[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06F 17/00 (2006.01)*

# [12] 发明专利申请公开说明书

[21] 申请号 200480025365.4

[43] 公开日 2006 年 10 月 11 日

[11] 公开号 CN 1846206A

[22] 申请日 2004.1.16
[21] 申请号 200480025365.4
[30] 优先权
[32] 2003.9.19 [33] US [31] 10/666,446
[86] 国际申请 PCT/US2004/001205 2004.1.16
[87] 国际公布 WO2005/038544 英 2005.4.28
[85] 进入国家阶段日期 2006.3.3
[71] 申请人 费舍－柔斯芒特系统股份有限公司
地址 美国德克萨斯州
[72] 发明人 盖瑞·K·洛 大卫·L·底特兹
特雷费·邓肯·舒雷斯
朱利安·K·奈多

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 王 琦 宋志强

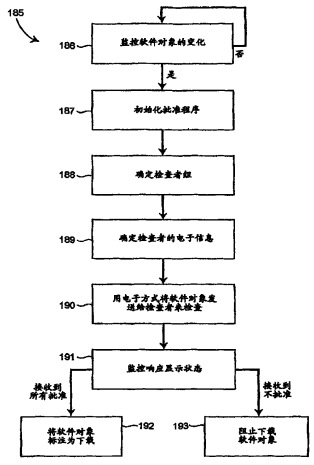
权利要求书 7 页 说明书 32 页 附图 16 页

[54] 发明名称

用于批准过程控制系统与安全系统软件对象的综合电子签名

[57] 摘要

本发明公开了一种软件对象批准系统，该系统与过程控制或安全系统环境相结合，尤其与过程控制或安全系统设计环境相结合，以执行和管理在该过程控制系统和安全系统环境内创建的新软件对象的电子批准。该软件对象批准系统用电子方式生成表示实体组的识别信息，在过程控制或安全系统内实施软件对象之前需要通过该实体组的批准。然后该系统可以将软件对象发送给这些实体，并从每个实体接收关于该软件对象的批准的电子指示。该批准系统阻止过程控制或安全系统实施该软件对象，直到该实体组内的每个实体均批准了该软件对象为止。



1. 一种在安全测量系统中使用的软件对象批准方法，该方法包括:

响应于在软件对象设计环境中对软件对象做出的改变，获取表示实体组的电子识别信息，在安全测量系统内实施软件对象之前需要通过该实体组的批准;

采用电子方式将用于检查该软件对象的请求发送给该实体组内的每个实体;

从该实体组内的每个实体中接收关于批准或不批准该软件对象的电子指示；和

阻止该软件对象在该安全测量系统内的实施，直到该实体组内的每个实体均提供批准该软件对象的电子指示。

2. 根据权利要求 1 所述的方法，其中用电子方式发送用于检查该软件对象的请求包括通过通信网络用电子方式通知该实体组内的每个实体。

3. 根据权利要求 2 所述的方法，其中用电子方式发送该请求包括向该实体组内的每个实体发送电子邮件消息。

4. 根据权利要求 1 所述的方法，其中阻止该软件对象在该安全测量系统内的实施直到该实体组内的每个实体均提供批准该软件对象的电子指示包括，如果该实体组内的每个实体均批准该软件对象，允许该软件对象被下载到该安全测量系统中。

5. 根据权利要求 1 所述的方法，其中获取表示实体组的电子识别信息包括确定风险降低因子，并基于该风险降低因子选择实体组。

6. 根据权利要求 5 所述的方法，其中获取表示实体组的电子识别信息包括用该风险降低因子确定安全测量级别，并基于所确定的安全测量级别选择实体组。

7. 根据权利要求 6 所述的方法，其中获取表示实体组的电子识别信息包括用该安全测量级别确定该实体组中的人员数目。

8. 根据权利要求 6 所述的方法，其中获取表示实体组的电子识别信息包括

用该安全测量级别确定该实体组中的人员的工作位置。

9. 根据权利要求 1 所述的方法，进一步包括对从该实体组内的一个或多个实体接收的关于批准或不批准该软件对象的电子指示进行记录。

10. 根据权利要求 1 所述的方法，其中获取表示需要其批准的实体组的电子识别信息包括提示设计者输入电子识别信息。

11. 根据权利要求 1 所述的方法，其中获取表示需要其批准的实体组的电子识别信息包括确定该实体组中的人员数目。

12. 根据权利要求 1 所述的方法，其中阻止该软件对象的实施包括阻止该软件对象被下载到控制环境中。

13. 根据权利要求 1 所述的方法，其中阻止该软件对象在该安全测量系统内的实施包括存储超驰密钥，并且使用户能够在该实体组内的每个实体均提供批准该软件对象的电子指示之前，使用该超驰密钥来下载该安全测量系统中的软件对象。

14. 根据权利要求 1 所述的方法，进一步包括检测何时在该软件对象设计环境中对该软件对象做出改变。

15. 根据权利要求 14 所述的方法，其中检测何时在该软件对象设计环境中对该软件对象做出改变包括，当对该软件对象做出改变时，改变与该软件对象相关的版本号。

16. 根据权利要求 14 所述的方法，其中检测何时在该软件对象设计环境中对该软件对象做出改变包括，检测何时在该软件对象设计环境中创建新的软件对象。

17. 根据权利要求 14 所述的方法，其中检测何时在该软件对象设计环境中对该软件对象做出改变包括，检测用户何时在该软件对象设计环境中初始化批准程序。

18. 根据权利要求 1 所述的方法，进一步包括为测试目的监控软件对象，以确定用于该软件对象的测试何时逾期。

19. 根据权利要求 18 所述的方法，其中确定用于该软件对象的测试何时逾

期包括在用于该软件对象的测试逾期之后，为该软件对象计算新的风险降低因子，并将该新的风险降低因子与该软件对象的原风险降低因子比较。

20. 根据权利要求 18 所述的方法，进一步包括当用于该软件对象的测试逾期时，生成要被发送给用户的告警信号。

21. 根据权利要求 18 所述的方法，进一步包括当用于该软件对象的测试逾期时，生成要被发送给用户的工作定单。

22. 一种在包括处理器的过程控制系统中使用的软件对象批准系统，该软件对象批准系统包括:

计算机可读介质；和

软件，被存储在该计算机可读介质上，并且适于由该处理器执行，以:

在软件对象设计环境中对该软件对象做出改变之后，获取表示实体组的电子识别信息，在过程控制系统内在线实施该软件对象之前需要通过该实体组的批准;

用电子方式将用于检查该软件对象的请求发送给该实体组内的每一个实体;

从该实体组内的每个实体接收关于批准或不批准该软件对象的电子指示；和

阻止该软件对象在该过程控制系统内的实施，直到该实体组内的每个实体均提供批准该软件对象的电子指示。

23. 根据权利要求 22 所述的软件对象批准系统，其中该软件通过向该实体组内的每个实体发送电子邮件消息来用电子方式发送请求。

24. 根据权利要求 22 所述的软件对象批准系统，其中该软件通过确定风险降低因子，并基于该风险降低因子选择实体组，来获取表示该实体组的电子识别信息。

25. 根据权利要求 24 所述的软件对象批准系统，其中该软件通过用该风险降低因子确定安全测量级别，并基于所确定的安全测量级别选择实体组，来获取表示该实体组的电子识别信息。

26. 根据权利要求 25 所述的软件对象批准系统，其中该软件通过基于该安全测量级别确定该实体组中的人员数目，来获取表示该实体组的电子识别信息。

27. 根据权利要求 25 所述的软件对象批准系统，其中该软件通过基于该安全测量级别确定该实体组中的人员的工作位置，来获取表示该实体组的电子识别信息。

28. 根据权利要求 22 所述的软件对象批准系统，其中该软件记录从该实体组内的一个或多个实体接收的关于批准或不批准该软件对象的电子指示。

29. 根据权利要求 22 所述的软件对象批准系统，其中该软件通过提示设计者输入电子识别信息，来获取表示需要其批准的实体组的电子识别信息。

30. 根据权利要求 22 所述的软件对象批准系统，其中该软件检测何时在该软件对象设计环境中对该软件对象做出改变。

31. 根据权利要求 30 所述的软件对象批准系统，其中该软件通过检测何时在该软件对象设计环境中创建新的软件对象，来检测何时在该软件对象设计环境中对该软件对象做出改变。

32. 根据权利要求 30 所述的软件对象批准系统，其中该软件检测用户何时在该软件对象设计环境中初始化批准程序。

33. 根据权利要求 30 所述的软件对象批准系统，其中当该软件检测到在该软件对象设计环境中对该软件对象做出改变时，该软件改变与该软件对象相关的版本号。

34. 根据权利要求 22 所述的软件对象批准系统，其中该软件存储超驰密钥，并且使用户能够在该实体组内的每个实体均提供批准该软件对象的电子指示之前，使用该超驰密钥来下载该过程控制系统中的软件对象。

35. 根据权利要求 22 所述的软件对象批准系统，其中当该软件对象为测试目的被下载到该过程控制系统时，该软件还监控该软件对象，以确定用于该软件对象的测试何时逾期。

36. 根据权利要求 35 所述的软件对象批准系统，其中该软件在用于该软件对象的测试逾期之后，通过为该软件对象计算新的风险降低因子，来确定用于

该软件对象的测试何时逾期，并将该新的风险降低因子与该软件对象的原风险降低因子比较。

37. 根据权利要求 36 所述的软件对象批准系统，其中当用于该软件对象的测试被确定为逾期时，该软件还生成要被发送给用户的告警信号。

38. 根据权利要求 36 所述的软件对象批准系统，其中当用于该软件对象的测试被确定为逾期时，该软件还生成要被发送给用户的工作定单，该工作定单指定要为该软件对象执行的测试。

39. 根据权利要求 22 所述的软件对象批准系统，其中该软件对象是被用于在该过程控制系统中实施安全程序的安全系统软件对象。

40. 一种在具有一个或多个处理器的加工厂中的过程控制或安全测量系统中使用的批准系统，该批准系统包括:

计算机可读介质;

第一例行程序，被存储在该计算机可读介质上，并且适于在该一个或多个处理器上执行，以响应于对软件对象做出的改变，用电子方式将用于检查该软件对象的请求发送给该实体组内的每一个实体；和

第二例行程序，被存储在该计算机可读介质上，并且适于在该一个或多个处理器上执行，以阻止该软件对象在该过程控制或安全测量系统中的实施，直到该实体组内的每个实体均提供批准该软件对象的电子指示。

41. 根据权利要求 40 所述的批准系统，进一步包括第三例行程序，其适于在该一个或多个处理器上执行，以获取表示该实体组的电子识别信息，在该过程控制或安全测量系统内实施该软件对象之前需要通过该实体组的批准。

42. 根据权利要求 41 所述的批准系统，其中该第三例行程序适于通过确定风险降低因子并基于该风险降低因子选择实体组，来获取表示该实体组的电子识别信息。

43. 根据权利要求 42 所述的批准系统，其中该第三例行程序适于通过用该风险降低因子确定安全测量级别，并基于所确定的安全测量级别选择实体组，来获取表示该实体组的电子识别信息。

44. 根据权利要求 43 所述的批准系统，其中该第三例行程序适于通过基于该安全测量级别确定该实体组中的人员数目，来获取表示该实体组的电子识别信息。

45. 根据权利要求 43 所述的批准系统，其中该第三例行程序适于通过基于该安全测量级别确定该实体组中的人员的工作位置，来获取表示该实体组的电子识别信息。

46. 根据权利要求 40 所述的批准系统，其中该第一例行程序适于通过向该实体组内的每个实体发送电子邮件消息，来用电子方式发送请求。

47. 根据权利要求 40 所述的批准系统，其中该第二例行程序适于记录从该实体组内的一个或多个实体接收的关于批准或不批准该软件对象的电子指示。

48. 根据权利要求 40 所述的批准系统，包括第三例行程序，其适于在该一个或多个处理器上执行，以通过提示人输入电子识别信息，来获取表示需要其批准的实体组的电子识别信息。

49. 根据权利要求 40 所述的批准系统，其中该第二例行程序适于存储超驰密钥，并且使用户能够在该实体组内的每个实体均提供批准该软件对象的电子指示之前，使用该超驰密钥来下载该过程控制安全测量系统中的软件对象。

50. 根据权利要求 40 所述的批准系统，包括第三例行程序，其被存储在该计算机可读介质上，并且适于在该一个或多个处理器上执行，以检测何时对软件对象做出改变。

51. 根据权利要求 50 所述的批准系统，其中该第三例行程序适于响应于检测对该软件对象做出的改变的该第一例行程序，改变与该软件对象相关的版本号。

52. 根据权利要求 50 所述的批准系统，其中该第三例行程序适于通过检测何时在软件对象设计环境中创建新的软件对象，来检测何时对该软件对象做出改变。

53. 根据权利要求 50 所述的批准系统，其中该第三例行程序适于通过检测用户何时在该软件对象设计环境中初始化批准程序，来检测何时对该软件对象

做出改变。

54. 根据权利要求 40 所述的批准系统，进一步包括第三例行程序，适于在该一个或多个处理器上执行，以便为测试目的而监控正在该过程控制或安全测量系统中在线操作的软件对象，以确定用于该软件对象的测试何时逾期。

55. 根据权利要求 54 所述的批准系统，其中该第三例行程序适于在用于该软件对象的测试逾期之后，通过为该软件对象计算新的风险降低因子，并通过将该新的风险降低因子与该软件对象的原风险降低因子比较，来确定用于该软件对象的测试何时逾期。

56. 根据权利要求 55 所述的批准系统，其中该第三例行程序适于当该新的风险降低因子与原风险降低因子相差特定量时，生成要被发送给用户的告警信号。

57. 根据权利要求 55 所述的批准系统，其中该第三例行程序适于当该新的风险降低因子与原风险降低因子相差特定量时，生成要被发送给用户的工作定单，该工作定单指定要为该软件对象执行的测试。

# 用于批准过程控制系统与安全系统软件对象的综合电子签名

## 相关申请

本申请是部分后继申请，要求2002年8月2日提交的标题为“用于批准过程控制系统软件对象的综合电子签名”的未决美国专利申请No. 10/211,903的优先权，其全部内容被专门合并于此以资参考。

## 技术领域

本申请涉及过程控制系统，更具体地讲，涉及在过程控制系统中使用的软件对象的批准。

## 背景技术

过程控制系统通常包括用来执行某些制造加工过程或其他控制过程的许多套设备。该多套设备耦合至多个控制器，该控制器包括以某些方式操控设备的过程控制软件指令，以完成制造加工或控制过程。过程控制软件可以实现为在控制器（或其他计算机）上运行以执行任何控制功能的软件对象。例如，在某些过程控制环境中，可以对软件对象进行布置以实施不同的执行阶段，这些执行阶段一般与各种类型的过程步骤相关。特别地，执行混合阶段的软件对象可以与执行过程的混合步骤的硬件相关。应该明白，实施某一执行阶段的每个软件对象均执行某些分立功能，并且与其他对象进行通信以执行更复杂的控制程序。

当定义或创建要在例如成批处理中使用的控制程序时，工程师可以从模板软件对象开始，其中具有通配控制逻辑以实现特定的功能，例如成批处理中的执行阶段。由于这些模板软件对象的通配属性，在用于特定的过程控制环境之前，必须基于它们要执行的步骤的详细情况来修改或定制这些软件对象。例如，通常适于操作混合设备的混合阶段，必须进行定制以便在特定的持续时间内，

以特定的速度来操作特定的一台混合设备。处方（recipe）一般用来定制或修改执行阶段。正如其名称所暗含的，处方包括下载到过程控制硬件上的多组指令，用于执行专门的任务，例如制作饼干，生产药品或控制其他过程。处方通常比阶段更具体，并且实际上包括其中各个阶段的使用。例如，饼干制作处方可能包括可以由混合阶段执行的混合步骤。然而，与混合阶段相比，该饼干制作处方指定了混合应当执行的持续时间和速度。因此，处方指定了定义混合阶段操作的参数。

以类似的方式，可以创建用在安全测量系统（safety instrumented system）中的软件对象，该安全测量系统用来在由分离过程控制系统控制的加工厂中提供安全或停工程序，或其他安全相关功能。典型地，安全测量系统可以拥有一个或多个可编程的安全控制器，通过使用安全相关的软件对象，来检测该加工厂内的有危害的、危险的或不合需要的情况，以便在检测到这样一种情况时，采取某些行动，例如停止该过程、转变过程内的流向、撤除电力，等等。

可以容易地理解，改变由过程控制系统执行的处方或改变安全系统软件对象会强烈地影响过程控制系统或安全系统的操作。例如，下载已经被意外改变的、或以另外的未经授权方式而变化的处方，可能会该加工厂的输出带来有害的影响，从而导致生产出不符合产品规范的产品，并最终造成利润的损失。尽管用于诸如饼干之类的产品的处方（可以实现为软件对象）的改变可能生产出明显有缺陷的饼干（例如，未充分烹调、未带有足够的巧克力夹心，等等），但不是所有的处方变化都将导致生产出具有立即可察觉的缺陷的产品。例如，加有过多盐的饼干在生产过程中可能并不容易发现。然而，顾客可能注意到饼干的咸度，并可能对制造商表示不满及抱怨，这就可以确定用于饼干的处方发生了不可接受的变化，从而导致了饼干的召回。然而，在类似饼干生产的情况下，未经授权的处方变化最坏也就是造成顾客的不满，而用于例如药品生产的未经授权的处方变化可能具有更加严重的问题。特别地，改变了药物质量或组分的处方变化可能会造成所得到的药物无效或毒性。因此，与饼干中的巧克力夹心的质量不同，药物组分的变化是不容易检测到的，因为药物可能看起来与未发

生变化或正当制造的药物具有相同的颜色和稠度。

以类似的方式，在安全系统中使用的软件对象的未经授权或不正确的变化，可能会导致未被检测的危险情况，或者导致响应于危险情况而采取的不正当操作，这对于在该工厂附近工作或生活的人们来说可能是危及生命的，而根本不用提及对工厂自身的危害。因此，当实际上并不存在危险情况时，发生故障的安全系统软件对象可能会错误地检测到危险情况，并关闭工厂。

由于工厂的生产线通常涉及生产能力、时间和/或原材料中的重大投资，因有缺陷的处方或安全系统有故障的启动而不得不报废正处于进行中的生产，可能会对执行该生产过程的实体以及被期待接收由该生产过程生产的产品的其他实体，产生实质上不利的财政冲击。例如，用于制作诸如酒、啤酒、乳酪等涉及发酵产品的处方，经常需要几周或几个月的过程处理时间，以及大量的原材料投资。

通常，用于过程控制系统的处方以及包括安全系统软件对象的其他软件模块或对象由工程师或科学家来书写，这些工程师或科学家要求诸如研究或生产小组等各种实体在将其下载到过程控制系统或安全系统之前，批准该处方或安全系统软件。然而，过程控制系统软件的批准过程通常通过流通备忘录或批准请求，在某些情况下通过以更加不正式的方式请求输入来实现的。此外，除了过程控制系统与其中执行的处方或其他软件对象的应用知识以外，很少有障碍来阻止将未经批准的软件下载到过程控制系统或安全系统，以便在加工厂内在线使用。

在使用安全测量系统的设备工厂中，例如石油和天然气提炼等，已经试图执行标准操作程序（SOP），其要求来自于组织的一个或多个个体在该软件可以在生产系统中执行之前，手动地表示出它们对特定软件的批准。实际上，标准草案 IEC615511 除了定义不同的批准级别来区分安全完善级别（SIL）之外，还要求这样的批准。例如用于设备工厂的生效计划可以包括 SOP，该 SOP 要求如果 SIL 是 2 级或 2 级以下，安全测量系统执行的安全功能由相同部门的同级来批准，而如果 SIL 是 3 级或 3 级以上，要求由不同部门的同级来批准。

众所周知，SIL 是在 IEC61508 标准中定义的措施，其定义了关于当假设要做一件事时，能够对该系统做出假设它要做的事情指望多少的系统完善性。更具体地，SIL 用提出要求时失败的平均可能性（PDFavg）来定义。与 PFDavg 的倒数相关的风险降低因子，定义了使用安全测量功能之前的过程风险与常常为该过程或该台设备而实现的风险“可容许量”之间的差值。基本上，风险降低因子是“绝对风险”，其不具有除以所建立的“可容许风险”的安全测量函数。风险降低因子和 SIL 都是为安全系统内的每个不同安全测量功能定义的，其中将各个安全测量功能设计为识别需求，然后针对每个危险情况，将系统带至安全状态。

在已经实施了安全测量功能批准过程的设备工厂中，批准通常是利用包括手动途径和电子途径在捏的两个可能途径之一来处理的。在手动途径中，要批准的软件对象的打印复本（即安全功能软件的打印复本）被手动地发送给每个批准者以进行检查，并且以纸件格式手动地收集所有的批准签名。在电子途径中，电子文档管理系统用来将软件对象的电子版本（即描述该软件的一系列屏幕截图，或其他基于文本和图形的文件）发送给所要求的批准者以进行检查。在这种情况下，以电子格式收集所有的批准签名。

然而，这两种途径都具有严重的缺陷。特别是，在文档批准过程和软件执行的安全测量系统之间没有直接链接。由于文档批准过程出现在安全测量系统外部，因此批准者不能检查请求他们在其本地环境中（例如在安全测量系统内部）批准的软件对象，并因此可能存在关于正在检查的文档的正确性的问题。此外，由于文档批准过程出现在安全测量系统或与之相关的设计系统外部，因此在安全测量系统内部不存在这样的机制，其能够保证未经批准的软件对象不能执行，直到所有批准完成为止；或者其能够保证如果软件对象发生了变化的话，用于该软件对象的所有先前批准都要宣告无效（即该软件转变为未经批准的状态）。

另外，分离的批准和安全设计系统使得系统不可能在该软件对象的软件开发检查追踪内保存批准的记录。而且，由于批准系统未链接至安全测量系统，

因此两个系统都必须独立地进行验证，这将是耗时且重复的。

发明内容

一种软件对象批准系统被与过程控制或安全系统环境相结合，更具体地说，与过程控制或安全系统设计环境相结合，以执行和管理该过程控制系统和安全系统环境内创建的新软件对象的电子批准。例如，一种在过程控制系统和/或安全系统中使用的系统和方法，用电子方式生成表示实体组的识别信息，在该过程控制或安全系统内实施软件对象之前需要先通过该实体组的批准。该系统和方法可以从该识别信息内表示的每个实体接收关于该软件对象的批准的电子指示，并且可以阻止该过程控制或安全系统执行该软件对象，直到该识别信息内表示的每个实体均批准了该软件对象为止。此外，该系统和方法可以选择性地使该过程控制或安全系统能够基于该电子指示执行该软件对象。

在该过程控制或安全系统中使用的软件对象批准系统和方法也可以或替代地响应于接收多个实体中至少一个未批准该软件对象的电子指示，或者当该软件对象以某种方式发生改变和变化时的电子指示，来确定该软件对象未得到批准。其后，该系统和方法可以响应于接收到多个实体中的每一个均批准了该软件对象的另一电子指示，来确定该软件对象得到了批准，并且响应于该批准，该系统和方法能够将该软件对象下载到该过程控制或安全系统中。

附图说明

图 1 是过程控制系统的局部方框图，其中包括综合电子软件对象批准系统，以便批准执行过程设备的控制的一个或多个控制软件对象；

图 2 是对象结构的方框图，示出图 1 中过程控制系统的典型逻辑分级或构造；

图 3 是更为详细的方框图，更加详细地示出图 2 中对象结构的一部分；

图 4 是具有与过程控制系统相结合的安全系统的示例性加工厂的方框图，其中该安全系统包括综合电子软件对象批准系统；

图 5A 和 5B 是批准例行程序的示例性流程图；

图 6 是软件对象编辑器例行程序的示例性流程图；

图 7 是授权建立例行程序的示例性流程图；

图 8 是与图 7 中授权建立例行程序相关的示例性用户界面；

图 9 是添加例行程序的示例性流程图；

图 10 是与图 9 中添加例行程序相关的示例性用户界面；

图 11 是删除例行程序的示例性流程图；

图 12 是修改例行程序的示例性流程图；

图 13 是与图 12 中修改例行程序相关的示例性用户界面；

图 14 是软件对象授权例行程序的示例性流程图；

图 15 是与图 14 中软件对象授权例行程序相关的示例性用户界面；

图 16 是批准例行程序的示例性流程图；

图 17 是与图 16 中批准例行程序相关的示例性用户界面；

图 18 是拒绝例行程序的示例性流程图；

图 19 是示出未经批准的软件对象状态的示例性用户界面；和

图 20 是下载例行程序的示例性流程图。

具体实施方式

下面将详细描述用于用电子方式控制软件对象的批准和下载的方法和系统，该软件对象例如是安全测量系统内过程控制系统或软件例行程序中的处方，并且上述方法和系统可以用来使软件对象的作者能够自动地和/或用电子方式获取检查人员或小组的批准，该检查人员或小组必须在对象被下载到过程控制系统或安全测量系统之前，或者在过程控制系统或安全测量系统中执行之前，对该软件对象进行授权。这些方法和系统使检查者能够在将要使用它的环境中检查软件对象，从而所检查的软件对象尽可能的准确。另外，由于该批准系统与过程控制或安全系统设计环境相结合，因此该批准系统能够提供一种机制，以确保未经批准的软件对象不能够执行，直到所有的批准完成为止，并且确保

如果软件对象发生了变化，则用于该软件对象的所有先前批准都要被宣告无效（即该软件转变为未经批准的状态）。另外，该综合软件对象批准系统使过程控制或安全系统有可能在该软件对象的软件开发检查追踪内保存批准的精确记录。

如果需要的话，可以通过大量不同的技术来通知软件对象的检查者或签署者，并且基于该通知，检查者和签署者可以检查该软件对象，并批准或拒绝该软件对象。如果每个检查者均批准该软件对象，则该软件对象可被下载到过程控制系统或下载到安全测量系统上。附加功能可以包括使各类人员或实体（例如检查者、作者、商业小组或其他人）能够检查软件对象的批准状态，如果该软件对象发生变化则自动地移除授权，当发生变化时自动地改变该软件对象的版本，等等。

尽管借助于以下例子，将软件对象批准系统和方法描述为用于过程控制系统内处方的批准和下载，或者用于安全系统环境内软件对象的批准和下载，但是此处描述的系统和方法也可以有利地用于其它类型的软件对象，例如其他过程控制环境中的单元、阶段（phase）、图形等等。此外，此处借助于例子描述的软件对象批准系统和方法，可以用于批准和下载单一的软件对象，和/或在相同时期或不同时期批准和下载一组相关或无关的软件对象。

另外，应当容易理解，此处描述的软件对象批准系统和方法可以有利地连同版本控制元件一起使用。在标题为“过程控制系统中的版本控制和检查追踪”的美国专利 No. 6,449,624 中公开了一个示范类型的版本控制软件，其全部内容专门被合并于此以资参考。

现在参见图 1，示例性过程控制系统 10 包括通过以太网连接 15 耦合至多个工作站 14 的多个控制器 12。这些控制器 12 也通过一组通信线路或总线 19 耦合至与过程相关的设备或装置（用附图标记 16 概括标明）。仅作为举例，可以是艾默生过程管理公司销售的 DeltaV™ 控制器的多个控制器 12，能够与控制元件进行通信，例如在整个过程 16 内分布的现场设备及现场设备内的功能块，执行最好利用面向对象的编程技术来实施的一个或多个过程控制例行程序或软

件对象，从而实现过程 16 的所需控制。工作站 14（例如，可以是个人计算机）可以包括设计软件 17，设计软件 17 由一个或多个工程师或其他用户用来设计要由控制器 12 执行的过程控制例行程序或软件对象，从而与控制器 12 进行通信，以下载这些过程控制例行程序或软件对象，并在过程 16 的操作期间接收和显示有关过程 16 的信息。另外，批准软件 18 能够以可通信联络的方式连接至设计软件 17 并与之结合为一体，以提供使用设计软件 17 设计或修改的处方或其他过程控制例行程序或对象中任意一个的批准。

每个工作站 14 均包括存储器 20，用于存储诸如配置设计应用程序之类的应用程序，并用于存储诸如有关过程 16 配置的配置数据之类的数据。每个工作站 14 还包括处理器 21，其执行应用程序 17 和 18 以使用户能够设计和/或修改过程控制例行程序或软件对象，并能够将这些过程控制例行程序或软件对象下载到控制器 12 中。同样，每个控制器 12 均包括存储器 22，用于存储配置数据和要被用于控制过程 16 中的过程控制例行程序，并且包括处理器 24，其执行过程控制例行程序以实施过程控制策略。如果控制器 12 是 DeltaV 控制器，那么它们可以通过工作站 14 中的一个向用户提供控制器 12 内过程控制例行程序的图形描绘，这些工作站 14 阐明了过程控制例行程序内的控制元件，以及配置这些控制元件来提供过程 16 的控制的方式。

图 1 中的系统 10 还可以包括网络 30，一个或多个工作站可以连接至该网络。网络 30 可以使用任何合适的网络来实现，例如因特网、内联网、局域网（LAN）、广域网（WAN）或任意其他合适的网络。尽管将网络 30 表示为具有硬连线连接，应当容易理解，这样的网络可以是无线网络，或者可以是既包括硬连线部分也包括无线部分的网络。

大量终端 32 也可以通过网络 30 连接到工作站 14 上。每个终端 32 均可以包括耦合至处理器 36 的存储器 34，该处理器 36 适于执行被存储在存储器 34 上的指令。在一个示例性实施例中，终端 32 可以是个人计算机或任意类似的处理设备，与当今已知的常规个人计算机中可得到的相比，该处理设备可以包括相同或更多的处理能力和存储器。

回到对图 1 的过程控制系统 10 的说明，控制器 12 通过总线 19 以可通信联络的方式连接至三组类似配置的反应器，在这里称为反应器_01、反应器_02 和反应器_03。反应器_01 包括反应器容器 100、两个输入阀门 101 和 102 以及输出阀门 103，两个输入阀门连接至向反应器容器 100 提供流体的控制流体输入管线，而输出阀门通过流体输出管线连接至反应器容器 100 的控制流体流出口。设备 105，其可以是例如温度传感器、压力传感器、液面表等的传感器，或者是诸如电子加热器或蒸气加热器的某些其他设备，在反应器容器 100 中或被布置为靠近反应器容器 100。同样，反应器容器_02 包括反应器容器 200、两个输入阀门 201 和 202、输出阀门 203 和设备 205。同样，反应器容器_03 包括反应器容器 300、两个输入阀门 301 和 302、输出阀门 303 和设备 305。如图 1 所示，多个控制器 12 通过总线 19 以可通信联络的方式耦合至阀门 101－103、201－203 和 301－303，并且耦合至设备 105、205 和 305，以控制这些元件的操作，从而执行关于反应器单元的一个或多个操作。这些操作可以包括诸如注满反应器容器、加热反应器容器内的原料、倾倒反应器容器、清洗反应器容器等等。

图 1 所示的阀门、传感器和其他设备可以是任意所需种类或类型的设备，包括例如现场总线（Fieldbus）设备、标准 4－20mA 设备、HART 设备等，并且可以使用任意已知或所需的通信协议与控制器 12 相互通信，例如现场总线协议、HART 协议、4－20mA 模拟协议等。另外，其他类型的设备可以连接至控制器 12 并由控制器 12 来控制。并且，其他控制器也可以连接至控制器 12，并通过以太网通信链路 15 连接至工作站 14，以控制与过程 16 相关的其他设备或区域，而这些附加控制器的操作可以按照任意所需的方式，与图 1 所示控制器 12 的操作协同一致。

一般而言，图 1 的过程控制系统 10 可以被用来执行成批处理，举例来说，其中工作站 14 或控制器 12 之一执行成批执行的例行程序 40，该例行程序是高级控制例行程序，其指示一个或多个反应器单元（以及其他设备）的操作来执行生产产品的一系列不同步骤（通常称为阶段），该产品例如是食品、药物或其他药品，等等。这些步骤或阶段通常使用软件对象来实施，这些软件对象能够

被下载到系统 10 内的一个或多个处理器 21 和 24 之中，并由它们进行初始化和执行。

为了实施不同阶段，成批执行的例行程序 40 使用通常被称作处方的东西，它是一种软件对象，指定要执行的步骤、与这些步骤相关的数量和次数以及这些步骤的序列。用于一个处方的步骤可能包括，例如，用适当的材料或配料注满反应器容器、混合反应器容器内的材料、在一定量的时间内将反应器容器内的材料加热到某一温度、腾空反应器容器并随后清洗该反应器容器以准备下一次成批运行。每一个步骤均定义了成批运行的阶段，而成批执行的例行程序 40 能够使控制器 12 对这些阶段中的每一个执行不同的控制算法。当然，专门的材料、材料的总量、加热温度和时间等对于不同的处方可以是不同的，并因此这些参数可以取决于所加工制造或生产的产品和所使用的处方，一个成批运行一个成批运行地发生变化。本领域技术人员能够理解，尽管此处为图 1 所示反应器单元中的成批运行描述了控制例行程序和配置，但是如果需要的话，这些控制例行程序可以用来控制其他所需设备，以执行任意其他所需的成批处理过程运行，或执行持续的处理过程运行。

在高级层面，在操作的相关部分中，位于工作站 14 之一的人员或实体可以使用设计软件 17 来创建或修改处方或其他软件对象，并且批准软件 18 可以用电子方式请求来自于各种授权实体的批准，例如生产、工程技术、质量保证或管理。授权实体可以使用工作站 14 或终端 32 来检查所讨论的处方和/或其他软件对象，并批准或拒绝该处方和/或其他软件对象。所讨论的软件对象的批准和拒绝可以传达给请求该对象批准的人员或实体，或者传回批准例行程序 18，批准例行程序 18 能够追踪谁批准了该软件对象，谁没有批准该软件对象。一旦软件对象得到了请求他们来批准的所有实体的批准，批准例行程序 18 就使得该软件对象能够被下载到多个控制器 12 之一，或者被下载到成批执行的例行程序 40 中，以用于过程控制系统 10 内的实施或执行。

图 2 的对象树示出了软件对象的例子，该软件对象可以用与批准软件 18 协同工作的设计软件 17 来创建和下载。图 2 的软件对象仅作为软件对象（除了上

述处方之外）的例子而提供，其可以使用此处描述的综合电子批准系统来创建和批准，当然也可以使用该系统来创建和批准其他软件对象。使用软件例行程序来实施的图 2 的软件对象用方框来图示，而在没有方框的树中的对象上面显示对象的一般类别（或对象类型）。如图 2 所示，过程控制系统 10 包括一个或多个区域，例如可以是加工厂内的建筑物或其他地理区域标志。在图 2 的对象树中，过程 16 拥有被命名为建筑物_01、建筑物_02 和建筑物_03 的三个区域对象。每一个区域均可以分为多个过程单元，每一个过程单元对应于在该区域中执行的过程的不同方面。图 2 的建筑物_01 区域对象被示为包括标记为单元_01 和单元_02 的两个过程单元对象。举例来说，单元_01 可能会涉及单元_02 中所用产品组分的制造。每个单元对象均可以包括零个或更多单元分类，该单元分类标识过程单元中所用硬件的类别或分组。一般而言，单元分类是拥有一组相关设备的共同配置的指名对象，并且更具体地说，是具有即使不完全相同也非常类似的生产过程用检测仪表的单元的集合，它们中的每一个均执行即使不完全相同也非常类似的过程内功能。通常将单元分类对象命名为描述它们所属的过程控制系统内单元的类型。图 2 包括混合_罐（Mix_Tank）分类、反应器单元分类和进料_罐（Feed_Tank）分类。当然，在大多数过程控制系统或网络中，可以提供或定义许多其他类型的单元分类，包括例如干燥器单元、进料头单元和硬件的其他独立或逻辑分组。

如图 2 的反应器单元所示，每个单元分类对象可以具有单元模块对象，和与之相关的阶段分类对象。单元模块对象一般指定所指名单元分类内重复硬件的某些情形，而阶段分类一般指定能够应用于与单元分类相关的单元模块的阶段。更具体地，单元模块对象是拥有用于单一过程单元的所有变量和单元阶段（在此后定义）的指名对象，并且通常被命名以标识专门的过程设备。例如，图 2 的反应器单元分类具有反应器_01、反应器_02 和反应器_03 单元模块，其分别对应于图 1 所示的反应器_01、反应器_02 和反应器_03。混合_罐单元分类和进料_罐单元分类同样具有对应于过程 16 内特定硬件或设备的特定单元模块。然而，为了简便起见，与混合_罐和进料_罐单元分类相关的设备均没有在

图 1 中示出。

阶段分类是一个指名对象，其拥有能够在属于相同单元分类的多个单元上运行的阶段，以及能够在多个不同单元分类上运行的阶段的共同配置。大体上，每个阶段分类均为不同的控制例行程序（或阶段），它由控制器 12 创建和使用，以控制相同或不同单元分类内的单元模块。通常，每个阶段分类均根据动词来命名，该动词描述了在单元模块上执行的动作。例如，如图 2 所示，反应器单元分类具有填充阶段分类，该阶段分类用来填充图 1 中的反应器容器 100、200 或 300 中的任意一个；加热阶段分类，该阶段分类用来加热图 1 的反应器容器 100、200 或 300 中的任意一个；倾倒阶段分类，该阶段分类用来腾空图 1 的反应器容器 100、200 或 300 中的任意一个；以及清洗阶段分类，该阶段分类用来清洗图 1 的反应器容器 100、200 或 300 中的任意一个。当然，可以有与该单元分类或任何其他单元分类相关的任何其他阶段分类。填充阶段分类既与反应器单元分类相关又与进料_罐单元分类相关，因此能够用来执行反应器单元模块以及进料_罐单元模块上的填充功能。

阶段分类通常可以看作是软件例行程序或对象，其可以由成批执行的例行程序来调用以执行由该成批处理过程的处方定义的整个成批处理过程所需的某些功能。阶段分类可以包括零个或多个阶段输入参数，该输入参数基本上是从该成批执行的例行程序或另一阶段分类提供给阶段分类软件例行程序或对象的输入；零个或多个阶段输出参数，该输出参数基本上是传回给该成批执行的例行程序或另一阶段分类的阶段分类例行程序的输出；零个或多个阶段消息，该消息可以是要显示给用户关于该阶段分类操作的消息，以某种方式与该阶段分类相关的其他阶段分类的相关信息；以及零个或多个阶段算法参数，该阶段算法参数使参数在阶段逻辑模块（PLM）或基于该阶段分类的单元阶段中被创建。在阶段的执行期间将这些阶段算法参数用作临时存储单元或变量，并且对于用户或成批执行的例行程序来说不必是可见的。阶段分类包括一个或多个阶段算法定义（PAD），一般而言该 PAD 是用来实施该阶段的控制例行程序。同样，阶段分类还具有零个、一个，两个或更多单元分类的关联列表，并且该列表定

义了这样的单元分类，能够为该单元分类申请该阶段分类，并因此能够为该单元分类申请该阶段分类的 PAD。填充阶段分类的关联列表不仅包括反应器单元分类，还包括进料_罐单元分类。

图 3 描绘了图 2 所示某些对象的更详细版本，以及这些对象之间的相互关系。在图 3 中描绘了两个单元分类，即反应器单元分类 50 和进料_罐单元分类 52。反应器单元 50 具有一个单元模块 54，即反应器_01。可以存在其他单元模块，只是它们在图 3 中未被示出。单元模块 54 定义了某些与反应器单元分类 50 相关的反应器参数，换句话说，反应器_01 的容量是 300 且反应器_01 不包括搅拌器。同样地，两个阶段分类与反应器单元分类 50 相关，包括填充阶段分类 56 和倾倒阶段分类 58。填充阶段分类 56 包括使用两个别名，即＃INLET－VALVE＃和＃LEVEL＃，来设计的 PAD（在其右侧以图形形式表示为 SFC）。这些别名实际上用在填充阶段 56 的 PAD 中的所示方框中，但是可替换地，也可以用在 PAD 逻辑内的其他任何地方。填充阶段分类 56 还包括被定义为 TARGET_LEVEL 的输入，和被定义为 FINAL_LEVEL 的输出。尽管将别名表示为用数字符号（＃）来分隔或标注，任何其他标识符都可以用来定义别名，该别名必须在阶段的初始化阶段就进行替换。同样，倾倒阶段分类 58 包括在其右手侧以图形形式示出的 PAD，具有＃OUTLET_VALVE＃和＃LEVEL＃的别名、定义为 RATE 的输入、定义为 FINAL_LEVEL 的输出和定义为 ACTUAL_RATE 的算法参数（由该 PAD 使用），这些可以在 PAD 的执行期间用作临时存储单元。

图 1－3 示出了过程控制系统，其中可以创建软件对象并用来执行传统的过程控制功能，而图 4 示出了综合过程控制系统和安全测量系统，其包括综合的设计和批准软件，可以用来创建、改变和批准过程控制系统和安全测量系统中任何一个，或两者内同样的或其他软件对象。特别地，如图 4 所示，加工厂 10 包括与安全系统 114（用虚线表示）相结合的过程控制系统 112，其通常作为安全测量系统（SIS）来操作运行，监控和超驰（override）由过程控制系统 112 提供的控制，从而最大化加工厂 10 可能的安全操作。加工厂 10 也包括一个或

多个主工作站、计算机或用户界面 116（它们可以是任意类型的个人计算机、工作站、PDA 等），它们可以由工厂人员来访问，例如过程控制操作员、维护人员、安全工程师，等等。在图 4 所示的例子中，两个用户界面 116 被显示为连接至两个分离的过程控制/安全控制节点 118 和 120，并通过公用通信线路或总线 122 连接至配置数据库 121。通信网络 122 可以利用任何所需的基于总线或非基于总线的硬件，利用任何所需的硬连线或无线通信结构和利用任何所需的或合适的通信协议来实现，例如以太网协议。

一般而言，加工厂 10 的节点 118 和 120 中的任何一个均包括通过总线结构连接到一起的过程控制系统设备和安全系统设备，该总线结构可以被提供在其中附有不同设备的底板上。在图 4 中将节点 118 示为包括过程控制器 124（其可以是冗余的一对控制器）以及一个或多个过程控制系统输入/输出（I/O）设备 128、130 和 132，而将节点 120 示为包括过程控制器 126（其可以是冗余的一对控制器）以及一个或多个过程控制系统 I/O 设备 134 和 136。过程控制系统 I/O 设备 128、130、132、134 和 136 中的任一个均以可通信联络的方式连接至一组有关过程控制的现场设备，在图 4 中图示为现场设备 140 和 142。过程控制器 124 和 126、I/O 设备 128－136 以及控制器现场设备 140 和 142，通常组成图 4 的过程控制系统 112。

同样，节点 118 包括一个或多个安全系统逻辑解算器 150、152，而节点 120 包括安全系统逻辑解算器 154 和 156。逻辑解算器 150－156 中的任一个均为具有处理器 157 的 I/O 设备，处理器 157 执行存储在存储器 179 中的安全逻辑模块 158，并且以可通信联络方式连接以提供控制信号给安全系统现场设备 160 和 162，和/或从安全系统现场设备 160 和 162 接收信号。另外，节点 118 和 120 中的任一个均包括消息传播设备（MPD）170 或 172，其通过环形总线连接 174（在图 4 中仅示出了该总线的一部分）以可通信联络的方式相互耦合在一起。安全系统逻辑解算器 150－156、安全系统现场设备 160 和 162、MPD170 和 172 以及总线 174，通常就组成了图 4 的安全系统 114。

仅作为举例，对可以是艾默生过程管理公司销售的 DeltaV$^{TM}$ 控制器或任何

其他所需类型的过程控制器的过程控制器 124 和 126 进行编程，以便使用 I/O 设备 128、130 和 132（用于控制器 124 的）、I/O 设备 134 和 136（用于控制器 126）以及现场设备 140 和 142，来提供过程控制功能（利用一般被称作控制模块的东西）。特别地，控制器 124 和 126 中的任一个均实施或监视存储在其中的或以另外方式与之相关的一个或多个过程控制例行程序（这些例行程序是软件对象，且可以由互连的软件对象组成），并且与现场设备 140 和 142 以及工作站 114 进行通信，以便以任何所需的方式来控制过程 110 或过程 110 的一部分。现场设备 140 和 142 可以是任何所需类型的现场设备，例如传感器、阀门、发送器、定位器等，并且可以符合任何所需的开放、专有或其他通信或编程协议，包括例如 HART 或 4－20 毫安协议（如为现场设备 140 所示），任意的现场总线协议，例如 FOUNDATION®现场总线协议（如为现场设备 142 所示），或 CAN，Profibus，AS-Interface 协议，此处仅指出了一些。类似地，I/O 设备 128－136 也可以是使用任何适当通信协议的任何已知类型的过程控制 I/O 设备。

图 4 的安全逻辑解算器 150－156 可以是任何所需类型的安全系统控制设备，其包括处理器 157 和存储安全逻辑模块 158 的存储器，安全逻辑模块 158 适用于在处理器 157 上执行，以利用现场设备 160 和 162，提供与安全系统 114 相关的控制功能。当然，安全现场设备 160 和 162 可以是任何所需类型的现场设备，其符合或使用任何已知或所需的通信协议，例如以上所提及的那些。特别是，现场设备 160 和 162 可以是这种类型的安全相关现场设备，该类型通常是用分离的专用安全相关控制系统来控制。在图 4 所示的加工厂 110 中，将安全现场设备 160 描绘为使用专用或点对点通信协议，例如 HART 或 4－20 毫安协议，而将安全现场设备 162 示为使用总线通信协议，例如 Fieldbus 协议。安全现场设备 160 可以执行任何所需的功能，例如关闭阀门，关闭开关，等等。

在节点 118 和 120 中使用公用底板 176（用穿过控制器 124、126，I/O 设备 128－136，安全逻辑解算器 150－156 以及 MPD170 和 172 的虚线表示），以将控制器 124 和 126 连接至过程控制 I/O 卡 128、130 和 132 或 134 和 136，以及连接至安全逻辑解算器 150、152、154 或 156，并且连接至 MPD170 或 172。

控制器 124 和 126 也以可通信联络的方式耦合至总线 122 并作为总线 122 的总线仲裁器来操作，以便使 I/O 设备 128－136、逻辑解算器 150－156 以及 MPD170 和 172 中的任何一个均能够通过总线 122 与任一工作站 116 进行通信。

应当理解，每个工作站 116 均包括处理器 177 和存储器 178，并且至少一个工作站存储一个或多个适用于在处理器 178 上执行的配置、批准、诊断和/或查看应用程序。在图 4 的分解图中将配置应用程序 180、批准应用程序（或例行程序）181 和查看应用程序 182 图示为存储在一个工作站 116 中，而将诊断应用程序 184 图示为存储在另一个工作站 116 中。然而，如果需要的话，这些和其他应用程序可以在不同的工作站 116 中，或者在与加工厂 10 相关的其他计算机中存储和执行。一般而言，配置应用程序 180 向安全工程师提供配置信息，使安全工程师能够配置（设计）加工厂 10 内的某些或所有元件，并能够将该配置存储在配置数据库 121 中。作为由配置应用程序 180 执行的配置活动的一部分，安全工程师可以为过程控制器 124 和 126 创建或改变控制例行程序或控制模块（即软件对象），可以为任一或所有安全逻辑解算器 150－156 创建安全逻辑软件模块 158（包括创建和编程输入、表决和其他功能块，以用在安全逻辑解算器 150－156 中，甚或用在控制器 124 和 126 中），并且可以在通过批准例行程序 181 接收到这样做的适当授权之后，通过总线 122 和控制器 124 和 126，将这些不同的控制和安全模块下载到过程控制器 124 和 126 以及安全逻辑解算器 150－156 中合适的一个。同样，配置应用程序 180 也可以用来在通过批准例行程序 181 接收到这样做的适当授权之后，创建其他程序和逻辑并将其下载到 I/O 设备 128－136、现场设备 140、142、160 和 162 中的任意一个等等。如果需要的话，可以为每个过程控制系统 112 和安全系统 114 存在分离的一组配置和批准例行程序，从而使这些系统的设计活动相互隔离。

查看应用程序 182 可以被用来向用户提供一个或多个显示，例如提供给过程控制操作员、安全操作员等，其包括有关过程控制系统 112 和安全系统 114 的状态的信息，如果需要的话，可以显示在分离的视图中，也可以显示在同一视图中。例如，查看应用程序 182 可以是告警显示应用程序，其接收并向操作

员显示告警的指征。如果需要的话，这样一种告警显示应用程序可以采用如以下专利所公开的形式，标题为“包括告警优先级调整的过程控制系统”的美国专利 No. 5,768,119 和标题为“过程控制网络中的综合告警显示”的美国专利申请 No. 09/707,580，这两篇专利都转让给了本专利的受让人，并被特意合并于此以资参考。然而，应当理解，这些专利的告警显示和告警标识可以接收并显示来自于综合告警显示中过程控制系统 112 和安全系统 114 两者的告警，以便能够将来自于系统 112 和 114 两者的告警发送给执行告警显示应用程序的操作员工作站 114，并且可以辨识为来自于不同设备的告警。同样，操作员可以以与过程控制告警相同的方式来处理在告警标识中显示的安全告警。例如，操作员或用户可以使用告警显示来确认安全告警、关闭安全告警等，该告警显示能够使用通过总线 122 和底板 176 的通信，将消息发送给安全系统 114 内适当的过程控制器 124、126，从而关于安全告警采取对应的行动。以类似的方式，其他查看应用程序可以显示来自过程控制系统 112 和安全系统 114 两者的信息或数据，以便这些系统可以使用相同类型和种类的参数、安全和参照，因此来自系统 112 和 114 之一的任何数据均可以被集成到通常提供给过程控制系统的显示或视图中。同样，在通过以下更详细描述的电子签名过程接收到适当的授权之后，可以创建和实施对这些查看应用程序（它们是软件模块）的变化或新的应用程序。

无论如何，应用程序 180、181、182 和 184，以及任何其他应用程序可以将分离的配置和信号发送给过程控制器 124 和 126 中的任一个，并可以接收来自过程控制器 124 和 126 中的任一个以及来自安全系统逻辑解算器 150－156 中任一个的数据。这些信号可以包括与控制过程现场设备 140 和 142 的操作参数相关的过程控制相关消息，并可以包括与控制安全相关现场设备 160 和 162 的操作参数相关的安全级别消息。可以对安全逻辑解算器 150－156 进行编程，以辨识过程控制消息和安全消息，而安全逻辑解算器 150－156 能够在两种类型的消息之间进行辨别，却不能够进行编程或受到过程控制相关配置信号的影响。在一个例子中，发送到过程控制系统设备的编程消息可以包括某些场域或地址，

它们由安全系统设备辨识，并且阻止将这些信号用于对安全系统设备进行编程之中。

如果需要的话，安全逻辑解算器 150－156 可以使用与用于过程控制 I/O 卡 128－136 的硬件和软件设计相比，相同或不同的硬件或软件设计。用于过程控制系统 112 内的设备和安全系统 114 内的设备的轮换技术的使用可以最小化或消除普通原因的硬件或软件故障。此外，包括逻辑解算器 150－156 的安全系统设备可以使用任何所需的隔离和安全技术来降低或消除对由此实施的安全相关功能进行未经授权的改变的机会。例如，安全逻辑解算器 150－156 和配置应用程序 180 可能会要求具有特定权级的人或位于特定工作站的人对逻辑解算器 150－156 内的安全模块做出改变，而该权级或位置与对由控制器 124 和 126 以及 I/O 设备 128－136 执行的过程控制功能做出改变所需的权限或访问级别或位置不同。在这种情况下，只有在安全系统 114 内指定的或位于被授权为可以对安全系统 114 做出改变的工作站的那些人具有改变安全相关功能的权限，这最小化了安全系统 114 的操作出现讹误的机会。应当理解，为了实施该安全性，安全逻辑解算器 150－156 内的处理器估计输入消息的适当形式和安全性，并作为网守（gatekeeper）来操作，以影响对安全逻辑解算器 150－156 内执行的安全控制模块 158 所进行的改变。

以类似的方式，可以实施图 4 所示的批准例行程序 81，以避免未经过要求进行授权的其他个体（用名字或用工作位置）的正当授权，就对过程控制系统 112 和安全系统 114 中任一个或两者内的软件对象做出改变。特别地，批准例行程序 181 可以检测对配置、显示或查看应用程序内的软件模块所进行的改变，并避免未经过要求他们这样做的那些人的适当授权或批准，就将这些模块下载到过程控制系统 112 或下载到安全系统 114。

底板 176 在每一个节点 118 和 120 中的使用，使安全逻辑解算器 150 和 152 与安全逻辑解算器 154 和 156 能够在本地相互通信，以协调由这些设备中的任一个实施的安全功能，相互传递数据，或执行其他综合功能。另一方面，MPD170 和 172 进行操作，以便使广泛分布于工厂 10 内不同位置的安全系统 114 的各部

分仍然能够相互通信，从而在加工厂 110 的不同节点处提供协同的安全操作。特别地，MPD170 和 172 连同总线 174 一起协力使与加工厂 110 中不同节点 118 和 120 相关的安全逻辑解算器能够以可通信联络的方式级联在一起，从而允许根据所分配的优先级来级联加工厂 110 内的安全相关功能。可替换地，处于加工厂 110 内不同位置的两个或更多安全相关功能可以联锁或互连，而无须铺设到工厂 110 的分离区域或节点内的各个安全现场设备的专用线路。换句话说，MPD170 和 172 以及总线 174 的使用使安全工程师能够设计和配置安全系统 114，该安全系统 114 自然地分布于整个加工厂 110 中，但是它拥有其中以可通信联络方式进行互连的不同部件，以使不同的安全相关硬件根据需要来相互通信。该特征也提供了安全系统 114 的可伸缩能力，当需要附加的逻辑解算器时，或者将新的过程控制节点添加到加工厂 110 时，能够将附加的安全逻辑解算器添加到安全系统 114 上。

在一个实施例中，可以使用功能块编程范例对逻辑解算器 150－156 进行编程，以执行关于安全设备 160 和 162 的控制活动。特别地，如逻辑解算器 154 的一个安全控制模块 158a（存储在存储器 179 中）的扩充视图所示，安全控制模块可以包括一组以可通信联络方式互连的功能块（每一个均为软件对象），能够创建这些功能块并将其下载到逻辑解算器 154 上，以便在过程 110 的操作期间进行实施。如图 4 所示，控制模块 158a 包括两个表决器功能块 192 和 194，具有以可通信联络方式与其他功能块 190 互连的输入端，其他功能块 190 可以是例如模拟输入（AI）、数字输入（DI）功能块或者被设计为向表决器功能块 192 提供信号的其他功能块。表决器功能块 192 和 194 至少具有一个连接至一个或多个其他功能块 191 的输出端，其他功能块 191 可以是模拟输出（AO）、数字输出（DO）、实施原因和结果逻辑的原因和结果功能块、可以从表决器功能块 192 和 194 接收输出信号以控制安全设备 160 和 162 操作的控制和诊断功能块，等等。当然，能够以任何所需的方式对安全控制模块 158a 进行编程，以便包括以任何所需或有用的方式配置的任何类型的功能块来执行任何所需的功能。另外地或可选地，诸如 AI 和 DI 功能块的其他输入功能块可以直接耦合至

安全系统以提供安全逻辑控制模块，一旦出现了一个或多个由 AI 或 DI 块检测的事件，安全逻辑控制模块就通过激活一个或多个关闭的设备，对这些事件做出响应。应当理解，控制模块 158a 和此处的每个功能块都是分离的软件对象，可以将这些软件对象下载到安全系统 112 上，并且可以在操作期间改变它们，如果需要这样的话。然而，在可以实施这些创建或修改活动之前，这些软件对象可能需要通过批准例行程序 181 接收授权，这将在以下内容中进行更为详细的描述。

特别是，将批准例行程序 181 与配置应用程序 180（或者在加工厂内使用的其他设计应用程序）结合到一起，或者以可通信联络方式被捆绑到一起，从而确保以在线方式将该软件对象实际上下载到过程控制系统 112 或安全系统 114 之中，或者以另外的方式在过程控制系统 112 或安全系统 114 内进行实施之前，对所创建或改变的每一个新的或修改后的软件对象进行适当的授权或者检查。

应当理解，软件对象批准例行程序与安全测量系统（或过程控制系统）紧密地结合在一起，因此批准例行程序 181 可以利用安全测量系统的安全性。此外，由于批准例行程序 181 处在与过程控制或安全系统设计或配置软件 180 相同的环境中，因此检查者可以使用与用来开发它的相同工具来检查这些要批准的软件对象。因而，关于要检查的软件对象的准确性不存在任何问题。此外，批准例行程序 180 阻止将要求批准的软件对象下载到控制或安全环境中，直到进行完所有需要的批准为止。因而，过程控制或安全测量系统能够保证仅执行经过批准的软件对象。然而，如果需要的话，批准例行程序 181 也可以包括（例如存储）安全密钥，其为拥有该密钥的用户提供这样的能力，能够超驰该要求的强制，并下载未经批准的软件对象。

在操作期间，批准例行程序 181 可以检测对软件对象所进行的改变，并且可以促使对批准的软件对象的任意修改，从而使得软件对象的版本号增加。此外，当软件对象的版本号增加时，批准例行程序 181 将软件对象的状态自动变为未批准状态。结果，软件对象的这个新版本无法被下载，或者直到对软件对

象的新版本重新执行完所有的批准，才能够在过程控制系统中实施该软件对象的这个新版本。

另外，批准例行程序 181 可以将特定软件对象的所有批准和/或拒绝记录到与该软件对象相关的配置检查追踪中。作为这些特征的结果，软件对象的生效以过程控制或安全测量系统生效的整体部分的形式而出现。

图 5A 表示流程图 185，示出了可以由批准例行程序 181 实施的步骤，使用相同或不同的软件例行程序来提供过程控制和/或安全系统内的批准功能。在框 186 中，批准例行程序 181 监控软件设计应用程序（例如配置例行程序 180）或配置数据库，以确定何时以及是否对任一软件对象做出改变。框（或例行程序）186 可以通过检测现有软件对象的变化、新软件对象的创建、甚或通过接收例如软件对象设计者对批准过程的实施请求，确定对软件对象做出的改变。当然，框 186 可以一直等待实施该批准过程，直到对软件对象做出了所有改变为止，这是用例如软件设计者在设计应用程序中选择了表示完成该变化的按钮来进行指示。无论如何，当框 186 检测对软件对象做出的改变时，或者在其后的某一时刻，框 187 可以自动地或者在设计者的推动下，对批准程序进行初始化。

在批准程序期间，框 188（例如，批准例行程序 181 内）可以确定一组实体（可以包括一个或多个人），并且作为该过程的一部分，可以基于用户提供的或者在过程控制或安全系统的配置期间另外提供的信息，确定该批准所需签名的数目和类型（例如工作位置）。在一个实施例中，框 188 可以使用用户或配置工程师输入的风险降低因子（RRF）来确定所需批准的类型和数目。在这种情况下，用户可以为特定功能或软件对象输入要达到的所需 RRF，并且框 188 可以使用该 RRF 来确定所要求的 SIL 级别。接下来，框 188 可以利用例如查阅表，使用 SIL 级别来确定所要求签名的性质（例如，签名的数目，这些签名是否必须来自相同或来自不同的部门，检查者所占据的工作或位置的级别或类型，等等）。应当注意到，每个特定的安全测量功能均具有与之相关的 SIL，因此特定的 SIL 专用于安全测量功能，并可以一个安全功能又一个安全功能地发生变化。

无论如何，框 189 接下来确定实际上向其发送用于批准的软件对象的真实

人员。如果需要的话，所选小组内检查者的名字、电子地址或电子联系信息可以从相应的查阅表获取。另外地或可选地，检查者小组和相关的电子联系信息可以从配置工程师处直接获取，从对该软件对象做出改变的人那里获取，或者通过显示终端从任何其他合适的人那里获取。作为该过程的一部分，框 189 可以借助于或者不借助于软件对象设计者的帮助，来访问所存储的可能名字或办公室的列表（以及相关的电子地址等），并以任何所需或预定的方式从该列表中进行选择。可替换地，框 189 可以通过用户界面来提示某些监督人员，为该批准过程选择与所要求级别和部分相匹配的特定人员。

在选择实际的检查者之后，框 190 接下来将所创建或修改的软件对象用电子方式发送给所选检查者，并等待从检查者返回的关于是否批准所创建或修改的软件对象的消息。框 191 可以监控来自于检查者的响应，以确定何时（或是否）已经接收到所有的批准，并且如果所有检查者（或预定数目的检查者）都批准了所修改软件对象的话，则框 192 可以将该软件对象标注为能够下载。然而，如果未能接收到来自于所有检查者的响应，或者如果一个检查者已经拒绝了该软件对象，则批准例行程序 181 不能将该软件对象标注为可下载，由此阻止在过程控制或安全系统中使用该软件对象。

当然，批准例行程序 181 可以一直循环，直到接收到所有的响应，并且以任何所需的方式向设计者或用户提供响应。如果框 191 确定接收到特定数目的拒绝，则框 193 可以将该软件对象标注为需要进行修改或重新提交给批准者，由此使该软件对象能够下载。

当然，批准例行程序 181 中的任意一个或每一个框均可以将对软件对象做出的改变、该软件对象相关的批准和拒绝的集合以及有关批准过程的任何其他信息，记录到配置数据库或与该软件对象相关的检查追踪中。此外，如果需要的话，批准例行程序 185 可以追踪，并向设计者（甚或向其他检查者）显示有关检查过程状态的信息，例如检查者的身份，哪些检查者已经做出响应，哪些已经接受和/或哪些已经拒绝了该新的或修改后的软件对象，等等。如果需要的话，框 191 可以向未做出响应的检查者发送提示。

另外，一旦批准了软件模块，批准例行程序 185 就可以以在线方式，即在该软件对象驻存的过程控制或安全系统的操作期间，使用 RRF 来确定与该软件对象相关的安全功能或操作是否仍然满足其设计标准。特别地，配置者可以确定安全功能的哪一个元件需要周期性地进行测试、测试周期应当是多少、以及该测试如何影响安全功能的总体 RRF。这些细节通常在设计时确定，因此当执行这些功能时对于配置者而言这些细节是已知的。

如图 5B 所示，批准例行程序的在线监控部分 194 包括框 195，其监控各元件的测试。如框 196 所确定的，如果超出特定软件对象的周期测试时间间隔，则框 197 确定要达到的实际 RRF（基于不能执行安全功能测试的故障），并将该修改后的 RRF 显示给用户，例如安全系统监控者或操作员。框 198 也可以比较该修改的 RRF 和目标 RRF，并且当不再满足目标 RRF 时生成告警。如果需要的话，框 199 可以使用 SIL 中的信息，在测试时间间隔之前或者在已经超出测试时间间隔之后，自动生成工作定单（work order）（例如，规定要运行的测试），以便将 RRF 保持在其设计目标值或高于其设计目标值处，或者尽快将 RRF 返回到其设计级别。

应当理解，尽管在图 1 中示出了单一批准例行程序 18 并且在图 4 中示出了单一批准例行程序 181，这些例行程序的组成部分可以被存储在其他计算机或工作站上，以便检查者可以位于设计者以外的不同工作站处。在这种情况下，类似的或补充的软件能够被安装在以可通信联络方式连接至设计终端的一组检查者终端中的任何一个上（例如图 1 中示出的检查者终端 32），以便使检查者能够接收来自于设计终端处的例行程序 18 或 181 的批准消息，调用过程控制或安全系统中的软件以分析要检查的软件对象，并根据批准或拒绝以及该检查者想要做出的任何注释来做出响应。

此外，如以下所进行的更为详细的讨论，批准例行程序 18 或 181 可以具有任意数目的组成部分，这些组成部分执行不同的功能，例如选择检查者、修改软件对象等等。尽管结合图 6－20 将对这些组成部分中的某些进行更为详细的讨论，应当理解，可替代地或另外地，其他例行程序能够与该批准或设计例行

程序相关联。此外，尽管关于过程控制系统中使用的处方的批准，在图 6－20 中对大量子例行程序进行了讨论，应当理解这些例行程序同样也能够用于批准其他软件对象，例如安全系统中的软件对象。

现在转到图 6，可以由工作站 14 的一个或多个处理器 21 执行的处方编辑器例行程序 400，在框 402 处开始执行，在框 402 中用户或操作员创建或修改处方，该处方可以包括与之相关的软件对象的修改，以便在过程控制系统 10 中使用。应当容易理解，用户可以使用结合图 1－5 所描述的技术，或者使用任何其他合适的技术来创建或修改处方或其他软件对象。在创建或合适地修改了处方之后，控制从框 402 转到框 406。如以下结合图 7－13 所要进行的更为详细的讨论，在执行处方编辑器例行程序 400 之前，或者在处方或其他软件对象的修改和/或将其下载到系统 10 之前的任意其他时刻，可以至少执行一次授权建立例行程序 404（图 7）。通常，授权建立可以包括但不限于，指定需要他们进行批准以实施处方或其他软件对象的人员或实体，或者删除或修改签名者。

在框 146 处，在授权建立期间向每个签名者请求批准，以批准在框 402 创建或修改的处方。批准请求可以包括但不限于，将电子邮件发送给指定检查与授权建立例行程序 404 有关的处方的签名者，运行表示每个指定签名者的批准状态的报告，通过任何其他合适的通信方法将即时消息发送给要检查该处方的签名者，或向签名者发送通知。在框 406 处向每个签名者请求批准之后，处方编辑器例行程序 400 终止执行，或将控制返回到曾经调用处方编辑器例行程序 400 的另一例行程序。

结合图 7 和 8，提供授权建立例行程序 404 的更多细节，图 7 和 8 分别公开了用于授权建立例行程序 404 的流程图和用户界面屏幕。尽管授权建立例行程序 404 通常在系统启动时执行一次，但是可替代地，如果需要，授权建立例行程序 404 也可以执行不止一次。通常，如图 7 所示，一旦执行了授权建立例行程序 404，用户就可以分别选择在框 412、414 或 416 中添加、删除或修改处方签名者。在添加、删除或修签名者之后，控制从框 412、414 或 416 中转出，并使用户能够在框 410 处选择取消或终止授权建立例行程序 404 的操作，或者

再次使用框 412－416 来添加、删除或修改签名者。如果用户选择在框 410 中取消或终止授权建立例行程序 404，则授权建立例行程序 404 终止。

如图 8 所示，用户界面 420 包括处方授权建立表格 422，该表格允许用户选择界面按钮 424、426 或 428 来添加、修改或删除签名者。添加、修改和删除界面按钮 424－428 对应于（并且可以进行选择以调用由下述框所执行的功能）图 7 所示的添加、删除和修改框 412－416。结合图 9－13，提供关于框 412－416 中任意一个的更多细节，并且隐含地提供关于界面按钮 424－428 中任一个的更多细节。当添加、修改或删除签名者时，在文本框 430 中显示签名者的状态。如图 8 所示，文本框 430 包括列出了签名者名字的签名者描述栏 432，该签名者名字可以是人或实体的名字，并且还包括列出功能锁的功能锁栏 434，要求相应的签名者拥有该功能锁，由此控制对批准的访问。例如，如图 8 所示，要通过工程学、产品和质量保证来检查和解签/签署该处方，其对应于功能锁 RECIPE_APPROVAL_01。

同样在图 8 中示出的是两个复选框 436 和 438，其对应于启动处方授权和允许批准向所包含的处方传播（即子处方）。在操作中，当勾中复选框 436 时，启动该系统的启动处方授权特征，并启动授权建立过程。当未勾中复选框 438 时，表示该用户不能拥有传播授权的选项。相反地，如果勾中了复选框 438 的话，用户将会拥有向子处方传播授权的选项。例如，主处方可以由两个和更多的子处方组成，或者可以包含两个和更多的子处方，与主处方相关的批准可以自动地传播到这些子处方。当然，处方批准的这种自动传播可能会带来显著的时间节省，特别是对于包括大量子处方的处方而言。

用户界面 420 还可以包括取消（cancel）和 ok 界面按钮，它们分别用附图标记 440 和 442 来指示。界面按钮 440 和 420 对应于图 7 的取消/ok 框 410，并允许用户退出授权建立例行程序 404。尽管两个界面按钮 440 和 442 都能使用户退出授权建立例行程序 404，但取消界面按钮 440 终止授权建立例行程序 404，而不包括对处方授权建立做出任何改变。相反地，ok 界面按钮 442 允许用户退出授权建立例行程序 404，并且保存使用用户界面 420 期间对授权建立所做出

的各种改变。

现在转到图 9，提供描述添加例行程序的框 412 的更多细节。添加例行程序 412 在框 450 开始执行，框 450 接收由用户提供的功能锁选择。如图 10 所示，图形用户界面或弹出窗口 452 可以包括批准功能锁框 454，用户可以向其中输入批准功能锁的名字。例如，如图 10 所示，框 454 可以包括选择批准功能锁为 RECIPE_APPROVAL_03 的指示。

回到图 9，在框 450 接收到功能锁选择之后，框 460 接收由用户提供的签名者描述。例如，如图 10 的用户界面 452 所示，用户可以在框 462 中输入签名者描述。例如，在框 462 中显示描述“领队”，它表示用户要求将领队添加为具有批准功能锁 RECIPE_APPROVAL_03 的签名者。

在分别于框 450 和 460 处接收到功能锁选择和签名者描述之后，控制转到框 466，其确定是否丢失了功能锁或签名者描述中的任何一个，或者是否选择了分别由图 10 中附图标记 470 和 472 所示的取消或 ok 界面按钮。如果丢失了锁或描述，则控制从框 466 转到框 450。可替换地，如果框 466 中确定用户已经选择了取消或 ok 界面按钮 470 和 472，则添加例行程序 412 终止其执行，并将控制返回到图 7 的授权建立例行程序 404。如关于图 8 的用户界面 420 所进行的描述，取消界面按钮 470 的触动致使添加例行程序 412 终止其执行，而不保存其执行期间所做出的改变。相反地，如以上所指出的，ok 界面按钮 472 的触动致使添加例行程序 412 终止，并保存添加例行程序 412 的执行期间所做出的各种改变。如果添加例行程序 412 添加了新的批准者或签名者，则任何一个先前批准的处方（即已经收到了所有原先要求的批准的处方）均自动地变为未经授权，直到获得来自新近添加的签名者的批准。

结合图 11，提供删除例行程序 414 的更多细节，其连同图 8 的用户界面 420 一起操作。特别是，删除例行程序 414 在框 480 处开始执行，框 480 接收要删除签名者描述的选择。用户可以通过选择图 8 的用户界面 420 的文本框 430 中所示的签名者描述，提供这样的选择。在用户选择了要删除的描述之后，用户接下来触动删除界面按钮，以表明他或她删除所选签名者描述或签名者的意图。

在框480完成执行之后，控制转到框482，其接收用户请求的删除确认。例如，在用户选择要删除的签名者描述并触动删除界面按钮428之后，删除例行程序414可以请求用户确认他或她的愿望，通过在显示屏幕上向用户显示的用户界面图形，删除所选签名者描述。这样一种图形可以包括ok或取消界面按钮，其中ok界面按钮的触动（例如通过鼠标，键盘等进行选择）将确认用户删除所选签名者描述的愿望，而取消界面按钮的触动将放弃所选描述的删除。在框482接收到删除确认之后，删除例行程序414终止其执行，并将控制返回到授权建立例行程序404。

结合图12和13，提供关于图7的修改例行程序416的更多细节。修改例行程序416在框484开始执行，其从用户接收要修改签名者描述的选择。例如，用户可以选择图8中叫做质量保证（Quality Assurance）的签名者，并且接下来可以触动修改界面按钮426。在触动修改界面按钮之后，可以将例如图13所示用户界面486的用户界面显示给用户，并且该用户界面可以包括签名者描述框488和批准功能锁框490。用户界面486也可以包括ok和取消界面按钮492和494。在修改例行程序416接收到要修改签名者描述的选择（在这种情况下，已经为修改选择了签名者质量保证（Quality Assurance））之后，控制从框484转到框496。框496接收签名者描述修改，例如签名者名字的改变，批准锁功能或任何其他合适的改变。例如，在框488中用户提供签名者描述之后，用户可以修改签名者的名字，或者可以修改框490中显示的批准锁功能，并且可以选择ok或取消界面按钮492和494中的任何一个。如先前所描述的，ok界面按钮492的触动保存对签名者描述做出的各种修改。相反地，取消界面按钮的触动终止修改例行程序416，而不保存所作的修改。无论如何，界面按钮492和494中任何一个的触动均会终止修改例行程序416的执行，并将控制返回到图7的授权建立例行程序404。如同添加例行程序412的情况一样，签名者或批准者的自动修改将会导致要求该签名者的批准的任何一个先前批准的处方均变为未经授权。

至此，已经提供了添加删除和修改签名者或处方检查者或批准者的说明。

所描述的例行程序或者包含连同这些例行程序一起描述的功能的例行程序，可以在图 1 的工作站 14 和/或终端 32 中的任何一个内实施，或者用图 4 的任何一个工作站 116 实施。

尽管上述的附图和说明已经涉及了签名者的详述，图 14－18 涉及到可以由签名者执行的检查、批准或拒绝过程。图 14－18 所示的例行程序和用户界面可以在图 1 的终端 32 和/或工作站 14 上实施，或者在图 4 的任何一个工作站 116 上实施。特别地，存储器 20 和 34 中的一个或多个可以存储可由处理器 21 和 36 中的一个或多个执行的指令，从而执行代表该例行程序中各个框的操作。

现在转到图 14，处方授权例行程序 500 在框 502 处开始执行，其显示签名者以及与所检查处方有关的状态信息。例如，图 15 的用户界面 504 可以包括文本框 506，其具有许多纵栏 508－518，可以显示签名者身份、状态、用户类型、时间、注释和节点。签名者栏 508 列出了处方的批准所要求的签名，状态栏 510 列出了每个签名者的签名状态。例如，签名状态可以是空白的或待决的，批准的或拒绝的，其中空白状态或待决状态可以表示签名者还未检查该处方。用户栏 512 列出了负责大多数新近签名变化的用户类型。时间栏 514 列出了做出签名的大多数新近变化的时间。注释栏 516 列出了当签名者批准或拒绝该处方时他们所做出的任何注释，而节点 518 表示签名者批准或拒绝该处方所在的系统节点。例如，节点可以是图 1 的终端 32 和/或工作站 14 中的任何一个，或者是图 4 的工作站 116。除了下一个框 506 以外，用户界面 504 可以包括关闭、批准、拒绝和清除界面按钮 520－526，这些将结合图 14 的处方授权例行程序 500 进行描述。

在框 502 显示签名者和状态信息之后，框 530 接收签名者选择，其可以由用户通过选择界面按钮 520－526 中的任何一个来表明。特别地，如果用户触动了关闭界面按钮 520，处方授权例行程序 500 的控制就从框 530 转到框 540，框 540 关闭用户界面 504，终止处方授权例行程序 500 的执行，并将控制返回到曾经调用处方授权例行程序 500 的任何一个例行程序。

可替换地，如果用户触动了批准界面按钮 522，控制就从框 530 转到框 550，

框 550 代表批准例行程序。如图 16 所示，批准例行程序 550 在框 552 处开始执行，框 552 接收由用户提供的用户名和密码。用户界面 554，在图 17 中示出了它的一个例子，可以包括用户名和密码框 556 和 558，用户可以在其中输入他们的用户名和密码。

在框 552 完成执行之后，控制转到框 560，框 560 接收批准期间做出的用户注释。例如，图 17 的用户界面 554 可包括可以在其中键入注释的文本框 562。在框 560 完成执行之后，框 561 确定该用户是否得到授权。在框 561 中执行的授权检查可以验证在框 552 中接收的用户名和/或密码是有效的，和/或与该用户名和密码相关的用户是否得到授权，以做出这样的批准。如果在框 561 确定该用户得到了授权，则控制转到框 566。框 566 更新状态信息以反映批准。例如，文本框 562 包括文本注释“这一个已准备好生产”，在图 15 中也将该注释反映为在框 566 的执行之后批准该处方时，由生产签名者做出的注释。如果在框 561 处确定框 552 接收的用户名和密码中的任一个或两者都没有得到授权，则批准例行程序 550 终止。

如结合许多先前用户界面屏幕所描述的，图 17 的用户界面 554 包括 ok 和取消界面按钮 568 和 570，这两个按钮可以用来终止批准例行程序 550 的执行，同时保存或者丢弃在例行程序执行期间做出的改变。另外，如图 17 所示，可以提供复选框 572，以便使用户能够选择将批准传播给任何所包含的处方或子处方。

回来参见图 14 和 15，如果用户触动了图 15 的拒绝界面按钮 524，控制就从框 530 转到处方授权例行程序 550 的框 580。框 580 代表拒绝例行程序，在图 18 中可以找到它的更多细节。如图 18 所示，拒绝例行程序 580 的执行在框 582 处开始，在框 582 处，用户在控制转到框 584 之前输入用户名和密码。在框 584 处，签名者可以输入在拒绝该处方的过程期间所做出的注释。框 582 和 584 的操作类似于图 16 所示批准例行程序 550 的框 552 和 560 中的操作，除了框 582 和 584 连同拒绝该处方一起使用。在框 584 完成执行之后，控制转到框 585，框 585 执行类似于在图 17 所示的框 561 中所执行的授权检查。如果确定

用户在框585处得到授权，则控制转到框586。

框586更新状态信息以反映用户对该处方的拒绝。更新状态信息框586可以生成能够在图15的用户界面504上反映的信息，以反映签名者已经拒绝了处方的事实。尽管在图中未示出，拒绝例行程序580也可以使用类似于图17的用户界面554的图形用户界面，该用户界面554用来批准处方。

再次回到图14和15，如果用户触动了图15中的清除界面按钮526，则控制从框530处转到处方授权例行程序500的框590。框590可以被用来清除签名。例如，图15所示的签名者之一可以由用户来选择，并且可以使用界面按钮526来执行清除。然而，一旦已经下载了用于例如控制器12（图1）或工作站14（图1）来执行的处方，那么就不能撤销批准签名的影响。换句话说，一旦已经下载了处方（或任何其他软件对象）的话，就不能清除或拒绝签名（即批准）。

尽管上述说明涉及签名者的选择，并涉及处方的检查，如图19所示，用户界面600可以用来报告过程控制系统10内各处方的状态。例如，用户界面600可以包括许多纵栏602－610，这些纵栏分别表示处方名称、生产、工程技术（engineering）、质量保证和领队。简要地，处方名称栏602列出了所有未经批准的处方，而纵栏604－610列出了每个处方关于每个检查者或检查实体的状态。例如，名称为“OP_CHARGE”的处方关于生产、工程技术、质量保证和领队中的任何一个都是待决的。相比之下，生产、工程技术、质量保证和领队都已经批准了“PRC_PAINT”处方，但是“PRC_PAINT”还没有得到质量保证的批准。因此，“PRC_PAINT”处方仍然是未经批准的。用户界面600也可以包括关闭和打印界面按钮612和614，这两个按钮可以用来关闭用户界面600，或者打印用户界面600以显示包含在纵栏602－610内的信息。

一旦所有签名者都检查和批准了处方，该处方就可以被下载到图1所示的一个或多个控制器12或图4的控制器176之中，或者在这些控制器内实施（或者其他软件对象可以被下载到图4的安全逻辑模块150－156之中，或需要将这些对象下载到其上的任何一个现场设备中）。如图20所示的下载例行程序630

是可以实现该下载的一种方法。下载例行程序 630 在框 632 处开始执行，框 632 生成下载脚本。在框 632 中生成了下载脚本之后，控制转到框 634 处，框 634 确定该处方是否没有被检查出局（即检查入局），或者确定该用户是否提供了密钥，即使在处方被检查出局的情况下，该密钥仍然能够完成该处方的下载。例如美国专利 No. 6,449,624 中所公开的版本控制软件可以用于与下载例行程序 630 相连接。如果框 634 确定该处方被检查出局并且未提供密钥的话，控制转到框 636，框 636 取消该下载，并终止下载例行程序 630 的执行。可替换地，如果该处方没有被检查出局，或者如果已经提供了密钥的话，控制从框 634 转到框 638，框 638 确定该处方是否得到授权，或者用户是否提供了专用密钥，该密钥能够完成对未经授权的处方的下载。处方授权可以包括但不限于确保所有的签名者都已经批准了该处方。如果框 638 确定该处方未得到授权并且没有提供密钥，控制转到框 636，框 636 在终止下载例行程序 630 之前取消该下载。在替代方案中，如果框 638 确定该处方得到授权或者已经提供了密钥，则控制转到框 640，框 640 设置下载标签。该下载标签可以是一个或多个注释语句，或附加于下载项目上的其他类似的电文信息（texual information），该下载项目包括该下载的时间、日期、版本和发起者（或用户）。另外，下载标签还包括所下载的各个项目（例如处方）的详细列表。接下来在框 642 将该处方发送给运行时间系统，该运行时间系统可以具体体现为例如图 1 中的控制器 12 的形式。在框 642 的执行之后，下载例行程序 630 终止执行，并将控制返回到曾经调用下载例行程序 630 的例行程序。

根据上述内容能够意识到，直到与该软件对象相关的所有签名者或批准者都批准了该软件对象之后，当前未得到批准的软件对象才能够下载或者由过程控制或安全系统实施。因此举例来说，新的软件对象或处方必须得到人员和/或其他实体的预定列表或小组（例如，由授权建立例行程序 404（图 7）生成的人员和/或其他实体的列表）的批准。另外，自动修改过的先前批准的软件对象或处方将变为未经授权，因此必须得到其所有相应签名者或授权者的重新批准，从而如在图 20 的框 638 和 640 中举例所示，下载修改过的软件对象或处方。

尽管在此已经对根据本发明的教导而构建的某些装置进行了描述，但本专利的覆盖范围却并不局限于此。相反，本专利覆盖了本发明教导的所有实施例，只要其清楚地落入所附权利要求的范围之内，无论是在字面上还是在其等同物的教义之下。

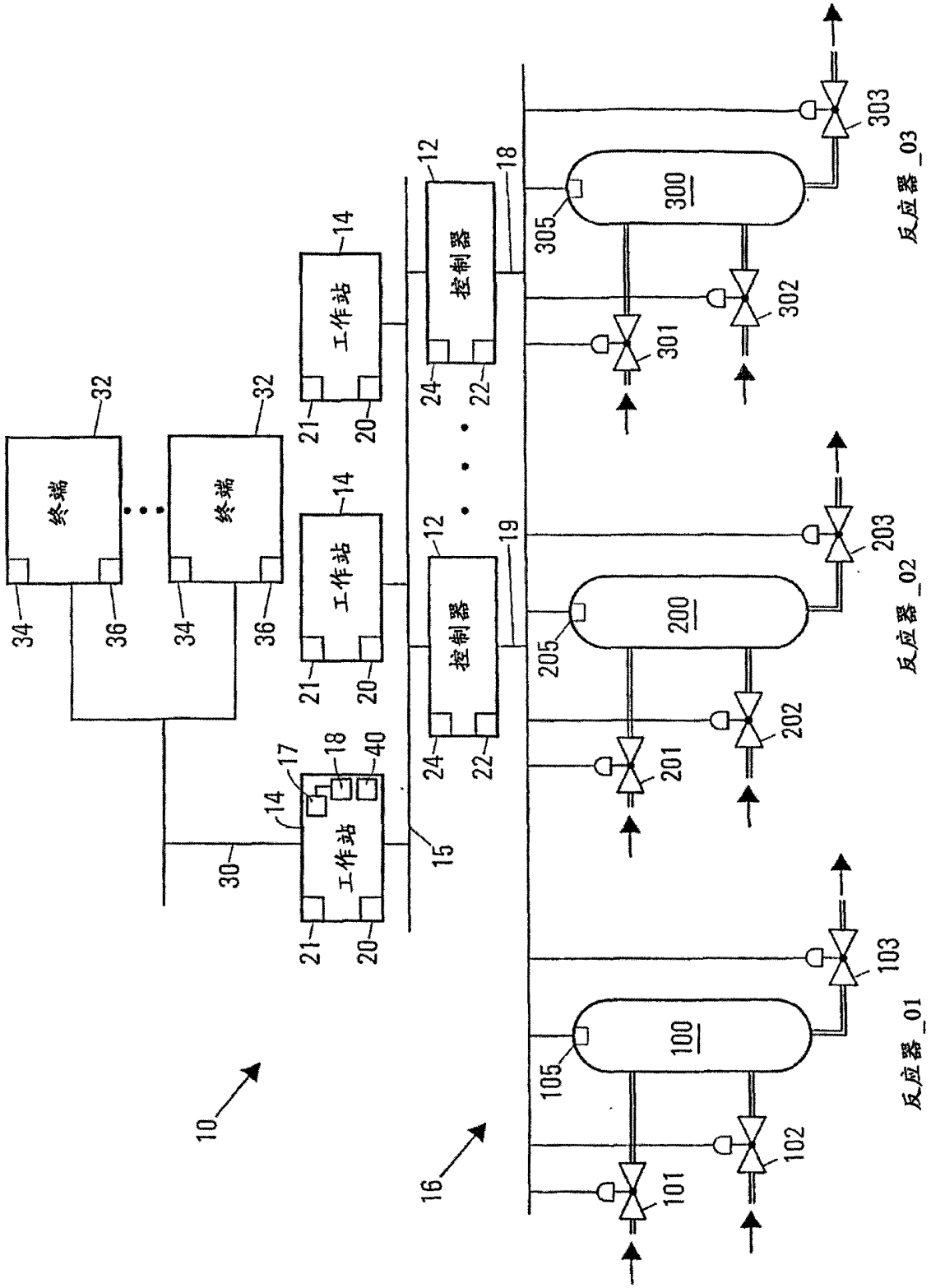

终端
终端
工作站
工作站
工作站
控制器
控制器
反应器_01
反应器_02
反应器_03
100
200
300
101
102
103
105
201
202
203
205
301
302
303
305
10
12
14
15
16
17
18
19
20
21
22
24
30
32
34
36
40

图 1

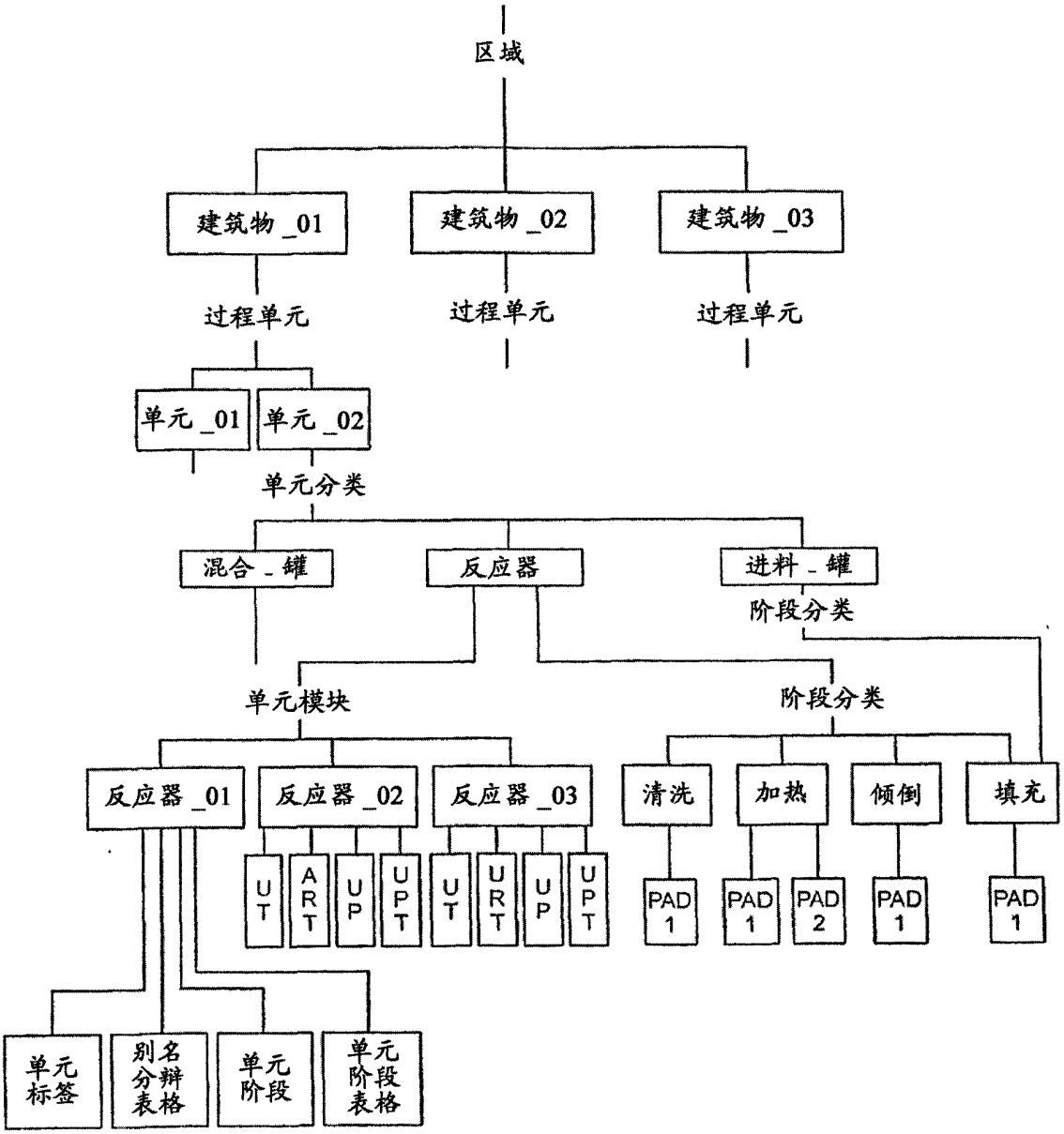

区域
建筑物 _01
建筑物 _02
建筑物 _03
过程单元
过程单元
过程单元
单元 _01
单元 _02
单元分类
混合 _ 罐
反应器
进料 _ 罐
阶段分类
单元模块
阶段分类
反应器 _01
反应器 _02
反应器 _03
清洗
加热
倾倒
填充
UT
ART
UP
UPT
UT
URT
UP
UPT
PAD 1
PAD 1
PAD 2
PAD 1
PAD 1
单元标签
别名分辨表格
单元阶段
单元阶段表格

图 2

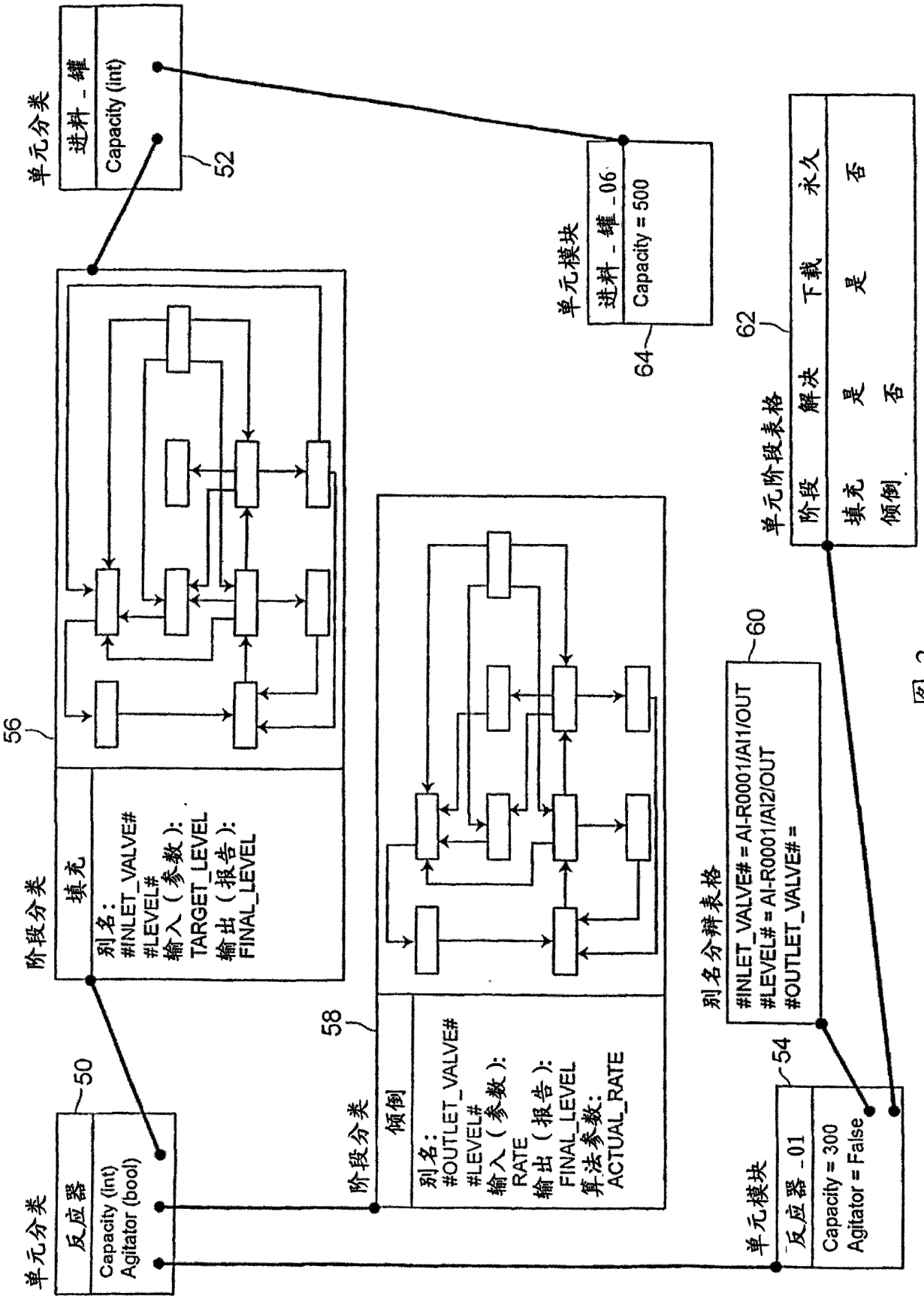

单元分类
反应器
Capacity (int)
Agitator (bool)
50
阶段分类
填充
列名:
#INLET_VALVE#
#LEVEL#
输入(参数):
TARGET_LEVEL
输出(报告):
FINAL_LEVEL
56
阶段分类
倾倒
列名:
#OUTLET_VALVE#
#LEVEL#
输入(参数):
RATE
输出(报告):
FINAL_LEVEL
算法参数:
ACTUAL_RATE
58
单元分类
进料_罐
Capacity (int)
52
单元模块
进料_罐_06
Capacity = 500
64
列名分辨表格
#INLET_VALVE# = AI-R0001/AI1/OUT
#LEVEL# = AI-R0001/AI2/OUT
#OUTLET_VALVE# =
60
单元模块
反应器_01
Capacity = 300
Agitator = False
54
单元阶段表格
62
阶段 解决 下载 永久
填充 是 是 否
倾倒 否

图 3

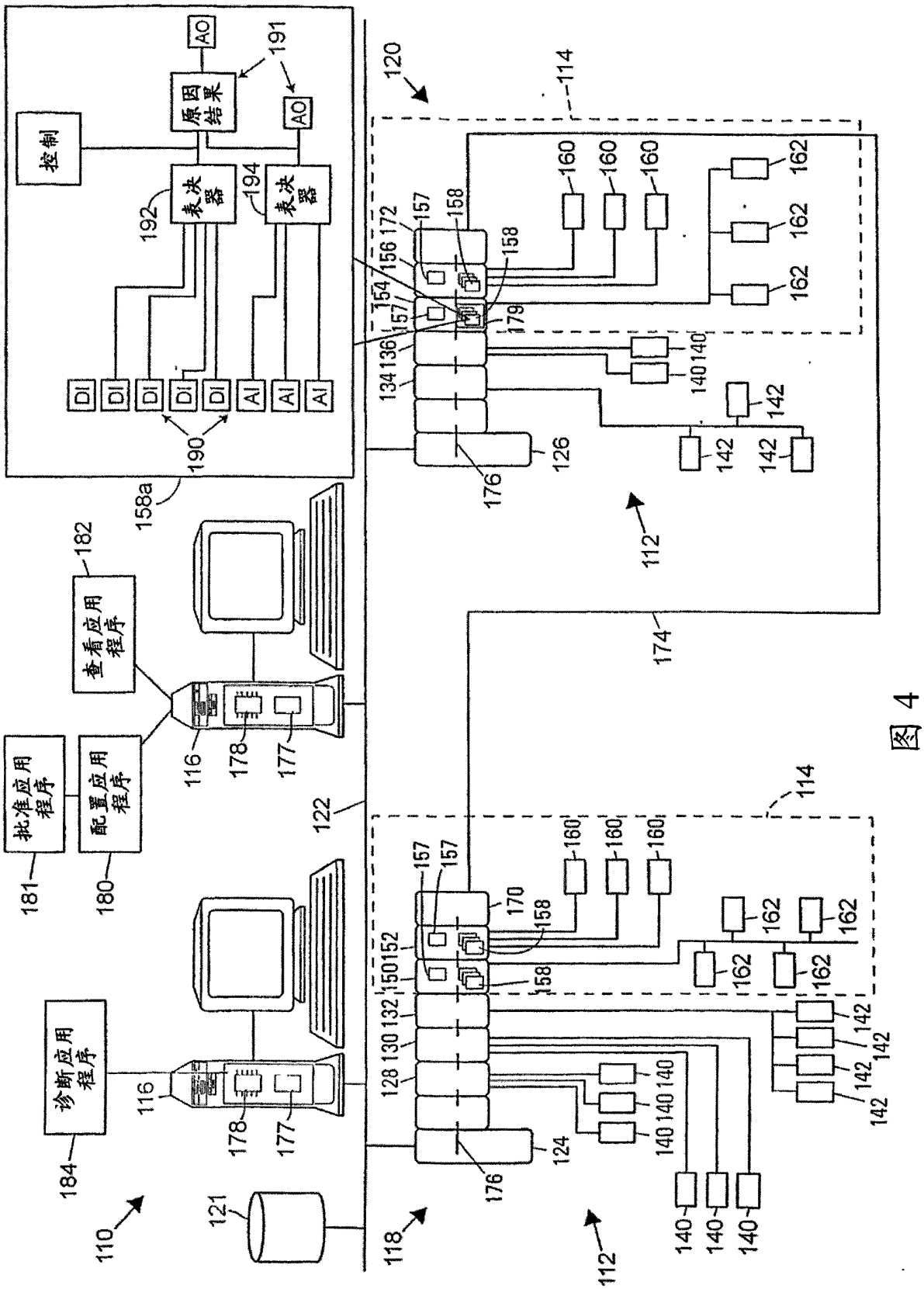

控制
原因结果
表决器
表决器
AO
AO
DI
AI
查看应用程序
批准应用程序
配置应用程序
诊断应用程序
110
112
114
116
118
120
121
122
124
126
130
132
134
136
140
142
150
152
154
156
157
158
160
162
170
172
174
176
177
178
179
180
181
182
184
190
191
192
194

图 4

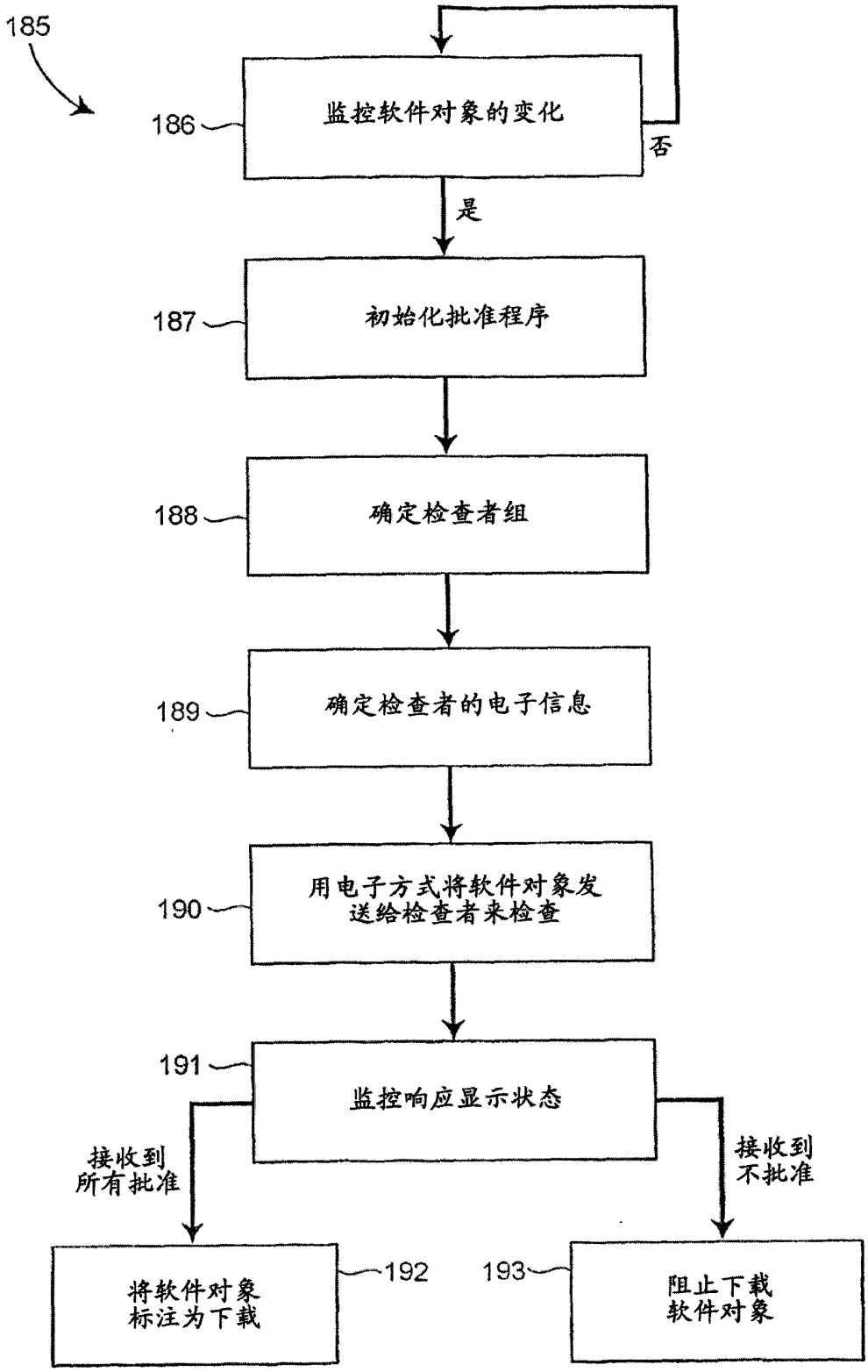

185
186
监控软件对象的变化
否
是
187
初始化批准程序
188
确定检查者组
189
确定检查者的电子信息
190
用电子方式将软件对象发送给检查者来检查
191
监控响应显示状态
接收到所有批准
接收到不批准
192
将软件对象标注为下载
193
阻止下载软件对象

图 5A

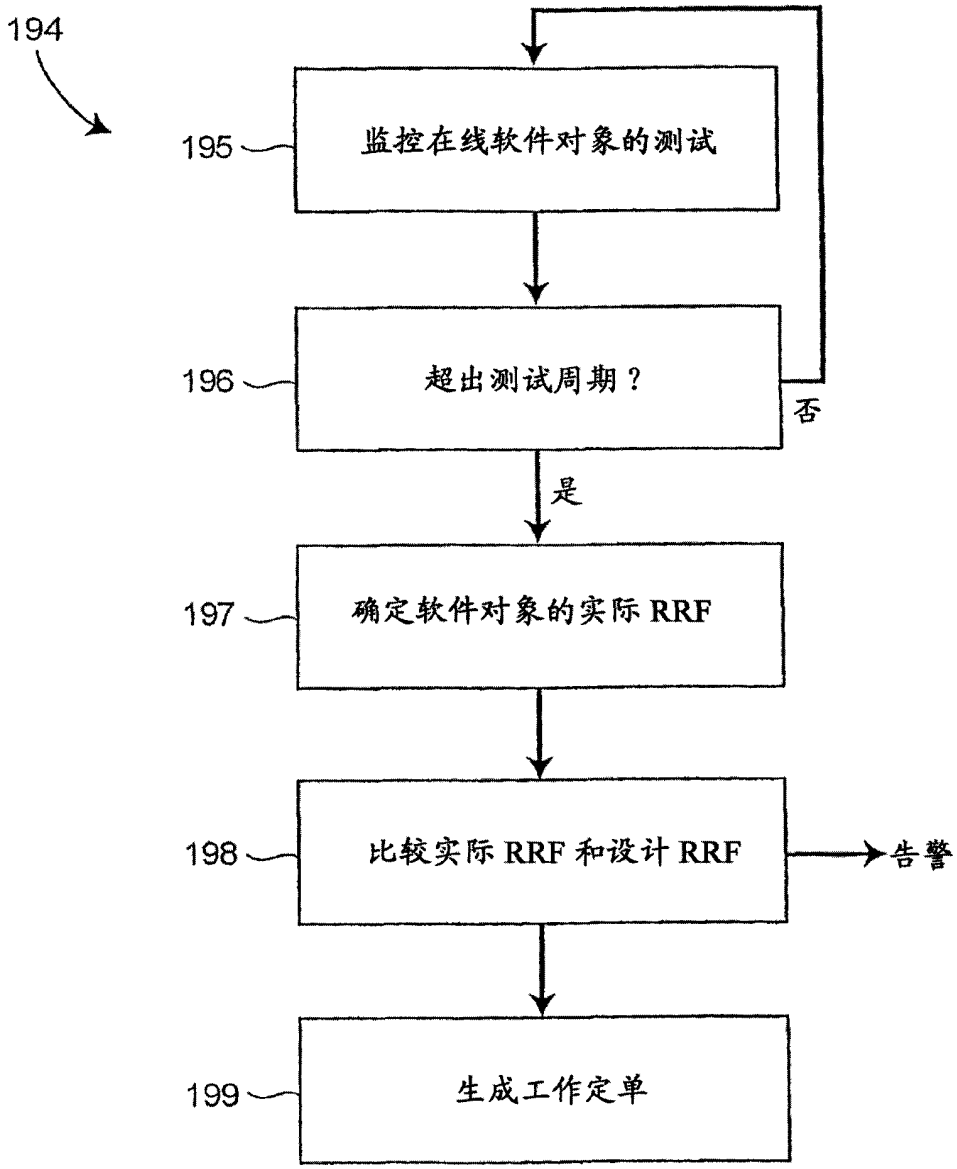

194
195
监控在线软件对象的测试
196
超出测试周期？
否
是
197
确定软件对象的实际 RRF
198
比较实际 RRF 和设计 RRF
告警
199
生成工作定单

图 5B

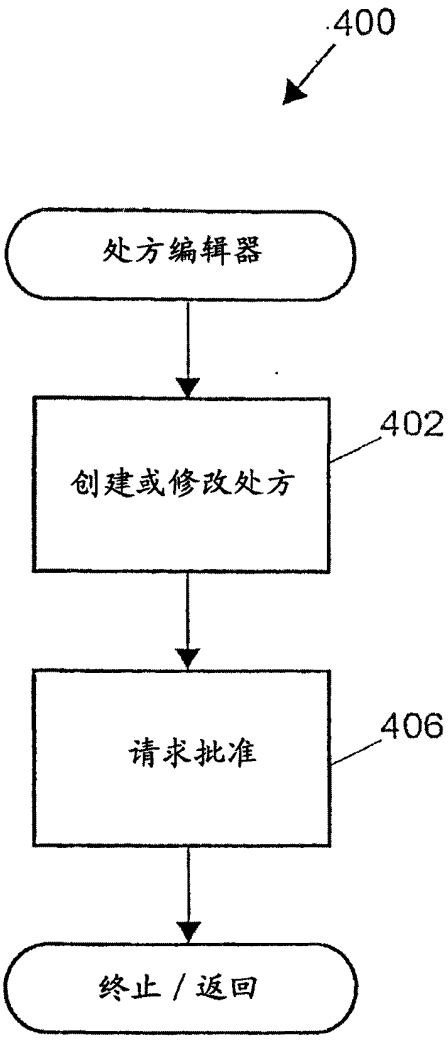



图 6

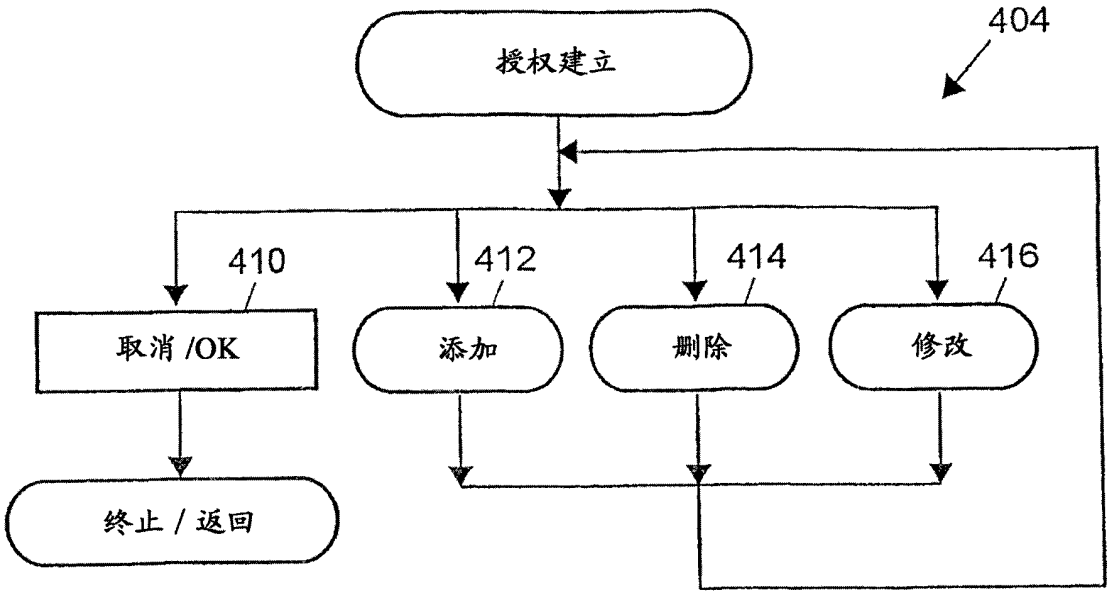

授权建立
404
410
412
414
416
取消 /OK
添加
删除
修改
终止 / 返回

图 7

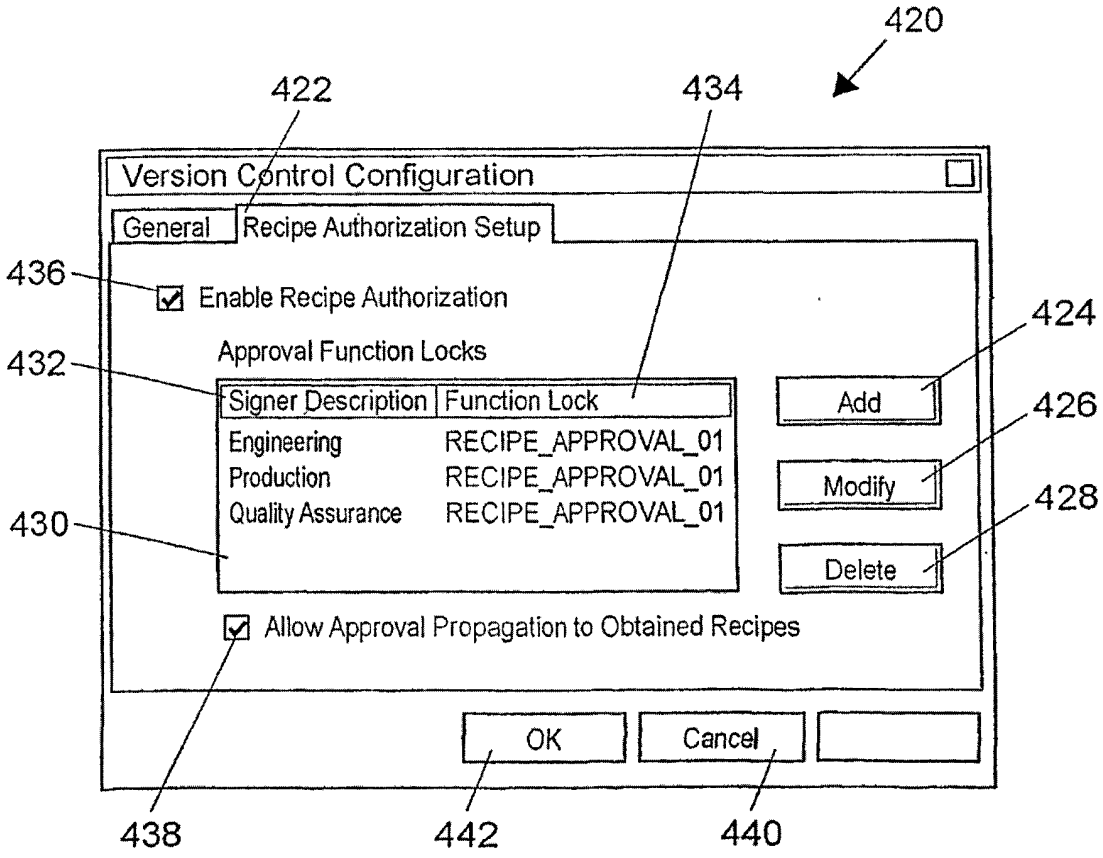

420
422
434
Version Control Configuration
General
Recipe Authorization Setup
436
Enable Recipe Authorization
Approval Function Locks
432
Signer Description
Function Lock
Engineering
RECIPE_APPROVAL_01
Production
RECIPE_APPROVAL_01
Quality Assurance
RECIPE_APPROVAL_01
430
Add
Modify
Delete
424
426
428
Allow Approval Propagation to Obtained Recipes
OK
Cancel
438
442
440

图 8

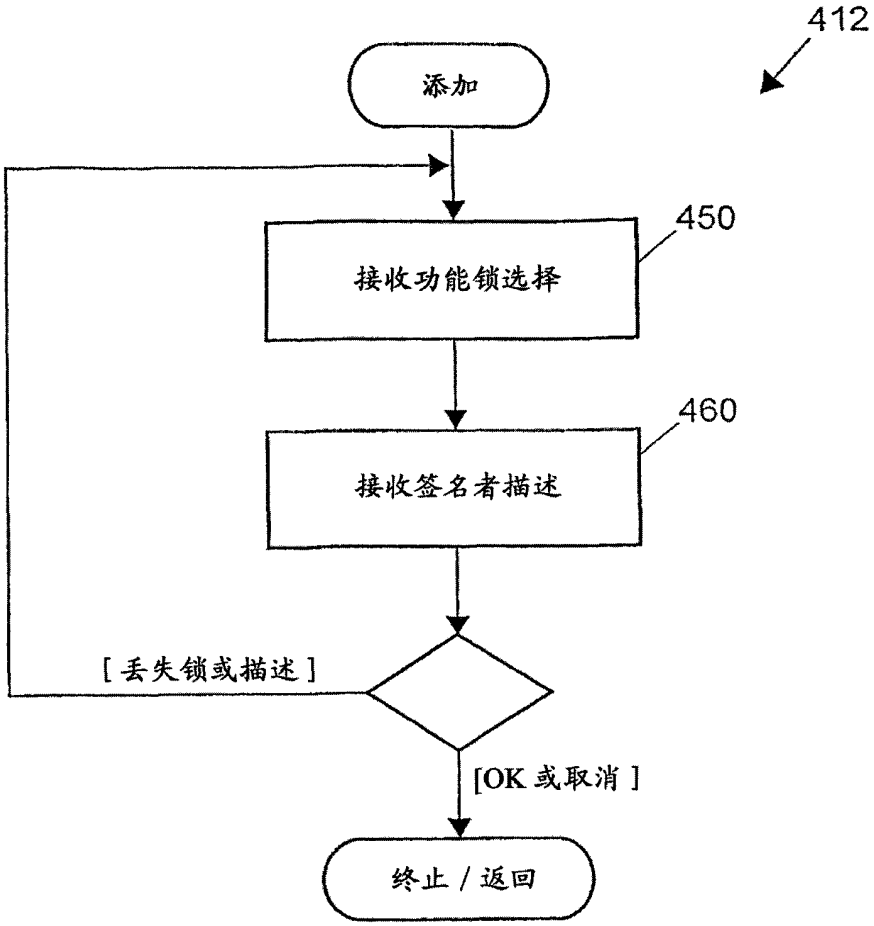

412
添加
450
接收功能锁选择
460
接收签名者描述
[丢失锁或描述]
[OK 或取消]
终止 / 返回

图 9

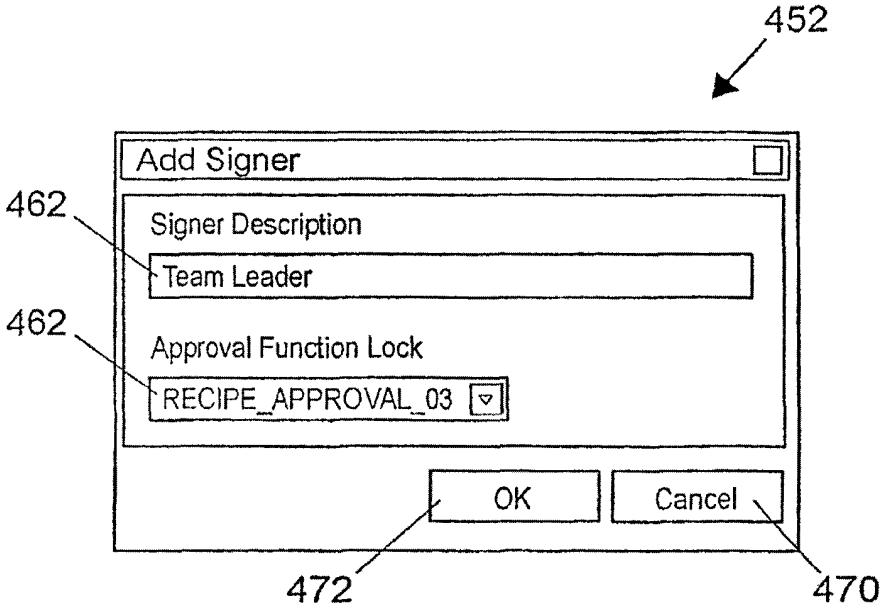

452
Add Signer
462
Signer Description
Team Leader
462
Approval Function Lock
RECIPE_APPROVAL_03
OK
Cancel
472
470

图 10

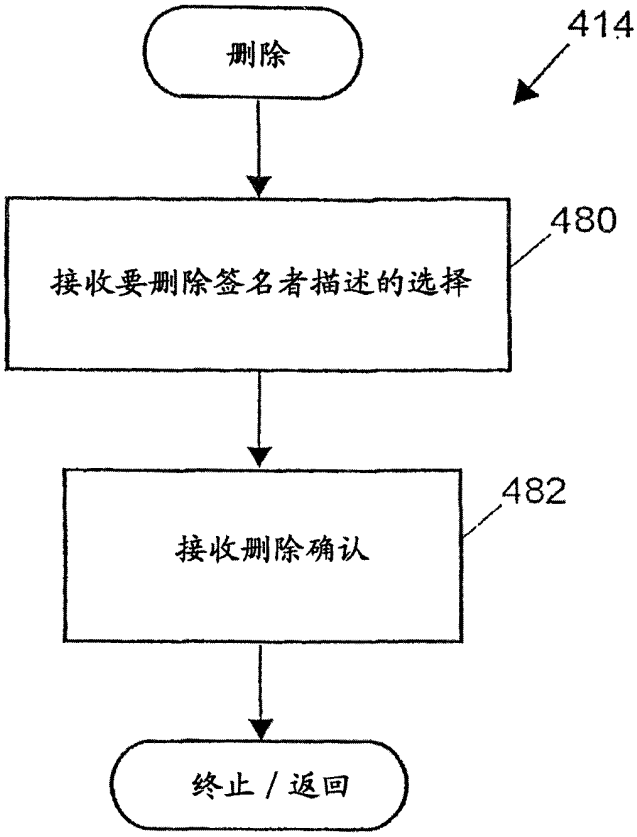



图 11

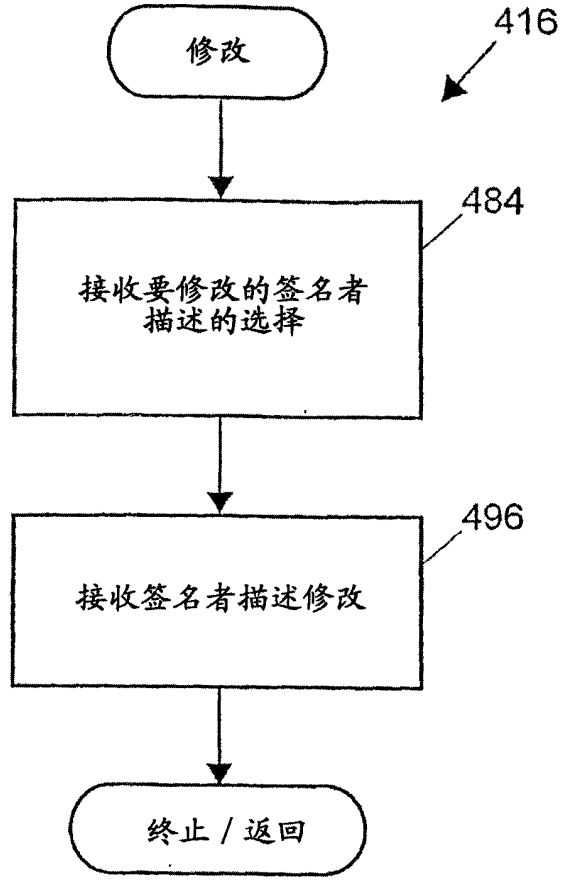

修改
416
484
接收要修改的签名者描述的选择
496
接收签名者描述修改
终止 / 返回

图 12

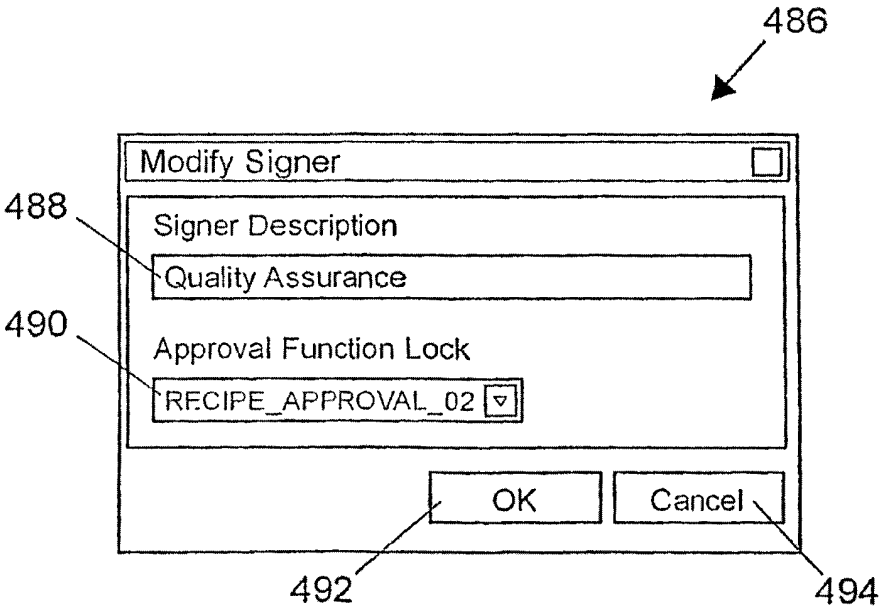

486
Modify Signer
488
Signer Description
Quality Assurance
490
Approval Function Lock
RECIPE_APPROVAL_02
OK
Cancel
492
494

图 13

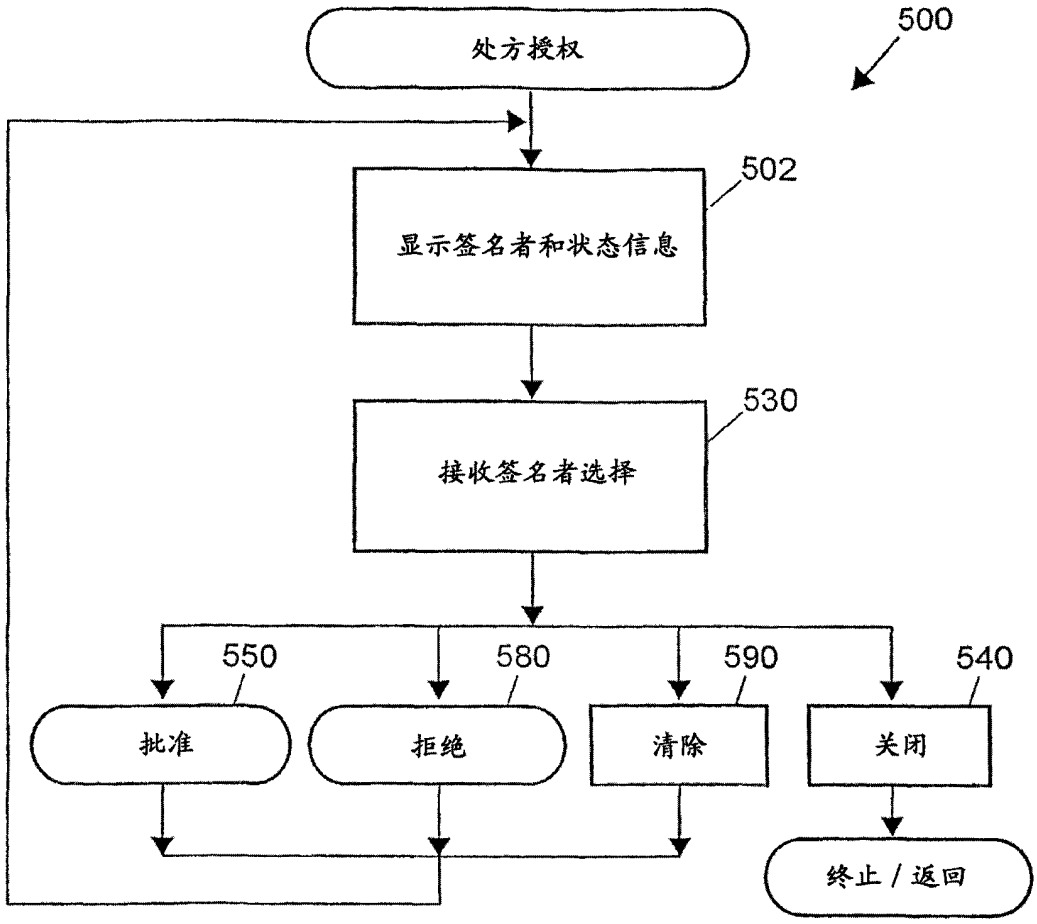

处方授权
500
502
显示签名者和状态信息
530
接收签名者选择
550
580
590
540
批准
拒绝
清除
关闭
终止 / 返回

图 14

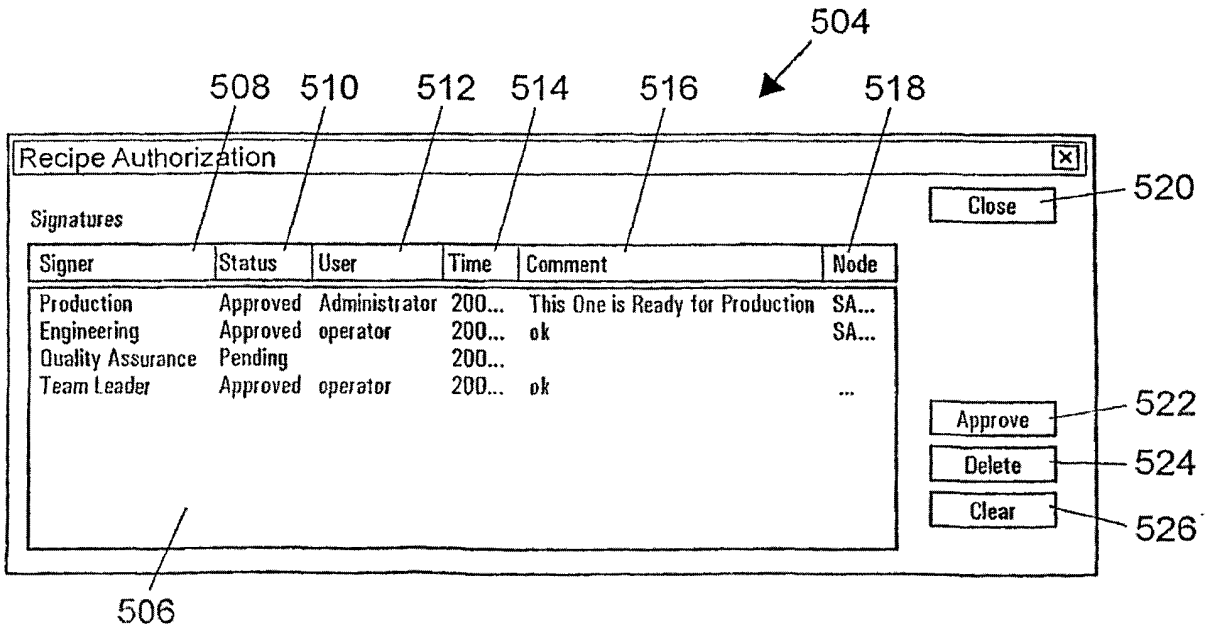

504
508
510
512
514
516
518
Recipe Authorization
Signatures
Signer
Status
User
Time
Comment
Node
Production Approved Administrator 200... This One is Ready for Production SA...
Engineering Approved operator 200... ok SA...
Quality Assurance Pending 200...
Team Leader Approved operator 200... ok ...
Close
520
Approve
522
Delete
524
Clear
526
506

图 15

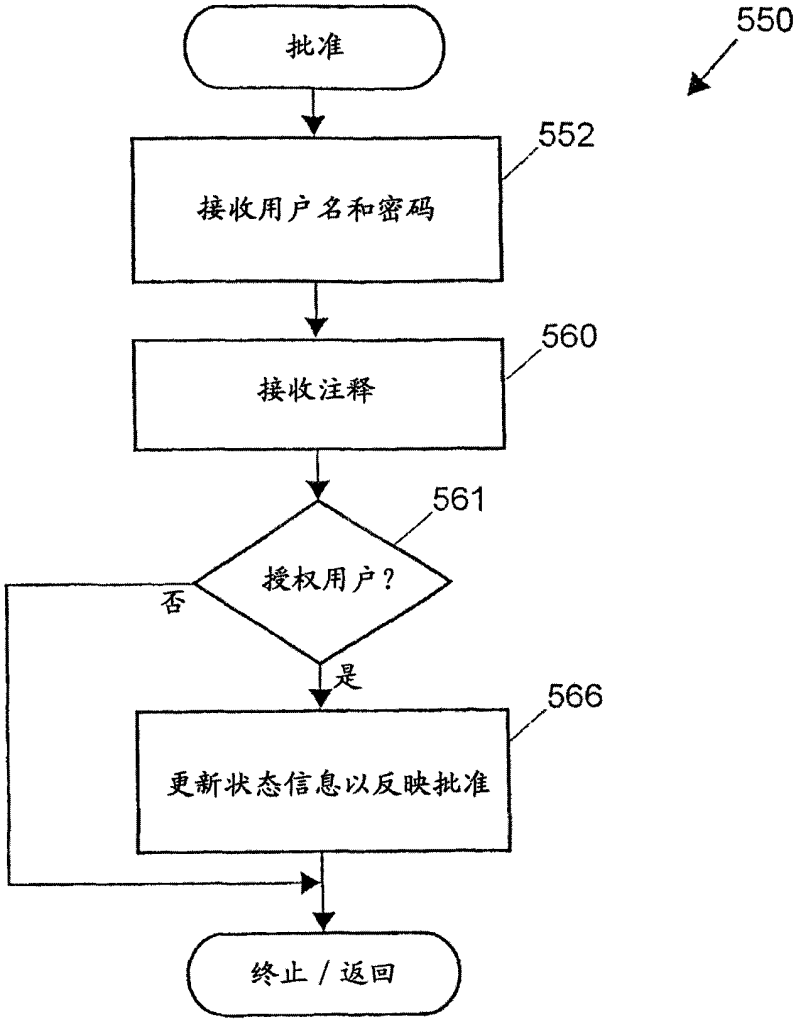

批准
550
552
接收用户名和密码
560
接收注释
561
授权用户？
否
是
566
更新状态信息以反映批准
终止 / 返回

图 16

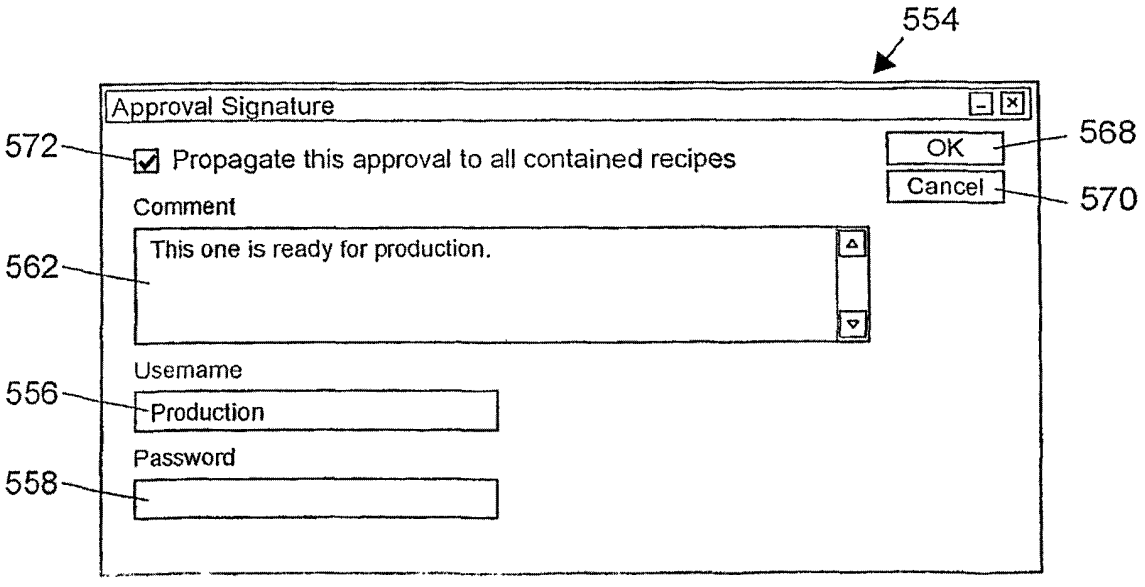

554
Approval Signature
572
Propagate this approval to all contained recipes
OK
568
Cancel
570
Comment
562
This one is ready for production.
Username
556
Production
Password
558

图 17

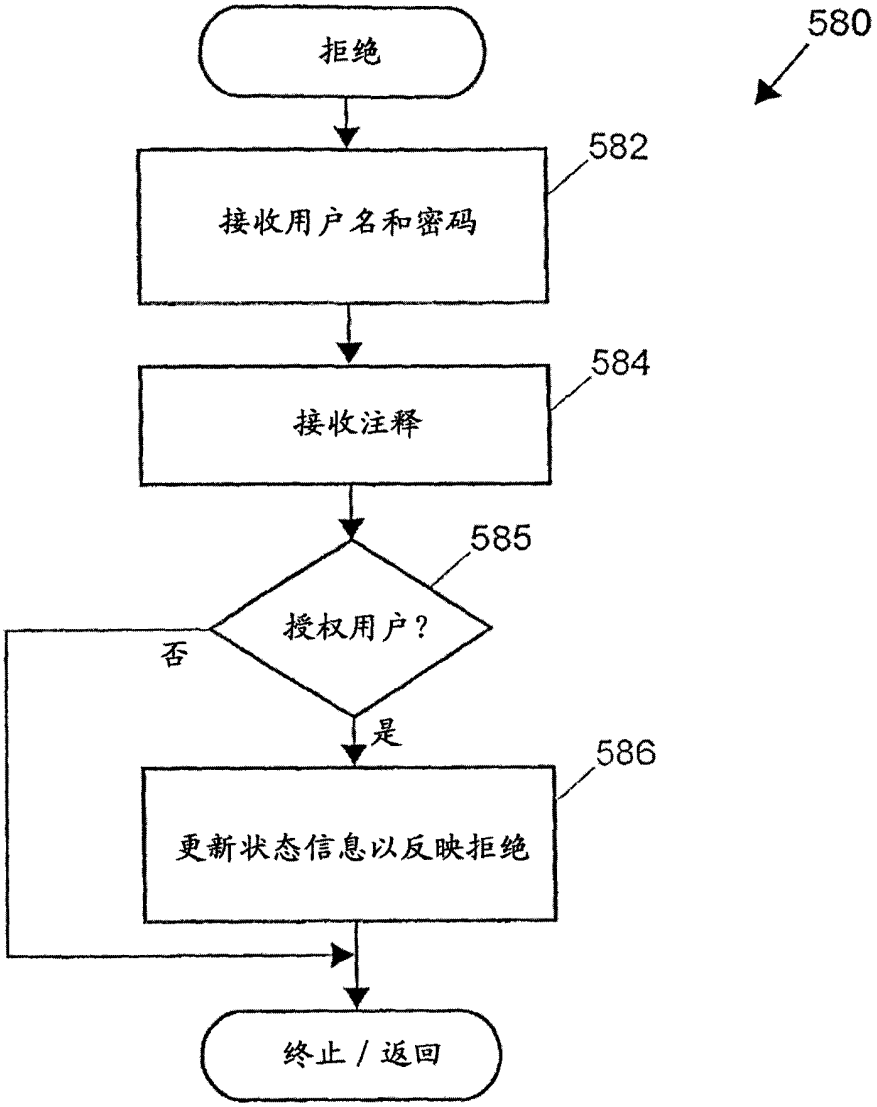

580
拒绝
582
接收用户名和密码
584
接收注释
585
授权用户？
否
是
586
更新状态信息以反映拒绝
终止 / 返回

图 18

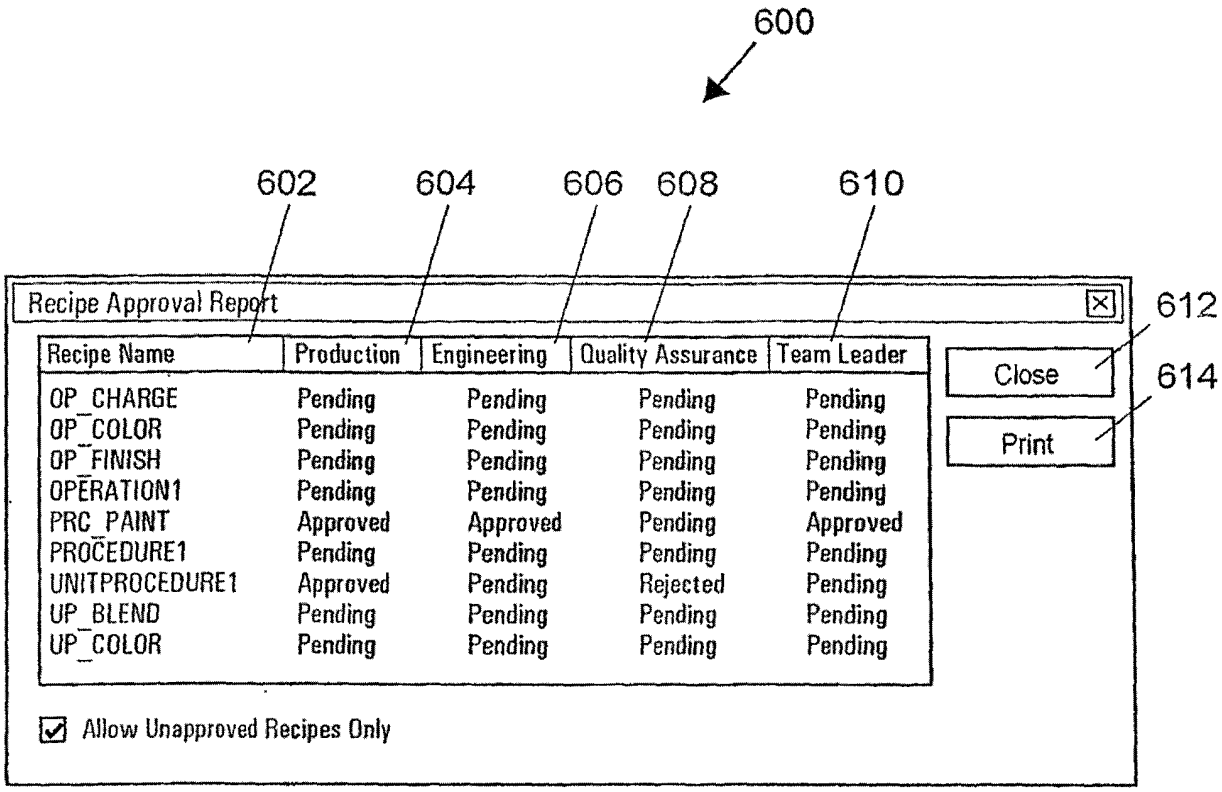

600
602
604
606
608
610
612
614
Recipe Approval Report
Recipe Name
Production
Engineering
Quality Assurance
Team Leader
OP_CHARGE Pending Pending Pending Pending
OP_COLOR Pending Pending Pending Pending
OP_FINISH Pending Pending Pending Pending
OPERATION1 Pending Pending Pending Pending
PRC_PAINT Approved Approved Pending Approved
PROCEDURE1 Pending Pending Pending Pending
UNITPROCEDURE1 Approved Pending Rejected Pending
UP_BLEND Pending Pending Pending Pending
UP_COLOR Pending Pending Pending Pending
Close
Print
Allow Unapproved Recipes Only

图 19

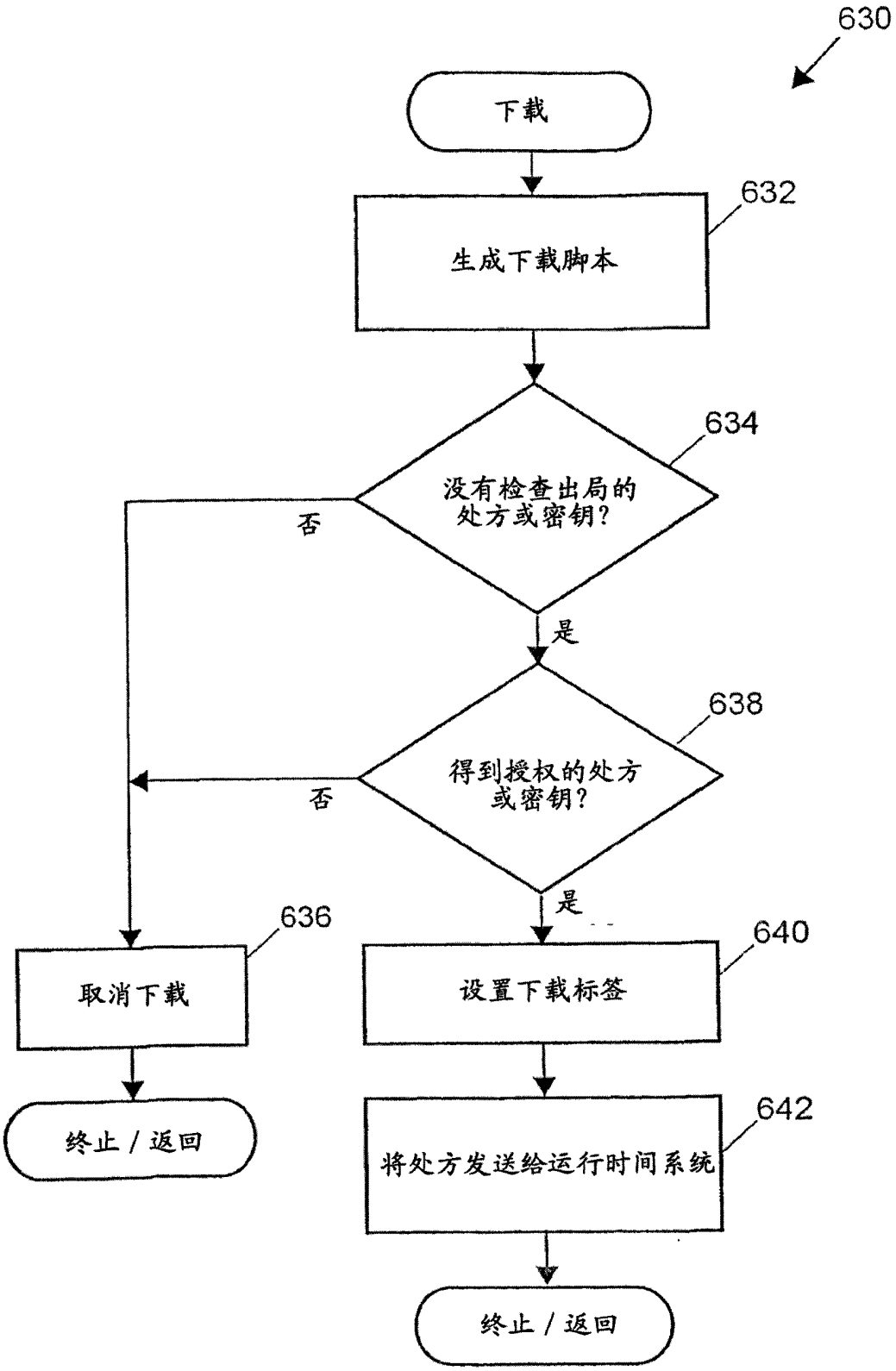

630
下载
632
生成下载脚本
634
没有检查出局的处方或密钥?
否
是
638
得到授权的处方或密钥?
否
是
636
取消下载
640
设置下载标签
642
将处方发送给运行时间系统
终止 / 返回
终止 / 返回

图 20