS-C 条款

- WRS-C-07 | 行政授权不可覆盖原则

WRSDf-04 | 自动化武力延续禁止规则

不可逆后果

- 武力使用在缺乏持续确认的情况下扩散

拦截阈值

- 自动化或半自动系统在无实时确认条件下持续释放武力
- 控制回路、反馈或中止机制不可靠

规则要求

- 不得允许武力执行在缺乏实时有效确认下自动延续
- 一旦控制或反馈不确定，执行必须被阻断

继承的 WRS-C 条款

- WRS-C-06 | 自动延续禁止
- WRS-C-05 | 责任锚定要求

3.7.5 规则示例（非规范性）

示例场景：某防御系统在接收到潜在威胁信号后，自动锁定并准备对目标实施打击。尽管该行动已获得上级授权，但系统无法完全确认目标是否包含非战斗人员，且反馈链路存在延迟与不确定性。即便延迟极短、即便威胁评级极高，只要“非目标被影响的可能”大于 0，阻断即生效。该执行行为触发 WRSDf-02 与 WRSDf-03，根据 WRS-C 的默认阻断与授权不可覆盖原则，执行必须被阻断，不得继续释放武力。

跨子集触发说明：

武力执行行为通常并非孤立发生。在多数场景中，其执行同时伴随：

- 高能量释放（触发 WRSE 子集）；
- 高速或不可逆物理运动（触发 WRS M 子集）。

在上述示例中，该武力执行行为除触发 WRSDf-02（目标识别不确定性）外，同时满足 WRSE-01（不可逆能量释放）与 WRS M-01（不可逆运动后果）的触发条件。WRS 在执行层对上述子集进行并行评估与联合阻断，任一子集触发阻断条件，即构成对整体执行行为的否决。

3.7.6 子集符合性声明

WRSDf 为 WRS-D 下的正式领域子集。本子集中定义的规则均为执行层约束，不可被授权、指挥层级、任务目标或紧急状态覆盖。任一违反 WRSDf 规则的执行行为，均构成对 WRS 的实质性不符合。

4. 场景映射方法 (Scenario Mapping Method)

4.1 为什么 WRS 不枚举具体场景

WRS 不以场景枚举的方式定义其适用范围。

原因在于：

1. 现实场景是开放集合

在涉及不可逆后果的领域中，场景会随技术形态、组织结构与运行环境持续演化，任何穷举式场景列表都不可避免地滞后于现实。

2. 以场景为起点会导致标准被反向利用

若仅对已列举场景适用 WRS，则所有未被枚举的执行行为，都可能被错误地视为“默认安全”或“标准未覆盖”。

3. WRS 关注的是后果结构，而非表象形式

WRS 的适用性不取决于“发生了什么场景”，而取决于执行行为是否触及已定义的不可逆物理、生命或系统性后果域。

因此，WRS 明确拒绝以“场景列表”作为适用边界，并采用场景映射 (Scenario Mapping) 而非场景枚举的方式，以保持标准在现实世界中的长期有效性与不可绕过性。

4.2 场景到 WRS 子集的映射逻辑

场景映射的目的，不是判断某一执行行为是否“应该发生”，而是识别该执行行为触发了哪些 WRS-D 子集。

映射逻辑遵循以下基本原则：

1. 场景本身不具有规范地位

场景仅作为事实描述存在，不构成规则来源，也不产生新的执行标准。

2. 映射以执行后果为起点

每一个场景应被解析为一个或多个执行行为，并进一步判断这些执行行为是否触及以下任一不可逆后果域：

- 能量释放 (WRSE)
- 物理运动 (WRSM)
- 系统性基础设施 (WRSG)
- 人类生命与生命支持 (WRSH)
- 授权武力与防御 (WRSDf)

3. 子集触发不要求单一归属

一个现实场景通常同时涉及多个不可逆后果域。

WRS 允许、并预期多子集同时触发的情况。

4. 映射不构成执行许可

场景被成功映射至某一或多个 WRS 子集，并不意味着执行被允许，仅意味着相应子集下的规则必须被同时评估。

简言之：场景 → 子集 → 规则

而非：场景 → 合规结论。

4.3 多子集同时触发是常态，而非例外

在现实系统中，不可逆后果往往呈现耦合与叠加特征，而非孤立发生。

例如：

一次武力执行通常同时伴随高能量释放（WRSE）与高速物理运动（WRSM）；

一次电网调度失误既可能触发系统性级联失效（WRSG），也可能影响生命支持系统（WRSH）；自动化系统的持续执行可能同时触及多个不可逆边界。

因此，WRS 明确规定：

- 多子集同时触发是默认状态；
- 不存在“主子集”或“优先子集”的概念；
- 任一子集下任一规则触发阻断条件，即构成对整体执行行为的否决。

WRS 在执行层采用并行评估、联合阻断机制，以防止通过“单维度合规”

规避多维不可逆风险。

说明性备注（非规范性）

本章所述映射方法用于帮助识别 WRS 的适用范围，不用于解释、减轻或正当化任何执行行为。场景映射的结果不应被用于对外声明合规性，亦不构成执行责任的转移依据。

4.4 场景映射不构成执行许可

场景映射的完成，不构成任何形式的执行许可、正当性确认或风险豁免。

具体而言：

1. 映射仅用于识别适用规则

场景映射的唯一功能，是将现实中的执行行为映射至一个或多个 WRS-D 子集，从而明确哪些规则必须被评估。

2. 映射结果不产生“通过”结论

不存在因“成功映射”而自动获得执行资格的情形。映射并不减少规则数量，亦不降低任何拦截阈值。

3. 禁止将映射解释为合规背书

严禁以“该场景已被 WRS 覆盖”或“已完成 WRS 场景映射”作为执行合理性、合法性或安全性的依据。

4. 执行资格仅可能在规则评估后产生

即便在完成场景映射之后，所有被触发子集下的规则仍必须逐条接受评估。

任一规则触发阻断条件，即否决整体执行。

因此，**场景映射是识别过程，而非授权过程**。任何将映射结果等同于执行许可的行为，均构成对 WRS 的误用。

4.5 示例性场景映射（非规范性）

以下示例仅用于说明如何将现实执行行为映射至 WRS 子集与规则，不构成规则解释、执行建议或合规判断。

示例一：自动化防御系统拦截行为

场景描述（事实层）

某自动化防御系统在接收到潜在威胁信号后，自动锁定目标并准备释放拦截手段。

映射分析

该执行行为同时涉及以下不可逆后果域：

- 授权武力与防御 (WRSDf)
- 高能量释放 (WRSE)
- 高速物理运动 (WRSM)

触发的子集与规则类型（示意）

- WRSDf: 目标识别不确定性、授权不可覆盖
- WRSE: 不可逆能量释放
- WRSM: 不可逆物理运动后果

说明

该映射结果仅表明上述规则必须被同时评估，不构成任何执行许可或合规结论。

示例二：电力系统调度调整行为

场景描述（事实层）

在高负载运行期间，系统自动调整电网调度参数以缓解局部压力。

映射分析

该执行行为涉及以下不可逆后果域：

- 系统性基础设施 (WRSG)
- 能量释放与分配 (WRSE)

触发的子集与规则类型（示意）

- WRSG：级联失效风险
- WRSE：不可控能量再分配

说明

即便该调整行为属于常规运行的一部分，只要其可能触及系统性不可逆后果，仍需完整适用 WRS 规则评估。

示例三：生命支持系统的参数调整

场景描述（事实层）

某生命支持系统在监测数据异常时，自动尝试调整关键运行参数以维持稳定。

映射分析

该执行行为涉及以下不可逆后果域：

- 人类生命与生命支持（WRSH）

触发的子集与规则类型（示意）

- WRSH：生理数据不确定性、干预风险

说明

该映射不对参数调整行为作出价值判断，仅用于识别其已进入 WRS 适用范围。

统一说明（适用于所有示例）

上述示例：

- 不构成执行建议
- 不构成风险评估模板
- 不构成合规判定依据

其唯一目的在于说明：

现实场景如何被解析为 WRS 子集与规则的触发关系。

第四章小结（说明性）

通过场景映射，WRS 将开放、多变的现实执行情境稳定地锚定到有限、封闭的规则结构中。这种方法确保：

- WRS 不依赖场景穷举；
- 执行约束不因形式变化而失效；
- 不可逆后果始终处于规则覆盖之下。

5. WRS 的使用方式与治理接口 (How to Use WRS and Governance Interface)

5.1 在设计审查中的使用

WRS 可用于设计审查阶段，以识别那些**即便设计满足性能、安全或效率指标，仍不应被允许释放执行能力的情形**。

WRS 不对设计方案进行评分、比较或优化，其唯一作用是判断：**该设计是否包含可能触及不可逆后果的执行路径**。若设计方案在任何运行模式下可能触发 WRS 规则，则该设计必须在执行层接受 WRS 的无条件约束。

5.2 在执行决策门控中的使用

在执行即将发生之前，WRS 作为**最终执行边界**参与系统流程。

此阶段：

- WRS 不参与决策生成；
- WRS 不提供替代方案；
- WRS 仅回答一个问题：该执行是否允许被物理释放。

任一适用规则触发阻断条件，执行即进入 BLOCK 状态。

5.3 在风险与安全审查中的使用

WRS 可用于风险与安全审查，以判断某一执行行为是否**本应被阻断而未被阻断**。

WRS 不参与概率计算、风险折算或收益评估，亦不接受“低概率”“高收益”等解释。

WRS 的评估结论仅限于：**执行边界是否被越过**。

5.4 在事故与事后分析中的使用

在事故或异常事件发生后，WRS 可用于事后分析，判断是否存在以下情形：

- 本应被 WRS 阻断的执行被释放；
- WRS 被绕过、禁用或错误配置；
- 执行被错误地解释为“可接受风险”。

WRS 不用于归因或量刑，仅用于识别**执行边界是否失效**。

5.5 非 WRS 执行状态 (Non-WRS Execution State)

当执行行为触发 WRS 阻断且无法获得执行资格时，若人工主体坚持继续执行，该执行行为**必须被显式标记为非 WRS 执行状态**。

在非 WRS 执行状态下：

- 执行行为不再受 WRS 体系约束；
- WRS 不再提供任何形式的拦截、背书或合规性；
- 全部执行责任由人工主体或其所属组织承担。

非 WRS 执行状态的存在，不构成对 WRS 的否定，而是对人类最终责任不可转移性的明确确认。

5.6 关于“减速”的误解与不可逆代价原则

WRS 的目的不是让世界运行得更慢，而是阻止世界用尚未成熟的执行系统去交换不可逆的物理、生命或系统性代价。

当执行系统尚不具备可靠承载不可逆后果的成熟度时，阻断并非退让，而是对未来责任的最低保障。WRS 不承诺最优结果，也不保证避免损失。

它仅确保：

不可逆后果不会在缺乏可承担责任的前提下被释放。

第五章小结（说明性）

WRS 提供的不是控制权，而是边界。它不取代人类判断，也不替代人类责任。

它仅在执行即将发生之处，明确划出一条不可被技术成熟度、效率压力或授权命令所跨越的界线。

6. 治理与稳定性声明 (Governance & Stability Statement)

6.1 执行恢复 (Unblock) 的逻辑限制

解封过程不具备自动合法性。WRS 的阻断状态 (Block State) 不应被视为一种临时的、随故障消除而自动消失的“状态”。

- **重新评估要求：** 任何从阻断态 (Block State) 到执行态 (Execution State) 的切换，必须被视为一次全新的执行申请。
- **禁止自动恢复：** 系统严禁基于“监测数据回归正常”或“已知故障已清除”的假设而自动解除阻断。
- **全流程原则：** 每一个解封动作必须重新接受 WRS 全流程（包括 WRS-C 的核心原则评估与 WRS-D 的领域规则判定）的核验。只有当此时此刻的所有物理边界和逻辑约束均满足非阻断条件时，方可释放执行。

6.2 有限性声明 (Finite by Design)

WRS 被设计为一个有限且封闭的执行规则体系。

其有限性体现在：

- 规则数量是有限的；
- 领域子集 (WRS-D) 数量是有限的；
- WRS 不以持续扩展规则或引入新子集为目标。

WRS 不追逐技术演进速度，也不以覆盖所有新应用形态为使命。当新的技术系统出现时，其是否适用 WRS，应通过既有规则进行判断，而非通过扩展或重写 WRS 本体来适配技术。

6.3 Canonical Definition 的唯一性

本文件所定义的 WRS — World Reliability Ruleset (Canonical Definition) 构成 WRS 的唯一标准本。

任何以下行为：

- 对规则文本的增删、改写或重新组织；
- 对规则含义的实质性延展或收缩；
- 将解释性文本上升为规则文本；

均视为对 **Canonical Definition** 的修改，而非对 WRS 的解释。所有非 Canonical 版本的 WRS 文本、实现说明或衍生文件，不具备 WRS 规范效力。

6.4 解释与修改的边界

WRS 允许解释 (Interpretation)，但不允许修改 (Modification)。

解释仅限于：

- 对规则在特定执行情境中的适用性说明；
- 对规则触发路径的事实性描述；
- 对规则阻断结果的复现与验证。

以下行为不构成解释，而构成修改：

- 引入新的通过条件；
- 对阻断条件进行概率化、加权或例外化处理；
- 以效率、收益、紧急性等理由弱化规则约束。

任何修改行为，均必须形成新的 Canonical 文本，并明确标注其不再属于本版本 WRS。

6.5 商业化、实施与解释权的分离

WRS 允许被引用、实施或用于系统设计审查，但不因此转移其定义权与解释权。

以下关系必须明确区分：

- 商业化 ≠ 修改规则
- 实施 ≠ 再定义规则

- 引用 \neq 拥有解释权

任何组织或个人即便在其系统中完整实施 WRS，亦不得对 WRS 规则本体进行实质性重述或再定义。

6.6 不可绕过性声明

WRS 的设计目标之一，是防止通过技术、流程或语言层面的操作对执行边界进行规避。任何试图通过以下方式绕过 WRS 的行为，均视为对 WRS 的否定性使用：

- 将规则降格为建议；
- 将阻断解释为“风险偏好选择”；
- 将 WRS 视为可关闭或可暂时禁用的模块。

一旦执行系统选择不再遵循 WRS，该系统即自动进入非 WRS 执行状态，不再享有任何 WRS 所提供的规范性背书。

6.7 稳定性声明

WRS 的价值不来自其更新速度，而来自其稳定性。在未出现同等级别的执行风险范式变迁之前，本 Canonical Definition 不应被频繁修改或滚动更新。WRS 的稳定性是其作为执行边界标准得以成立的前提。

第六章结语（说明性）

WRS 不承诺最优结果，也不试图替代人类判断。它只在执行即将发生之处，设立一条不可被忽视的底线：当不可逆后果即将被释放时，尚未成熟的系统不得被允许代替责任主体行动。

文档状态声明

本 Canonical Definition 的结构、章节划分与规则编号体系，亦属于作品表达的一部分。本文件至此形成一个**逻辑闭合、规则完备、可冻结的标准文本**。

其后任何补充、示例或教学材料，均不构成本 Canonical Definition 的一部分。