基于有限状态自动机的带上位机门禁系统的实现与验证

李宗泽

摘要：有限状态自动机理论被广泛运用于专用电子设备与计算机软件的设计与验证。利用有限状态自动机的理论，可以从数学形式上说明设计的完整性与正确性。本文将有限状态自动机的设计方法与门禁系统的开发相结合，介绍了利用有限状态自动机设计并验证系统的基本方法，设计实现了一款带上位机的门禁系统，并对其正确性进行了测试。

关键词： 有限状态自动机 门禁系统 系统测试 实时系统

1.引言

有限状态自动机(FSM)被广泛运用于系统设计与验证中。有限状态自动机拥有有限数量的状态，状态之间根据输入进行转移，可以很好地模拟出现实工业生产等场合设备的工作状态，是一种研究离散事件动态系统的数学模型。在发展的过程中，有限状态自动机理论与计算机科学、自动化等学科紧密联系，被广泛应用于系统的设计及正确性分析，因其具备数学层面的完整描述方法与严密逻辑而具有很高的应用价值。对于部分健壮性需求极高，差错容忍性低的系统，使用有限状态自动机系统进行设计的方式广受赞誉。Bell就曾指出使用形式化方法对于验证航天器系统可靠性的有效之处。[1]

随着电子技术的快速发展与物联网、智慧生活等概念的提出，越来越多的电子控制设备被应用于生活之中，为提高生产效率与生活质量产生了积极的意义。对于部分要求较高安全性的场合，使用传统的电子设计方式由于缺乏严密的数学表述，存在产生漏洞的可能，进而产生安全隐患，这往往会带来不可挽回的损失。因此，可以将有限状态自动机的理论引入产品的设计过程，以确保产品的安全性，同时减少测试的人工消耗与时间损失，提高设计过程的自动化水平。王琳琳等人[2]在WEB应用系统测试之中采用了有限状态自动机的方法，取得了良好的成效。黄志强等人[3]在自动控制软件领域给出了利用有限状态自动机设计的基本方法。实践已经证明，有限状态自动机理论在硬件设计与软件开发领域都发挥着十分积极的影响。

门禁系统属于生产生活中常见的电子系统。可采用专用集成电路、FPGA、单片机等方式组合实现。部分门禁系统有较高的安全需求，并要求一定的实时响应能力，可以在入侵发生时快速进行相应，具备实时系统的特征。本文将有限状态自动机的理论引入门禁系统的设计之中，给出了一个配备上位机的门禁系统的设计，并对其正确性进行了验证。

2.系统建模

使用有限状态自动机进行门禁系统的设计，首要的任务是对真实世界中的门禁系统进行建模，该模型主要关注门禁系统的功能以及约束性条件。因此首先给出一个门禁系统的功能需求。本文设计的门禁系统目的是对来访人员进行甄别，准许符合身份认证的人员进入。在识别到错误的或者不希望的信息之后，门禁系统将发出错误提示。在遭受极端情况如入侵时，该系统必须迅速发出警报并采取紧急措施。为了管理准许进入的人员信息，门禁系统应包含一个特权用户(privileged user)。在识别特权用户的信息后门禁系统进入管理员模式，可以在此模式下添加、删除新用户。在具体实现中，门禁系统采用硬件集成电路与上位机相结合的方式实现。本文主要关注硬件集成电路的模型建立与实现。

给出有限自动机的基本概念：有限自动机的概念于20世纪50年代提出，其创立者包括Moore、Hoffman等人。通常，有限状态自动机被形式化地定义为一个五元组[4]M = ( Q, Σ, δ, q0 , F)。 其中：

(1) Q是状态的非空有穷集合。∀ q∈Q，q称为M的一个状态

(2) Σ称为输入字母表。输入的字符串为Σ上的字符串

(3) δ称为状态转移函数。δ:Q×Σ→Q。对∀(q,a)∈Q×Σ，δ(q,a)=p表示M在状态q读入字符a，将状态变成p并将读头向右移动一个带方格而指向输入字符串的下一个字符。

(4)q0为M的开始状态，q0∈Q。

(5)F为M的终止状态集合，F⊆Q。∀q∈F，q称为M的终止状态。

若对此M进行进一步的约束，使得对于任意的q∈Q，a∈Σ，δ(q,a)均有确定的值，则称此FA为确定的有限状态自动机(DFA)。

若将δ的定义改为：δ:Q×Σ→Q。对∀(q,a)∈Q×Σ，δ(q,a)={p1,p2,…,pm}表示M在状态q读入字符a，可以选择地将状态变成p1,p2,…,pm，并将读头向右移动一个带方格而指向输入字符串的下一个字符。则此FA被称为NFA。NFA相比DFA在形式上更加灵活，但可以证明两者是等价的。

确定的有限状态自动机具有易于由程序实现，且能够很好地描述一个有限状态系统的工作状态。本文设计的门禁系统，同样可以采用确定的有限状态自动机的形式给出描述。可将门禁系统视作由专用硬件电路与上位机结合组成的一个系统，其中上位机可以通过相关的外设接收外部的信号，如添加用户信号、信息卡读取信号等。通过内置的处理程序，上位机处理输入信号并向硬件电路输出对应信号。底层硬件电路接收上位机传达的信号并据此操纵底层硬件，完成开门、关门、报警等功能。因此，对门禁系统模型的分析，需要从上位机与底层电路两方面进行考量。

首先给出门禁系统整体的功能需求。结合之前对门禁系统的功能分析，在此给出本文设计的门禁系统应该识别的信号以及期望的门禁系统给出的相应操作：

1.特权用户登录信号

接收到此信号后，门禁系统将进入管理员模式。可以在此模式下进行新用户的添加与旧用户的删除。

2.退出管理员状态信号

接收此信号后，门禁系统退出管理员模式，返回普通模式。

3.添加新用户信号。

接收此信号后，门禁系统进入用户添加模式，并等待新用户姓名与新用户信息卡信息的输入。接收到新用户姓名与新用户信息卡后门禁系统完成创建新用户操作。

4.删除用户信号

接收此信号后，门禁系统从可进入的人员名单中删除指定的项。

5.信息卡识别信号

接收此信号后，门禁系统根据输入的信息卡信息是否符合期望决定是否打开大门。门开启后相应的硬件会确保人员进入后大门重新关闭。

6.入侵发生信号

当检测到有入侵发生时，门禁系统会锁死大门并发出警报。

门禁系统的基本功能由硬件集成电路与上位机共同实现。现分别给出硬件集成电路与上位机需接收的信号以及需实现的功能，并说明他们之间的交互关系。

硬件集成电路模块需要识别的信号以及需进行的对应动作如下：

1.识别特权用户的登录信息并传递至上位机

特权用户有特有的登录方式（如特制信息卡）。硬件电路可以对其进行识别并发送信号给上位机，使其进入管理员模式。

2.在管理员模式下添加新用户时，需要接收新用户的姓名信息与信息卡信息并传送至上位机。其中，信息卡信息的采集采取读卡器读取的方式。

3.在普通模式下，硬件电路可以读取用户信息卡，并将信息送入上位机。上位机在读取信息后进行比较验证，根据此信息卡是否有效发送相应的控制信号。硬件电路接收上位机发送的验证信号并决定是否打开大门。在打开大门的同时，硬件集成电路将会记录用户到来/离开的时间并上报给上位机。

4.硬件集成电路配备有相应的传感器监控硬件状态。一旦察觉到入侵出现，将会立刻进入紧急状态并发出警报。同时会向上位机发送入侵相关的信息。

上位机模块需要识别的信号以及需要进行的对应操作如下：

1.接收来自硬件集成电路模块的特权用户登录信号并进入管理员模式。

2.在管理员模式下接收通过硬件集成电路模块传递的新用户名与新用户卡信息，并进行添加操作，将新用户添加至可进入用户名单。

3.在管理员模式下接收通过硬件集成电路模块传递的删除用户信息信号并将选定的用户从可进入名单中删除。

4.在普通模式下接收硬件集成电路传递来的信息卡信息，并经过处理、比对，发送相应的信号给硬件集成电路模块，决定其是否打开大门。

5.在接收到入侵信号时进入紧急状态，记录遭受的入侵的相关信息。

考虑到以上的功能分析，以及DFA与NFA的定义，现根据有限状态自动机的模型分别给出硬件集成电路与上位机的模型。其中硬件集成电路采用DFA的模型，上位机采用NFA的模型。

硬件集成电路：

考虑DFA模型的形式化定义M = ( Q, Σ, δ, q0 , F)。对于硬件集成电路的模型，给出除δ外每一元素对应的内容。为了便于理解，从Σ开始介绍。

Σ：Σ为输入字母表，在此模型中指传递给硬件集成电路的信号。根据之前的分析，  
Σ={p\_login,p\_exit,add\_name,add\_card,delete\_name,card\_info,card\_first,card\_second,wrong\_card,reset,danger,ok}

这些信号有些来自于上位机系统，有些来自于硬件电路如读卡器。

现给出每个信号的解释：

p\_login:特权用户登录信号。硬件拥有对特权用户的检测能力。当检测到正确的特权用户登录信号后，可视作硬件接收到p\_login信号。

p\_exit:特权用户退出信号。当特权用户选择退出时，上位机向硬件电路发出登出信号p\_exit，使其退出管理员模式，回归正常模式。

add\_name:在管理员模式下，特权用户向门禁系统添加新用户时，先向上位机发送姓名信息，随后上位机通过add\_name信号通知硬件电路准备读取新用户的信息卡信息。

add\_card:当上位机通知硬件电路准备读取新用户信息卡后，此时新用户需将信息卡放至信息采集硬件上。硬件识别其为有效的信息卡后向硬件电路发送add\_card信号。硬件电路会将此时采集到的信息卡信息上报给上位机。

delete\_name:在管理员模式下删除已添加用户时，上位机向硬件电路发送deletename信号。硬件电路接收此信号后进入等待删除完成状态。

card\_info：当硬件电路配备的读卡器读取到信息卡信息后，即向硬件电路发送card\_info信号标志已经读取到信息卡信息。硬件电路会将读取到的具体信息卡信息发送至上位机。

card\_first:上位机识别硬件电路发来的信息卡信息，若确定此信息卡有效，并且是第一次申请（即申请进入），则向硬件电路发送card\_first信号。硬件电路此时开门放行并将此信息卡对应用户的状态改为“已经进入”。除此之外还可以进行计时等其他操作。

card\_second:上位机识别硬件电路发来的信息卡信息，若确定此信息卡有效，并且是第二次申请（即申请离开），则向硬件电路发送card\_second信号。硬件电路此时开门放行并将此信息卡对应用户的状态改为“已经离开”。除此之外还可以进行记录此用户进入时间等其余功能。

wrong\_card: 上位机识别硬件电路发来的信息卡信息，若确定此信息卡无效，则向硬件电路发送此信号。硬件电路提示错误信息。一段时间后提示错误信息的部件会向硬件电路发送reset 信号。

reset:此信号可来自上位机或硬件，用于使硬件系统返回初始状态。

danger:当检测到入侵发生时硬件电路接收到danger信号进入紧急状态。

ok:硬件系统在许多状态下需要与上位机进行通讯。当上位机确认接收到信号或已经完成处理后会向硬件电路发送此信息。

需要进行说明的是，在一个系统中已经注册的用户可以有无限多个。在同一时刻也可以有多个用户同时位于安防场所内，因此门禁系统需要记忆的状态有无限多种，这显然超出了DFA的表示能力。因此，在本文中，给出的状态模型以及状态转移图将视为只有一个用户的状态。对于有多个用户的情况，可以视为门禁系统可以同时实现无数个子线程，每个线程均对应文中给出的一个状态机。门禁与不同的用户之间进行交互的时候，分别使用不同的子线程。同样，发送向硬件电路中的信号也会标注自己对应的线程号从而被送向对应的状态机。以此完成模型的简化。

Q：Q是状态的有穷集合。根据之前的分析，可以认为硬件集成电路对应的有限状态自动机有以下的状态：

Q0：即为启动后的初始状态。在此状态下硬件电路随时监测外部发来的信号并根据到来的信号转移至相应的状态。

Q1：为管理员模式态。在此状态下可以进行添加新用户与删除新用户的操作。

Q2：等待添加用户信息卡状态。此状态下硬件电路会监视信息卡采集器并将采集到的信息转交上位机。

Q3：等待确认用户添加状态。此状态下硬件电路等待上位机发来的确认信号ok。在此之前不能响应其他请求。

Q4：等待确认删除用户状态。此状态下硬件电路等待上位机发来的确认信号ok以确认删除用户操作完成。在此之前不能响应其他请求。

Q5：接收到信息卡状态。此状态下硬件电路会将采集到的信息卡信息转交上位机，并等待上位机发来的后续信号。

Q6：接收到进入请求状态。此状态表示硬件电路第一次接收到有效信息卡，即接收到有效的进入申请之后的状态。在此状态下，硬件电路会开门放行并在确认申请进入者进入后重新关闭大门。与此同时向上位机汇报进入时间。

Q7：接收到离开请求状态。此状态表示硬件电路接收到有效的请求离开信号后的状态。在此状态下硬件电路会向上位机汇报离开的时间。

Q8：接收到错误的卡信息状态。在此状态下硬件电路会给出表示卡错误的提示。

Q9：紧急状态，表示遭受入侵或其他紧急状态。在此状态下硬件电路会立刻锁死大门并发出警报。同时会向上位机发出入侵信号。

q0:开始状态。此系统的开始状态只有一个，即起始状态Q0。

F：终止状态。若对进入的句子进行识别，最终进入终止状态，说明进入的句子是合理的。对于此门禁系统，如果发来的信息序列是符合常理的，那么系统最终会进入Q0或Q1状态。因此终止状态集合为{ Q0，Q1}。

下面对于上位机系统采用同样的方式进行建模分析。

首先给出上位机模块需要识别的信号以及需进行的对应动作。

1.接收来自硬件系统传来的信息卡信号，并根据此信息卡是否为特权用户信息卡，是否有效，是进入还是离开，向硬件电路发出对应的控制信号。

2.接收来自硬件系统的入侵信号，并进入紧急状态，尝试联络外界发出警报。

3.在管理员模式下接收新用户的姓名信息与信息卡信息，并创建新用户。

4.在管理员模式下接收要删除用户的姓名，并删除用户。

考虑到以上的功能分析，结合NFA模型的形式化定义M = ( Q, Σ, δ, q0 , F)。对于硬件集成电路的模型，给出除δ外每一元素对应的内容。为便于理解，从Σ开始介绍。

Σ：Σ为输入字母表，在此模型中指传递给硬件集成电路的信号。根据之前的分析，Σ={card\_info,p\_exit,name,deletename,intrude,reset,ret}

现给出每个信号的解释：

card\_info：表示硬件电路传递来的信息卡信息。在接收此信息后上位机将会运转判定程序，确定此卡信息是否有效，是否为权限用户，是申请进入还是申请离开。并因此进入不同的状态，向硬件电路发送不同的信息。

name：表示添加新用户时输入的新用户姓名。接收此信息后，上位机等待新用户的信息卡信息并据此创建新用户。

deletename：表示删除用户时传递来的要删除用户姓名信息。上位机据此进行删除用户操作。

intrude：入侵信号。在接收此信号后上位机进入紧急模式，将会寻求向外界发出警报。

reset：复位信号。接收此信号后上位机复位。

ret：上位机需要运行许多处理程序，由于采用了FA的模型，本模型中将处理程序运行结束返回视为一条“输入信号”。实际上这是由上位机内部自行产生的信号。进行这种处理可以使我们用NFA描述上位机的行为模式。

Q：Q是状态的有穷集合。根据之前的分析，可以认为上位机对应的有限状态自动机有以下的状态：

Q0：此状态为上位机的初始状态，在此状态下上位机等待传递来的信号并作出相应的行为，并转移至其他状态。

Q1：此状态为上位机处理信息卡信息状态。上位机在接收到硬件电路传递来的信息卡信息后进行处理程序对信息卡进行判断，并发送对应的信号至硬件电路。

Q2：此状态为管理员模式。在此模式下上位机可以接收相应信息完成新用户添加与删除已有用户的操作。

Q3：此状态为添加新用户时等待新用户信息卡状态。上位机等待新用户的信息卡从硬件电路模块传递，以完成新用户添加操作。

Q4：此状态为等待创建新用户操作完成状态。当上位机接收到要添加的用户的姓名与信息卡后，他进入此状态等待创建完成。

Q5：此状态为等待删除操作完成状态。当上位机在管理员模式下接收到要删除用户的姓名后，他进入此状态等待删除操作完成。

Q6：此状态为信息卡错误状态。当上位机接收到输入的信息卡信息并判定其无效时，其进入此状态向硬件电路发送错误信号。

Q7：此状态为警报状态。在此状态下上位机将试图向外界发送警报信息。

q0:开始状态，对应Q0。

F：终止状态。在此模型中，正常工作状态下，上位机处理完请求后总是会回到Q0或Q2状态。因此F={ Q0, Q2}。

3.系统实现

系统的具体实现，即完成硬件电路状态机以及上位机模块对应的有限状态自动机的状态转移函数δ。根据模型建立阶段对两个状态机的建模分析，可以得出其状态转移函数如下，其中各状态的具体解释见第二部分系统建模：

对于底层硬件电路，有：

δ(q0,p\_login) = q1 代表硬件电路接收到特权用户信息卡，进入管理员模式Q1。

δ(q0,card\_info) = q5 代表硬件电路接收到普通信息卡信息，进入Q5状态。

δ(q0,danger) = q9 代表硬件电路接收到危险信号，进入Q9状态。

δ(q0,p0) = q0 其中p0∈{Σ-{p\_login,card\_info,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q0状态直至接收到可以引发状态转移的信号。

δ(q1,p\_exit) = q0 代表硬件电路在Q1接收到特权用户登出信号，进入Q0状态。

δ(q1,add\_name) = q2 代表硬件电路在Q1接收到添加新用户姓名信号，进入Q2状态。

δ(q1,delete\_name) = q4 代表硬件电路在Q1接收到删除新用户姓名信号，进入Q4状态。

δ(q1,danger) = q9 代表硬件电路在Q1接收到危险信号，进入Q9状态。

δ(q1,p1) = q1 其中p1∈{Σ-{p\_exit,add\_name,delete\_name,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q1状态直至接收到可以引发状态转移的信号。

δ(q2,danger) = q9 代表硬件电路在Q2接收到危险信号，进入Q9状态。

δ(q2,add\_card) = q3 代表硬件电路在Q2接收到新用户信息卡信息，进入Q3状态。

δ(q2,p2) = q2 其中p2∈{Σ-{add\_card,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q2状态直至接收到可以引发状态转移的信号。

δ(q3,danger) = q9 代表硬件电路在Q3接收到危险信号，进入Q9状态。

δ(q3,ok) = q1 代表硬件电路在Q3接收到来自上位机的添加完成信号ok，进入Q1状态。

δ(q3,p3) = q3 其中p3∈{Σ-{ok,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q3状态直至接收到可以引发状态转移的信号。

δ(q4,danger) = q9 代表硬件电路在Q4接收到危险信号，进入Q9状态。

δ(q4,ok) = q1 代表硬件电路在Q4接收到来自上位机的删除完成信号ok，进入Q1状态。

δ(q4,p4) = q4 其中p4∈{Σ-{ok,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q4状态直至接收到可以引发状态转移的信号。

δ(q5,card\_first) = q6 代表硬件电路在Q5接收到上位机发来的信号card\_first，表示有人请求进入，进入Q6状态。

δ(q5,wrong\_card) = q8 代表硬件电路在Q5接收到上位机发来的信号wrong\_card，表示接收到错误的卡信息，进入Q8状态。

δ(q5,danger) = q9 代表硬件电路在Q5接收到危险信号，进入Q9状态。

δ(q5,p5) = q5 其中p5∈{Σ-{card\_first,danger,wrong\_card}}代表硬件电路接收到此刻不希望的信号，其将保持在Q5状态直至接收到可以引发状态转移的信号。

δ(q6,danger) = q9 代表硬件电路在Q6接收到危险信号，进入Q9状态。

δ(q6,card\_second) = q7 代表硬件电路在Q6接收到上位机传来的card\_second信号表示申请离开，进入Q7状态。

δ(q6,p6) = q6 其中p6∈{Σ-{card\_second,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q6状态直至接收到可以引发状态转移的信号。

δ(q7,danger) = q9 代表硬件电路在Q7接收到危险信号，进入Q9状态。

δ(q7,ok) = q0 代表硬件电路在Q7接收到上位机传来的添加操作完成信号ok，进入Q0状态。

δ(q7,p7) = q7 其中p7∈{Σ-{ok,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q7状态直至接收到可以引发状态转移的信号。

δ(q8,danger) = q9 代表硬件电路在Q8接收到危险信号，进入Q9状态。

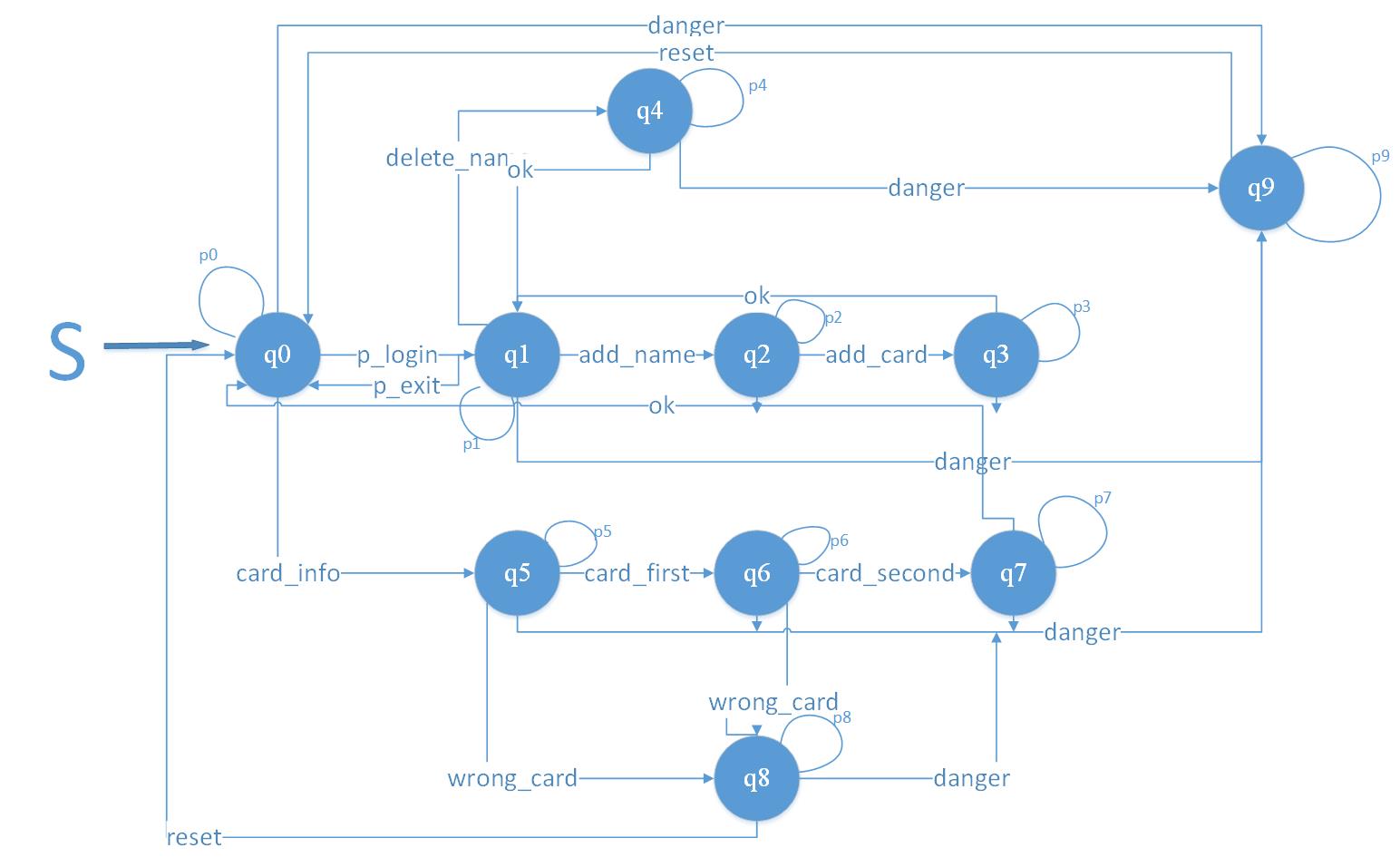
δ(q8,reset) = q0 代表硬件电路在Q8接收到归位信号，进入Q0状态。

δ(q8,p8) = q8 其中p8∈{Σ-{reset,danger}}代表硬件电路接收到此刻不希望的信号，其将保持在Q8状态直至接收到可以引发状态转移的信号。

δ(q9,reset) = q0 代表硬件电路在Q9接收到归位信号，进入Q0状态。

δ(q9,p9) = q9 其中p9∈{Σ-{reset }}代表硬件电路接收到此刻不希望的信号，其将保持在Q9状态直至接收到可以引发状态转移的信号。

由此可以绘制出硬件电路对应的DFA的状态转移图如下：



对于上位机模块，采取NFA进行描述，有：

δ(q0,card\_info) = {q1 , q2 , q6 } 代表上位机接收到信息卡信息，若为正常的信息卡，则此进入Q1状态，若为特权用户信息卡，则此进入Q2状态，若为错误的信息卡，则此进入Q6状态。运行相应处理程序。

δ(q0,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

δ(q1,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

δ(q1,ret) = q0 代表上位机运行的处理程序运转完成，返回Q0状态。

δ(q2,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

δ(q2,name) = q3 代表上位机在管理员模式下接收到添加新用户姓名信号，进入Q3状态。

δ(q2,delete\_name) = q5 代表上位机在管理员模式下接收到删除用户信号，进入Q5状态。

δ(q2,p\_exit) = q0 代表上位机在管理员模式下接收到登出信号，回到正常的工作模式即Q0状态。

δ(q3,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

δ(q3,card\_info) = q4 代表上位机在管理员模式下接收到添加新用户姓名信号后，接收到新用户信息卡信号，进入Q4状态。

δ(q4,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

δ(q4,ret) = q2 代表上位机运行添加用户程序结束，返回Q2状态。

δ(q5,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

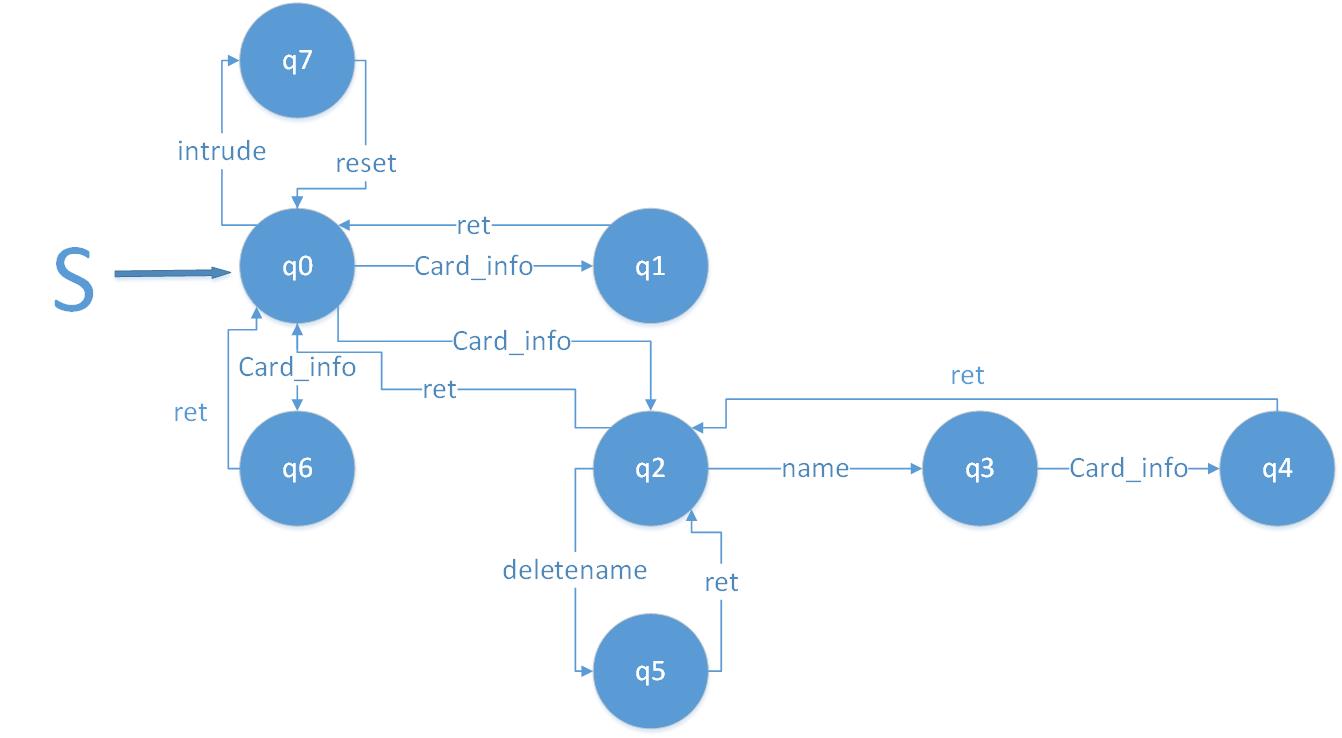
δ(q5,ret) = q2 代表上位机运行删除用户程序结束，返回Q2状态。

δ(q6,intrude) = q7 代表上位机接收到硬件电路传递的入侵发生信号，进入Q7状态，即进行警报。

δ(q6,ret) = q0 代表上位机运行输出错误信息程序结束，返回Q0状态。

δ(q7,ret) = q0 代表上位机在警报状态接收到返回信号，返回正常工作状态q0。

其对应的NFA的状态转移图如下：



4.系统验证

对于模型正确性的验证，可以采用软件工程中测试软件的相应原则。甚至测试的具体过程也可使用有限状态自动机(FSM)进行。Yongfeng Yin1, Bin Liu, Hongying Ni等人[5]就指出，利用状态的软件测试技术可以完全地验证系统的表现是否符合预期。刘攀,缪淮扣,曾红卫等[6]介绍了使用FSM完成软件验证的测试理论、方法及评估。本文仅从方法论角度提出使用FSM对门禁系统进行测试的基本方法，并不聚焦于讨论其具体细节。

在门禁系统的实际应用中，如果对其的使用是正确的，那么门禁系统最后总会停留在起始状态或管理员模式状态，即上位机与硬件电路对应的FA最终停留在终止状态。对于上位机对应的NFA，由于NFA在一定程度上具有智能，其正确性依赖于其软件的具体实现，因此较难验证。本文只考虑对硬件电路对应的DFA进行验证。验证借助计算机编程实现，其具体步骤包括：1.构造DFA对应的验证程序，其接受输入并不断完成状态的变换。2.构造有效输入消息队列。3.使用构造出的状态机模型接收构造的有效输入消息队列，并一步步观察其接收后的状态是否符合需求，以及其最终能否进入终止状态。验证的具体实现不在本文关心的范围之内。

5.总结

有限状态自动机理论与电子工程、计算机科学等领域联系密切。通过有限状态自动机完成系统的设计与验证，可以提高设计的质量，确保设计出的系统具有较高的安全性与行为的确定性，从而减少设计出现缺漏，从而出现意料之外的情况，进而造成经济损失与生命财产损失的情况。此外，有限状态自动机理论的运用可以使系统的设计过程实现规范化、流程化，方便后续的测试，也方便对系统进行修改与优化。同时，规范化设计可以降低设计需求的人力成本与时间成本，加速产品设计实现的周期。在高精密度、高安全需求的产品设计领域如航天器设计，利用有限状态自动机进行设计的方法已经得到广泛的应用。本文使用有限状态自动机的理论设计了一款带上位机的门禁系统，具有较强的实际意义，同时也为使用有限状态自动机理论进行电子产品的设计与开发提供了思路，存在一定的参考价值。

参考文献

[1] D. G. Bell, G. P. Brat. Automated software verification & validation: an emerging approach for ground operations. Proc.of the IEEE Aerospace Conference, 2008: 1–8.

[2]王琳琳,刘耀军 基于有限状态自动机极小化的 Web 应用系统测试 [J] 太原科技大学学报 ,2017, 38(1):11-14

[3]黄志强,苏颖 有限自动机在自动控制软件设计中的应用 [J] 华北电力大学学报,2002,29(1):49-51

[4]蒋宗礼,姜守旭 形式语言与自动机理论: 第三版[M] 北京: 清华大学出版社,2013

[5]Yongfeng Yin1, Bin Liu, Hongying Ni:Real-time embedded software testing method based on extended finite state machine，Journal of Systems Engineering and Electronics Vol. 23, No. 2, April 2012, pp.276–285

[6]刘攀,缪淮扣,曾红卫等 基于 FSM 的测试理论、方法及评估［J］计算机学报,2011,34(6):965-984．