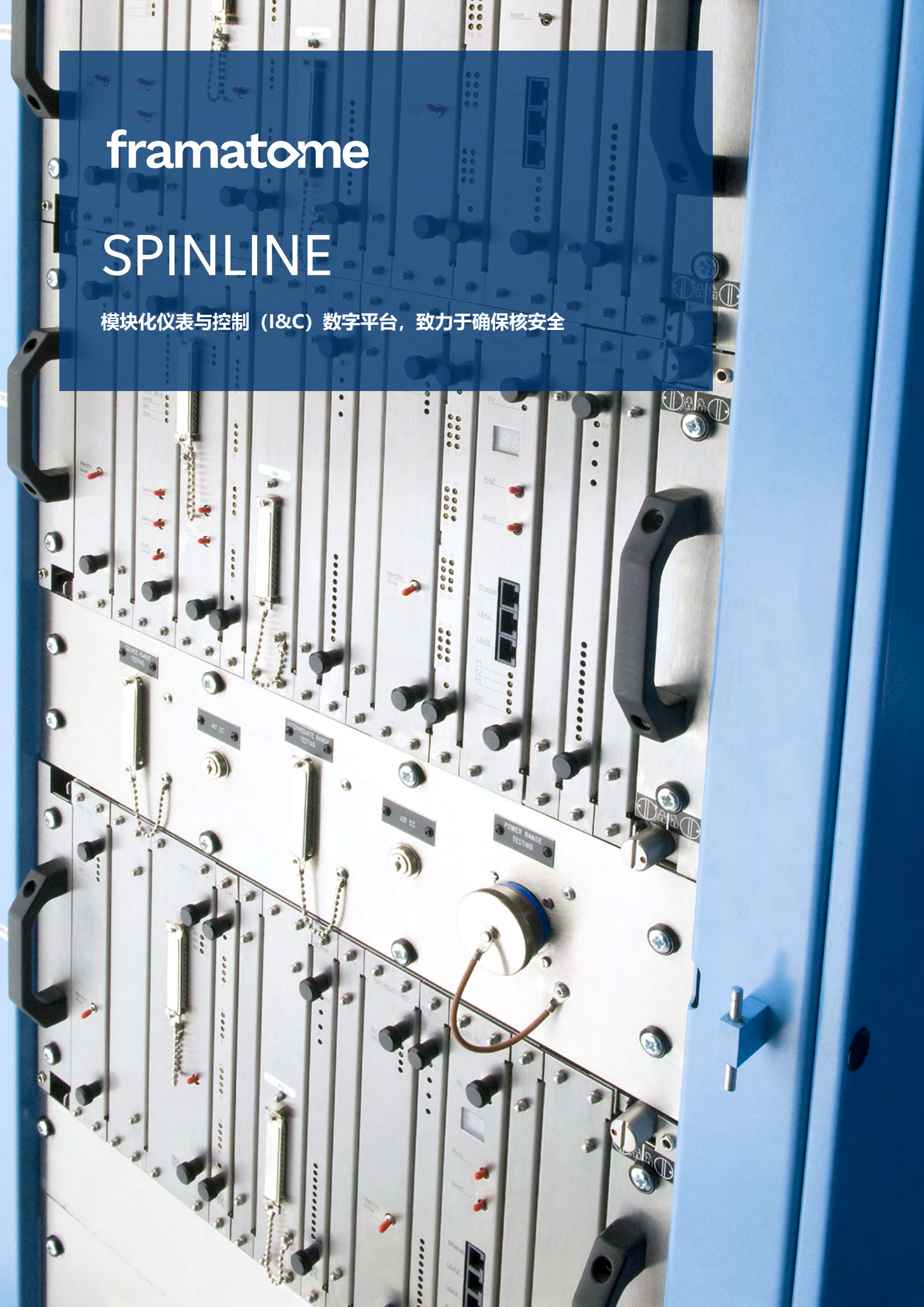
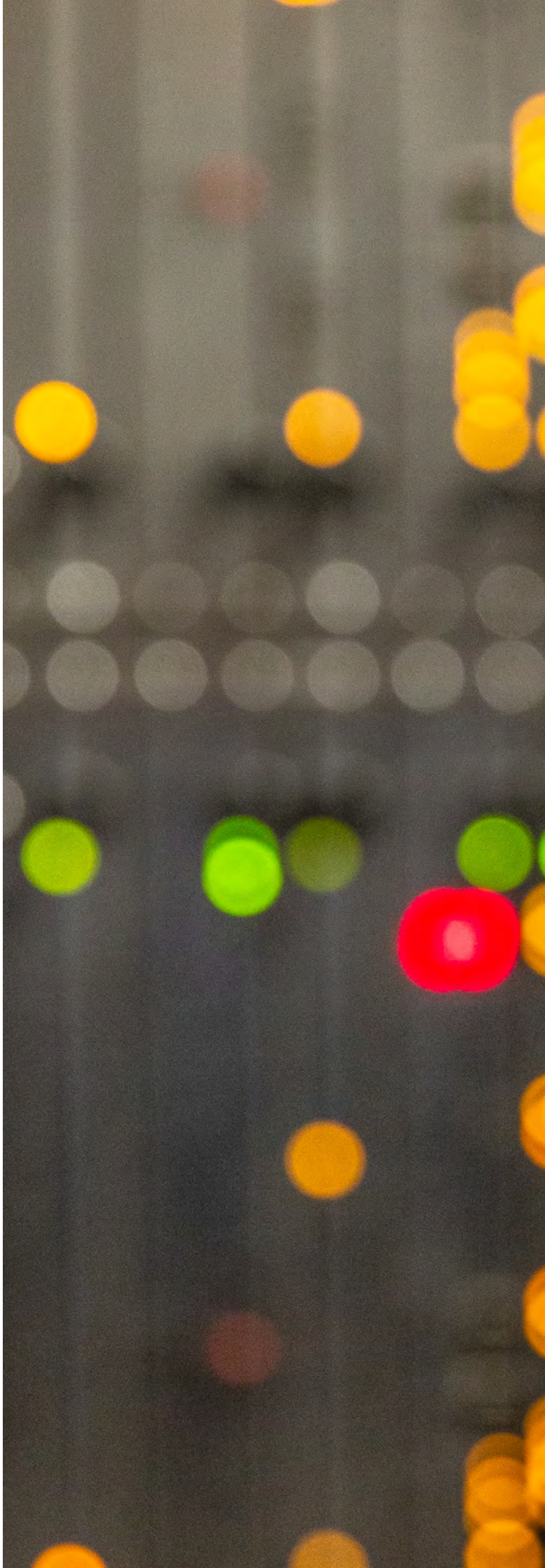
framatome

SPINLINE

模块化仪表与控制（I&C）数字平台，致力于确保核安全



目录



关于 Spinline

Spinline是专门为核安全仪控应用而设计的法马通最新的数字化技术解决方案之一

Spinline是一个专用于开发或升级核反应堆安全系统的模块化数字解决方案。

Spinline专门设计用于无法通过传统DCS和PLC系统实现的A类1E级安全功能（IEC-61226）。

安全可用

Spinline使得公用事业部门能够提高核电厂的安全性和可用性。Spinline的安全导向设计允许并包括诸如确定性行为、故障安全、容错、冗余、物理和功能隔离、功能多样性、在线监控和自动定期测试等特定功能，并通过自检、自动定期测试和故障安全导向来提高可用性。

久经考验

Spinline 拥有 50 年的经验，已被成功安装在全球超过 90 座核反应堆中，这使得法马通成为全球该领域经验最为丰富的公司。

2009 年，法马通完成了 Dukovany 核电厂（捷克共和国）的仪表与控制 (I&C) 系统改造，该项目历时 9 年，被认为是世界上最重要的仪表与控制 (I&C) 系统现代化改造项目之一。

目前，Spinline 正被用于法国20台EDF 1300MW 机组的仪控 (I&C) 系统的现代化改造，这也是全球最大的现代化改造项目，并于2018年成功地对芬兰两座Loviisa VVER工厂的关键部分进行了现代化改造。

法马通提供安全仪表与控制 (I&C)

模块化

Spinline 设计用于执行核电厂和研究堆仪表与控制 (I&C) 数字系统的安全功能。

Spinline 既可用于新建核电厂的保护系统，如反应堆保护系统(RPS)、中子测量仪表系统 (NIS)、过程仪表系统、工程安全特性驱动系统（ESFAS）、应急柴油发电机（UDG/EDG）仪控系统和柴油机负荷排序系统，也可用于在运核电厂的现有安全仪表与控制 (I&C) 系统的现代化改造。

鉴证标准

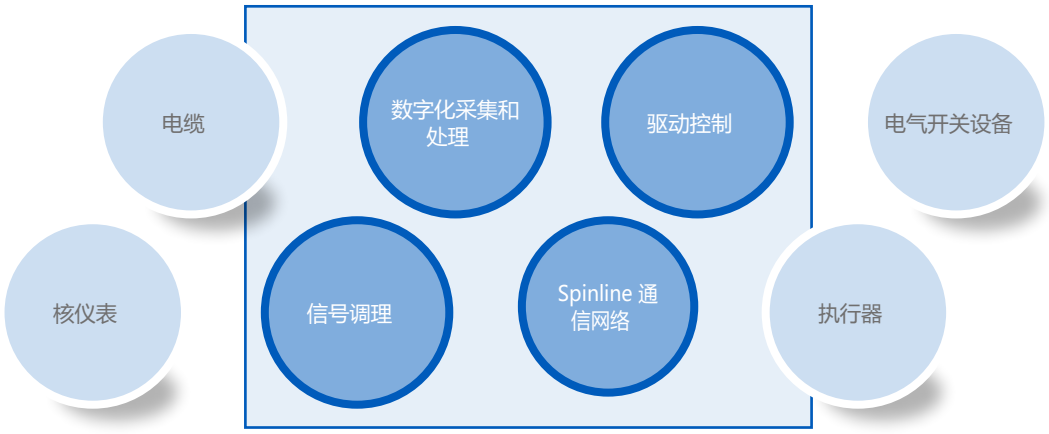
Spinline 的技术是依据核仪表与控制 (I&C) 系统固有的苛刻安全要求而专门设计，软件的开发则严格遵循国际、美国、欧洲和当地标准，硬件方面完全满足电磁兼容性 (EMC)、环境和地震条件要求。

成本效益高

Spinline 是一项安全的投资。基于严格有效的开发方法，Spinline采用最新组件，确保法马通的客户能够从最佳的仪表与控制 (I&C) 数字技术中受益，最大程度优化其运营效率。

长期支持

法马通还可与客户签署长期支持协议（LTSA）来提供Spinline及其他技术服务，此类协议涵盖合同范围内（安装后最长25年）的培训、维护、备件和其他服务。Spinline被包含在数个这样的合同中，因此将至少维护和更新至2053年。



Spinline 周边装置：从传感器到执行器

实现A类1E级安全仪控（I&C）功能的模块化数字解决方案


framatome
framatome
framatome

设计特点

Spinline专为核安全应用而设计

核电厂的电力生产必须安全高效，仪表与控制 (I&C) 系统，特别是安全仪表与控制 (I&C) 系统，是实现该目标的关键所在。

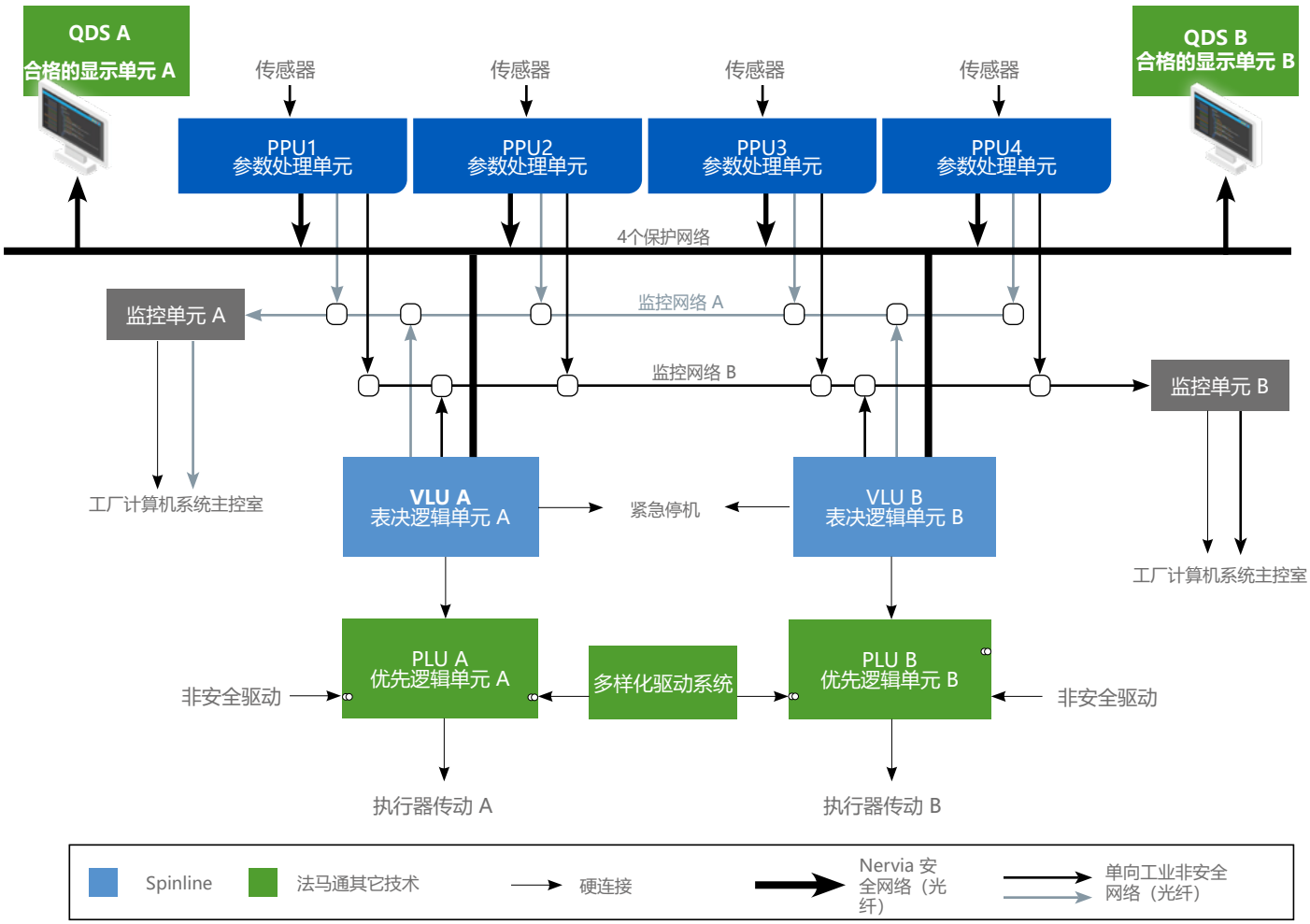
国家、安全部门和公用事业部门的基本要求是：

- 高水平的安全性和可用性
- 符合国际标准
- 资质符合核标准
- 最先进的技术和性能
- 符合核电厂生命周期（即备件和技术的可用性）
- 成本效益高

Spinline 的设计旨在反映这些要求，并提供以下功能：

- **故障安全架构**：Spinline 确保在检测到故障的情况下，与CPU关联的输出进入预设值状态。未检测到的故障可能会影响系统安全性。
- **容错（包括单一故障准则）**：Spinline 可以满足任何冗余要求。
- **功能多样性**：可用于保护系统免受常见原因故障的影响。
- **功能性隔离**：通过通信手段和隔离设备确保隔离，避免冗余部件之间的故障传播。
- **确定性**：对于所有处理，相同的输入产生相同的输出，并保证响应时间。
- **操作和维护方便。**
- **灵活性**：无需进行任何硬件修改就可以修改系统功能
- **模块化**：Spinline 有两种交付方式，作为机架集成到现有机柜（用于升级改造目的），或以完整机柜形式交付。
- **可扩展性**：Spinline 适用于各种规模的仪表与控制 (I&C) 系统。它可用于诸如可进行采集、功能处理和表决的分布式处理四通道反应堆保护系统等高度分布式架构，还可用于更加紧凑的架构，例如具有两个源量程通道、两个中间量程通道和四个功率量程通道、且不对处理进行单独分配的中子测量仪表系统。
- **成本效益高**：Spinline 以其无与伦比的可靠性和精确性使得公用事业部门能够有效地运营核电厂，减少停机时间。

基于Spinline的反应堆保护系统示例



技术历史与演变

当前的Spinline技术源自项目的持续开发，为客户提供一流的数字技术

Spinline是法马通公司开发的专用于核仪表与控制系统的最新模块化数字技术解决方案之一。

Spinline在其 50 年的发展历程中不断更新，以提高可靠性/可用性和响应时间性能，使维护和操作更容易，满足电磁兼容性要求，缩短项目开发时间，成为核安全系统数字技术的国际标准。

Spinline 技术的关键步伐和日期

模拟系统

非基于软件

- **法国**
  900MW 核电厂

1970

P4 SPIN

8位
微处理器

- **法国**
  1300MW P4 核电厂

1980

N4 SPIN

16位
微处理器

- **法国**
  1450MW N4 核电厂

1990

SPINLINE3

32位
微处理器

- **Dukovany**
- **Tihange**
- **Metzamor**
- **秦山**
- **Kozloduy**
- **Fessenheim**
- **Bugey**

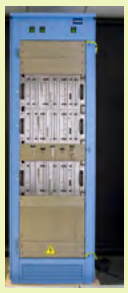
2000

SPINLINE

32位
微处理器

- 新网关
- 重新设计的 CPU 板
- 提升信号管理能力
- 可调节电源
- NERVIA 网络
- 光纤
- CLARISSE SSDE

- **中国**
  CPR1000 项目
- **法国**
  VD3-1300MW 项目
- **芬兰**
  Loviisa 改造项目

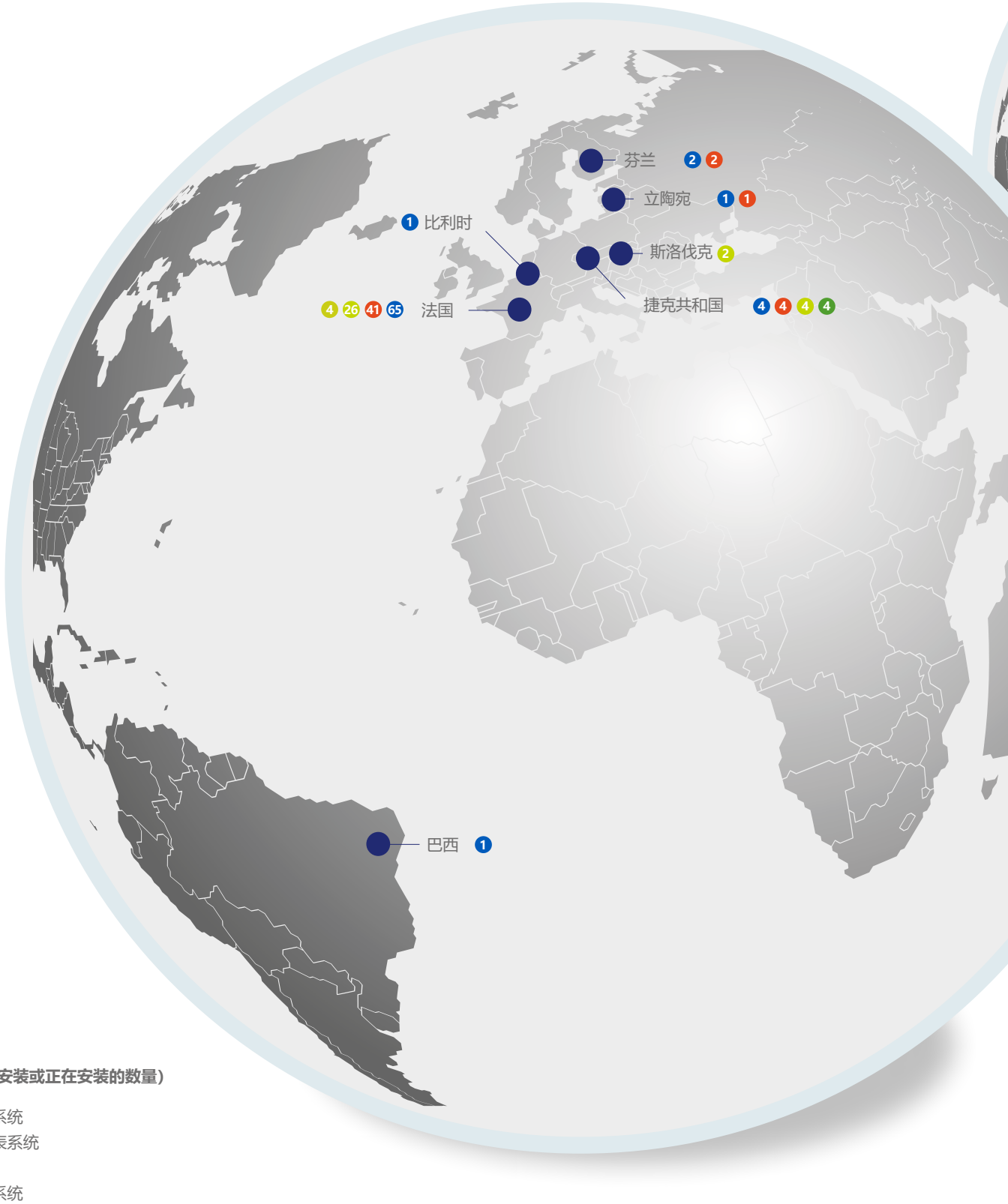


2010

经验与业绩

Spinline基于全球多项改造项目及新建项目、超过50年和1840堆年的经验

Spinline技术拥有50年的历史，已被成功安装在全球超过90 座核反应堆，这使得法马通公司成为全球该领域经验最为丰富的公司。



系统业绩
（按各个国家已安装或正在安装的数量）

- 反应堆保护系统
- 中子测量仪表系统
- 反应性仪
- 柴油机加载系统

法国

PWR 反应堆 - 58 座

自 20 世纪 70 年代起，法马通公司就一直是EDF（法国电力公司）的原始供应商，为其在法国的 58座反应堆提供安全仪表与控制 (I&C) 系统。1984 年，法马通公司在 Paluel 机组上开发并安装了第一个数字化集成保护系统。作为专注于核安全仪表与控制 (I&C) 的最新一代数字平台，Spinline正是从这一独特经验中发展而来。

2011 年底，EDF 再次对法马通公司委以重任，选择Spinline作为用于法国 1300MW 核反应堆（20 座）安全仪表与控制 (I&C) 系统现代化改造的技术。在这个为期 14 年的项目中，法马通为反应堆保护系统和中子测量仪表系统提供 Spinline技术。

芬兰

VVER 4400 - 2 座

2014年，法马通公司与Fortum公司签署了Loviisa核电厂仪控系统现代化改造协议，主要涉及核安全和安全相关系统。

法马通交付的新安全级别系统（包括反应堆停堆）基于Spinline数字安全平台。

该项目名为“ELSA”，于2016-2018年分三个阶段成功实施。

中国

PWR 反应堆 - 35 座

自 20 世纪 80 年代以来，法马通公司一直向中国提供安全关键核仪表和堆芯控制仪表与控制（I&C）系统，涉及中国 85% 以上的在运或在建的核反应堆，包括所有中国自主设计的核反应堆。

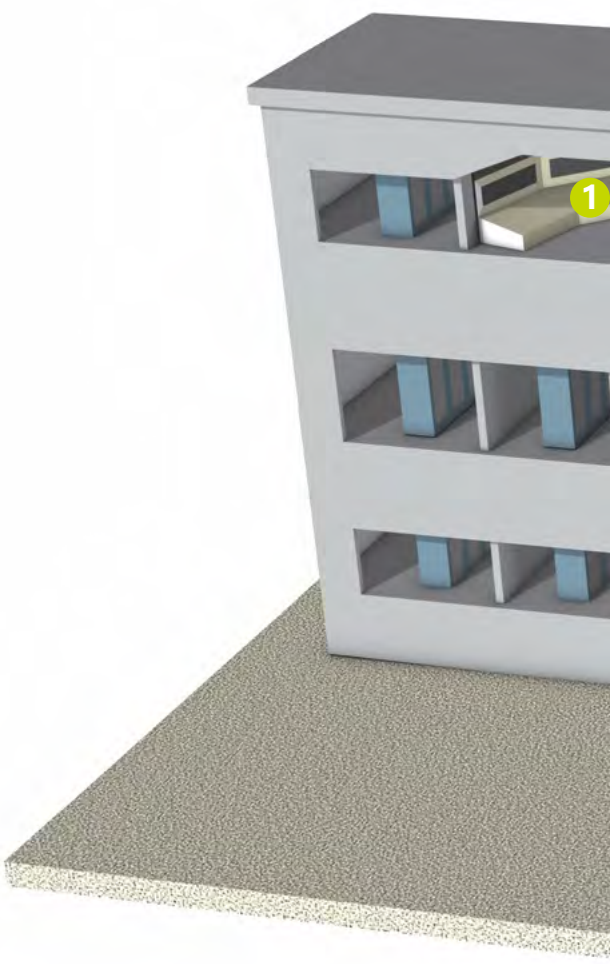
Spinline技术已被中国公共事业部门选择用于CPR1000核反应堆群（22 座反应堆）的中子测量仪表系统。

主要应用

Spinline可用于任何核安全仪表与控制(I&C)系统

Spinline的设计灵活且安全，能满足当今核电厂所需仪表与控制(I&C) 架构最苛刻的功能和安全要求。这使得Spinline非常适用于新建核电厂所采用的系统，诸如反应堆保护系统（RPS）、工程安全特性驱动系统（ESFAS）、应急柴油发电机（UDG/EDG）仪控系统、柴油机加载系统或中子测量仪表系统（NIS），也同样适用于在运核电厂的现有安全仪表与控制 (I&C) 系统的现代化改造。

以下是使用法马通 Spinline技术的一些应用示例。



反应堆保护系统

用于监控反应堆的关键运行参数，在紧急情况下自动停堆，并决定需要执行的纠正措施。

纠正异常情况时，Spinline RPS 会激活所有相关电路，包括：
- 紧急停止反应堆堆芯（通过将控制棒插入反应堆堆芯来中断核裂变反应）
- 安全注入
- 启动辅助给水
- 蒸汽管线和给水管线隔离
- 安全壳喷淋和隔离

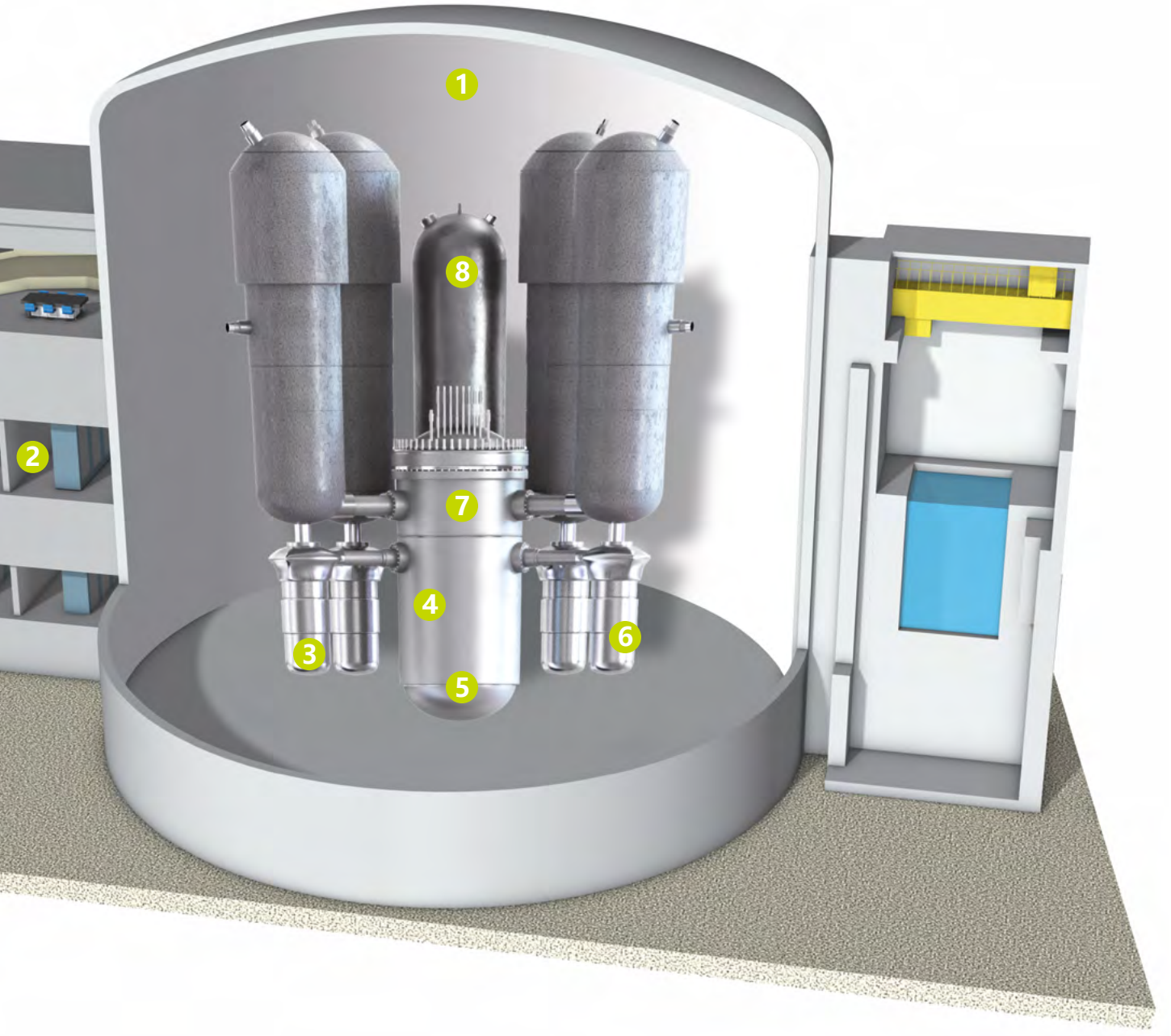
中子测量仪表系统

法马通数字化中子测量仪表系统 (NIS)通过堆外中子探测器测量所得的中子通量实现永久监测：
- 瞬时核能
- 功率波动
- 反应堆径向和轴向功率分布情况

法马通 NIS 由堆外中子探测器（源量程、中间量程和功率量程探测器）、控制和保护处理单元、符合人体工程学的本地或远程人机界面和执行器组成。

柴油机加载系统

柴油机加载系统在厂外电源丧失和后续恢复时提供启动柴油发电机组的逻辑，并根据预先设定的时间顺序加载保护措施。它与反应堆保护系统一起运行。
法马通柴油机加载系统通过了 1E/A类认证，符合国际核标准。
当收到丧失电压的信息时，法马通柴油机加载系统将启动以下顺序：
- 发出命令启动柴油发动机
- 当柴油机准备就绪时，系统自动从主电源切换到柴油发动机
- 切断电源负载
- 重新以预先设定的顺序载入电源负载



1 反应堆保护系统
专设安全设施驱动系统
柴油机加载系统
反应堆停堆断路器

2 核电厂过程控制计算机

3 温度传感器
压力变送器

4 中子测量仪表系统
堆外中子探测器
反应性仪

5 堆内中子探测器

9 硼表

7 棒控系统
棒位指示系统
棒位传感器

8 安全阀控制系统
稳压器热控制单元

系统开发

根据整个系统的生命周期，法马通开发了以Spinline为基础的应用系统

法马通根据符合质量保证手册要求的高质量流程开发了基于 Spinline 的核应用系统。

这些流程符合国际规范和标准，特别是：

- 用于管理安全要求（质量保证）的国际原子能机构 (IAEA) GS-R-3准则（原 50-C-QA）和 NQSA NSQ -100
- 美国核能管理委员会发布的《美国联邦法规》第 10 篇第 50 部分（缺陷和不合规报告）
- 国际标准：IEC 61513（关于系统开发）、IEC 60880、IEC 60780、IEC 60980

管理系统开发的一般原则如下（见下图）：

- 依据系统开发生命周期、嵌入式软件开发和设备开发生命周期开发每一个系统
- 通过项目管理流程对生命周期活动进行指导和规划
- 考虑每个开发级别的安全要求，实施适当的具体措施
- 定期检查开发阶段 (GRSX) 以便掌控流程进度
- 系统开发周期和技术开发的各个级别均包含 V&V 和质量鉴定活动
- 在整个开发过程中进行严格的配置和变更管理
- 监管要求和合同标准框架是系统开发的基础

安全系统设计和V&V生命周期

系统要求规范	系统规范	系统详细设计与实施	系统集成与验证	系统安装和调试
• 系统要求规范	• 系统架构规范	• 系统详细设计		
	• 初步安全分析	• 安全分析		
	• 鉴定策略		• 环境鉴定分析和测试	
	• 系统验证规范	• 系统验证开发	• 系统验证	
		• 现场测试规范	• 现场测试开发	• 现场测试和调试
	• 系统安装策略	• 现场安装规范	• 现场安装设计	• 现场安装

设备设计与鉴定

软件开发和 V&V


LSA2
LSA1
P1
P2
P3
CG
CG
CG
VPP
Alim 48V/5V-24V
5V
24V

先进的技术特征

Spinline的模块化功能简化了各种安全功能和架构的实现

Spinline 提供一套适用于开发更好的 A 类 1E 级仪表与控制 (I&C) 系统的组件：

- 软件组件，如系统软件、数据库、CLARISSE 系统和软件开发环境 (SSDE)
- 硬件组件，如机柜、机架和主板

这些部件均根据安全级系统的要求设计，以便轻松满足客户和监管机构的要求。

最先进的数字技术

Spinline 基于数字技术，因此，功能需求的实现变得更加容易，免除了对于特定硬件开发的需求。

Spinline 这一基于软件的解决方案的主要优点：

- 功能需求得以实现：采用 Spinline 硬件组件、CLARISSE 系统和软件开发环境，可以在不需要特定硬件开发的情况下开发任何类型的仪表与控制 (I&C) 功能。
- 模拟值稳定且精度高：数字化后，模拟输入信号和触发阈值不再受模拟偏移的影响，也无需进一步调整或校准。
- 适应性强：在不影响 I/O 接口的情况下，功能需求的变化可以在软件层面进行处理。当需要更改 I/O 时，系统参数将进行相应调整，必要时可添加 I/O 板。
- 系统监督：可以在不增加安全分类单元复杂性的情况下实现对安全仪表与控制 (I&C) 系统的监督，非安全分类监控站可免费使用安全网络上提供的数据。
- 自动定期测试：Spinline 提供合适的功能，可最大限度地实现每个功能的定期测试的自动化。

模块化和可扩展性

Spinline 硬件和软件组件具有模块化和可扩展性：

- Spinline 适用于各种规模的仪表与控制 (I&C) 系统，从简单的有I/O 板无冗余的单个单元到复杂的系统，例如具有 40 多个单元、冗余和功能多样性、表决、本地和远程测试单元的集成保护系统。
- Spinline 有两种交付方式：作为机架集成到现有机柜（改造），或作为完整机柜交付。机架和机柜的内容可进行调整，以满足系统要求。

分布式系统

Spinline 组件设计用于构建分布式系统，即几个处理单元协同工作以执行应用功能的系统。

Spinline 提供以下类型的处理单元和通信链路：

- 处理单元由带有 CPU 板、输入/输出板和网络通信接口的机架组成。处理单元可以是专用的：采集单元 (AU)、功能单元 (FU) 和无表决输出单元 (OU) 或有表决输出单元 (VU)。
- 通信链路：NERVIA 网络是安全系统内的标准通信链路，可实现单元间安全高效的数据交换。无论环境如何，它总是以确定的刷新率提供确定数量的数据。
- 其他链路：网关可用于以太网，如有需要，还可以在处理单元或标准 PC 上链接到其他网络。

可调节的系统架构

Spinline 单元和链路可将以下两个基本架构方案结合起来：

- 流方案：通过 NERVIA 网络链接的单元可以进行流线式工作。例如，第一个单元从传感器获取输入并将值传送到网络。第二个单元处理这些值，并将结果通过输出板直接发送给执行器，或通过网络发送给第三个单元（例如，表决单元）。
- 并行方案：通过 NERVIA 网络链接的单元可以并行工作。例如，第一个单元在网络上发布数据，然后该数据可以由两个或多个并行工作的单元处理。并行方案用于在多个单元之间进行拆分处理，以满足多样化要求，这也是需要冗余时的基本方案。

根据需要，将流方案和并行方案结合起来，构建实际的系统架构以提供足够的多样性和冗余，符合安全仪表与控制 (I&C) 要求。

冗余系统

Spinline 组件和分布式功能可以方便地构建冗余系统。

Spinline 提供两种类型的冗余管理：

- 基于硬件的主动冗余管理：由一个或多个单元组成几个单独的通道（通常为 3 或 4 个）。来自每个通道的输出指令通过输出板发送至硬件表决逻辑。
- 基于软件的主动冗余管理：主要通过从多个通道或分区接收数据的单元（输出单元或功能处理单元）实现。

确定性行为

Spinline 确定性行为可满足响应时间要求，避免过载情况。

- 各单元之间经网络交换的数据已经过预先定义并具有系统性（所有单元间的数据交换均在固定表格中进行配置）。
- 由于单元和网络之间的异步性，系统响应时间并非固定不变，而是由最大值限制。使用每个单元和网络的最大响应时间来评估系统的最大响应时间。

Spinline 的确定性可确保仪表与控制 (I&C) 输出始终在计算出的最大响应时间限制内发送。

地理和电气隔离

- 核电厂使用光纤进行 NERVIA 网络上的单元间通信，以实现地理和电气隔离。
- 单元和网络之间的异步接口：NERVIA 网络上的单元间交换在硬件级别和协议级别均不同步。此特点避免了由于单个单元或网络故障导致多个单元挂起的风险。由于网络运行不受所连接网络的状态影响，因此更容易对冗余单元进行管理。
- “1E 单元/非 1E 单元”隔离：由于 NERVIA 网络的安全特性，Spinline 可以将 1E 单元与非 1E 单元完全隔离，或在需要时，允许 1E 单元与非 1E 单元交换数据。Spinline 的特性确保非1E 单元不能阻止 1E 单元执行其安全功能。

根据数据的安全重要性，可采用不同的 NERVIA 网络实现通信隔离。

安全导向技术

Spinline 硬件和软件组件设计用于实施安全仪表与控制 (I&C) 系统。这些组件包括安全导向功能，以防止（即检测并采取动作）仪表与控制 (I&C) 系统由于内部或外部原因而导致系统内可能发生的故障。

系统安全导向功能：

- Spinline 处理的每个数据都有一个相关的有效字段，用于显示此数据的状态（“OK”或“Non OK”），软件和硬件组件根据该有效性信息处理数据，并相应地更新其状态。
- 每个单元监控其相关单元和网络，并在检测到无效数据时采取适当的措施。监控是根据每个被监控单元的预期时间跨度，通过检查具体变量的演化而完成。

硬件安全导向功能：

- 内部硬件故障、电源丢失或检测到 CPU 扫描中断（看门狗）时，输出卡会输出默认安全值。
- 对 CPU 时钟进行监控，防止可能的频率漂移。

软件安全导向功能：

- 系统软件包括适当的防御性编程，以确保控制和数据流中不存在不一致现象。检测到的任何不一致均会引发 CPU 停止，进而触发输出的预定义状态。
- 应用软件可以包括一致性检查和属性断言，以防止可能的设计或运行故障。

硬件 - 机柜和机架

法马通机柜和机架根据核要求和标准进行设计、制造和鉴定

Spinline 硬件由机柜、机架、电路板和电缆组成，适用于新建核电厂或升级改造项目中的核仪表与控制 (I&C) 系统和设备。

硬件根据核要求和标准设计、制造和验证。

标准机柜

机柜符合 IEC 60529 标准，保护指数为 IP32 和 IK07，符合IEC60980 规定的抗地震应力能力。其配有电源、机架、冷却风扇、输入输出电缆接口、内部接线和显示设备，并设计为能够承受规定的温度并符合 EMI 标准。

机柜特点：

- 机械标准：19″（38U 可用）
- 设计配有 19″ 机架
- 每个机柜最多 5 个机架

机柜可根据规格进行调整：

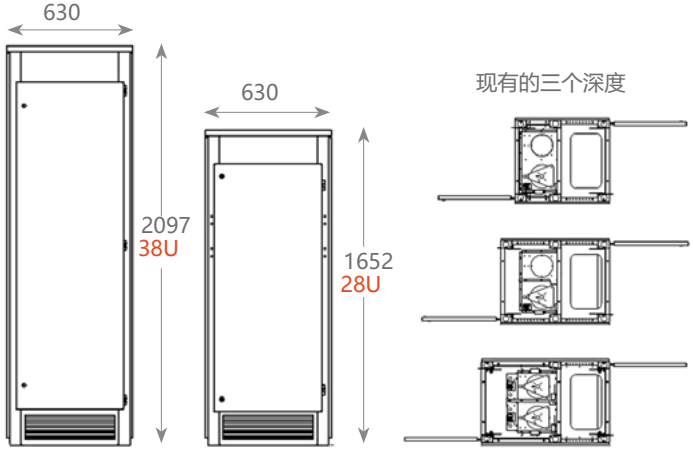
- 顶部或底部接线
- 移动接线盒，避免在现代化改造的情况下修改接线
- 伸缩提升环

机柜包括：

- 由铆接部件制成的框架
- 侧板和前后门
- 前门配有锁，可以为素面或上釉
- 最多可安装 5 个机架的滑轨
- 接线区可从后面板接入
- 带通风槽的顶板
- 带分隔式顶板的强制通风罩

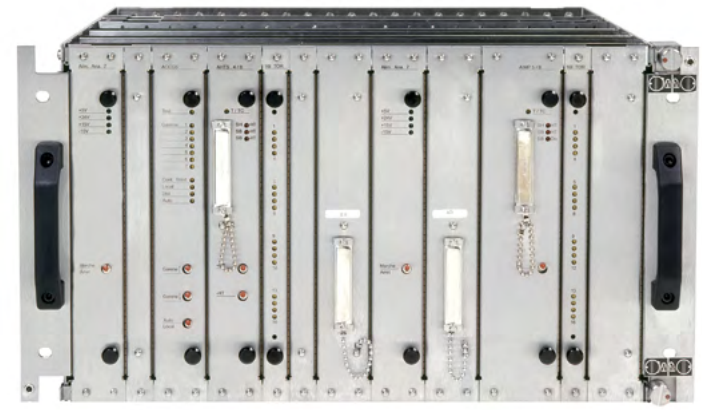
通风罩配有上限温度传感器

（60℃±3℃；140°F±5.4°F）和下限旋转风扇转速传感器。



Spinline 机柜的典型尺寸 （mm）

可以设计定制机柜以满足特定的客户要求。



标准机架

- 19″ 6U 机架的设计可承受现行适用标准中定义的温度、EMI、振动和地震。

包括：

- 含铆接和栓接件、EMI 防护装置的框架
- 一个或两个印刷电路底板，其中电路板连接器装有与电路板类型相匹配的按键
- 外形尺寸：482 × 265.5 × 504 mm（宽×高×深）

接线

机柜和机架的设计便于标准的连接和客户预定义的电缆与接线板的连接。

保密和安全

Spinline机柜的特点：

- 开门检测和报警机制
- 监测风扇系统的健康状况
- 监测电力系统的健康状况

硬件 - 电路板

为安全而设计的电路板

法马通设计和制造的系统使用：

- 数字处理板（Spinline）
- 信号采集板
- 信号调节板
- 专用电路板

整个系列包括用于电源、输出继电器等的附加板。所有这些电路板的设计都符合法马通公司为核安全仪表与控制（I&C）的需要而开发的标准机架和机柜。
Spinline电路板通过底板上经过验证的专用并行通信总线进行通信。
该总线由法马通专为核应用而设计，是标准化VME总线的简化和安全版本。
省略了多总线和总线仲裁功能，以获得简单性和确定性。

检测到故障时的安全行为
输出板可以在检测到故障状况时将其输出设置为预定义的安全值。若 CPU 未能在预定义时间段内下发新数值，看门狗定时器会自动切换输出。

支持定期测试
Spinline 提供板载手段，可切换到有定期试验装置产生/接受的信号，从而提升将定期测试纳入自动化范围的便利性。

故障模式和影响分析（FMEA）以及可靠性分析
由于 Spinline 组件的设计符合核安全要求，因此，所有电路板都已经过 FMEA 和可靠性分析。

操作简单安全
电路板安装在机柜内的机架中，机架与机柜背面的接线相连。
电路板的插入和移除不会对后部连接造成干扰，并且可以在系统继续运行时进行更换。此外，电路板支持系统运行时的热拔插，且不同电路板槽之间有防误插功能。

电路板的主要类型

处理器和通信板

- CPU 板 UC25，6个 NERVIA 端口，2个 LSA
- NERVIA 网关板（NERVIA GW），允许从 NERVIA 网络到以太网之间进行单向传输（Modbus TCP或UDP，其它按需协议）
- 专用于 NERVIA 的10 Mbits Hub 板，具有 8 个以太网端口，6对双绞线和2根光纤
- PCI NERVIA 板，安装在装有 PCI 的计算机上，与 4 个以太网NERVIA 点和一条 PCI 总线相连接

电源板

- 24V 电源板“I.ALIM 24V”：该板产生稳压直流电压

标准化输入/输出板

- 32通道数字信号采集
- 16通道模拟信号采集
- 32通道数字信号输出
- 继电器和制动器控制的32通道数字信号输出
- 12通道模拟信号输出

中子通量采集板和模块

- 探测器采集：源量程（脉冲）、中间量程（带伽马校正的电流）、功率量程（只有一个板用于具有2或6个垂直截面的功率探测器）、AHT1/B、AHTS4/B
- 宽量程调节模块，用于宽量程或事故后（US NRC RG 1.97）通道

专用电路板

- 计数率采集
- 温度采集（热电偶和PT100）
- 自给能中子探测器信号采集
- 特定的输入/输出卡件

便于操作和维护的硬件工具

Spinline的设计旨在尽量减少核电厂员工的运行和维护工作量。

这是一套由标准工业 PC 操作并提供用户友好型人机界面的专用工具，可帮助操作员进行系统监控和维护。

LDU：本地显示装置

用户可通过本装置，根据规定范围和安全协议检查和设置处理参数，参数和数值可分别进行检查和设置，或者加载为用于对新单元进行有效配置的组。

LDU 是一款配有专用软件的笔记本电脑，并装载有Spinline 系统数据。

MMU：监控和维护装置

监控和维护装置 (MMU) 持续检查 Spinline 系统中组件和数据的正确性。一旦系统中发生需要关注的事件，它会立即发出信号。

一些典型事件包括：

- 传感器、电路板或电源硬件故障
- Spinline 机柜门打开
- 不同冗余通道之间的信号或参数值不一致

它有助于轻松确定故障原因，并开始纠正维护，它通过打印和归档功能维护事件日志文件。

MMU 是运行 Windows Server 2019的机架式工业计算机，配备 15 英寸 LCD显示屏、键盘、CD-ROM、NERVIA 网络端口和以及用于发送远程报警信号的数字输出单元。

ATU：自动测试单元

维护团队均可以借助该单元在安全系统上进行所需的全部测试，无论是在全功率运行期间进行在线测试还是在停堆期间进行离线测试。

它包括最先进的功能：

- 定义测试集
- 在测试阶段以图形方式显示数据
- 分析和归档测试结果

ATU 可作为安装在安全系统机柜中的机架式单元，或是由多个系统共享的移动单元。ATU 包括一台运行 Windows 的工业计算机，配备LCD 显示屏、键盘和打印机。

软件

Spinline软件设计符合核工业的安全要求

Spinline 软件由两个主要组件组成：

- 操作系统软件为标准软件，以处理单元 CPU 板使用的软件组件形式提供。它提供必要的基本功能，包括应用软件使用的通信、数据采集、数据发射和服务等功能。
- 应用软件为专用软件，专为项目而开发，用于实现符合用户需求的仪表与控制（I&C）应用功能。

CLARISSE 系统和软件开发环境是一个专门的软件工厂，提供用于配置 Spinline 处理单元和 Nervia 网路所需的软件工具和数据库，以及客户特定应用软件的开发。

操作系统软件

操作系统软件是一个复杂度最低的软件层级，用于实现 I/O 和通信链路板以及应用软件发送的本地和远程数据之间的连接。

它还执行持续的硬件测试，并向应用软件提供服务。

系统软件根据软件相关 1E级安全系统的核标准，特别是 IEC60880 进行开发和验证。

可以通过 CLARISSE 系统和软件开发环境的配置工具对操作系统软件进行调整，以符合应用需求。

这些工具允许设计者对 NERVIA 网络和处理单元 I/O 板的数据进行配置。

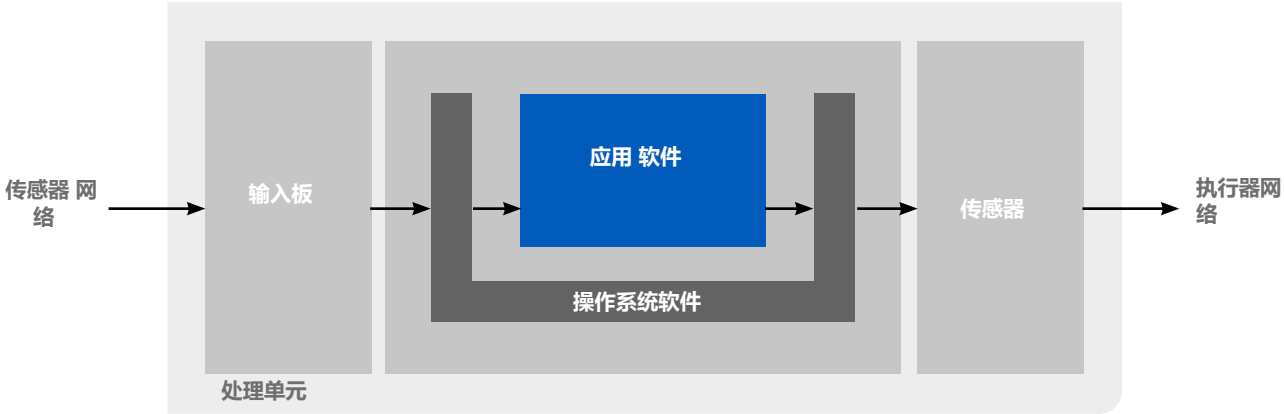
应用软件

应用软件执行应用功能，Spinline 应用软件专用于安全仪表与控制 (I&C) 系统的监控、控制和保护功能。

主要特征：

- 顶层设计：从顶层视角开始进行应用程序设计，并通过功能和数据的细化步骤层层推进，相关细节被添加到适当的级别（信息隐藏概念）。
- 数据流组织：程序作为一组通过电线连接的功能块输入，从左侧的输入数据流向右侧的输出指令。电线根据数据类型传送数据，功能块通过布尔运算符、数字运算符或函数转换数据。
- 单一任务：与系统软件关联的应用程序作为单个连续程序循环运行，一次循环即为一次扫描。每次扫描时，根据固定输入图像和先前扫描的相关结果计算输出。中断时无法进行处理，也不能进行多任务处理，这样可以避免潜在死锁、资源共享和过载问题，它有助于展示响应时间要求的执行情况并简化软件设计。
- 同步法：应用程序的设计满足同步假设，即程序在预定义和受控的时间框架内对输入事件做出反应。

Spinline的CPU板提供足够的性能，以满足核领域典型仪控保护功能的处理需求。此外，CPU的负载与输入的实际值无关。



处理单元：硬件/软件架构

系统软件开发环境 (SSDE)

SSDE 用于自动配置系统软件、网络架构、网络站和单元之间的信息交换。

- **仪表与控制 (I&C) 功能的输入**：采用基于图形设计的工具SCADE（安全关键应用程序开发环境）对仪表与控制 (I&C) 功能进行描述，其语言是一种基于严格的文本、图形语法、以及明确定义语义的框图形式。SCADE 易于使用，无需专门的编程技巧。
- **SCADE 规范仿真**：能够从应用程序设计的早期阶段进行仿真。
- 通过它，设计师可以检查其规范的实际行为。
- 在测试和验证阶段，它也可以用于检查最终规范的其他功能。
- **自动代码生成**
- **验证和确认**：使用适当的工具检查每个软件设计步骤。
- **文件制作**：大部分文件为自动生成。
- **软件配置管理**

软件开发方法基于 IEC 60880 标准

开发方法符合标准的软件开发周期，并在每个阶段结束时得到具体的文件和审查结果。成立单独的验证和确认小组来实现以下目标：

- 检查规格、设计和编码
- 执行形式化的关键部件测试
- 验证软件

该方法旨在尽早发现错误，并在不超出计划成本和进度表的情况下达到所需的质量水平。软件验证期间观察到的残差数极低。

软件工程工具

在整个系统和软件开发周期中，Spinline 使用一套工具来确保软件质量。

- **软件开发工具**：保证整体应用的一致性。
- **代码检查工具**：测量软件内在复杂性、评论率等质量指标。
- **单元测试工具**：使用“白箱”和“黑箱”方法尽可能早地根据规范检查编码。
- **目标机架上的软件集成和验证工具**：允许开发人员在最终环境中测试整个软件应用（已经完成所有单个元件的测试）。
- **闪存组件生产工具**：确保以前测试的软件与在 REPROM 电子组件中的存储之间的一致性。

人机界面

为了确保最大的安全性，我们主要提供继电器和线对线组件来控制系统（抑制、手动控制、定期测试准备等），可以根据特定需求来实施数字化分类 HMI。

IEC 60880 软件安全生命周期的开发活动

NERVIA

用于 A 类 1E 级功能的通信网络

NERVIA 是一个独特的安全分类网络，为安全仪表与控制 (I&C)系统提供高效、安全和可靠的数据通信。

NERVIA能简化并保护布线

- 节省数百条点到点连接电线和数十个点对点通信链路
- 使用铝箔屏蔽双绞线和光纤
- 连接机柜内的机架、安全设备内的机柜、核电厂仪表与控制 (I&C)系统和控制室内的安全设备
- 由于物理链路大幅减少，可以降低接线安装和维护成本
- 采用连续自检型 NERVIA 链路代替了之前需要按照一定的周期间隔进行测试的链路，进而增强接线的可靠性

NERVIA 是A 类 1E 级兼容架构设计的关键组成部分：

- 使安全仪表与控制 (I&C) 系统设计更容易：
  - 冗余符合单一故障准则
  - 在不同的处理单元中实施功能多样性
  - 实现通道之间的地理和电气隔离
  - 在所有核电厂条件下执行确定性响应时间
  - 与非A 类 1E 级系统的通信能力
- 硬件符合A 类 1E 级核标准
- 协议和软件完全符合 IEC 60880 要求

NERVIA 是一个安全的网络

- 协议简单，专用于仪表与控制 (I&C) 系统
- 处理单元无法在其网络内存空间外进行写入
- 使用 CLARISSE SSDE 预定义数据通信布局，并将其刻录到相关处理单元的闪存中。在核电厂运行期间，这些布局无法更改
- NERVIA 可阻止病毒入侵和对安全数据的远程写入访问
- NERVIA 网络内的故障，无论是有意还是无意，都会立即被所有主动站点检测到，进而触发相应的安全措施

NERVIA 致力于高安全性“硬实时”仪表与控制 (I&C)

- 数据流驱动通信（非事件驱动）：每个站点会定期发送一组预定义的变量值。数据流驱动通信完全符合仪表与控制 (I&C) 系统的要求
- 静态数据块描述（非动态数据块）：应用数据被组织成连贯的数据块，通过逐扫描进行快速传输，或者通过多次扫描进行缓慢传输。无论核电厂条件如何，静态数据块都会提供稳定的网络流量
- 基于时间的方案的确定性：无论站点的状态是否 OK，每个站点在网络扫描时都有预先定义的指令，并已分配好用于网络访问的固定时间窗口。这种基于时间的静态数据块方案可提供确定的扫描时间
- 广播协议（非点对点协议）：一个站点发送的每条消息均被网络上的所有其他站点接收。这种广播协议有助于冗余架构设计，并触发恰当的降级机制
- 容错功能：
  - NERVIA 协议具有完全确定性，不受任何中断的影响
  - NERVIA 协议属完全分布式，不需要静态或动态主站点
  - NERVIA 站点和媒体不断进行自检
  - 在发生内部故障或网络异常时，NERVIA 站点会执行安全导向行为
  - NERVIA 站点电源开/关平稳，对网络扫描没有影响

NERVIA 允许访问非安全系统

- NERVIA 安全网络可通过 NERVIA 网关连接到非安全设备，如工业计算机
- 可以使用 Spinline NERVIA 网关板与其他设备（如 PLC 或监控系统）进行通信。此模块经过简单配置后，允许基于 MODBUS TCP/IP 协议将 NERVIA 网络上交换的信息传输到的其他网络

安全

用于 Spinline 的计算机安全方法

法马通的仪表与控制 (I&C) 系统严格遵循计算机和信息安全程序，该程序的制订基于通用及核相关规范、法马通集团程序和最先进技术。
Spinline专为核应用而设计，具有安全的开发和操作环境，可防止未经授权的修改，并执行设计要求，提高设计、运行和维护期间的完整性和可靠性。

法马通的开发环境受到一般安全原则的保护：
- 物理和环境安全：物理访问受到限制和监控
- 人力资源安全：对员工和承包商的参考编号进行检查，并签署NDA
- IT 系统访问控制：限制和监控网络、应用程序和 IT 系统的使用

Spinline 在开发、测试和安装过程中的特定程序：
- 采用软件生命周期流程，能防止和检测未经授权的修改：
  - 严格控制设计流程；可追溯的配置管理系统；独立的 V&V 和测试
- Spinline 软件不包含多余功能：
  - 专有操作系统软件 (OSS) 仅执行有限的功能；特定应用软件无法修改 OSS；通信网络为法马通专有的 “NERVIA” 网络；
- 在初始化和每个处理周期时检查 Spinline 代码的完整性：
  - 软件加载在闪存上；定期验证校验和值；
- Spinline 硬件具有故障检测功能，并具有经过验证的高可靠性记录

在运行、测试和维护过程中，还执行以下特定程序：
- 生产代码更改需要物理访问并从其机架中卸下主处理器板，而这会受到管理控制的限制，并且打开机柜门会引起警报
- 无法远程访问 Spinline 系统：
  - Nervia 协议不允许动态修改；若添加一台机器以修改数据或删除一个节点，会立即被检测到；与外部系统的单向通信需要通过硬件来实现；
- Spinline 系统的维护和测试仅允许本地访问：
  - 需要物理访问；允许动作已预先定义，且受到限制

法马通的仪表与控制 (I&C) 计算机和信息安全程序基于 ISO 27001、27002 以及诸如 IEC 62645、62859、 IAEA NSS-17 和 NRC RG 1.152 之类的核专用指南。

此外，我们还提供不间断培训课程，提高专家的专业知识和人数， 以便为我们的客户提供适当的具体方案。

标准

Spinline得到了主要国际安全机构的认证（法国、中国、芬兰、美国、捷克共和国等）。

一般安全要求

国际	IAEA GSR part 2	安全领导和管理（2016）
	IAEA SSG-30	核电厂结构、系统和部件的安全分类（2014）
	IAEA SSR-2/1	核电厂安全：设计
	IAEA SSG-2	核电厂确定性安全分析
	IAEA SSG-39	核电厂仪表与控制系统设计
	IEC 60671	核电厂 - 安全关键仪表与控制系统 - 监控测试
	IEC 60812	系统可靠性分析技术。故障模式和影响分析流程
	IEC 61226	核电厂 - 安全关键仪表与控制 (I&C) 系统 - 仪表与控制 (I&C) 功能的分类
	IEC 61227	核电厂 - 控制室 - 操作员控制
	IEC 61500	核电厂 - 安全关键仪表与控制 - 用于执行A类功能系统的数据通信
	IEC 61513	核电厂 - 安全关键仪表与控制系统 - 系统的一般要求
美国	10 CFR 50	核电厂一般设计标准（附录 A）
	NUREG 800, 第7章	用于审查核电厂安全分析报告的标准审查计划
	IEEE 338	核电站安全系统周期监督检测准则
	IEEE 603	核电站安全系统准则
欧洲	RCC-E	电气和仪控系统及设备的设计和施工规则
	RFS	核反应堆的基本安全规则
	CRT	技术规则文件（EDF）

具体硬件设计要求

国际	IEC 60960	核电厂安全参数显示系统的功能设计准则
	IEC/IEEE 60780-323	核电厂 - 安全系统的电气设备 - 质量鉴定
	IEC/IEEE 60980-344	核设施 - 安全关键设备 - 抗震鉴定
	IEC 60709	核电厂 - 安全关键仪表与控制系统 - 分离
	IEC 60068-2	环境测试
	IEC 60987	基于计算机的系统的硬件设计要求
	IEC 62808	核电厂 - 安全关键仪表与控制系统 - 隔离装置的设计与鉴定
	IEC 62566	用于执行 A 类功能系统的 HDL 编程集成电路的开发
	IEC 62566-2	核电厂 - 安全关键仪表与控制 - HDL编程集成电路的开发 - 第2部分：执行B类或C类功能系统用HDL编程的集成电路
	IEC 61000- 系列 4	电磁兼容性
美国	IEEE 308	核电站 1E 级电力系统的标准规范
	IEEE 379	将单一故障准则应用于核电站安全系统的标准规范
欧洲	EN 50081-2	电磁兼容性 - 通用发射标准
	EN 50082-2	电磁兼容性 - 通用抗扰度标准
	EN 55011	工业、科学和医疗 (ISM) 射频设备 - 射频干扰特性 - 限值和测量方法

具体软件设计要求

国际	IEC 60880	核电厂 - 安全关键仪表与控制系统 - 执行A类功能的基于计算机的系统的软件方面
	IEC 62138	核电厂 - 安全关键仪表与控制系统 - 执行B类或C类功能的基于计算机的系统的软件方面
美国	IEEE 7-4.3.2	核电站安全系统数字计算机的标准规范
	NRC 1.152	核电厂安全系统计算机使用标准
	NRC 1.168	核电厂安全系统数字化计算机软件的验证、审核和监查
	NRC 1.169	核电厂安全系统中使用的数字计算机软件的配置管理计划
	NRC 1.170	核电厂安全系统数字计算机软件测试文件
	NRC 1.171	核电厂安全系统数字计算机软件单元测试
	NRC 1.172	核电厂安全系统数字计算机软件要求说明
	NRC 1.173	开发用于核电厂安全系统中数字计算机软件的软件生命周期流程
欧洲	RFS	用于安全系统的软件

硬件质量鉴定

Spinline设备按照国际标准进行质量鉴定

Spinline设备按照国际标准进行测试和验证。以下示例符合 IEC 标准。如有任何有关公司设备是否符合任何其他标准的问题，请联系法马通公司。

典型环境测试

测试内容	测试条件
温度和电压组合试验	最低温度 5°C (41°F)
变化试验	板最高温度 55°C (131°F)
机柜最高温度	40°C (104°F)
湿度	93% RH at 40°C (104°F)

稳定性测试

进行稳定性测试以评估硬件在一段时间内的性能。测试按以下顺序执行：

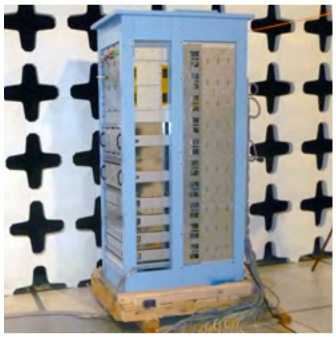
测试内容	测试标准	测试条件
连接和断开连接	CRT 80.C.012.01	连接器 50次
振动	IEC 60068-2-6 test Fc 1 g	10 至500 Hz 10个循环
快速温度变化	IEC 60068-2-14 test Na	-25°C +70°C (-13°F +158°F) 5个循环
干热	IEC 60068-2-2 test Bb	16小时 70°C (158°F)
湿热	IEC 60068-2-30 test Db	2 个 24 小时循环 最高温度：55°C (131°F)
冷却	IEC 60068 2-1 test Ab	-25°C (-13°F) 16小时

抗震性能鉴定

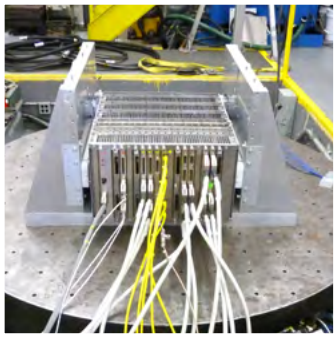
根据双轴法进行抗震试验，采用特大地震的加速度水平和反应谱，以涵盖现场位置的所需反应谱。

测试内容	测试标准
抗震测试	IEC 60980
抗震性能鉴定的推荐规程	IEC 68-2-6
抗震测试法和时程分析法	IEC 68-3-3 or IEC 68-2-57

该分析用于验证配置，对以往在类似硬件配置上执行的测试结果进行检查。这些质量鉴定符合 IEEE 323 和 IEEE 344 标准。



质量鉴定 - EMC 测试



质量鉴定 - 抗震测试

电磁兼容性

Spinline的设计可以抵抗高强度的干扰，这对现有核电厂和研究堆的现代化改造特别重要。

Spinline 无论是抗干扰还是发射方面均符合 IEC 61000 标准规定的测试和级别要求。

抗扰度

通用抗扰度标准 IEC 61000-6-2 适用，该标准包括：

测试标准	领域	级别	规范
IEC 61000-4-2	静电放电抗扰度试验	3	A
IEC 61000-4-3	电磁场抗扰度试验	3	A
IEC 61000-4-4	快速瞬变抗扰度试验	3	A
IEC 61000-4-5	浪涌抗扰度试验	2	A
IEC 61000-4-6	射频场感应的传导骚扰抗扰度试验	3	A
IEC 61000-4-8	工频磁场抗扰度试验	3	A
IEC 61000-4-12	环形波抗扰度试验	2	A
IEC 61000-4-18	阻尼振荡波抗扰度试验	2	A

2 级：实施额外的外部保护，达到 3 级或以上。

发射

通用抗扰度标准：EN 50081-2 适用，该标准包括：

测试标准	领域	级别
EN 55011/EN 55022/ CISPR 11	频率范围为 30-1000Mhz 的辐射干扰	A
EN 55011/EN 55022/ CISPR 11	频率范围为 0.15-30 Mhz 的传导干扰	A

软件质量鉴定

Spinline软件严格遵守IEC 60880要求和建议

我们的软件按照国际标准进行测试和验证。以下示例符合 IEC 标准。如有任何有关公司软件是否符合任何其他标准的问题，请与我们联系。

IEC 60880 是一套要求和建议，适用于核电厂安全系统中用于 A 类1 级安全功能的计算机所需的高可靠性软件。

IEC 60880 第 1 部分提出了安全性、简单性和可维护性的要求和指导原则：

- 安全性
  - 旨在生产“零错误软件”的开发过程
  - 安全导向功能
  - 防御性编程
  - 确定性行为
  - 硬件和软件监管
- 简单性
  - 避免不必要的特征和功能
  - 避免使用中断
  - 避免复杂的操作系统
- 可维护性
  - 优先采用以应用为导向的语言
  - 使用软件工具
  - 使用可以理解的形式

IEC 60880 第 2 部分给出了其他要求：

- 防止共模故障
- 软件工具
- 预先存在的软件的质量鉴定

IEC 60880 强制性要求采用“必须”进行表示，而推荐做法采用“应该”表示。

Spinline 设计不仅符合所有适用的“必须”要求，还满足所有适用的“应该”建议，从而实现所有基于 Spinline 软件的组件的安全性、简单性和可维护性。

由于 Spinline 严格遵守 IEC 60880 的要求和建议，因此，我们可以为客户提供以下独一无二的安全功能：

- 所有软件组件全部可以更新
- 在系统应用层面的嵌入式软件保持尽可能的简单化
- 安全网络和单元的确定性行为
- 能够通过标准化设备满足专门的安全应用功能需求

系统功能验证

在交付给客户之前，机柜和相关联的所有系统都会进行独立测试。

在系统开发的各个阶段，都需要执行质量鉴定活动，包括验证活动。在这些活动中，系统功能验证是需要法马通和客户共同参与的最重要步骤之一。

Spinline 硬件和软件经过单独测试和验证后，按照国际标准对整个集成系统进行测试和验证。如 IEC 61513 所述，目标是证明其符合：

- 功能规格
- 性能要求
- 界面规格

在此过程中，待交付机柜将被逐步集中于法马通公司，并在互连平台上进行测试。

涉及多个系统的功能验证，将分为两个阶段执行：首先是单系统测试（第一个测试阶段），然后是集成系统测试（第二个测试阶段）。

对于 1 级系统或 A &B 类功能，所谓的互连测试由不参与设计和开发的系统V&V团队进行。

单系统功能验证

第一个测试阶段（每个系统单独进行测试）的主要目标是：

- 系统功能图中定义了所有系统功能测试，这些测试以一种具有完全代表性的方式涵盖所有信号范围和计算得出的参数范围
- 系统响应时间测量（采集 - 处理 - 表决 - 系统输出激活）
- 系统精度测量（采集 - 处理 - 系统输出激活）
- 嵌入式显示和监控功能的测试
- 定期测试程序的执行情况测试
- 维护程序的执行情况测试
- 降级模式下或故障时的系统行为测试
- 耐久性测试

多系统功能验证

第二个测试阶段（集成系统测试）的主要目标是：

- 每个系统之间电气和软件界面兼容性的测试，包括：
  - 所有输入/输出系统界面（数字、模拟和网络）硬件分配
  - 系统之间共享的所有数字和模拟信号的电气范围
  - 网络协议的软件兼容性
- 涉及多个系统的功能测试
- 整体响应时间测量（采集 - 处理 - 表决 - 执行器界面激活和/或显示/报警激活）
- 整体精度测量（采集 - 处理 - 执行器界面激活和/或显示/报警激活）
- 功能规范（包括故障情况下的行为）

经验证的测试手段

为了在交付的系统中实现所有这些测试，法马通已开发出经过验证的可配置的合格测试手段，允许创建复杂的测试脚本。

我们的测试平台可通过静态和动态模拟正常运行、预期运行事件和事故条件下的输入信号来测试系统。

每次执行测试脚本都会生成自动日志，包含最终结果和定位故障所需的日志信息。

法马通已开发出经过验证和鉴定的测试方法和工具，能创建可测试最复杂配置的脚本


MSA
MSA

长期服务

Spinline技术在仪控系统的整个生命周期中得到支持

Spinline为您的仪表与控制 (I&C) 系统的未来扩展和功能改进提供了长期和低成本维护的理想条件。

法马通了解公用事业部门所面临的监管要求和商业压力。

公用事业部门需要最大限度地提高生产效率，使核电厂能安全可靠地运行更长时间，以尽量减少停机时间，并及时提供可靠支持。

法马通长期致力于保持其在板卡、机架和系统层面的制造、修改、维修和测试能力，这意味着要寻找硬件老化、技术发展、技能培训和工具维护的解决方案。

法马通对核仪表与控制 (I&C) 的长期支持服务包括：
- 报废管理
- 现场维护和维修
- 备件管理和供应
- 用户培训
- 升级管理
- 修改和改造

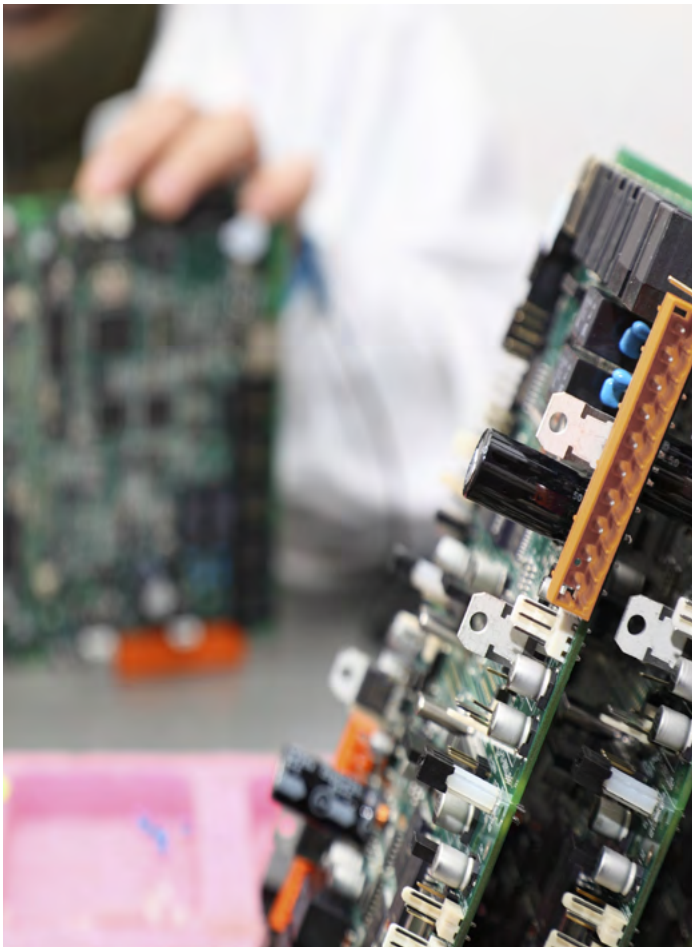
法马通确保为 Spinline 技术提供所有这些服务。

示例: 电路板的长期维护

在调试使用长达 30 年后，法马通将继续提供相同的板卡来更换在运和测试板卡，这意味着测试设备以及测试机器操作员的知识和技能也会在相同的时期内得到维护。

自法马通涉足核工业以来，我们在世界各地提供的板卡数量已逾 200 万块。我们不断从客户和现场工程师处获得反馈，以便持续不断地更新我们的技术。通过统计分析相关的反馈意见，使得我们能够提供最佳数量的板卡，以备进行现场更换。

最后，公司保证在必要时提供技术熟练的工程师予以协助。



维护核电厂的成本效益

法马通是全球核能市场的领导者，因其为全球核反应堆持续提供创新、数字化和增值解决方案而获得广泛认可。凭借在全球范围内的专业知识以及久经考验的可靠性和性能记录，法马通为核电站提供设计、维护、组件安装、燃料以及仪控系统等服务。
每天，法马通在全球各地的16,000多名员工，都在不断致力于帮助客户提供更加清洁、更加安全和更加经济的低碳能源。

访问网址：www.framatome.com, 请关注我们
推特：@Framatome_ 领英：Framatome.

法马通由法国电力集团（EDF-75.5%），三菱重工（MHI-19.5%）和Assystem（5%）持有。

扫描二维码，获取更多解决方案

framatome

Framatome
Tour AREVA. 1 Place Jean Millier
92400 Courbevoie, France

ic@framatome.com
www.framatome.com