第一章 绪论

1.课题研究背景

随着工业规模的不断扩大，对于工业厂房的控制技术也变得越来越复杂。期初，各种控制面板分布到各个工业现场，需要大量的人力资源来维护这些相互独立的面板，但是这样不能对整个工业生产过程有一个全局的概览。随后人们发现，可以手动记录每个面板相关的生产信息，然后将其传输到控制中心，这样就可以让控制中心可以很容易的了解到各个底层生产间的状况，同时可以形成一个整体了解，然后做出相应的抉择。这种控制方式一般包含一个控制中心，多个分布在各处的控制点。控制点负责采集现场的实时生产情况，控制中心负责结合各个控制点反馈的实际数据，然后做出对应的处理。这种架构是很好的，但是存在着一个问题，那就是需要大量的人力资源，每个控制点将会配置一个以上的工人，负责记录数据以及执行相关的命令，同时还要周期地向控制中心上报数据。这样会导致两个问题，一是不能及时的将现场数据反馈给控制中心，使其及时地做出决定，这样就会使得有些紧急事件无法被恰当适时地处理，可能会造成整个生产流程的中断，从而导致巨大的损失。同时由于控制中心的工作人员会由于分析的不到位，导致不能得到有效的结果，因此可能会下达错误的命令。再则由于命令是由控制中心下达的，各个控制点可能不能及时的收到命令，因此造成命令不能按时执行，也有可能中断整个生产过程；二是在整个控制过程中，需要大量的人力资源，将会使得整个生产成本增加，同时由于人工操作会带来很多不确定性，因此大大影响了整个控制系统的可靠性和稳定性。

随着通信协议的不断成熟以及图形显示技术的发展，上述问题得到了解决。人们为每个控制点设计一套独立的控制系统，让其可以很好的监视生产状况，同时记录分析整个现场数据，并且可以独立的执行相关的命令。当然整个控制系统中也存在一个控制中心，负责监视整个生产过程。但是此时控制点和控制中心的数据交换已经不再通过人力进行，而是通过一些可靠的通信协议进行传输。由于图形显示技术的发展，以及计算机计算能力的提升，设计一套复杂的算法来对整个控制流程进行控制以及显示就变得现实和正确了。根据不同的工业的控制需求设计对应的控制算法，使得整个控制过程变得简洁可靠。可以看出这一次进步使得整个工业控制消除了上面提到的两个缺陷，同时还使得系统变得更可靠更安全。因为，由于不是由操作人员来进行数据传输，这样就使得生产情况可以及时的传达到控制中心以及控制命令可以迅速的发送到各个控制点；同时由于设计了高效的控制算法，使得数据可以预先得到有效的处理，这样决策人员就可以根据预处理出的结果做出更加精准的决定。

控制技术经过不断发展，整个工业控制已经达到了高度自动化。人们也总结出了整个工业控制的层次，这样更有利于对每个层次设计出高效的算法以及解决方案，同时也使得功能独立，降低了耦合性。一般工业控制操作分为五个层次：

* 工业现场(Field Level)：包含各种现场设备，包括温度传感器，各种终端控制器等。
* 直接控制层(Direct Control)：包含各种工业化的I/O模块，一般都带有自己的处理器。
* 工厂监控层(Plant Supervisory)：包含一台或多台监控计算机，它们负责从各个控制点收集数据，然后为监控人员展示整个生产状况的画面，同时将监控人员的命令下达到相应的控制点。
* 产品控制层(Production Control)：目标是对整个产品生产的全局监控，以及做出相关上层决策。
* 生产调度层(Production Scheduling)：对多条产品线进行安排。

其中工厂监控层是比较复杂的一层，主要的软件部分和计算部分都在这一层，因此是研究探索的核心。国外将其称为SCADA(Supervisory control and data acquisition)，国内对应地称作组态软件。其实这是一种控制系统架构，它利用计算机技术，网络数据交换协议和高层的图形化界面进行监控和管理，使得下层的可编程逻辑控制器的相关的终端控制器对生产现场进行直接控制。通过SCADA监控计算机系统，操作人员可以通过图形化操作界面来监视生产情况，同时还可以通过它向下层控制器设置相应参数，达到控制的目的。因此SCADA的核心理念就是为了找到一种通用的方法，使得能够和分布在各个地方的终端控制器通信，达到控制的目的。为此，随着科技的不断的发展，SCADA的结构也在不断的变化。到目前为止总共经历了四代变化：

* 集中式时代：早期的SCADA系统的计算任务是交给小型机来完成的，由于当时的通用网络服务还没有建立起来，因此只能用一些使用环境比较受限的通信协议，从而使得SCADA系统无法与外界或远程的系统交互，只能相对独立地工作。而且此时的SCADA系统一般会配置一台主机来进行数据备份，以防发生意外导致信息丢失，因此相应的系统也产生了，如数字设备公司(Digital Equipment Corporation)生产的PDP-11系列。
* 分布式时代：SCADA系统将信息和命令分发到各个站点，这些站点通过局域网连接起来，因此可以达到近似的实时性。每个站点将会负责与各自相关的特殊任务，与第一代SCADA系统相比将节省不少开支。但是由于网络协议还没有普及和标准化，局域网所用的传输协议是私有的，除协议的开发人员之外，很少有人能够正确的使用这些协议，因此会为SCADA系统带来一些安全隐患。
* 网络时代：相对于分布式时代，网络时代提供了功能完善的网络通信协议，使得其信息交互更加高效更加安全。而且对于那些跨度很大的SCADA系统，只有网络协议才能更好的满足其需求。同时将网络加入到SCADA系统中，可以使得几个平行的SCADA系统都能够进行交互，从而让控制范围更加大。
* 物联网时代：随着云计算技术的成熟，一些企业开始提供商业的云计算服务，SCADA系统也开始采用物联网的相关技术来缩减成本，增加系统的可整合性。因此使得SCADA系统可以近似实时的报告目前的状态，同时由于云服务环境的提供了良好的水平伸缩性，在这种环境下实现较为复杂的算法也变得更加容易。早先，SCADA系统的数据收集对于终端设备是采取一对一的映射的，后来发现这种方法比较笨拙，因此提出了数据模型这种解决方案。在数据模型中，每种设备在SCADA软件中都有与之相对应的虚拟表示，这种虚拟表示不仅可以反映设备的地址映射情况，而且还可以携带其它相关信息，那将非常有利于SCADA系统对设备的有效管理。

2.国内外研究现状

2.1组态软件简介

上文简要地介绍了SCADA系统，国内将其称为组态软件，两者在软件结构上是保持一致的，因此下文将统一使用组态软件来表示两者。组态软件拥有很好的伸缩性，小到只有几十个控制点的系统，大到上千控制点的系统，都可以通过组态软件进行组态，而且往往能够得到很好的成本效益。组态软件一般用在工业领域（如工业生产，过程控制，能源控制，加工等），基础设施领域（如水利，物流，灌溉系统，油气管道控制，电力传输等）和一些基于大型设施的处理过程（如楼宇，机场，船舶，太空站等）。

组态软件一般由以下几个部分组成：

1. **监控计算机：**这是整个组态软件系统的核心部分，涉及到计算机，负责与现场控制器通信的软件以及一个运行在操作台的人机交互软件。它汇集来自多个处理过程的数据，并且还要负责发送控制命令到各个现场设备。在稍小一些的组态软件运行系统中，监控计算机可能就只有一台PC机，人机交互界面是其中的一部分。而在稍大一些的组态软件运行系统中，整个监控中心可能会包含多个有显示界面的计算机，多台负责采集数据的服务器，一套分布式软件以及灾难恢复服务器。同时为了增强系统的可靠性，这些服务器还需要支持双冗余和热备份，从而可以使得在意外发生时，系统还能恢复控制与监视。
2. **远程终端单元：**也称作RTU(Remote terminal unit)，往下与各种传感器相连，往上通过网络与监控计算机相连。RTU作为一种智能I/O，往往具有独立的控制功能，如利用梯形图来完成布尔逻辑操作。
3. **可编程逻辑控制器：**即PLC(Programmable Logic Controller)，与RTU相同，往下与各种传感器相连，往上通过网络与监控计算机相连。但相比RTU，PLC具有更强的控制能力，而且支持一种或多种IEC 61131-3编程语言对其编程。由于PLC相较于RTU更加经济，更加通用，扩展性更好而且支持可配置，所以目前使用RTU的地方都被PLC替换掉了。
4. **通信设施：**即用于监控计算机系统和RTUs或PLCs之间的通讯模块，通常使用的是工业标准协议或制造商专有协议。通过监控计算机给出的最近的一条命令，RTUs或PLCs能够自主地完成控制操作，而且相当接近实时状态。同时通信设施还要保证，通信连接的部分损坏并不会影响整个工业生产过程的控制，而且一旦通信恢复，操作人员将能够继续进行监视和控制。此外一些关键的系统还会采用双冗余数据高速通路，即通过分离的路由器进行数据传输，从而保证通信的可靠性。
5. **人机界面：**即HMI(Human-Machine Interface)，监控系统的操作窗口。人机界面通过虚拟图表，警告页面，事件日志页面以及趋势图等构成。利用采集回来的数据，然后改变各种虚拟图表以及其他页面的状态，从而形成一个工业现场的概览图。一般人机界面是为操作人员准备的，其目的就是收集外部设备的数据，形成报告，发出相关警告，发送相关通知，从而达到一种集中控制。虚拟图表是由一些代表与处理过程相关的元素的线或符号组成的，往往随着数据的变化，形成一种动画的效果。对整个工业控制过程的操作也是通过人机界面完成的，一般设计鼠标操作，键盘操作或屏幕触摸。比如存在这样的一个例子，使用组态软件设计了一个抽水泵控制的系统，整个人机界面采用动画的形式展现这一过程，期间操作人员可以通过人机界面上的开关按钮来控制水泵的开关，当用鼠标点击关闭按钮，此时界面将显示出水泵关闭的效果，即水流量减少，实时地反馈到界面上。可以看出整个人机界面主要包含了两部分：现场情况反映，通过实时采集现场设备的数据，然后利用形象的动画，将其生动的展现给监控人员；控制现场，通过人机界面上的一些虚拟按钮，操作人员可以采取点击的操作，然后形成相应的命令，最后通过互联网络将其发送到工业现场，达到控制的目的。此外，人机界面还将为用户提供历史数据的浏览功能。
6. **报警处理：**是组态软件中比较重要的一部分。系统监视器将会不断地检测报警条件是否满足，而且还要决定何时可以触发一个报警事件。一旦一个报警事件被侦测到了，系统将会采取行动（如触发一个或多个报警指示器，邮件或短信通知远程管理人员等）。在多数情况下，组态软件运行系统的操作人员可以肯定某些报警事件的存在，但这也只能关闭部分报警指示器，一定要报警条件被清除，这时所有的报警指示器才可以关闭。报警条件一般分为两种：明确的报警条件，如报警条件是某个变量达到了某一确定数值，或通过一系列计算，得出了一个具体数值，从而满足了报警条件，其核心就是报警条件是非常明确的；不明确的报警条件，如某一数值达到某一范围，即会触发相应报警，此时报警条件是限制在某一范围的。报警指示器的目的是为了吸引操作人员的注意，以便使其做出恰当的操作，一般包括报警声，在屏幕上弹出一个警示框，或在屏幕相关区域进行特殊颜色的标识。
7. **PLC/RTU编程：**智能RTU或者标准的PLC都能够在没有监控计算机的干预下自主地执行一些简单的逻辑处理。这些设备都能使用标准化的控制编程语言进行编程，从而使其执行相关的处理逻辑。这类不像一些高级的编程语言，需要大量的专业知识才可以进行设计，它们往往语法简单，易于掌握。这就使得组态软件运行系统的工程师可以在RTU或者PLC上实现基础的控制算法，从而简化整个控制逻辑。

2.2组态软件发展趋势

如前文所述组态软件的概念源于SCADA，而SCADA主要是国外的产物，因此组态软件的发展也主要集中在国外，目前市场上比较知名的国外组态软件有Wonderware公司的InTouch，西门子公司的WinCC和Intellution公司的iFIX等；随着国内工控技术的累积与发展，同时借鉴了国外知名的组态软件，也出现了一批优秀的组态软件，如北京亚控公司的组态王，大庆三维公司的力控。国内的组态软件主要的优势在于本土化做得很好，同时积极吸取国外组态软件的优点，也使得自己的市场竞争力得到提升。

组态软件的发展主要体现在以下两个个方面：

* 运行平台：早期由于DOS系统比较盛行，组态软件主要运行在此操作系统下，由于此时的处理器大多是16位的，因此对应的组态软件也是16位的，这就大大限制了组态软件的功能，不能提供生动的图画显示，不能承载过多的计算，不能运行复杂的算法等等，同时所控制的设备数也受限制。随后随着Windows系列系统的诞生，处理器的升级，组态软件也朝着功能丰富化的方向发展，组态软件可以运行复杂的动画，可以模拟复杂的器件，可以实现复杂的控制算法，同时控制能力也得到大大提升。今后组态软件的发展是朝着多平台的方向发展的，要求不仅能够在传统的PC平台上运行，还要能够在移动设备上运行。
* 通信环境：起初组态软件的通信协议只是局限在一些商用的授权通信协议上，可互联的范围很小，随着网络技术的发展和成熟，组态软件也开始逐渐接纳TCP/IP协议，这就使得组态软件的控制范围可以跨越生产间、跨越工厂。随着云计算技术的发展，为了更好的管理数据，组态软件也开始采用云计算的概念，同时这样也为使用者节省了开支。

由于组态软件从使用一些私有的授权协议转为使用一些标准协议或一些开源的解决方案，同时大力提倡网络化，这虽然使得组态软件运行系统可以更好的互联，但同时也为网络攻击提供了方便之门。组态软件一般用在一些比较大型的设施中，如电力控制系统等，这些设施往往影响到人们生活的方方面面，如果一旦被攻击，将会造成巨大损失。

组态软件系统存在的威胁主要分为两类。一是未授权的得到控制权，通常是人为的或意外被病毒感染。二是通过网络途径攻击，通过网络将病毒植入系统或劫持替换控制命令来达到获取控制权的目的，因为这些控制协议没有使用加密技术。

组态软件的安全问题也成为组态软件研究的一个重要部分，因为组态软件一般在一些基础领域使用，如果发生意外，将会对人们的健康和安全造成影响，因此为此投入更多的研究是值得的。

3.课题研究意义

通过使用组态软件提供的相关控件，开发人员可以通过拖拉的方式来构造人机界面，然后利用参数配置框来对系统监控流程进行配置，同时加上适当的动画效果可以达到再现整个生成过程的目的，这就是组态软件的使用方式。整个过程中开发人员不会进行大量的编程工作，只需要对生产工艺有深刻的了解就可以开发出带有人机界面的控制系统。在组态软件产生之前，开发一个控制系统，一般是先分析整个控制流程，然后用高级语言进行开发，整个开发周期很长，而且人力物力消耗很大，最关键的还是伸缩性扩展性非常不好。如果遇到需求的变动，可能将会导致整个软件架构的变动，将会带来不能承受的损失。同时，由于每个系统都是独立开发的，有些具有相同功能的模块被多次开发，这样导致费时又费力。组态软件通过将通用功能进行模块化，提供良好的扩展性，使得可以被反复利用，同时由于这些模块都是经过反复验证过的，因此可靠性更高。

通过以上简述，研究组态软件的架构与实现是非常有意义的，这将为相关领域带来更好的效益。

但目前的组态软件也存在相应的问题，这也是本文探索的根基。

1. 价格高：目前组态软件一般是以控制点的数量来进行付费的。即将一个控制系统中需要监控的项目抽象成一个个控制点，然后决定使用哪种付费方式，即使采用这种按需付费的方式也将是难以承受的，一个小型的系统可能将会为此支付数万元，大一些的系统将支付数十万元。这还不包括开发费用，只是授权使用费而已。
2. 功能繁杂：目前的组态软件讲究的是大而全。整个组态软件开发系统很大，包含各种各样的图元、图标、虚拟仪表等，提供多领域的解决方案。由于包含的内容多，因此使用流程也变得复杂，为此需要投入更多的人力进行学习。
3. 平台限制：目前组态软件一般运行在Windows系统上，由于移动设备的不断发展，以及其运算功能的不断增强，希望组态软件能够运行在移动设备或Linux平台的需求越来越强烈。
4. 应用场景单一：目前组态软件主要应用在工业控制领域，基础设施领域和一些大型控制环境中。随着各种智能设备的增加，设备之间的交互也变得很重要了，因此组态软件的控制方式很实用。
5. 可扩展性限制：由于目前的组态软件都是商用产品，对外暴露的接口很少，如果想要对其进行二次开发根本是不可能的。因此这就限制了组态软件在一些特殊领域的使用。

本文主要探讨如何利用QT这个跨平台应用程序开发框架，来开发一款轻量型组态软件。由于QT是基于C++的，并且使用其提供的API进行相关开发，可以保证在不同平台上使用不同的编译器得到相应平台的可执行程序，这样就使得该款组态软件满足了多平台支持的特性。其次，该组态软件的设计主要完成的是其整体框架的构建，其它比较特殊的模块（如与特殊领域相关的一些控制算法）不进行设计，但为其留好了接口，这样方便开发人员可以对该组态软件进行二次开发。同时该组态软件由于主要利用TCP/IP协议进行通信，因此可以将其利用到其他领域，如智能设备互联等。

4.论文主要内容及结构

本文主要给出一种组态软件的设计方法，并在QT开发平台上将其实现。开发出的组态软件希望能够满足跨平台的工作特性，并且能够在多种应用场合中使用，同时具有良好的可扩展性，能够让使用者进行二次开发。由于时间与工作量的关系，本文将主要描述整体框架的设计与实现，一些与特殊行业相关的功能模块或解决方案并没有进行设计与实现，但是为开发者保留了接口，方便其根据现实需求来实现。

论文包括以下章节：

第一章：绪论。主要描述了组态软件产生的背景，然后介绍组态软件的发展历程，最后描述了目前组态软件存在的问题，然后围绕这些问题描述了本课题的研究意义。

第二章：组态软件的总体框架设计及相关技术研究。主要描述了组态软件的组成，然后讨论了开发实现的工具与技术，接着给出了一个总体设计框架。

第三章：组态软件开发系统的设计与实现。

第四章：组态软件数据库系统的设计与实现。

第五章：组态软件通信系统的设计与实现。

第六章：组态软件的测试。

第七章：总结与展望。