Wuhan University
Journal of Natural Sciences

2016, Vol.21 No.1, 029-036

Article ID 1007-1202(2016)01-0029-08
DOI 10.1007/s11859-016-1135-z

A High-Assurance Trust Model for Digital Community Control System Based on Internet of Things

□ LI Hongtao[1] , XING Jinsheng[1†] , MA Jianfeng[2]

1. College of Mathematics and Computer Science, Shanxi Normal University, Linfen 041000, Shanxi, China;

2. School of Computer Science and Technology, Xidian University, Xi'an 710071, Shaanxi, China

© Wuhan University and Springer-Verlag Berlin Heidelberg 2016

Abstract: Security issues and Internet of Things (IoT) become indispensable part in digital community as IoT develops with the pervasive introduction of additional "smart" sensors and devices over the last decades, and it necessitates the implementation of information security principle in digital community system. A three-level criticality model to determine the potential impact is proposed in digital community system when various devices lost in this paper. Combining the actual security requirement of digital community and characteristics of IoT, a hierarchical security architecture including defense-in-deep cybersecurity and distribute secure control is proposed. A high-assurance trust model, which assumes insider compromise, which exists in the digital community, is finally proposed according to the security issues analysis.

Key words: digital community; Internet of Things(IoT); information security; security architecture; secure control

CLC number: TP 309.2

Received date: 2015-06-23

Foundation item: Supported by the National Science Foundation of China of Shanxi (2015011040).

Biography: LI Hongtao, male, Ph.D. candidate, research direction: network and information security. E-mail: lihongtao7758@163.com

† To whom correspondence should be addressed. E-mail: xingjinsheng@163.com

0 Introduction

Digital community is a connected community that combines broadband communications infrastructure with flexible and service oriented computing infrastructure based on open industry standards[1]. The digital community system encompasses everything from data perception to data transmission and control system. With the pervasive introduction of additional "smart" sensors and actuators over the coming decades, cybersecurity becomes more important than ever before, necessitating the implementation of information security principle throughout the entire digital community system.

Internet of Things (IoT) is the core technology of next generation and becomes focus of research in both academia and industry[2]. As an important part of digital earth, application of IoT technology is indispensable in the digital community. IoT not only accomplishes the information collection, information transmission and automatic control functions, but also enables the entire digital community system to be more convenient, secure and reliable. However, different from traditional networks, IoT owns unique characteristic including heterogeneous integration, collaborative autonomy and open interconnection, which may induce security issues for system security (privacy preservation of user, seamless connection between security protocols, etc.)[3]. Moreover, some security issues have not been fully exposed now. Once IoT is put into use in large scale, the current network architecture that seems to be secure will face a huge threat. Therefore, the security architecture of digital

community must conform to strict standards at the beginning of construction.

According to the actual security requirement of digital community and the characteristics of IoT, a high-assurance security trust model based on IoT technology for digital community is proposed in this paper. The rest of this paper is organized as follows: The network structure and functions of IoT-based digital community are described in Section 1. A criticality model from aircraft system that determines potential impact on system of IoT-based digital community is proposed in Section 2. In Section 3, we detail the proposed security architecture for digital community from cybersecurity and secure control aspects respectively. A high-assurance trust model for digital community is also proposed in Section 4 and a conclusion is given in Section 5.

1 Digital Community System Architecture Based on IoT

Digital community-oriented application architecture demands different application requirements according to the characteristics of IoT. Combining the basic network model of IoT with application requirements and technology supporting, the network structure of the digital community is assumed to be composed of sensory and control layer, network layer and application layer (see Fig.1). The details are depicted as follows:

1) Physical and control layer

Physical layer consists of sensory subsystem and control subsystem. Sensory subsystem accomplishes the overall perception of information. Sensory nodes measure, capture and transmit information all the time. Control subsystem accomplishes the control of field devices (home meter, water heaters, surveillance cameras, etc.).

2) Heterogeneous network layer

Heterogeneous network layer accomplishes data transmission between physical layer and application layer. The communication network includes 2.4 GHz network in family, 433 MHz network in residential area, Internet/CDMA/ GSM, etc.

3) Application layer

Application layer accomplishes information processing and human-computer interaction. Application layer provides services for users and realizes the intelligent applications by data analysis and processing, data mining and data integration (vehicle management, remote control, etc.).

IoT technology means not only the thing-to-thing interconnection in digital community, but also the community-to-community interconnection. There are a number of "smart" sensors, actuators in a community, and the perception data is transmitted to the communication network. Figure 1 shows the network architecture of IoT-based digital community.

2 Impact of Failure in IoT-Based Digital Community

IoT-based digital community encompasses every-

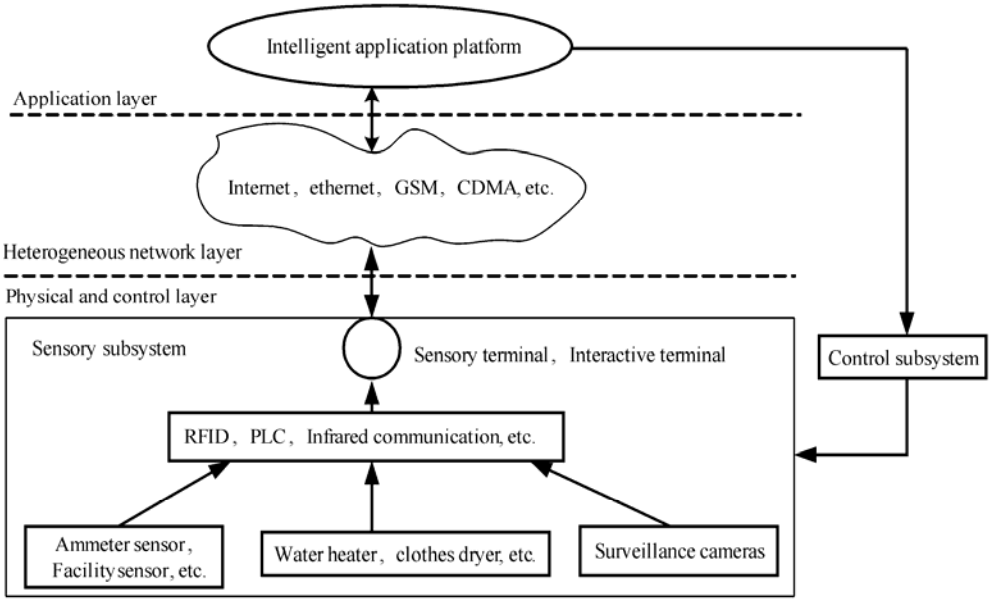

Fig. 1 IoT-based digital community network architecture

thing from sensory nodes to transmission and control systems. Therefore, the IoT-based system can be viewed as a networked system of systems with thousands of nodes. With the pervasive introduction of additional "smart" sensors and devices over the last decades, cybersecurity becomes more important than ever before. Thus, an appropriate cybersecurity control method for digital community is impending to the health of this system.

It is known that an aircraft is quite a complex but arguably safe system ever devised. Aircraft industry integrates "smart" sensors and actuators into a single system, and addresses the security issue well at the same time. Both aircraft system and IoT system were purpose-built devices. In both of these industries there are many similarities in system architecture and system controlling. Thus, aircraft system designing concepts can be applicable in parallel to the IoT-based digital community system. Aircraft industry categorizes various subsystems by their criticality to the overall system[4, 5]. The model defines three categories based on the impact of a subsystem failure (three levels: catastrophic, major, and minor impact) to the aircraft system. The proposed model in this paper is based, to some extent, on the model used in aircraft system. Therefore, we define three impact levels on reliability: High, Medium and Low. The three levels can be applied to the digital community as follows:

High: Failure of these systems induces failure of thousands of nodes;

Medium: Failure of these systems induces failure of hundreds of nodes;

Low: Failure of these systems induces local failure in a family.

We use a color key to designate these impact levels in Fig. 2. Using the three-level model discussed above, relative analysis of the digital community is demonstrated as follows. From the real-time operations perspective, the problem caused by loss of a facility depends on the situation. The detailed impact model of digital community is shown in Fig. 2(a). In this model, control system is assumed to be an integral and critical part and have the potential impact on high level. The transmission network is also assumed to have the potential impact on high level. Intelligent application platforms (IAFS) and sensory terminals are assumed to have the potential impact on medium level. Intelligent family devices such as advances metering infrastructure (AMI), home area networks (HANs) and managements systems (MS) are assumed to have low-level impact.

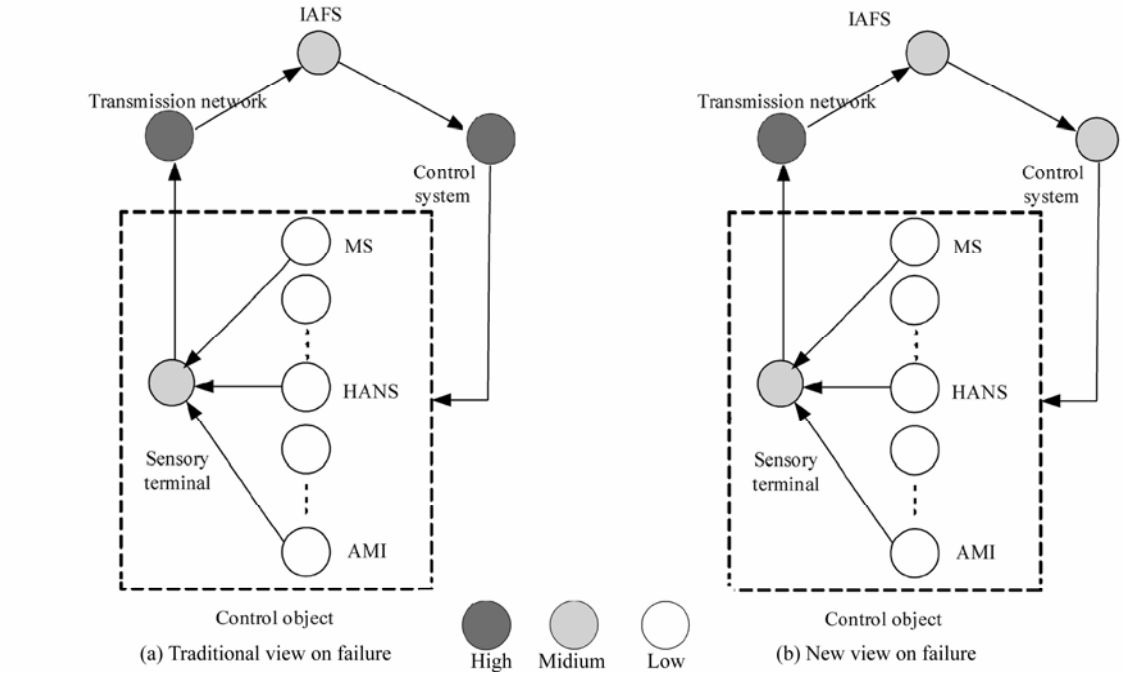

Fig. 2 Traditional and new view of impact of failure

In our new approach (see Fig. 2(b)), we confirm that a loss of reliable of control system should not cause the potential for high level impact on real-time operations. Rather than suggest that the control system is unimportant, we just want to note the difference between doing state estimate analysis and issuing the command sequence to implement the recommendations of that state estimate analysis. This is a new design concept we advocate in this paper. Usually, control systems determine the response to control objects according to what-if

analysis done by state estimate. However, the scenario is less common that the results of what-if analysis are preloaded onto the controlled objects (sensors, home facilities). That in and of itself will alleviate the impact caused by loss of reliable control system. The ideal scenario is that sensors and home facilities can perform their own what-if analysis based on direct communication with their adjacent facilities. An improper command sequence is issued to a generator[6], and the generator is destructed in the end. If the generator has the ability to sense local conditions and conduct what-if analysis on itself, the generator would evaluate the consequence of executing command sequence, and then the destruction of the generator would be avoided.

3 Security Architecture for Digital Community

Security researches on computer architecture mainly focus on cybersecurity and secure control these days. Based on the actual security requirement of digital community architecture, we make a detailed discussion to security architecture for digital community from cybersecurity and secure control aspects respectively.

3.1 Cybersecurity Architecture

With the introduction of modern programmable sensors and intelligent devices in digital community, the complexity of system at both the individual devices level and the overall system level is increased at the same time. This will inherently lead to more fragility and the possibility of cyberattack or inadvertent action, which increases the likelihood of unplanned failure of system. Therefore, cybersecurity becomes a more important factor than IDS), encryption system, role-based access control (RBAC) and firewalls. We suggest that a defense-in-deep security architecture should not only be a ploy "keep out" model, but also be equipped with the ability to safeguard against the threat already existing within the overall system. Figure 3 shows the hierarchical security architecture proposed for digital community system.

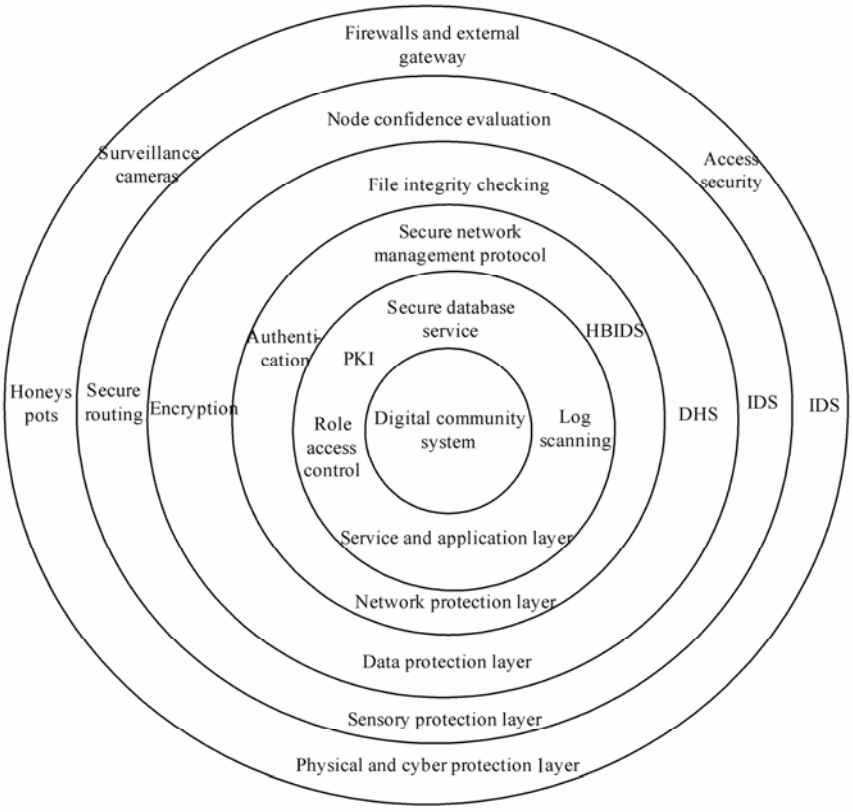

Fig. 3 Hierarchical defense-in-deep cybersecurity architecture

This hierarchical security architecture achieves the cybersecurity for digital community by the following protections, and certain security technologies may cut across multiple layers.

Physical and cyber protection layer includes physical and cyber perimeter protection of the digital community system. Physical security techniques include physical security facility, such as IDS and surveillance cameras. Cyber security techniques include firewalls and external gateway, access security, honeys pots and so on.

Sensory protection layer includes security controls for node capture attack, node control attack, denial of service (DoS), and passive attack. Examples of security techniques at this layer include node confidence evaluation, IDS, secure routing, etc. (Remarks: if here "of" is to be deleted, "Examples" should be "Example" as it modifies "security techniques")

Data protection layer includes security controls for data protection within physical and cyber perimeter. Techniques in this layer include data encryption in transit and data encryption at rest, DHS, file integrity checking, etc.

Network protection layer includes security controls for data transmission from originating node to destination node. Examples of techniques include secure network management protocol, host-based intrusion detection and security (HBIDS), authentication across network, secure broadcast/unicast, etc.

Service and application layer includes controls for accessing service and application for user in digital community. Example techniques at this layer contain privacy preserving for users, role-based access control, secure database service, key management, PKI, authentication, log scanning, etc.

3.2 Secure Control Architecture for Digital Community

Secure control is mainly to solve the problem of control security in the interconnected open system architecture. The control networks based on digital community are shown in Figs. 4 and 5. Figure 4 reflects that the control system architecture is largely hierarchical. Therein the control data flows in a hierarchical manner. The model shown in Fig. 4 is a typical model that researchers are familiar with. There is little communication or autonomous coordination between peer devices (sensory terminal and interactive terminal, water heater and clothes dryer, etc.) in this model.

With technology progressing, most devices are automatic and have been designed to be programmable and intelligent. These devices combine a local sensor, controller and actuator in a single unit (e.g., programmable sensor, automatic recloser). Each device works in an automatic mode and makes decisions based on its state. In this model, actions that need higher complexity or broader considerations are typically beyond the capacity of devices when these devices have been preprogrammed in what to do next. For decisions that are beyond their capacity to make, devices to some extent depend on commands received from higher hierarchy control system (see Fig. 4). The control system data predominately flows in a hierarchical manner. Herein it gives us a challenge to build an "overall-smart" digital community.

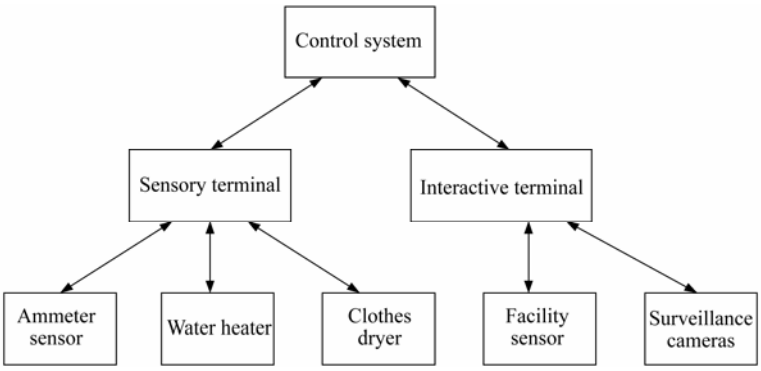

Fig. 4 Hierarchical control system architecture of digital community

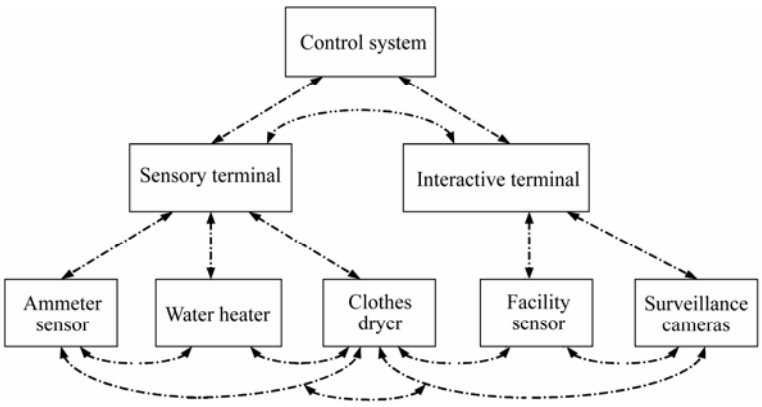

Fig. 5 New designed control system architecture of digital community

Figure 5 shows our new designed control system architecture model with increased communication or autonomous coordination between peer devices in a manner that is not exclusively dependent on control system commands. In this model, devices have the capacity of sensing peer device and coordinating with peer device beyond their traditional viewpoint. Decisions demanding higher complexity or broader considerations no longer entirely rely on control commands from control system. It is worth noting that we do not endeavor to decrease or eliminate lines of communication or coordination between control systems and devices. Instead, we concentrate on enhancing the distributed control system architecture, where communication or coordination between peer devices can be achieved even when losing control capability from control system. This is the core issue for our recommended approach of building a "self-healing" digital community.

There are many failure modes that can cause the loss of reliable control in control system, such as device failure, control system failure, communication link failure and improper or nonexistent commands from control system by a distracted/untrained operator. Bush[7] stated that focusing cyber security efforts just on preventing external attack is not sufficient. In reality, most external attack targets are aimed at gaining insider access. Thus, if the control system architecture can limit the insider damage (e.g. unplanned device failure or control system failure, damage caused by distracted/untrained operator), it will be more reliable than external malicious attack inherently. Many industrial accidents[8, 9] show that there is no evidence of external malicious attack being involved. Instead, these accidents occurred just because of the combination of insider unanticipated factors of control systems. Joseph[10] stated that had these control systems been reliable enough, these accidents would have not occurred.

It is noteworthy that increasing the reliability of control system will decrease the likelihood of similar accidents. However, this is not enough for building distributed control system architecture. In addition to increasing the reliability of control system, devices must be more autonomous with and be preprogrammed with next-step actions to be taken when failure modes occur. With this, distributed control system architecture, where devices gain a wide viewpoint than just sensing/sending data flow and communication or coordination between peer devices can be executed even when losing control capability from control system, is accomplished.

4 High-Assurance Trust Model for Digital Community

We propose a security architecture where devices and control system are given for distributing communication and coordination capability, as well as decision-making capability. However, from the real world utility viewpoint, devices and control system also should have the ability to judge whether to trust or not when it receives sensory data or command data flow. We consider that creating an all-encompassing enclave of trust is neither easy nor desirable. The control system architecture model proposed here assumes the compromise of devices or control system, that is to say the model is designed with the anticipation of insider component being compromised by inadvertent or malicious actions. Many solutions have been developed in this area (intrusion detection systems (IDSs) [11], intrusion prevention systems (IPSs)[12] and intrusion tolerant systems (ITSs)[13], etc.). IDS and IPS are proved to be effective for preventing outsider threat, but fail to address the insider threat (whether error- or malice-driven). ITSs, a newer technology in this research area, can accommodate failure of IDS and IPS, and have gained significant merit for addressing insider threat as a general approach. It also accommodates the threat that unpredictable people are already in systems.

Traditional control architecture for digital community is shown in Fig. 6, which is non-ITS. The devices or sensory terminals are in the state of blind trust in the control signals from control system. Control system receives information data from devices or sensory terminal and determines the action to be done, and then the de vices execute actions as instructed.

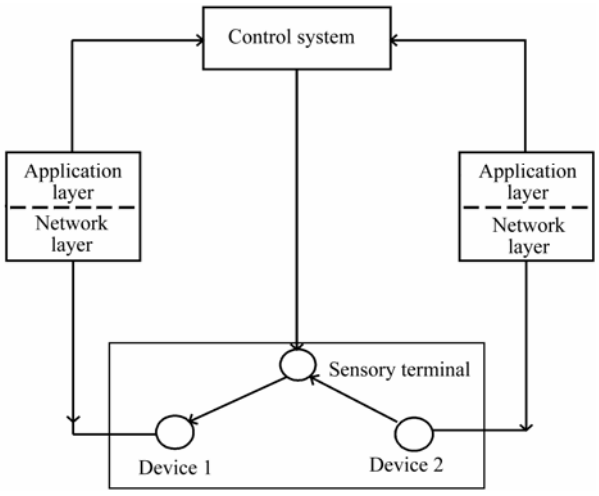

Fig. 6 Traditional view of digital community

It is noteworthy that devices or sensory terminals always believe that the command received from control system is reasonable and legitimate. However, this "blind trust" may cause catastrophic destruction in real world. For example, in the "Aurora Generator Test"[14], attackers issued illegitimate commands to the generator to connect the grid out of phase. Since the generator had no ability to synthesize the sensor data that would have told it the power was out of phase, it just executed what it had been instructed, and then the destruction occurred.

Figure 7 illustrates a new model of control architecture for digital community, where devices and sensory terminal/interactive terminals are given the ability to independently adjust whether or not the commands received are reasonable to execute. In this model, devices and sensory terminals/interactive terminals still transmit data to control system, and the control system still issues commands to the sensory terminal or device. The distinction of this new model is that devices or sensory terminals have intelligent ability to synthesize information from control system and sensors to determine whether or not to execute commands from control system. Thus, the proposed model here compensates for nonexistent, erroneous and malicious commands that come from control the system.

United States Department of Energy has strained every nerve to promote a genuinely autonomous and self-healing architecture[15]. However, it seems unlikely to be achieved independently without human-in-the-loop control system involving. An architecture, where devices and sensory terminal/interactive terminal have the ability of synthesizing information and validating reasonableness, will gain significant merit for true automation and self-healing activity. Characteristics of this model (see Fig. 7) can be described as follows: enabling devices and sensory terminals/ interactive terminals to do what-if analysis by themselves; synthesizing information, validating reasonableness and determining whether or not to trust when receiving commands from control system; evaluating the impact of received commands before executing. The characteristics mentioned above gain significant merit for the reliability of digital community system.

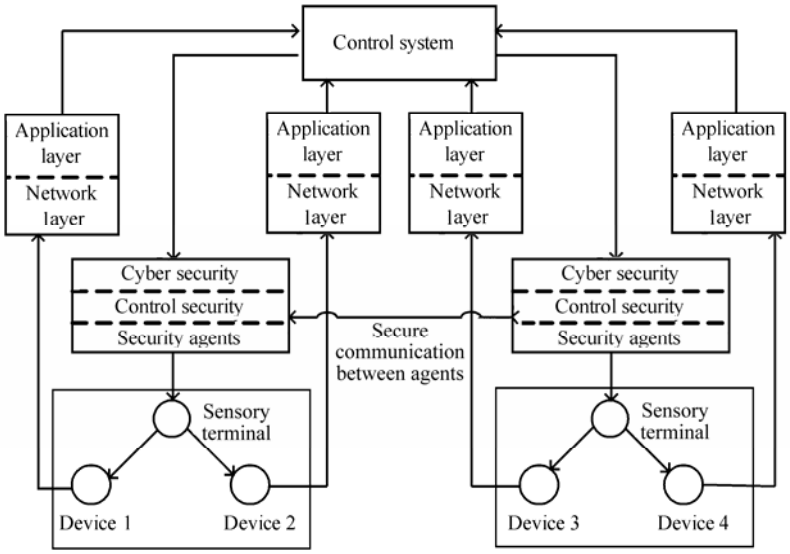

Fig. 7 High assurance digital community

5 Conclusion

Digital community develops with increasing introduction of additional "smart" devices and programmed sensor over the coming years, which will make cybersecurity issues more important and complicated. We use a three level_criticality model to determine the potential impact that exists in digital community system, and implement a defense-in-deep approach for security issue to increase digital community reliability. A high-assurance trust model, which assumes insider compromise existing in the digital community, is finally proposed according to the security issues analysis. The proposed security model provides more security services and less security management issues than related security models.

References

[1] Australian Unity. Australian unity wellbeing index [EB/OL]. [2010-05-10]. *http://www.australianunitycorporate.com.au/*

community/auwi/Pages/ default.aspx.

[2] Gubbi J, Buyya R, Marusic S, *et al*. Internet of Things (IoT): A vision, architectural elements, and future directions [J]. *Future Generation Computer Systems*, 2013, **29**(7): 1645-1660.

[3] Li S C, Li D X, Zhao S S. The internet of things: A survey [J]. *Information Systems Frontiers*, 2015, **17**(2): 243-259.

[4] Federal Aviation Administration. Advisory circular AC: 25-11A[EB/OL]. [2007-06-21]. *http://www.faa.gov/ documentLibrary/media/Advisory_Circular/AC*25.1435-1.*pdf.*

[5] Kopetz H. An integrated architecture for dependable embedded systems [C] // *Proc* 23*rd IEEE International Symposium on Reliable Distributed System*. Florianpolis : IEEE Press, 2004: 160-161.

[6] Meserve J. Sources: Staged cyber attack reveals vulnerability in power grid [EB/OL]. [2007-09-26]. *http://edition. cnn.com/*2007/*US/*09/26/*power.at.risk/.*

[7] Bush S F. *Smart Grid*: *Communication-Enabled Intelligence for the Electric Power Grid* [M]. West Sussex: Wiley- IEEE Press, 2014.

[8] Andersson G, Donalek P, Farmer R, *et al*. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance [J]. *IEEE Transactions on Power Systems*, 2005, **20**(4): 1922-1928.

[9] Federal Energy Regulatory Commission. 2009 Report on enforcemen [EB/OL]. [2013-08-09]. *http://ferclitigation. com/wp-content/uploads/*0005-*FERC-Preliminary-Findings-August*-9-2013-2002899_1.*pdf.*

[10] Joseph H. Final Report on the August 14, 2003 blackout in the United States and Canada: Causes and Recommendations [EB/OL]. [2004-04-25]. *http://energy.gov/sites/prod/ files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.*

[11] Abduvaliyev A, Pathan A K, Zhou J Y, *et al*. On the vital areas of intrusion detection systems in wireless sensor networks [J]. *IEEE Communications Surveys and Tutorials*, 2013, **5**(3):1223-1237.

[12] Sundaramurthy S C, Bhatt S, Eisenbarth M R. Examining intrusion prevention system events from worldwide networks[C]// *Proc BADGERS* 12 *ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, New York: ACM Press, 2012:5-12.

[13] Bessani A. From byzantine fault tolerance to intrusion tolerance [C] // *Proc* 5*th Workshop on Recent Advances in Intrusion-Tolerant Systems*, Hong Kong: IEEE Press, 2011: 15-18.

[14] United States Department of Energy, Infrastructure security and energy restoration division [EB/OL]. [2007-09-27]. *http*://*www.oe.netl.doe.gov/docs/eads/ead*092707.*pdf.*

[15] Prajapati J K. Smart grid—A vision for the future[C]// *Proc* 2012 *International Conference on Advances in Engineering, Science and Management* (*ICAESM*), Nagapattinam: IEEE Press, 2012: 672-677.

□