

PROVER®

打造一个更加安全的世界。

Prover iLock

最早的信号开发软件

集成工具包 效率无可匹及 安全性无与伦比



最早的信号系统开发软件

Prover iLock是一种用于设计、验证、确认、优化和归档的控制与信号应用的主导软件解决方案。25个以上的国家里的硬件供应商和运营商选用该产品。谈及削减成本、安全操作以及提高开发速度，Prover iLock无可匹及。



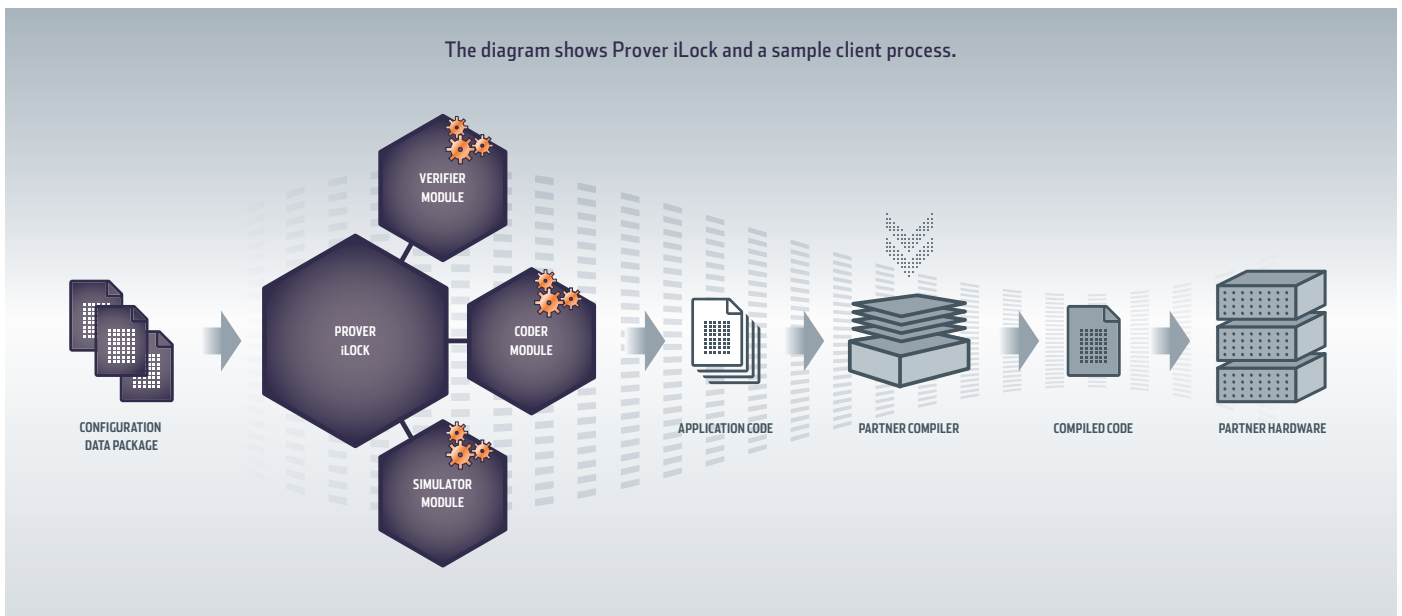
安全



高效



节约

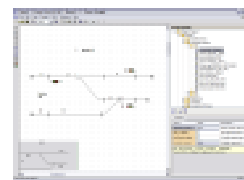
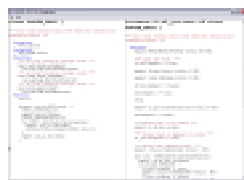


Prover iLock

信号应用快速说明

Prover iLock核心产品和信号应用可自动生成完整的应用设计、测试和安全规范。它是通过一套独立于应用的通用配置数据包和一个包括轨迹规划的高级说明来实现的。

Prover iLock还具有档案生成调试以及编码、继电器系统和控制表导入功能。



通用配置数据包

通用配置数据包是经过设计独立应用的。包括：

- + 一个包括所有图形对象的图标数据库。
- + 一个能详细说明设计原则的通用设计说明，该说明是用功能强大的谓词逻辑语言编写的。
- + 一个能详细说明测试结果的通用设计说明。其中，每个通用测试均采用应用编码输入和预想输出表达。

+ 一个能用谓词逻辑详细说明形式安全要求的安全说明。例如，相矛盾的信号绝不会同时进行示象。

一般情况下，每个应用类型和运营商都会创建一套配置数据包。工程师可以利用权限许可通过拓展Prover iLock现有的配置数据包，有效地创建新的配置数据包。

验证器模块

符合CENELECSIL-4认证 形式安全说明

Prover iLock验证器通过形式验证，可以确保应用编码满足所有应用安全要求。Prover iLock可以对Partner硬件、应用编码和应用安全说明建模，然后进行自动数学运算验证搜索。人们不必再去编写测试。如果出现与要求相矛盾的不安全方案，Prover iLock验证设备会将其发现，生成相应的测试并在调试器中显示出来。工程师找出并改正不安全的逻辑，重新运行Prover iLock验证器。

该方法与测试、模拟和回顾存在本质的不同。若对一切可能的方案和事件组合进行测试、模拟，基本的编码工作也许就需要数百万年的时间。一切测试方法都是从所有的方案中选出来的（数量一般不足全部方案的1%），再对这些方案进行测试。同时，应用编码操作对其他方案是否安全尚不得而知。

通过引入Prover iLock验证器，您不必再将检验限定在几个方案上。Prover iLock验证器证实，应用编码对所有方案均安全。

虽然一些人对此还很陌生，但形式验证可广泛用于铁路、半导体、航空电子学以及汽车工业。经过二十多年的发展，它已经成为一个成熟的、且经过检验的验证方法。

编码模块

合作伙伴的硬件自动生成编码

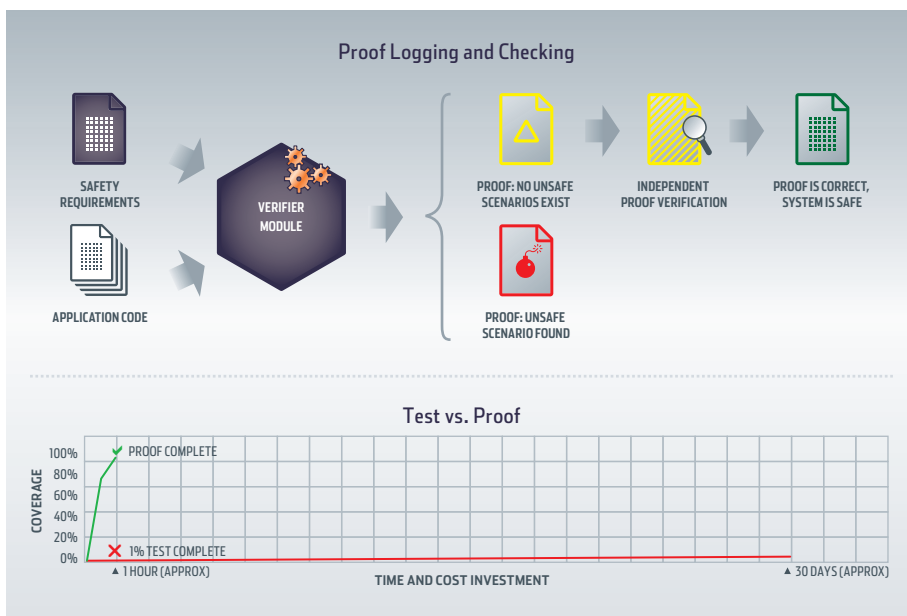
Prover iLock编码器会通过应用设计说明自动生成应用编码。由此将完全不必采用手动方式编写应用编码。编码工作所需的精力将用于通用的、可重复使用的配置数据包。Prover iLock 编码器支持包括IO和集成版创建文件在内的集中和分布式编码。对于一般的合作伙伴的硬件而言，该编码器所生成的编码是梯形逻辑格式，需用合作伙伴的编译器读取。欲获取合作伙伴产品列表，请与我们联系。

验证登陆

Prover iLock验证器是市场上出售的、唯一支持验证登陆的解决方案。在安全分析过程中，该工具会生成数十亿字节的验证日志。为了达到检验的目的，该日志可用独立的验证登陆检查器进行检查。如果验证日志中（在意料之中）没有发现任何错误，独立的验证登陆检查器将提供安全验证。该方法符合用于减少安全测试的CENELEC SIL-4要求，并且通过认证登陆检查器，该方法成本低，可独立验证。

能力和性能无可匹及

对于支持验证执行模式的Partner硬件而言，数百个火车路线的系统在数个CPU小时内便可得到全面验证。多年来，Prover投入250多名员工从事SAT和基于BDD模式检查、概括、模拟以及更改领域的研发。Prover iLock验证器将这些方法同其他具有不同优点和缺点的方法相结合，确保能力和性能无可匹敌。



模拟模块

操作要求的加速测试

利用Prover iLock模拟器，信号工程师可以迅速确定应用编码是否满足操作和功能要求。通过加速合作伙伴的硬件模拟，测试时间明显缩短。除非Prover iLock模拟器应用编码无法说明，模拟器会标记其他的所有编码，然后信号工程师可启动调试器，找出通用设计说明（如果应用已被导入，编码或继电器系统）中的逻辑错误，进行更正。

稳定器模块

自动稳定性验证与优化

利用Prover iLock稳定器，信号工程师只需按动控制键，便可实施稳定性验证和优化。该稳定器会对合作伙伴的硬件、应用编码、执行次序以及输入约束进行建模并加以分析。如果某个输入序列导致不稳定，Prover iLock稳定器会找出来并加以显示。如果不存在这样的序列，稳定器会生成更改的执行序列。该序列在很短的周期内便可达到稳定状态，且不会发出应用行为警报。

Prover科技公司

Prover科技公司提供控制和信号系统开发的软件产品和服务。该公司是一家创建于1989年的私营公司，总部位于瑞典的斯德哥尔摩，在法国和美国设有分公司。

Prover科技公司的主要客户包括空中客车公司 (Airbus)、安萨尔多 (Ansaldo)、庞巴迪 (Bombardier)、纽约市捷运局 (New York City Transit)、RATP (巴黎地铁)、瑞典国家铁路局 (Swedish National Rail)、泰雷兹 (Thales) 以及其他许多公司。

www.prover.com

PROVER®

Prover Technology AB
+46 (0)8 617 68 00
Rosenlundsgatan 54
118 63 Stockholm
Sweden

Prover Technology SAS
+33 (0)5 6227 5327
21, Rue Alsace Lorraine
31000 Toulouse
France

Prover Technology Inc.
+1-650-331-1575
1650 S. Amphlett Blvd, Suite 124
San Mateo, CA 94402
USA