



工作原理

50多年来，法马通一直在为世界各地的各类反应堆提供数字化和非编程安全仪控（I&C）系统。

Hardline平台是我们最新一代的非编程（硬接线）安全平台，专门设计用于实现A类、B类或C类（IEC 61226）和1E级核安全或安全相关的仪控（I&C）功能。

Hardline基于现代组件、架构和核安全设计流程，是法马通非编程技术发展的成果。

所有安全功能均基于硬接线技术，无需处理器或FPGA等可编程组件，因此不受软件共因故障（CCF）和网络安全威胁的影响。

Spinline技术是我们为A类&1E级应用提供的数字（编程）安全平台之一。



Multibloc	调制调解器 / BUX 模拟模块	动态逻辑 (ULS) 故障安全动态信号 (变压器)	Silimog 模拟
放大器操作，分立元件 法国 <ul style="list-style-type: none">EDF 900MW机组 (34台)EDF 1300MW机组 (20台)EDF 1450MW机组 (4台)CEA研究反应堆 国际 <ul style="list-style-type: none">中国 (4台)韩国 (2台)南非 (2台)	法国 <ul style="list-style-type: none">EDF 1300MW机组 (20台) 国际 <ul style="list-style-type: none">中国 (37台) 	法国 <ul style="list-style-type: none">EDF 1300MW机组 (20台) 	法国 <ul style="list-style-type: none">EDF 900MW机组 (34台)CEA研究反应堆 

Hardline的设计考虑到了灵活性和安全性，满足了现代核电站（NPP）中使用的非编程安全仪控系统严格的功能和安全要求。

这使得Hardline非常适用于新建核电站或翻新现有核电站中的安全仪控系统，它适用于多种安全仪控应用，包括：

- 多样化反应堆保护系统（DRPS）
- 执行器优先逻辑系统（PLS）
- 备用或事故后系统（PAMS/SAMS）
- 主反应堆保护系统（RPS）
- 柴油发电机的多样化仪控

Hardline可以轻松适应多种核电厂设计，包括PWR、VVER、BWR反应堆、研究反应堆和小型模块化反应堆（SMR）。

先进、稳定和标准化的技术

主要应用

Hardline 技术可用于多种应用

多样化的反应堆保护系统

现代核电站中的大多数反应堆保护系统都基于编程微处理器，这些微处理器可能会受到软件“共因故障”的影响。多样性保护系统是在主保护系统发生故障的同时，且出现偏离正常操作时所需的仪控系统。这意味着它可以检测事件，启动自动缓解（跳闸和ESFAS）并通知操作员。它还允许操作员处理事故后管理所需的监控和手动操作。

法马通提出的多样性保护系统基于Hardline非编程技术，因此不受软件共因故障（CCF）的影响。

优先逻辑系统

由于需要大量的保护功能，核电站的执行设备可以由几个独立的仪控系统控制。为了管理从多个控制系统发送的潜在冲突指令，优先逻辑系统收集所有这些指令，并根据预先建立的优先顺序控制执行设备。法马通提出了基于Hardline技术的专用非编程优先逻辑系统。

柴油发电机仪控系统（EDG、BDG）

当核电站机组与电网断开时，启动应急柴油发电机，并在发生故障时使用备用柴油发电机。这些柴油发电机保障了反应堆冷却系统等重要元件的电力供应，从而确保反应堆的可控停堆。Hardline可用于指挥该柴油动力的安全仪控系统，并在需要时保证其正确运行。

事故后监控系统（PAMS）和严重事故管理系统（SAMS）

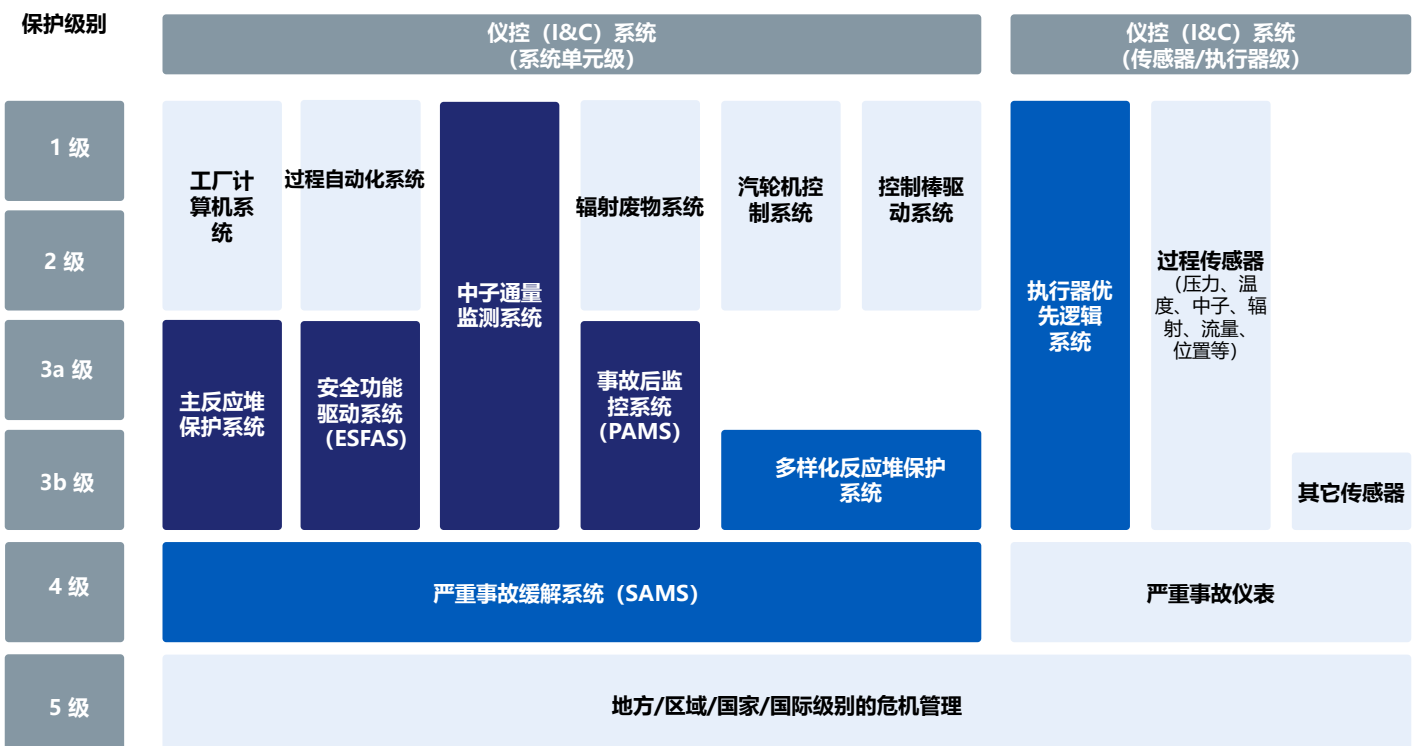
在事故发生期间和事故之后，仍必须根据情况的发展对反应堆的关键参数进行监控。可以采用专用的事故后监测系统（PAMS）来完成这项任务。

当事故恶化且主要（和多种）保护系统无法运行时，严重事故管理系统（SAMS）将触发额外的缓解措施，以终止堆芯损坏并保持安全壳完整。

这两个系统的要求因工厂设计、当地法规和现场特点而异，但Hardline的设计和性能保证其符合最严格的PAMS和SAMS要求。

主反应堆保护系统（改造和研究堆）

一些较旧的核电厂仍然使用其OEM模拟主RPS运行。为了延长其运营许可证，克服过时问题或满足新的安全要求，他们会对其安全系统进行整体或部分现代化改造，而使用Hardline技术能使他们受益于现代技术，而无需调整和对数字编程技术取证。类似地，更喜欢非程序化技术的新型或现代化研究反应堆可以受益于Hardline的简单系统设计，以实施其主要保护系统。



可能使用Hardline和Spinline的保护层级

Hardline

Spinline / TELEPERM XS / Tricon

架构

Hardline 模块化功能专为适应性和安全性而设计，可简化各种安全功能和架构的实施。

冗余

Hardline组件及其分布式功能可方便地构建高达4倍的冗余系统。这允许在具有适当隔离的冗余之间共享阈值、结果和传感器信号。结果在每个冗余中进行整理，并结合到驱动逻辑中以生成输出命令。

地理和电气分离

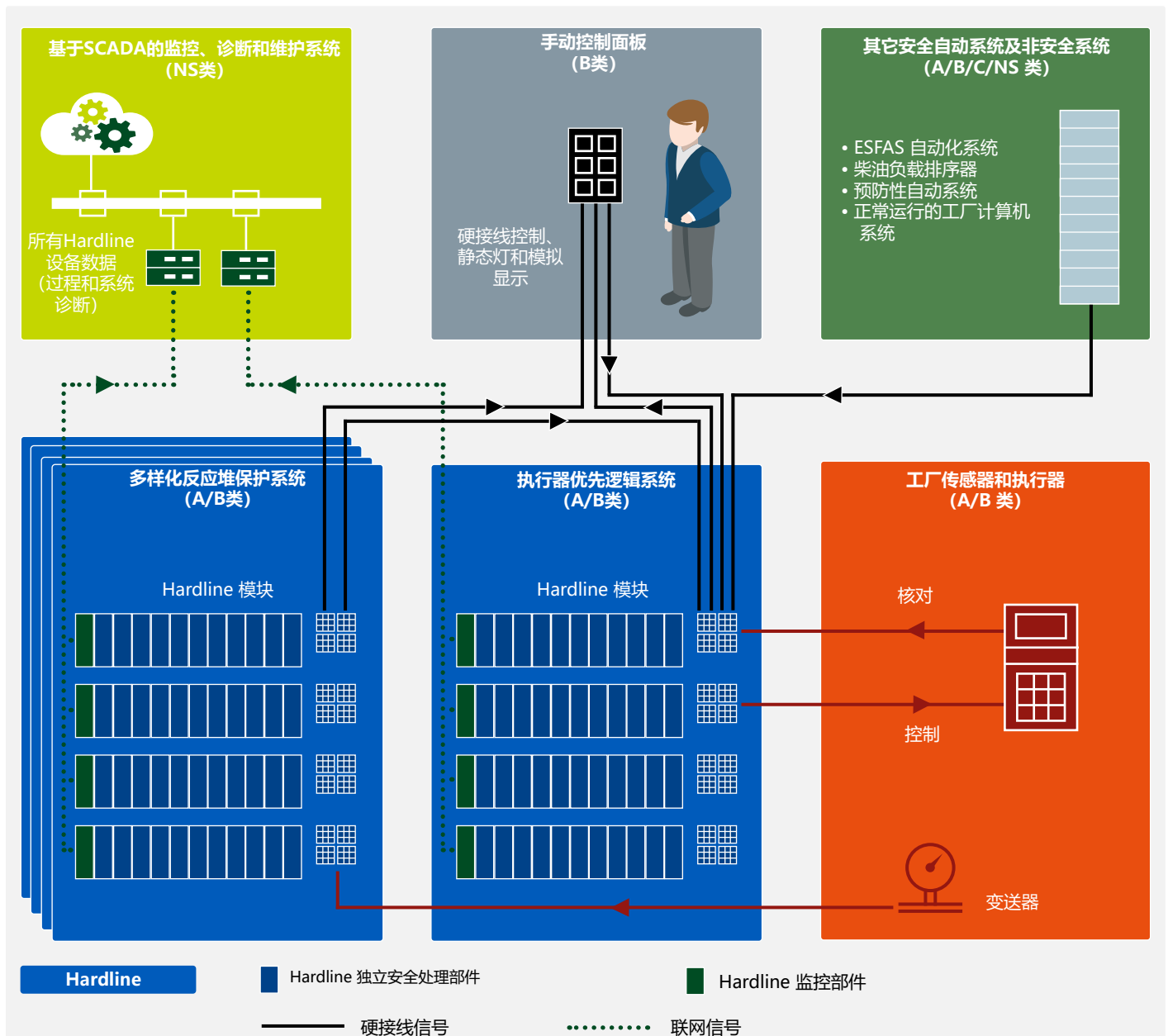
设备间交换是硬接线的，在两端使用电气隔离器以实现工厂内的高度隔离和地理隔离。

模块分离 (安全、监控和通信)

Hardline的安全功能由与监控和通信模块分离的非编程安全模块执行。Hardline的监控和通信模块与安全模块在物理上是分开的，并使用非编程分立电子元件来提供分离和隔离功能。

这些属性确保 Hardline 的通信元件永远不会阻止未编程的安全模块正确执行其安全功能。

Hardline的通信部件由仅充当“观察者”的设备组成，它们的隔离保证它们不会干扰安全功能。



Hardline系统架构典型示例

主要技术特征

Hardline是专用于安全仪控 (I&C) 系统的现代标准化技术

现代化技术

Hardline 是一种基于硬接线的现代非编程安全仪控 (I&C) 平台, 具有最先进的电子功能, 可提供:

- 具有模拟阈值和二进制故障安全逻辑功能的高功能可能性
- 具有故障检测功能的高度安全性和可用性
- 灵活性、可扩展性和升级的可能性
- 运维提升 (监控与自动诊断)

专用于安全类仪控 (I&C) 系统

Hardline 由专门设计的硬件组件组成, 适用于开发安全类仪控 (I&C) 系统:

- 设计用于承受相关标准中定义的恶劣条件 (例如温度、EMI、振动、地震) 的机柜和装置
- 执行二进制和模拟功能以及执行器控制的全系列非编程模块
- 具有标准 Modbus TCP 链接的通信网关设备, 允许集成监控功能和与外界接口

这些组件是根据高级系统功能设计的, 可以轻松满足客户和监管机构的要求。

Hardline 是50年安全模拟技术使用经验的结晶



标准化组件

Hardline硬件组件是标准化的（即模块化和可扩展性）：

- 模块化：Hardline 可以作为集成到现有有机柜中的单元（特别是在翻新的情况下）或作为全新机柜交付。可以调整单元和机柜的内容以满足系统要求
- 可扩展性：Hardline 可以适应任何规格的仪控（I&C）系统，从简单的系统（例如一个只有很少模块的设备，没有冗余），到复杂的系统（例如一个集成的、具有4重冗余的多样化保护系统，每个冗余、表决、本地和远程测试单元具有超过200个模块）
- Hardline 机架和机柜是标准配置，可以在生产后根据其特定内容进行配置（“延迟差异化”），这样可以缩短交付日期并在设计阶段后期进行调整
- 得益于优化的布线系统，机柜的内部布线并不复杂

大量的功能

二进制和模拟输入：

- 传感调节器
- EMC 滤波器
- 测试模式开关

模拟处理：

- 带滞后的可调高低阈值
- 信号选择器

输出：

- 测试抑制
- 输出继电器
- 信号隔离器

二进制：

- 表决器（1oo2、2oo2、2oo3、2oo4.....）
- 基于继电器的逻辑电路（或、与、非.....）
- 执行器控制逻辑
- 时间延迟控制
- 信号选择器

监控：

- 模拟和二进制隔离数字化转换器
- 通信网关

测试：

- 自动测试仪测试板
- 通信网关



硬件组件

Hardline是专用于安全仪控 (I&C) 系统的现代标准化技术

安全模式

通过非编程电子元件来实现隔离和分离功能，确保安全功能和通信模块之间的电气隔离、功能分离和独立性。

只允许从安全模块到通信模块进行单向数据交换。隔离和分离功能根据 IEC 62808 进行设计和鉴定，确保不会将故障从通信部件传播到安全模块。

隔离和分离功能集成在安全模块中，符合安全鉴定要求。

通信模块

Hardline通信模块提供与其它仪控 (I&C) 数字系统的单向通信功能。如图 4 所示，监控通信模块 C.11 COM 1 最多可监控 11 个安全模块，它与 Hardline 网关关联，允许从多达 22 个单元到上层监控和诊断系统的单向通信。

本地人机界面

Hardline 机柜面板上的本地人机界面提供了一组标准的键、按钮、LED，用于管理测试模式并允许故障排除，还可以根据要求定制专用的本地人机界面。

主要安全模块列表

模块编号	功能	输入/输出信号
A. THR	可调高低阈值	输入: 0(4)..20mA / 输出: 干接点
A. ISO	模拟隔离	输入: 0(4)..20mA / 输出: 0(4)..20mA
A. THC	带外部补偿的K型热电偶调节器 (0..1300°C)	输入: 0..60mV / 输出: 4..20mA
A. RTD	PT100 调节器 (0..400°C)	输入: 100..247mV / 输出: 4..20mA
B. REL 1 B. REL 2	带 NO 和/或 NC 触点的 SPDT 继电器	输入线圈: 24V _{DC} 输出接点: 干接点
B. SEQ	TON、TOFF 和 TPULSE 可调时间延迟和锁存功能	输入: 24V _{DC} / 输出: 干接点
B.PRIO	优先控制逻辑	输入: 24V _{DC} / 输出: 24V _{DC}
B. TST	测试开关功能	输入输出信号: 0(4)..20mA或24V _{DC} 测试开关指令: 24V _{DC} 线圈
P.DC/DC	24V _{DC} 隔离DC-DC转换器	输入输出: 24V _{DC}



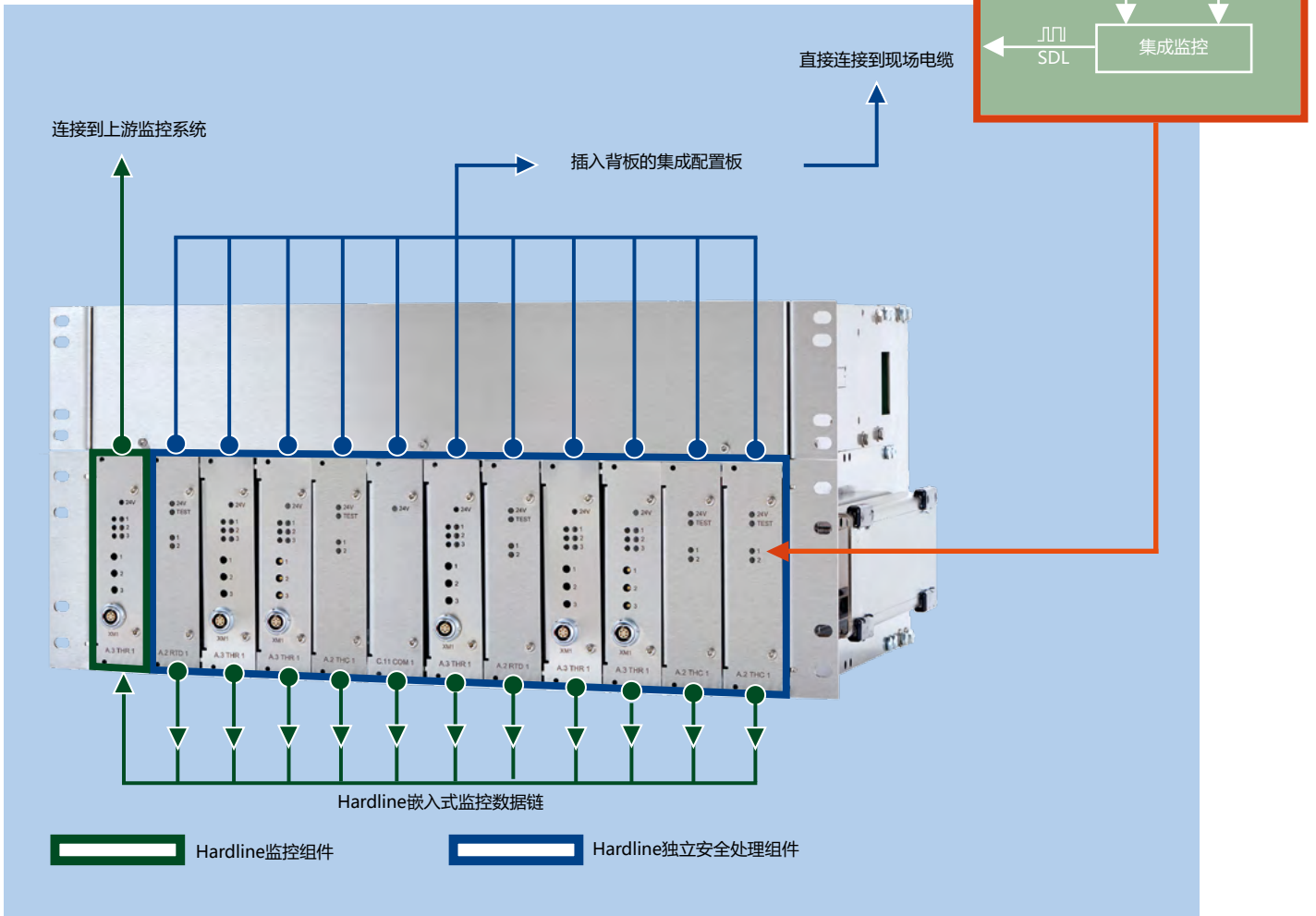
Hardline 模块

单位

一组连接的安全模块可确保安全，它们允许连接到上游传感器、仪控 (I&C) 系统、执行器开关设备以及 HMI 面板。

安全模块由可配置和接线的基本功能组成，以便通过插入背板的定制集成配置板来执行过程安全功能。

安全模块连接到通信总线，它们包括与非编程安全功能隔离且分离的通信电路。模块输入、输出和参数由通信模块监控。



应用一个Hardline单元的Hardline机架

硬件组件

Hardline是专用于安全仪控 (I&C) 系统的现代标准化技术

机柜

Hardline 模块可以安装在法马通的标准机柜的机架中，可以使用单面机柜和更深的双面机柜，以增加每个机柜安装模块的数量。

机柜最多可包含 6 个 Hardline 19 英寸机架。

机柜防护等级可高达IP31，抗震能力强。当对室内环境温度 (60°C) 有较高要求时，可以建立一个基于风扇的优化气流系统。

Hardline机架和机柜是标准配置，可以在生产后根据其特定内容进行配置（“延迟差异化”）。这样可以缩短交付日期并在设计阶段后期进行调整。

维护人员可以即时、轻松地访问机柜内系统的任何元件。

Hardline标准机柜特征：

高度	≤ 2100 mm
宽度 - 不含侧板	≤ 1000 mm
宽度 - 带侧板的4个机柜组	≤ 4100 mm
深度 - 不含背板和门	≤ 495 mm
开门所需的前部空间 (WxD)	≤ 1000 x 600 mm
重量	250kg

灵活的模块化技术



监控

类似于数字系统提供的、先进的监控系统和人机界面

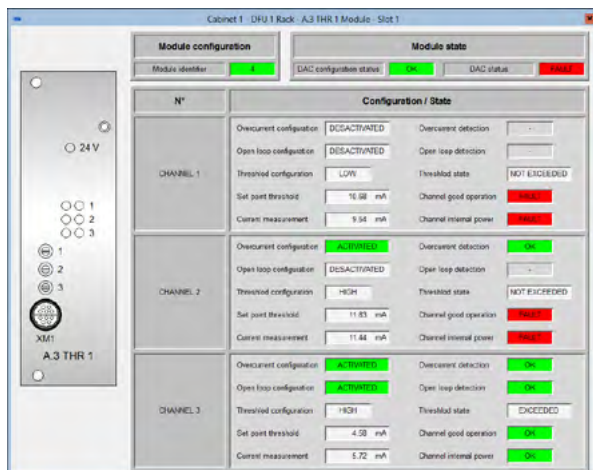
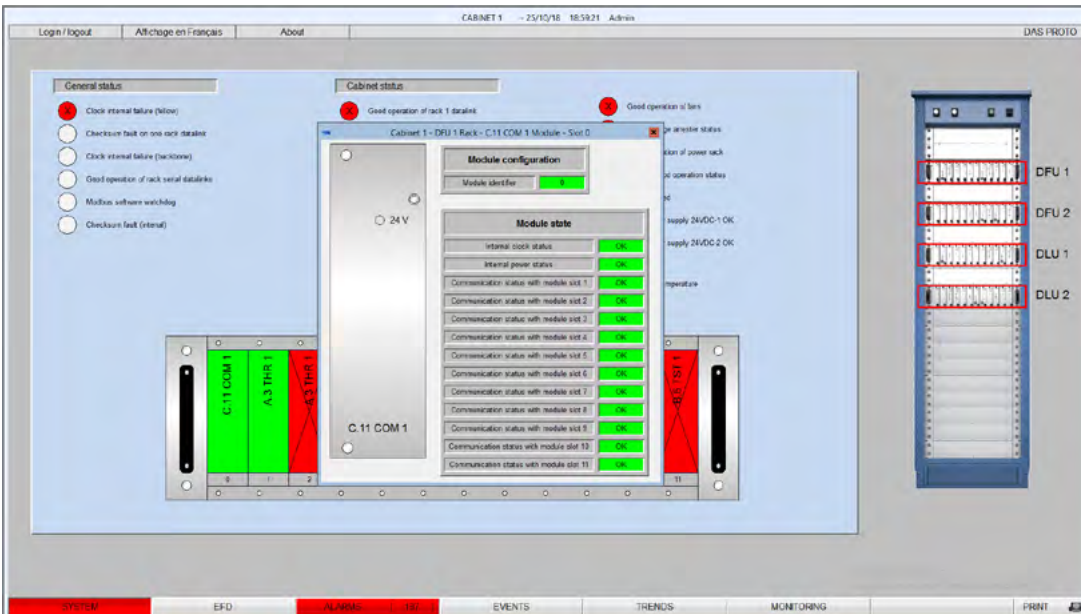
诊断和监测

每个安全模块都有一个单向串行数据链路，为通信模块提供必要的信号。通信模块具有单向串行数据链路，连接到与外部诊断单元通信的Hardline网关。

这些监控功能允许显示有关组件健康状态以及安全功能值和参数的相关信息。

Hardline为基于计算机的外部监控系统提供软件解决方案，其特点是：

- 与更高级别的工厂控制系统接口的网关功能
- 能够进行警报管理
- 用于故障排除的用户界面



模块和机架监控接口示例

标准/技术规范

Hardline根据以下规则和标准开发

安全要求

国际	IAEA GSR 第2部分	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	核电厂的安全 - 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/IEEE 60780-323	核电站 - 安全系统的电气设备 - 鉴定
	IEC 60812	系统可靠性分析技术: 故障模式和影响分析流程
	IEC 60709	核电厂 - 安全关键仪表和控制系统 - 分离
	IEC 60068-2 系列2	环境测试
	IEC/IEEE 60980-344	核设施 - 安全关键设备 - 抗震鉴定
	IEC 60987	基于计算机的系统的硬件设计要求
	IEC 61000 - 系列4	电磁兼容性
	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 61513	核电厂 - 安全关键仪表与控制 (I&C) 系统 - 系统的一般要求
	IEC 62003 ed2:2020	核电站 - 仪表、控制和电力系统 - 电磁兼容性测试要求
	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
	IEC 62566	执行B类或C类功能系统用HDL编程的集成电路
	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 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	
美国	10 CFR 50	核电厂通用设计准则 (附录A)
	NUREG 800, 第7章	核电厂安全分析报告审查计划
	IEEE 338	核电站安全系统定期监督试验准则标准
	IEEE 379	单一故障准则在核电站安全系统中的标准应用
	IEEE 603	核电站安全系统准则标准
欧洲	RCC-E	电气和仪控 (I&C) 系统及设备的设计和施工规则
	RFS	法国ASN - 核反应堆基本安全规则
	CRT	技术规则文件
	EN 55011 (A类)	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
	EN 61000-6-2	电磁兼容性 - 通用抗扰度标准
	EN 61000-6-4	电磁兼容性 - 通用发射标准
	TS 61000-6-5	电站和变电站环境的抗扰度

鉴定

Hardline已通过以下测试鉴定

法马通的所有硬件组件和系统均按照欧洲核标准、国际原子能机构 (IAEA) 50-C-QA 质量保证代码、IEC 61513 以及相关的 IEC 核特定标准和欧洲规范 RCC-E进行设计、实施和鉴定，该规范规定了核电站中使用的电气设备的鉴定要求。

Hardline 系统鉴定基于以下测试和分析：

- 合格品被定义为在最苛刻的配置中涵盖该技术的全部功能，它们在认证实验室中进行资格测试，以建立一套参考测试级别和批准的配置
- 根据对定制机柜设置的分析，将已安装系统的鉴定与参考鉴定进行比较配置

电气和制造测试

参考测试是在首个电子板、单元和机柜上进行的，它们允许操作员通过以下方式检查电气和功能特性以及制造质量：

- 目视和机械检查
- 电气测试
- 功能特性测试

老化测试

在环境和地震测试之前，需要对合格品进行老化测试，测试模拟了设备寿命的影响，包括：

- 连接器反复拔插
- 机械振动
- 快速温度变化
- 干热
- 湿热
- 寒冷
- 长时间运行测试

合格的环境条件

操作室环境温度 (柜级)	+1 至 +45°C (某些特定情况下超过 45°C)
推荐平均室内环境温度	+23°C
相对湿度	+40°C 时为 95%
符合 IEC/EN 62003的EMC稳定性	III 级：带标准外部布线 IV 级：带有增强型 EMC 外部布线
抗震和抗大型飞机坠毁	垂直和水平 ZPA 12 m/s ² 零周期加速度 (ZPA) 应用于机柜锚固结构。 法马通文件中提供了经过测试的能谱。



功能操作限制

- 缓慢和突然的电压变化测试
- 频率变化测试
- 热变化测试
- 耐湿测试
- EMC 测试在另外的段落中描述

环境测试是对合格品进行的。

EMC 鉴定测试

基于核环境的经验，法马通定义了一个标准的合规流程，对Hardline 产品系列中的每个项目执行 EMC 测试。EMC 测试是对合格品进行的。

抗震鉴定试验

使用覆盖测试能谱对合格品进行抗震测试。所应用的地震级别定义为足以涵盖设备在世界大部分地区可能承受的压力。

客户利益

Hardline是专用于核安全的、最新的非编程仪控 (I&C) 技术

以安全为导向

Hardline的硬件组件设计用于实施安全仪控 (I&C) 系统，其功能包括防御 (即检测和行动) 系统内部可能发生的故障，这些故障由仪控 (I&C) 系统内部或外部引起。其针对故障安全的功能如下：

- 模拟模块使用 4-20mA 电气范围。如果检测到硬件内部故障，输出设置为 0 或 +22mA，因此信号接收器不会显示错误信息
- 可以使用 Hardline 故障安全配置执行逻辑算法，在检测到硬件故障时将模块二进制输出设置为安全状态
- 表决模块允许检测非一致，允许操作员连续检测虚假激活以及在实际激活的情况下按需失败

不受软件共因故障和网络安全威胁

Hardline 技术基于硬接线，不需要任何软件，这保证了其它工厂安全数字系统不存在软件共因故障 (CCF) 的风险，而且 Hardline 技术不受网络安全威胁的影响。

可靠性

Hardline 旨在构建高度可靠的仪控 (I&C) 系统：

- 安全：系统的正常或异常操作或故障不会导致不安全状态
- 可用：系统始终履行其功能

核电厂仪控 (I&C) 系统的可靠性以安全为导向，并执行“单一故障”标准

- 单一故障不应妨碍系统安全和可用
- 两个同时独立的故障不应导致不安全状态

易于取证

同样，没有软件确保了与监管机构的直接取证阶段。

自我诊断和定期测试

Hardline模块在运行期间通过自我监控功能不断进行检查。

自检可以检测到大多数模块硬件故障并立即发出信号。

所有信号都受到持续监控，信号状态自动传输到监控系统：这种早期故障检测减少了维护需求。

Hardline安全系统可以设计为具有定期测试功能，可在离线或在线操作期间使用，定期测试可以模拟能触发保护动作的设备输入条件，它们适用于检测那些可能会阻止安全系统在需要时启动适当动作的潜在故障。

硬件可靠性

Hardline 电子板的设计符合安全1级 (IEC 61226) 的要求。

故障模式和影响分析 (FMEA) 可用于每个电子板，用于建立系统可靠性的故障率估计。这些估计有助于评估系统硬件架构对安全目标的实现情况以及定期测试之间所需的时间间隔。

实施技术的机柜和装置的设计、制造和验证符合安全1级的要求，它们经过全面的环境鉴定型式测试，例如抗震和 EMC 测试。

硬件可维护性

为了帮助客户满足他们的安全和可用性目标，Hardline 设计了故障避免、故障检测和修复功能：

- 通过使用高质量和合格的硬件组件实施的经过验证的设计来实现可靠性
- 故障检测通过本地和远程信号以及定期测试程序实现 100% 的覆盖率
- 轻松访问机柜内的硬件组件和布线
- 现场快速维修的备件政策



经验和业绩

Hardline是50年安全模拟和非编程技术使用经验的结晶

50多年来，法马通一直在设计、制造和维护使用非软件技术开发的非安全和安全仪控（I&C）系统。

我们为 1978 年至 1987 年间建造的 34 座 EDF 三回路 900MW PWR 提供了用于核仪表的 Multibloc 和用于逻辑功能的 Silimog，它们至今仍在运行。

在 2012 年启动的法国 20 座 1300MW 机组改造项目的框架内，根据运营商的新功能要求，对 ULS 动态逻辑系统进行了升级。法马通在最初于 80 年代开发的现有非编程仪控（I&C）系统中实现了新的电子功能。

对于 2014 年启动的 Loviisa 现代化改造项目，法马通更新了电子功能，以便向 Loviisa 核电厂提供非编程系统。

交付了两个非编程安全仪控（I&C）系统，使运营商能够提高工厂的安全性。

第一个系统允许安全手动命令优先于非安全自动命令。第二个系统为关键保护功能实现了额外的多样性，并为操作员提供了访问不同跳闸和 ESFAS 手动命令的权限。



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](https://twitter.com/Framatome) 领英：[Framatome](https://www.linkedin.com/company/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