Software Engineering and Applications 软件工程与应用, 2020, 9(5), 434-440
Published Online October 2020 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2020.95050

Hans汉斯

一种适应多芯场景的安全芯片业务测试系统设计

周　静[1,2]，付青琴[1,2]，刘　佳[1,2]，白雪松[1,2]，梁昭庆[1,2]

[1]北京智芯微电子科技有限公司，国家电网公司电力芯片设计分析重点实验室，北京
[2]北京智芯微电子科技有限公司，北京市电力高可靠性集成电路设计工程技术研究中心，北京
Email: zhoujing@sgitg.sgcc.com.cn, fuqingqin@sgitg.sgcc.com.cn, liujia8@sgitg.sgcc.com.cn, baixuesong@sgitg.sgcc.com.cn, liangzhaoqing@sgitg.sgcc.com.cn

收稿日期：2020年10月7日；录用日期：2020年10月21日；发布日期：2020年10月28日

摘　要

本文分析了多芯模组化智能电表的应用给安全芯片业务场景测试带来的挑战和问题，分析了传统测试方法中存在的缺陷，提出了能适应多芯业务场景的自动化业务测试系统。此方法通过提取用例，对安全芯片的业务进行模块化设计，提取密钥场景和芯片指令等可变量参数，封装SPI，7816，645协议，模拟多芯场景的业务交互流程，实现了业务流程的模块化和自动化，大大的提升了安全芯片业务流程测试的效率。

关键词

安全芯片，业务流程测试，模块化，多芯业务场景

A Multi-Core Adaptable Automatic Workflow Testing System Design for Security Chip

Jing Zhou[1,2], Qingqin Fu[1,2], Jia Liu[1,2], Xuesong Bai[1,2], Zhaoqing Liang[1,2]

[1]Key Lab of Power Grid Design and Analysis, State Grid Corporation of China, Beijing Intelligent Microelectronics Technology Co., Ltd., Beijing
[2]Beijing Electric Power High Reliability Integrated Circuit Design Engineering Research Center, Beijing Intelligent Microelectronics Technology Co., Ltd., Beijing
Email: zhoujing@sgitg.sgcc.com.cn, fuqingqin@sgitg.sgcc.com.cn, liujia8@sgitg.sgcc.com.cn, baixuesong@sgitg.sgcc.com.cn, liangzhaoqing@sgitg.sgcc.com.cn

Received: Oct. 7th, 2020; accepted: Oct. 21st, 2020; published: Oct. 28th, 2020

文章引用: 周静, 付青琴, 刘佳, 白雪松, 梁昭庆. 一种适应多芯场景的安全芯片业务测试系统设计[J]. 软件工程与应用, 2020, 9(5): 434-440. DOI: 10.12677/sea.2020.95050

Abstract

This paper analyzes the challenges and problems for workflow testing for introducing the multi-core energy meter, and the faults of traditional workflow testing of security chip, and proposes a multi-core adaptive automatic workflow testing for security chip. This method is based on user case extraction and the workflow modulization of security chip. It extracts the variables like key state and instructions, and encapsulates SPI, 7816, 645 protocol, to simulate the multi-core workflow. It realizes the workflow modulization and automation, and greatly improves the efficiency of the workflow test and regression test.

Keywords

Security Chip, Workflow Test, Modulization, Multi-Core Service Scenarios

1. 引言

2019 年 8 月 10 日，国网公司、中国电科院的专家发表了题为《新一代智能电能表支撑泛在电力物联网技术研究》的文章，指出国网多芯模组化三相智能电表应用设计技术与现行智能电表技术有很大的不同，颠覆智能电表的传统整机一体化设计技术，将采用多芯模组化应用创新设计，多芯涵盖计量、时钟、电压基准、存储、安全、通信、电源、显示、管理(MCU)等诸多个芯片。

芯片越多，密钥状态的组合就越多，这对传统的芯片业务测试工作提出了新的要求。如安全芯片业务测试，智能电能表通过嵌入安全芯片用于信息交互的安全认证，存在测试态和正式态两种模式，测试态用于电表挂装前的测试检验，正式态用于电表出厂挂装现场时使用。当主站对电能表进行参数设置、预存电费、信息返写和下发远程控制命令操作时，通过安全芯片进行安全认证、数据加解密处理以确保数据传输的安全性和完整性。这些功能都需要在两种密钥状态下进行完整的业务流程测试[1]。

传统的测试方法将密钥状态写入项目代码中，最多涉及的芯片数量不会超过 2 个，密钥场景有限。一旦芯片数量增加到多个，密钥场景组合成倍增加，传统的方式几乎无法灵活适应新的多芯模组化测试需求，只能对项目进行重新开发与设计。如何设计一种业务流程的测试方法，既能克服传统业务流程测试的缺陷，也能更有效地进行自动化测试和回归测试，适应多芯应用场景，是亟需解决的问题。

2. 传统安全芯片的业务流程测试方法

以某地方电力自管户手持机项目为例，对远程主站进行模拟，通过读卡器的方式接入手持机安全芯片，实现业务的远程主站测试；然后再对手持机安全单元和电表芯片进行各种芯片交互流程。如下表所示，测试主体包括模拟主站，手持机安全单元、电表 ESAM 芯片。手持机安全单元和电表安全芯片分别存在测试和正式两种密钥状态，对应的密钥状态测试场景如下表 1 所示。

现在由于电表升级需要挂装新的电表，手持机在维护原有电表支持的情况下，需要新增对新装电表的服务支持。这个升级相当于对未来多芯应用场景的一个模拟，从原本的 2 个安全芯片交互到现在的 3 个安全芯片间业务交互。

Table 1. Key scenario examples of hand-held device project for self management customer
表 1. 自管户手持机项目密钥场景示例

密钥测试场景	模拟主站	手持机安全单元	电表安全芯片
1	测试正式	测试(生产发行)	测试
2	测试正式	测试->正式	
3	测试正式	正式	测试
4	测试正式	正式->测试	
5	测试正式	测试(密码机恢复)	测试
6	测试正式	正式	测试->正式
7	测试正式	正式	正式

很明显传统方法[2] [3] [4] [5]存在的测试缺陷如下：

1、不支持交互业务的测试。特别是对于上表中的测试场景 6，密钥正式态时，实际的产品使用中，电表与手持机交互、电表与主站交互、手持机与主站交互，这些业务流程是交叉进行的，在实际测试中应反复对这一场景进行交叉压力测试以保证对测试场景的完整覆盖；

2、测试方法无法进行有效的继承和复用。在实际的业务流程中，测试方法写入项目代码中。特别是如密钥状态、电表芯片指令等属于可变关键参数，一旦写进代码，实际测试中需要根据测试场景不断地做调整。针对新增需求，1，3，5，6 的测试模块不同的只有密钥状态和电表芯片指令，其他测试条件相同，应该采用提取变量的方式对不变的测试场景进行封装和复用；

3、对增加的需求几乎无法快速响应。由于测试用例写入代码中，增加测试密钥场景或者增加测试用例，就需要相应的增加代码，不利于产品快速迭代和回归测试。如图，增加一个芯片，测试场景会基于不同的业务增加到 9~15 个，需要花费大量时间重新开发和其他现有芯片的交互代码，遍历各种可能的测试场景，代码开发量大。

3. 安全芯片业务流程自动化测试系统的设计与实现

为克服传统业务测试的不足、适应新的多芯模组化应用设计，本文以安全芯片的业务测试为例，提出一种芯片业务流程自动化测试方法。通过将测试用例从代码中提取出来，实现了业务流程的模块化后，提取密钥场景和芯片指令等可变量参数，封装 SPI，7816，645 协议，能灵活的进行业务流程的交互配置，满足了芯片业务流交互测试的需求。

本文将以该项目为例，对多密钥测试场景的用例和指令流进行了分析和工作量统计，验证了本系统的设计的有效性。系统的模块图如图 1 所示。

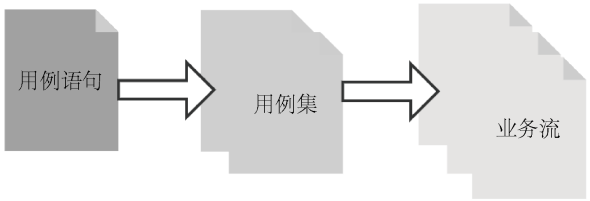
基于指令流的安全芯片业务流程自动化测试系统连接加密机、安全芯片和安全单元等硬件，对测试场景进行模拟，提取用例语句，封装用例集，形成业务流。同时提供了对 7816 和 SPI 协议支持模块，对不同的读卡器提供了支持，提供对芯片和卡片的读写功能；提供了 645 协议支持模块，为了实现真实的上表测试，对 645 协议进行了支持，测试人员可以根据实际的测试需要进行选择。

本文将重点介绍业务流的设计，业务流的设计采用了三层结构的设计[6]，如图 2 所示，提取单流程用例语句，将用例语句进行封装形成功能模块集，再通过组合功能模块集形成业务模块集供测试调用。

3.1. 用例语句

系统将业务流程的指令写入 Excel 或 SQLite 数据库中，内容见表 2，利用用例单元格内容指定调用

的业务功能模块，通过用例语句模拟指令流，并建立代码和用例语句之间的映射关系。通过修改用例语句，达到调用不同代码函数，执行不同指令流，从而实现将测试用例从代码中提取出来的目的。同时对命令进行了函数封装，公用的指令固定地写在函数中，提取需要灵活修改的参数放在用例中供用户修改，这里主要是密钥状态和芯片指令，这样不同的项目可以灵活的继承和复用。



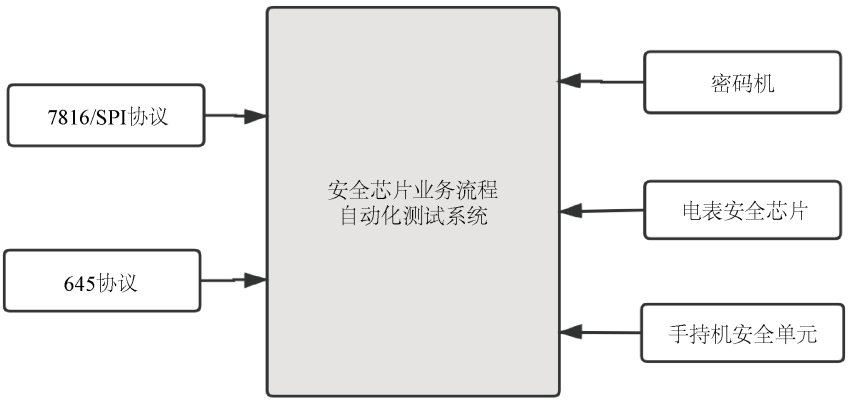


Figure 1. Instruction-based security chip automatic test system
图 1. 基于指令流的安全芯片业务流程自动化测试系统

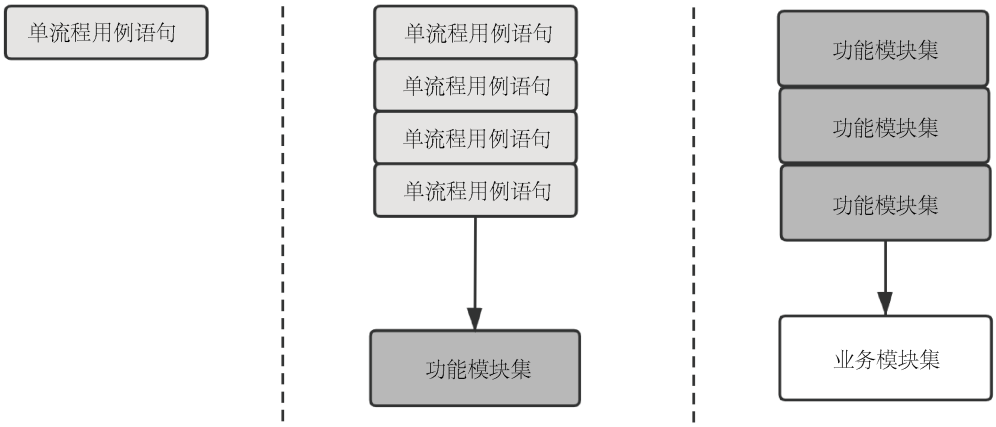


Figure 2. Process assembling diagram
图 2. 业务流设计图

Table 2. User case content examples
表 2. 用例单元格内容示例

类名	函数名	函数功能	入参 1	入参 2
Automation	IdAuth	身份认证	192.168.19.99	00
Automation	ESAM_IdAuth	读卡器指令发送	0000000000000003	

如表 2 所示，是一个远程身份认证的用例，在语句中指定了使用的类名和函数名，以及函数输入的参数，可以输入多个参数，示例中第一条语句是远程身份连接密码机发送身份认证命令，作为参数放在后面的是认证需要用到的密码机 IP 和安全芯片密钥状态。第二条语句向芯片发送指令，不同场景不同芯片指令不同。

3.2. 功能模块集

功能模块集实现了各个业务流程，对用例语句进行了组合和模块化，即把参数更新、远程控制、数据清零等业务功能模块化，对于不同的密钥测试场景，输入不同密钥状态值，从而实现正向或者反向的模块调用。

如表 3 列出了“参数更新”子模块。参数更新涉及 20 多个文件，每个文件的更新方式不同，有的是明文更新，有的是密文更新，需要测试全更新、部分更新或带偏移地址进行更新等不同更新方式。仅一个参数更新的模块就涉及至少 5 大类更新方式。如表 3 所示，这 5 大类更新方法涉及的用例共用了“参数读取”、“读卡器指令发送”和“更新校验”等三个子用例，一个文件的更新想要覆盖完整的测试需要至少 20 条子用例，那么十几个文件，就是上百条子用例。采用用例提取的方式，将这些变量提出，只需要在用例语句中去修改参数即可以灵活的配置不同的用例覆盖，这就是用例提取带来的便利性，也是测试用例复用的基础。

同时还支持在测试过程中对输入值进行动态的调整，这个功能支持能在不调整代码的情况下直接进行正向和反向测试，比如表 3 的示例，将入参 1 和入参 2 的值改为错误的值，放在下一行的语句，就可以同时进行正向和反向的测试。

Table 3. User case content examples of parameter update
表 3. 参数更新业务测试模块化示例

类名	函数名	函数功能	入参 1	入参 2
参数更新模块				
Automation	IdAuth	身份认证	192.168.19.99	00
Automation	ESAM_IdAuth	读卡器指令发送	0000000000000003	
Automation	ParameterUpdate1	参数更新	192.168.19.99	00
Automation	ESAM_ParaUpdate	读卡器指令发送		

3.3. 业务模块集

将测试流程中涉及的功能模块集和业务模块集做了总结，如图 3 所示。

以“手持机安全单元与电表交互”这个业务流程为例，该业务流程模拟手持机与主站交互获取任务列表和数据然后再与电表进行交互的业务流程，需要功能模块中的“身份认证”、“会话协商验证”、“获取业务列表”、和“电表远程控制”这些模块。

从图中可以清楚的看到，在实际的业务流程中，不同的业务模块的调用是交互进行的，采用这样的设计，在模拟业务流时是十分灵活的，可以实现各个层级模块的复用，在自动化测试和后续的回归测试中优势非常突出。

4. 测试结果及分析

为了更好说明本方法更适用于需求变更，仍然以该项目为例，如表 4，对比表 1，增加新装电表的支

持，相当于新增一个安全芯片，增加了 7 个密钥测试场景，即表 4 中 5~11。项目测试场景变更如下：

在现有测试系统的框架下，由于在用例语句中已经将密钥状态和芯片指令流提取出来，只需要对用例语句做改动，就可以直接复用原有代码，形成新挂装电表的用例集；使用这些用例集，按照已挂装电表的设计组装功能模块集；将功能模块集组合成新的密钥测试场景需要的业务模块集。代码的改动少。

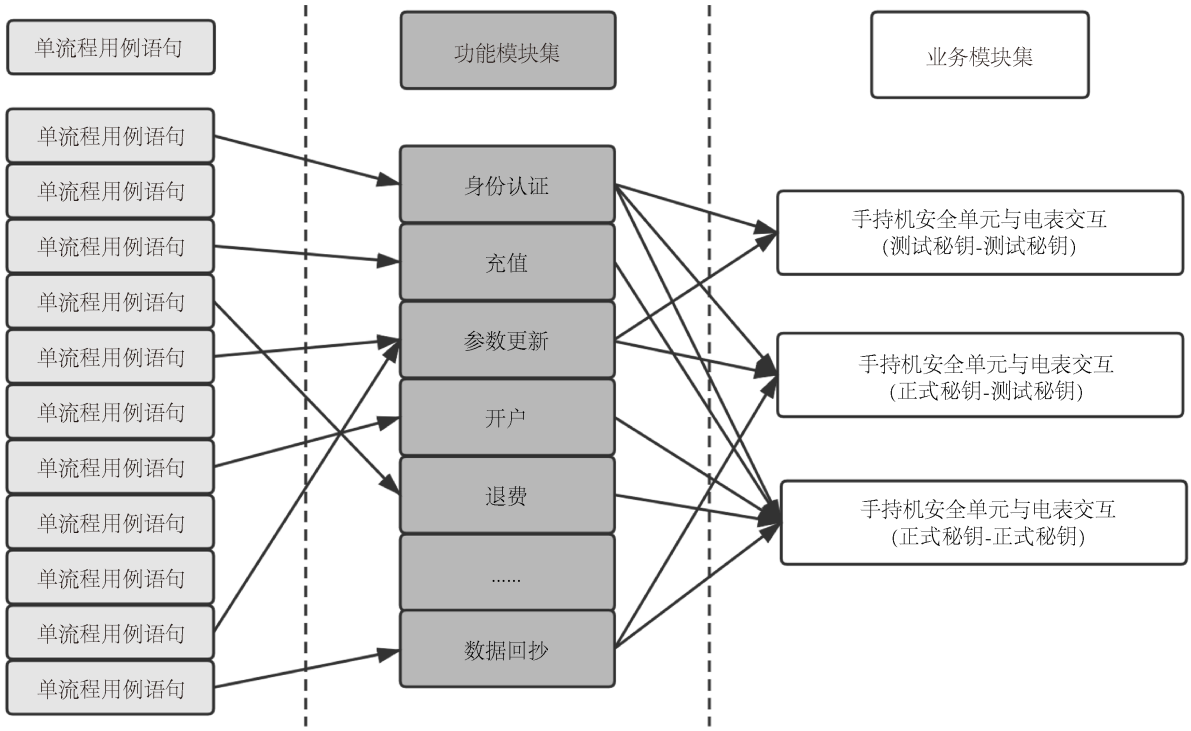


Figure 3. Process module sets
图 3. 业务模块集

Table 4. User case examples of parameter update in hand-held device project for self management customer
表 4. 自管户手持机项目需求变更密钥场景测试用例

密钥测试场景	手持机	已挂装电表安全芯片	新装电表安全芯片	主站交互流程用例数/指令数	表交互流程用例数/指令数	总用例数/总指令数
1	测试(生产发行)	正式		13/366	9/298	22/664
2	正式	正式		13/366	9/298	22/664
3	测试(密码机恢复)	正式		13/366	9/298	22/664
4	正式	正式->测试->正式			2/90	2/90
5	测试(生产发行)		测试	13/366	9/298	22/664
6	测试->正式			1		1/12
7	正式		测试	13/366	9/298	22/664
8	正式->测试			1		1/12
9	测试(密码机恢复)		测试	13/366	9/298	22/664
10	正式		测试->正式		2/90	2/90
11	正式		正式	13/366	9/298	22/664

若按照上表的数据进行统计，原两块芯片交互 68 个用例/2082 个指令流，增加一块不同 COS 的芯片，增加用例数 92 个/2770 个指令流，按照这个比例进行线性拟合，即假设每多增加一个芯片，只和原场景中的一个芯片进行交互，如下图 4 所示：

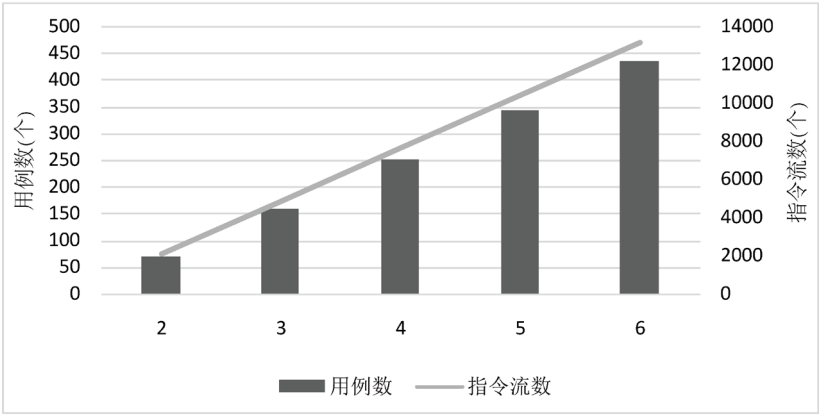


Figure 4. Test estimation diagram in multi-core application scenario
图 4. 多芯应用场景测试量估计图

如图所示，芯片增加会极大的增加测试用例和指令流的个数。如果把用例写入代码中，不仅测试工作量大幅提高，测试开发的工作量也将大幅的增加。而本方法，由于将测试用例、密钥状态和芯片指令可变量提取出来，使用了灵活的可组合的业务模块化方式对测试用例进行组合和复用，基本不涉及代码的开发，能适应快速迭代的产品开发进程，为多芯应用场景提供了快速有效的测试方法。

5. 结论

本文提出一种安全芯片业务流程自动化测试方法。通过构建基于用例语句的三层模块设计的自动化测试方法，模拟主站、手持机芯片、电表芯片的交互流程，将测试用例、密钥状态和芯片指令从代码中提取出来，实现了业务流程的模块化和自动化，并能灵活地进行业务流程的交互配置。在实际的业务测试应用中，相较于传统方法能更快地进行冒烟测试，积累的测试用例能进行广泛的自动化测试，在后期能更快地进行回归测试，保证了产品质量的同时保证了项目的进度，也为未来的多芯模组化三相智能电表的多芯应用场景测试提供了有益的思路。

参考文献

[1] 王爱英. 智能卡技术[M]. 北京: 清华大学出版社, 2009.

[2] 秦璐怡. 基于智能卡芯片的一种自动化测试方法[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2012.

[3] Fu, Q.Q. (2015) A Grey Lock Method to Support Multiple Pre-Freezing Mechanism in IC Card. CRC Press, Balkema, 1395-1400.

[4] Liu, J., *et al.* (2017) Implementation of IC Card Authentication Method Based on Self-Defined Algorithm. 2*nd International Conference on Electrical and Electronics: Techniques and Applications*, Beijing. 15-16 January 2017, 324-329. https://doi.org/10.12783/dtetr/eeta2017/7750

[5] 孔梦荣, 朱国华. 基于智能卡的远程认证体制[J]. 计算机工程与设计, 2008, 29(3): 606-608.

[6] Zhou, J. (2019) An Instruction Based Automatic Workflow Testing Method for Security Chip. *IEEE* 2*nd International Conference on Automation, Electronics and Electrical Engineering*, Shenyang, 22-24 November 2019, 564.