白皮书

为医疗设备开发 IEC 62304 合规的嵌入式软件

MathWorks®

无论您是嵌入式软件开发人员还是医疗设备工程师，都可以通过这本白皮书来了解医疗设备软件设计的最佳实践，其中涵盖从需求管理到设计、实现和集成，再到验证和测试的整个过程。您将了解如何生成更高质量的软件，同时减少设计错误和开发时间。

设想一下，您的团队正在开发控制系统以驱动外科手术机器人系统的一部分。该系统通过带触觉反馈控制的电机提供动力。开始设计之前，你们希望解决一些关键问题，例如：

- 如何确定电机尺寸以获得最佳功率和精度？
- 能否在不延误项目的情况下纳入后期需求变更？
- 在集成之前，如何在系统级别测试设计？
- 的设计流程是否符合 IEC 62304 等医疗标准？

Corindus CorPath GRX 外科手术机器人系统。

如果您的团队使用手写代码和基于文档的需求，则解决以上问题的唯一方法是反复试错或执行物理原型测试，无论是为手术器械、呼吸机、输液泵还是透析机应用，情况都是如此。如果某项需求发生变化，可能需要重新编码和测试整个系统，继而会导致项目延迟数周乃至数月。

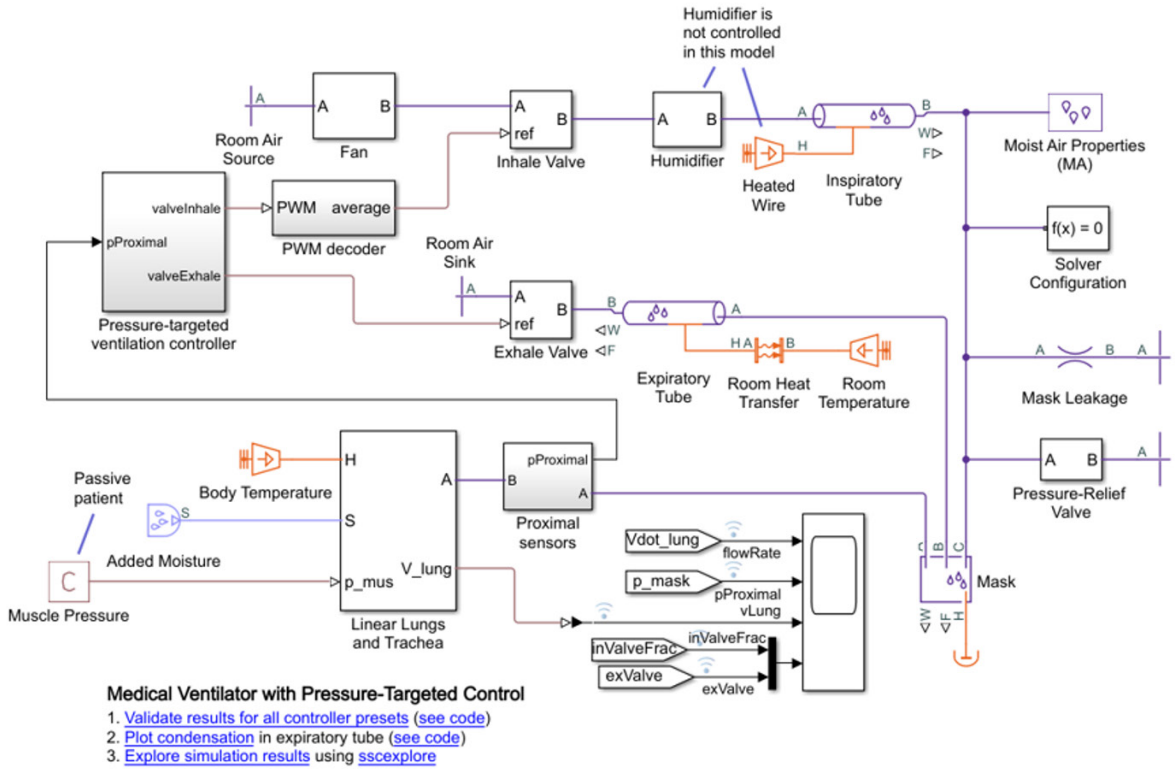
您的团队如果使用 MATLAB® 和 Simulink® 进行基于模型设计，则无需手写代码和使用文档，而是创建系统模型。以外科手术机器人系统为例，模型将由机械臂、电机和控制单元组成。您可以随时进行模型仿真，即时查看系统行为，测试多种假设分析场景，同时无需承担风险和延迟，也无需依赖昂贵的硬件。然后可以将设计集成到最终硬件中 - 所有这些都在 IEC 62304 合规的开发流程中进行。

> “基于模型设计使我们的小型产品开发团队能够在短短四个月内开发和演示遥操作机器人功能，从而减少了成本和开发时间。”
>
> *— Per Bergman, Corindus*

本白皮书介绍了如何使用基于模型设计进行医疗设备开发，提供了快速入门技巧和最佳实践。书中包含真实案例，展示采用基于模型设计的团队如何缩短开发时间，最大限度地减少集成问题，并交付安全关键型产品，同时遵守医疗设备法规和标准。

I. 什么是基于模型设计?

要理解基于模型设计，最好的方法是结合实例，以机械呼吸机的设计为例。



Simulink 和 Simscape 中的机械呼吸机模型。

医疗设备工程师团队着手打造阀门控制单元，用于调节机械呼吸机的流量、输气量以及吸气和呼气功能。由于工程师们使用基于模型设计，他们首先根据系统需求构建架构模型。

然后，团队开发了一个包括管道、阀门和加湿器的呼吸机模型。这种高级低保真度模型还包含将在控制单元中运行的控制算法，以及被控对象（在本例中是指连接到呼吸机的患者）模型。

团队通过在各种医院和急救场景下进行高级模型仿真来执行初始系统和集成测试，以验证系统是否正常运行，并且它可以响应不同的情况而不会给患者带来风险。

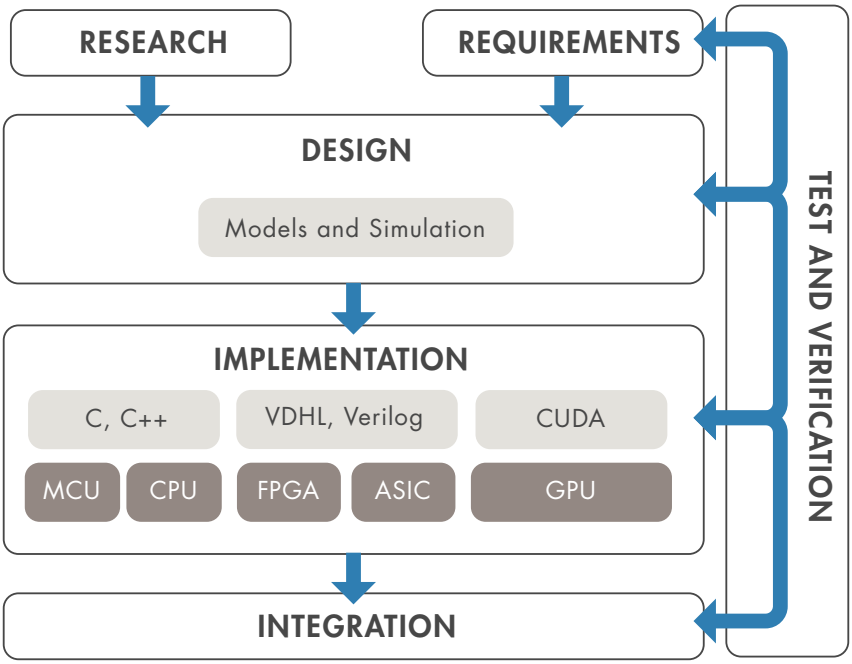
为了测试呼吸机的响应能力，团队以活跃患者的形式向仿真中增加了更多细节。他们对照规范不断测试和验证系统级行为。如果系统规模庞大且结构复杂，工程师可以独立开发和测试各个组件，但仍要在全系统仿真中频繁进行测试。

最终，团队针对系统及其工作条件建立了精细模型。该模型捕获了从所有研发工作中累积的系统 (IP) 知识。然后，工程师基于控制算法模型生成代码，从而执行软件测试和验证。他们还生成监管审批流程所需的所有单元和系统级测试文档。

通过快速原型设计完成硬件在环测试后，他们在生产硬件上实现生成的代码，以验证呼吸机的运行。

您将从该场景中看到，基于模型设计采用与传统开发工作流程相同的元素，但存在两个关键区别：

- 从需求设定到设计、实现和测试，系统模型始终占据开发流程的核心。
- 将工作流程中大量费时和易出错的步骤（例如编写代码、手动测试和文档）自动化。



基于模型设计的工作流程。

需求捕获和管理

传统工作流程基于文档捕获需求，交接可能引发错误和延迟。通常，创建设计文档或需求的工程师与设计系统的工程师并不是同一批人。两个团队对需求的认知很可能存在断层，这意味着两个团队并未建立持续清晰的沟通。

采用基于模型的设计，您可以在 Simulink 模型中编写、分析和管理需求。您可以使用自定义属性创建富文本需求，并将其链接到设计、代码和测试。同时，还可以从需求管理工具等外部源导入需求并进行同步。如果关联到设计的需求发生变化，您将会收到自动通知。此外，可以使用可追溯矩阵从需求一直追溯到生成的代码。因此，您可以直接评估需求变更如何影响模型和代码，并采取适当的行动。

案例研究：Corindus

Corindus 床边装置，带延伸臂和触摸屏。

"基于模型设计对于我们的创新能力至关重要，因为它使我们能够开发新功能并快速部署它们。我们可以快速构建原型，证明它满足需求，然后在进入产品开发阶段时对其进行完善。"

— Doug Teany，
Corindus 首席运营官

Corindus 开发并部署了一个机器人平台，使医生能够对数百至数千英里外的患者进行经皮冠状动脉介入治疗 (PCI) 或神经血管介入治疗 (NVI)。

该平台是该公司 CorPath® GRX 系统的扩展，允许医生在导管实验室的辐射屏蔽工作站对患者进行手术。Corindus 使用 MATLAB 和 Simulink 进行基于模型设计来创建系统，并增加了对视频和控制数据的实时传输支持。

对于原始系统，Corindus 希望在投入硬件之前通过仿真来验证机器人控制设计，从而加快开发速度。他们还希望通过实时仿真和测试来验证设计，并在嵌入式微控制器上实现。

为了添加远程功能，Corindus 团队需要将透视和血流动力学视频数据从患者所在位置实时发送给医生，并将操纵杆和其他控制数据传回。为了整合遥操作机器人功能，他们建立了一条通信链路，通过两台运行 Simulink Real-Time™ 的 Speedgoat 目标计算机在远程和本地站点之间传送视频数据和控制指令。

Tejas Patel 博士开展了首例人体远程遥操作机器人辅助经皮冠状动脉介入治疗 (PCI)。他在两天内为五名患者成功完成了五次手术，这些患者在位于印度艾哈迈达巴德的 Apex 心脏研究所，距离 Patel 博士 32 公里。

设计

在传统方法中，每一种设计思路都必须在物理原型上进行测试。因此，考虑到每一次测试都会增加项目开发时间和成本，工程师只能探索少数设计思路和场景。

在基于模型的设计中，工程师可以尽情探索无穷无尽的各种思路。需求、系统组件、IP 和测试场景全被捕获到模型中，而且由于可以进行模型仿真，您可以在构建昂贵硬件之前更早地开始研究设计问题和疑问。您可以快速评估多种设计思路，权衡设计折衷方案，了解每一项设计更改将会产生的系统影响。

案例研究：Weinmann

MEDUMAT Transport 呼吸机。
Image © Weinmann Medical Technology。

"使用 MATLAB 和 Simulink 进行基于模型设计使我们能够处理日益增加的复杂性，并且可以帮助我们获得合规性认证。使用模型而不是手写代码使嵌入式软件更易于维护和重用，并且方便我们向认证机构解释我们的技术。"

— Florian Dietz 博士，Weinmann

MEDUMAT Transport 呼吸机将氧气和空气的混合气体送入和排出需要呼吸支持的患者的肺部。它设计用于急救护理和医院内或医院间转运。

MEDUMAT Transport 有多种传感器来测量压力、流量、温度和摩尔质量（用于测量氧浓度）。这些传感器与先进的气动和电磁阀相结合，使 MEDUMAT Transport 成为 Weinmann 开发的最先进、最复杂的呼吸机。为了找到该系统的最佳算法，工程师需要评估众多设计备选方案。

Weinmann 的工程师们认识到，他们的传统流程，即手写嵌入式软件对于这个项目来说不可行。

为了克服这一挑战，他们开发了被控对象模型，其中包括硬件组件以及人类肺部的机械模型。团队还对控制器及其状态机进行了建模，包括一个跟踪待机、启动、关闭和其他工作模式的状态机，以及一个管理整个通气过程的状态机。系统级控制器模型作为支持模块化软件设计和架构基本需求的子系统层次结构的顶层。

在对控制器和被控对象运行闭环仿真后，团队生成了控制系统和传感器信号处理子系统的生产代码。他们将代码分别部署到 Infineon® 和 Texas Instruments™ MCU，并对模型中的每个子系统执行单元测试。

代码生成

在传统工作流程中，嵌入式代码必须基于系统模型或从零开始手动编写。软件工程师按照控制系统工程师编写的规范编写控制算法。从编写规范、编写算法代码到调试手写代码，此过程中的每一步都既费时又容易出错。

采用基于模型的设计时，您无需手动编写数千行代码，而是可以直接从模型中生成代码。这避免了手写编码错误，并且模型在控制系统工程师与软件工程师之间架起桥梁。生成的代码可用于原型设计或生产。代码可以针对特定处理器架构进行优化并与手写的既有代码集成。

案例研究：World of Medicine

WOM 的 50L 气腹机。

"Simulink 使我们能够在短时间内生成稳定的控制系统。我们对整个系统进行建模，包括状态机和级联 PI 控制器。接着对该模型进行完善，以提高稳健性和响应速度，然后通过快速控制原型设计和生成的嵌入式代码对其进行验证。"

— *René Pätznick, WOM*

腹腔镜检查和其他微创手术必须在腹部狭窄的空间内进行。为了增加手术器械的活动自由度，医生使用气腹机向体腔内吹入二氧化碳气体以扩大体腔。WOM 是用于腹腔镜和子宫镜检查的气腹机和泵技术的市场领导者，它使用基于模型设计来加速高质量气腹机控制软件的开发。

在过去的类似项目中，WOM 工程师使用传统的开发工作流程，需要手写代码。使用这种方法时，工程师直到流程后期才能识别并纠正设计和编码错误，从而会延误软件交付。

因此，对于新型气腹机开发，WOM 工程师转向基于模型设计。他们使用测量的输入/输出数据来创建腹腔的非线性数学模型，然后将该模型整合到包括压力传感器、作动器和其他硬件组件的被控对象模型中。

接下来，他们开发了一个控制模型，其中包含两个级联比例积分 (PI) 控制器，分别用于流量和压力。团队通过对控制模型与被控对象模型运行闭环仿真来验证控制功能。

为了验证设计的实时性能，他们从控制模型生成 C 代码，并将其部署到与原型气腹机中的传感器和作动器相连接的实时硬件上。在根据客户意见完善设计后，团队生成了目标 Arm® Cortex-M® 处理器的产品级代码。

经过全面的集成测试和系统级测试后，WOM 获得了 FDA 和欧洲监管机构的批准，该新型气腹机现已投入生产和临床使用。

测试和验证

在传统开发工作流程中，测试和验证通常安排在应用程序完成后，因而难以识别及纠正设计和编码阶段引入的错误。

在基于模型设计中，测试和验证贯穿整个开发周期，从您开始建模需求和规范的那一刻起，直到完成设计准备好进行集成的那一刻。虽然您要更频繁、更彻底地进行测试，但也是在节省时间，因为您可以证明您的设计满足需求：通过模型中捕获的需求，您可以验证需求并将其追溯到设计、测试和代码。您可以自动生成测试、创建测试报告，并使用静态分析和形式化方法检查是否符合编码标准和指南。

案例研究：ITK Engineering

采用 ITK Engineering 的无传感器无刷电机控制的牙钻。

"我们的被控对象模型准确地反映了电机行为，这使我们能够在开发早期验证我们的控制器和硬件。我们快速找出了首个硬件原型出现错误的根本原因。"

— *Alexander Reiss，ITK Engineering*

与有刷电机相比，无传感器无刷直流 (BLDC) 电机的运行磨损更少，并且更可靠、更安静、更易于维护和消毒。与带传感器的 BLDC 电机相比，无传感器 BLDC 电机更便宜且更小巧。然而，开发无传感器控制所需的复杂算法需要的工程工作量要多很多。

ITK 工程师需要设计和优化转子位置估计器，以及符合医疗设备软件 IEC 62304 标准的牙钻电机的复杂级联控制。

项目开始时，还没有原型电机。为了满足客户的项目期限，ITK 必须同时开发控制器软件和电机硬件。

使用基于模型设计，ITK 工程师设计、优化、实施和测试了无传感器 BLDC 电机控制器。根据现有电机的数据表和客户提供的信息，工程师在 Simulink 中对 BLDC 电机进行建模，包括其电气和机械组件。

在将其浮点控制器设计转换为定点后，他们重新运行仿真以验证定点模型。团队还开发了对单个模型组件执行批量单元测试的 MATLAB 脚本。

用在牙钻中的控制器和无传感器 BLDC 电机目前正批量生产。

II. 快速入门

尽管您和您的团队可能已经了解到迁移至基于模型设计将带来的益处，但您也难免担忧可能面临的种种组织、后勤及技术风险和挑战。本节解答了工程团队考虑采用基于模型设计时提出的常见问题，并提供一系列经实践验证的技巧和最佳实践，帮助这些团队管理过渡事宜。

问：引入基于模型的设计会对工程分工造成怎样的影响？
答：基于模型的设计并不会取代控制设计和软件架构方面的工程专业知识。采用基于模型的设计，控制系统工程师不仅可以提供传统书面形式的需求，还能提供模型和代码形式的可执行需求。软件工程师可以减少在手动编写应用程序软件上花费的时间，腾出更多时间执行架构建模；为操作系统、设备驱动程序及其他平台软件编写代码；以及执行系统集成。控制系统工程师和软件工程师自开发流程早期就能介入系统级设计。

问：当我们转向基于模型设计时，对现有的代码会有什么影响？
答：它可以成为设计的一部分；您的系统模型可以同时包含原生设计建模组件和既有组件。这意味着您可以逐步引入既有组件，同时继续进行系统仿真、验证和代码生成。

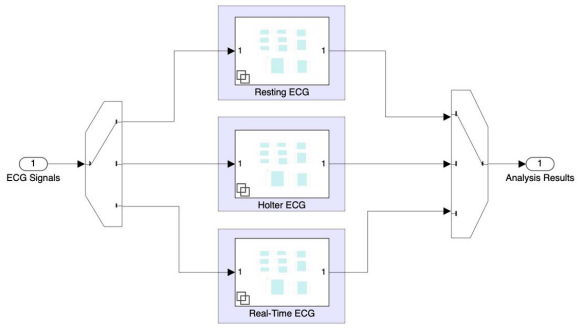
问：在采用基于模型的设计时，是否存在推荐做法？
答：尝试新方法和设计工具不免带来风险。根据一些团队的成功经验，要降低此类风险，不妨逐步引入基于模型的设计，采取有针对性的步骤帮助推进项目并避免速度减缓。不同规模的企业都选择从小团队级别开始采用基于模型的设计。他们通常从单个项目入手，快速致胜并在早期成功的基础之上继续推进和延伸。积累经验后，他们开始在部门级别推广基于模型设计，使模型成为团队整个嵌入式系统开发项目的核心。

问：基于模型设计是否符合 IEC 62304 软件开发流程？
答：您可以使用基于模型设计为医疗设备开发 IEC 62304 合规的嵌入式软件。基于模型设计将验证和确认纳入工作流程，从而确保软件在集成到医疗设备之前经过全面测试和验证。此外，IEC 62304 要求的文档部分将自动生成，以符合法规要求。基于模型设计中使用的大多数 Simulink 工具已通过 TÜV SÜV 认证，可用于 IEC 62304 合规开发工作流程。

以下**四个最佳实践**已在多个团队的实践中证明有效：

- **使用项目的一小部分进行试验。**选择一个新的嵌入式系统领域，构建软件行为模型，然后基于模型生成代码，是一个不错的开始方式。团队成员只需投入少量精力即可掌握新工具和新方法，从而完成这项小调整。该结果能够呈现基于模型设计的一些关键优势：
  - 无需手动编码即可创建高质量的代码。
  - 代码与模型行为一致。
  - 采用模型仿真，不仅可以更轻松地调试算法，还能获得更为深层的信息，胜过基于桌面动态地测试 C 代码。
- **添加系统级仿真，在初始建模成果的基础之上继续推进项目。**如本文的前几节所示，您可以通过系统仿真确认需求、调查设计问题以及开展早期测试和验证。系统模型无需实现高保真度；所包含的细节只需确保接口信号采用正确的单位并连接适当的信道同时确保能够捕获系统的动态行为即可。您可以通过仿真结果提前了解被控对象和控制器的行为模式。
- **使用模型解决特定设计问题。**即使不开发全尺寸被控对象、环境和算法模型，您的团队也可以获得有针对性的帮助。例如，假设您的团队需要为作动系统使用的螺线管选择参数。他们可以开发一个简单模型，在螺线管四周绘制概念性“控制体积”，包括驱动因素和作用因素。团队可以测试各种极端工况并提取基本参数，但不必推导方程。之后，团队可以存储此模型，以用于解决其他设计问题或融合至今后的项目。
- **从基于模型设计的核心元素入手。**基于模型设计的直接优势包括：支持创建组件和系统模型；通过仿真测试和确认设计；自动生成 C 代码以进行原型设计和测试。在此基础上，您可以进一步考虑采用高级工具和实践，引入建模指南、自动合规性检查、需求可追溯性及软件构建自动化。

案例研究：Khawaja Medical Technology



在 Simulink 中建模的心电图信号分析算法。

"我们在基于模型设计上的投资获得了显著回报，包括产品质量提高、开发时间缩短，以及 ISO 和 IEC 认证加快。"

— Antoun Khawaja 博士，
Khawaja Medical Technology

心电图 (ECG) 数据分析对于心脏病的识别和治疗至关重要。它适用于各种诊断环境，包括临床前、临床、门诊和家庭环境，以及新药临床试验。

作为心脏药物开发和审批过程的一部分，制药公司必须调查新药对心脏的影响。这涉及分析心电图信号以识别异常并确保心脏药物安全。

Khawaja Medical Technology 的工程师已经开发出全新的先进算法，可以完全自动化心电图信号分析。该算法能够实时监测和分析来自正在休息、锻炼或佩戴 Holter 监护仪的受试者的心电图信号。工程团队使用 MATLAB 和 Simulink 进行基于模型设计，为自动化 ECG 分析开发和部署算法。

团队使用 Simulink Check™ 检查他们的模型是否符合建模指南和标准 (包括 IEC 62304) 。他们使用 Simulink Test™ 编写并执行基于仿真的测试，从测试追溯到需求，并使用 Simulink Coverage™ 测量测试覆盖率。

他们还开发了一组 MATLAB 类，用于为信号处理和分类层创建可重用的系统对象。这些系统对象执行各种任务，如检测心电图信号中的峰值，测量信号特征，对心律失常进行分类以及诊断心室肥大、心肌梗塞和其他心脏疾病。

利用这些工具，Khawaja Medical Technology 得以将开发时间缩短 40%，加快 ISO 13485 和 IEC 62304 标准合规进程，并在几个月内 (而不用几年) 构建出原型。

基于模型设计的工具

基础产品

MATLAB

分析数据、开发算法及创建数学模型

Simulink

嵌入式系统建模和仿真

需求捕获和管理

Simulink Requirements

编写需求、管理需求并将需求追溯到模型、生成的代码和测试用例

System Composer

设计和分析系统架构与软件架构

设计

Simulink Control Design

线性化模型并设计控制系统

Stateflow

使用状态机与流程图进行决策逻辑的建模和仿真

Simscape

建模和仿真多域物理系统

代码生成

Simulink Coder

从 Simulink 和 Stateflow 模型生成 C 和 C++ 代码

Embedded Coder

生成针对嵌入式系统优化的 C 和 C++ 代码

HDL Coder

生成用于 FPGA 和 ASIC 设计的 VHDL® 和 Verilog® 代码

GPU Coder

为 NVIDIA GPU 生成 CUDA 代码

测试和验证

Simulink Test

开发、管理和执行基于仿真的测试

Simulink Check

衡量设计质量、跟踪验证活动并验证标准合规性

Simulink Coverage

测量模型和生成的代码的测试覆盖率

Polyspace® 产品

证明 C/C++ 代码中不存在严重的运行时错误

Simulink Design Verifier

识别设计错误、证明需求合规及生成测试

IEC Certification Kit

针对 IEC 62304 认证鉴定代码生成和验证工具

了解更多

这些资源将帮助您的团队快速掌握基于模型设计。

交互式教程

MATLAB 入门之旅

Simulink 入门之旅

Stateflow 入门之旅

Simscape 入门之旅

视频

Simulink 概述 (2:15)

使用 MATLAB 和 Simulink 进行基于模型的设计 (2:08)

Simulink 控制快速入门 (11:30)

现场或自定进度培训课程

MATLAB 基础

Simulink 系统和算法建模

使用 MATLAB 和 Simulink 进行控制系统设计

其他资源

咨询服务

MATLAB 和 Simulink 在医疗设备领域的应用