Combinatorial Methods for Testing Communication Protocols in Smart Cities

Dimitris E. Simos[1], Ludwig Kampel[1], and Murat Ozcan[2]

[1] SBA Research, A-1040 Vienna, Austria
{dsimos,lkampel}@sba-research.org
[2] Siemens Building Technologies CPS Software House; Chicago, USA
murat.ozcan@siemens.com

Abstract. In this paper, we conduct a feasibility study for combinatorial methods applied to widely used communication protocols in smart city environments. Even though, our initial results reveal no failures in the involved products, the approach looks promising in terms of software reuse and test efficiency.

Keywords: Combinatorial testing, BACnet protocol, smart cities

1 Introduction

A report conducted by the Centre of Regional Science at the Vienna University of Technology identified six main axes (dimensions) along which a ranking of 70 European middle size cities can be made [3]. These axes are: a smart economy; smart mobility; a smart environment; smart people; smart living; and, finally, smart governance.

Moreover, a study documented in [6] shows that Americans spend 87% of their time indoors. This gives us sufficient justification to consider smart buildings a main factor of smart cities. In modern smart buildings various hardware pieces and processes, such as lights, air vants, air condition, fire alarm, water etc., have to be properly coordinated (and centrally controlled). To be able to facilitate the communication between these interacting parts, they also have to be compliant to a common communication protocol.

In this paper, we focus on the Building Automation and Control Networks Protocol (BACnet) which is an interoperable communication protocol for building automation and control networks. When a piece of hardware or software is BACnet compliant, this means it can communicate with the hardware and software of any other BACnet compliant vendor. BACnet compliance is an essential aspect of every research and development project at major corporations like Siemens Building Technologies, Honeywell, Johnson Controls, Schneider Electric and others.

Our motivation for this work is to propose a combinatorial method for testing communication protocols in buildings, as a means to provide an intelligent way which could increase the quality of smart buildings in smart cities. As a proof-of-concept of this early stage devised methodology we develop a combinatorial model for the widely used APOGEE Insight® workstation which acts as a BACnet client.

2 Combinatorial Models of the BACnet Protocol

For BACnet testing the standard processes so far has evolved around exhaustive testing, and user-defined specification testing (e.g. by contractual work with third parties). Hence our first steps for proposing a thorough testing methodology for the BACnet protocol is novel in that sense and also could aid the practitioners by utilizing specific advantages of combinatorial testing, which are explained below.

Introduction to Combinatorial Testing . Combinatorial testing (CT) is a highly sophisticated testing methodology, that is capable of producing comparable small test sets (e.g. when compared to exhaustive testing), while at the same time providing guarantees of (certain) input space coverage. To apply CT to a system under test (SUT), it is necessary to have an *input parameter model* (IPM) of the SUT [5]. To devise an IPM for an SUT it is necessary to identify *input parameters* and their respective *values*, such that an input to such a model can be represented by parameter-value assignments. Engineering an IPM can be a tedious and time intensive task itself [2]. The underlying mathematical primitives of CT are covering arrays (CAs), which are discrete structures appearing in *combinatorial design theory*, and can be represented as matrices with specific coverage properties [7]. To further apply CT, the parameters of the IPM are matched with the columns of an appropriate CA, such that a row of the CA can be interpreted as an assignment of values to the parameters of the IPM. Translating all rows of a CA in such a way, the mathematical properties of CAs guarantee that the generated test set is a *t-way test set*, i.e. a test set which ensures that all t-way combinations of parameter-value assignments are tested, once all tests have been executed [7]. Note that the general problem of constructing a t-way test set is believed to be NP-hard as it is tightly coupled with hard combinatorial optimization problems (see [4]). A study from the National Institute of Standards and Technology (NIST) [7] shows that in all tested software products all faults rely on the interaction of at most six input parameters. This means that all faults in the tested software products can be triggered using a 6-way interaction test set, which is generally much smaller than an exhaustive test set, but yet achieving the same testing quality.

Application to the BACnet Protocol via the APOGEE Insight® product. We propose to apply CT to the BACnet client as this is utilized by the APOGEE Insight® workstation, a commercial tool manufactured by Siemens Inc., in order to reduce the time and costs for the testing cycle. Considerably, as the APOGEE Insight® has to be tested newly for every vendor the test setup needs a lot of time and thus, resources.

A *BACnet Event* can be characterized as any change in the value of any property of any object that meets a particular criteria. The purpose of an Event Enrollment Object (EEO) is to define an event and offer the engineer an association with the occurring event and the transmission of notification messages.

Vendors and building control products of those vendors may have varying implementations for EEO configurations in the user interface (UI). Until recently, the Siemens legacy building control product, Siemens APOGEE Insight® Workstation, could have above 5 million ways to configure an EEO. Given that one configuration takes one second to execute (a conservative estimate), the total effort spent towards exhaustive testing makes apparent the need for more intelligent testing methodologies. Due to its complicated nature the EEO configuration was previously left open for the user and most of these configurations could be invalid. If the configuration was invalid at the workstation, once the EEO was downloaded to the field panel, it would show a configuration error for the EEO. The EEO would then need to be modified at the field panel or it would have to be modified at the workstation and re-downloaded to the panel.

For practical testing, to be able to execute the generated test set, one needs to be able to input EEOs into the System. This is however enabled by the Harmonization tool of APOGEE Insight®. The steps below, describe a high-level view of a CT methodology for testing the EEOs.

1. Devise IPMs for the EEO configurations.
2. Generate t-way test sets using an intelligent CT generation algorithm (e.g. the IPO strategy as this is implemented by the widely used ACTS tool [8]).
3. Then the test sets are fed to the Harmonization Tool.
4. The EEO configurations are downloaded to the field panels, where the field panels should show configuration OK if the EEOs were configured correctly.
5. Finally the EEO configurations can be bulk-uploaded to the workstation from the panel. EEOs should show configuration OK if they were configured correctly.

Due to space constraints the devised IPMs for the EEOs and the derived 2-way test sets are available upon request. We briefly, sketch below how an IPM for a reduced EEO configuration looks like together with a (reduced) test set:

An EEO can be modelled consisting of the following parameters that can be configured assigning the respective subsequent values to them:

- *ObjectType* (OT): Analog-Input (AI), Analog-Output (AO)
- *EventType* (ET): Floating-Limit (FL), Out-of-Range (OoR)
- *SetPointType* (SPT): Schedule (S), Trend-Log (TL)
- *SetPointProperty* (SPP): Start-Time (ST), Present-Value (PV)

A 2-way test set for this IPM of the reduced EEO can be attained by computing a (binary) covering array (of *strength* 2) with four columns and replacing the entries in the columns with the values of the corresponding parameter. The resulting test set covers all 2-way combinations of parameter-value assignments, see Figure 1.

c_1	c_2	c_2	c_2
0	0	0	1
0	1	1	1
1	0	1	1
1	1	0	0
0	0	1	0

OT	ET	SPT	SPP
AI	FL	S	PV
AI	OoR	TL	PV
AO	FL	TL	PV
AO	OoR	S	ST
AI	FL	TL	ST

Fig. 1. On the left hand side a covering array (of strength 2), and on the right hand side the derived 2-way test set for the IPM of the reduced EEO.

3 Further Remarks

The initial challenge in this study was how to best test EEO configurations in the most efficient manner. We have conducted sample experiments with the derived test sets from our combinatorial models that are still ongoing. So far approximately 1000 test cases have been executed versus the APOGEE Insight®, however an initial investigation of the test results revealed no faults. Nevertheless, a final conclusion can only be made once the whole testing cycle is completed.

In addition, as future work we want to devise real world tests, also for other tools besides APOGEE Insight® for the BACnet protocol, and shift focus to security in smart cities [1].

Acknowledgment. This research was carried out in the context of the Austrian COMET K1 program and publicly funded by the Austrian Research Promotion Agency (FFG) and the Vienna Business Agency (WAW).

References

1. Baig, Z.A., et al.: Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation 22, 3 – 13 (2017)
2. Bartholomew, R., Collins, R.: Using combinatorial testing to reduce software rework. CrossTalk 23, 23–26 (2014)
3. Centre of Regional Science: Smart cities, Ranking of European medium-sized cities. Available at `http://www.smart-cities.eu/download/smart_cities_final_report.pdf`, Accessed on 2018-02-10
4. Cheng, C.T.: The test suite generation problem: Optimal instances and their implications. Discrete Applied Mathematics 155(15), 1943 – 1957 (2007)
5. Grindal, M., Offutt, J.: Input parameter modeling for combination strategies. In: Proceedings of the 25th Conference on IASTED International Multi-Conference: Software Engineering. pp. 255–260. SE'07, ACTA Press, Anaheim, CA, USA (2007)
6. Klepeis, N.E., Nelson, W.C., Ott, W.R., Robinson, J.P., Tsang, A.M., Switzer, P., Behar, J.V., Hern, S.C., Engelmann, W.H.: The national human activity pattern survey (nhaps): a resource for assessing exposure to environmental pollutants. Journal of Exposure Science and Environmental Epidemiology 11(3), 231 (2001)
7. Kuhn, D., Kacker, R., Lei, Y.: Practical combinatorial testing. NIST Special Publication 800-142 (2010)
8. Yu, L., Lei, Y., Kacker, R.N., Kuhn, D.R.: ACTS: A combinatorial test generation tool. In: 2013 IEEE Sixth International Conference on Software Testing, Verification and Validation. pp. 370–375. IEEE (2013)