Impact of Open Systems Dependability on IoT and SoS

Takaaki Matsumoto
Software Reliability Enhancement Center (SEC)
Information-technology Promotion Agency, Japan (IPA)
Japan

I. INTRODUCTION

Information technology (IT) system is getting more and more deeply incorporated in various key socioeconomic infrastructures that support our daily lives, including financial services, public services, communication services, and transportation services, that once it fails, it would have a tremendous impact on our living and business environment. In order to sustain safe and secure socioeconomic activities, we need to further improve the dependability of IT system that support our key infrastructures.

According to the survey conducted by IPA/SEC, the number of IT system failures that had significant effects on socioeconomic activities in Japan based on press releases has been trending upward in most of the recent years since 2009 through 2015. In 2015, it reached 45 incidents per year, which is almost three times more than in 2009.

Furthermore, a wide variety of devices surrounding us are becoming to be equipped with software as well as IT systems, and the operation of these devices is generally controlled by that software. Among these devices are automobiles, trains, and airplanes, which could become a direct threat to our lives if they fail.

When we work on the improvement of dependability in these software-based systems, we tend to consider that hardware eventually deteriorates based on the length and frequency of its use, but software does not. We have, however, come to realize that relative deterioration also occurs with software, as a result of various changes in their usage caused by, such as, the progress of related technologies and fluctuation of users' skills. It is therefore getting extremely difficult to thoroughly define the risk management requirements in the design phase.

To improve the dependability of software-based systems, we should make the most of failure cases information that actually occur during the operation phase and realize and improve open systems dependability for business continuity and recurrence prevention.

II. IPA'S APPROACH TO IMPROVE SYSTEMS DEPENDABILITY IN THE IOT ENVIRONMENT

Although the dissemination of IoT is expected to further enrich and sophisticate our social living, we may encounter further issues that product and service providers cannot predict nor assume the magnitude of impact they may cause, as the interconnection across a wide variety of products increases and becomes more complex.

We can connect a mobile phone to a car through the Internet for automatic parking. But safety and security constraints of a car are definitely stricter than those of a mobile phone and malfunction of a mobile phone may cause serious accident brought by a car. We should therefore be more aware and attentive about the potential safety and security risks, when connecting these products with one another through the Internet.

To address these issues, IPA/SEC has been developing a set of guidelines to achieve high dependability of systems used in the IoT environment. So far, we have established four guidelines, i.e., Guideline for Software Quality, Guideline for Safety and Security by Design, Framework for Development of Dependable Consumer Devices, and IoT Safety/Security Development Guidelines.

In IoT Safety/Security Development Guidelines, we identified the requirements for safety, security and reliability that should be taken into consideration in the development phase of IoT products and services. In this publication, we identified 17 guidelines that should be considered by the management, developers and operators in order for them to develop and operate safe and secure IoT products and services. These guidelines have been deliberately designed to be applicable to the development of a wide range of IoT products and services used in various industries.

III. 3. STANDARDIZATION ACTIVITIES OF THE GUIDELINES

We are promoting and disseminating IoT Safety/Security Development Guidelines towards various application domains and bringing them to the table of international standard bodies.

We are proposing development of international standards based on IoT Safety/Security Development Guidelines to ISO/IEC JTC 1 which is responsible for development of standards related to Information Technology, and actively contributing toward developing international standards. Specifically, we, as member of Japanese National Body, proposed to develop Security Guidelines for IoT Solutions based on IoT Safety/Security Development Guidelines to JTC 1/SC 27 in charge of standardization of information security, and are now preparing for a New Work Item Proposal. Furthermore, we are also preparing for another new work item Framework for Specifying Designing Requirements of IoT

Systems/services to JTC 1/SC 41 in charge of standardization of IoT and related technologies.

IV. Challenges for Dependability of Complex System (SoS)

Today, we are witnessing the emergence of a wide variety of complex system, namely system of systems (SoS). When we work on the development of SoS, we may encounter many challenges which rarely arise in the development of simple or monolithic system. These include:

- System elements operate independently.
- System elements have different life cycles.
- The initial requirements are likely to be ambiguous.
- Complexity is a major issue.
- Management can be complicated.
- Fuzzy boundaries cause confusion.

In order to cope with these challenges, there is a need to capture the entire SoS with a bird's-eye view. To achieve this, an effective way would be to take a disciplined systems engineering approach.

Based on this background, IPA/SEC has launched an initiative to accelerate the utilization of systems engineering approach in Japan. Since the definition of systems engineering varies and its process is not so clear, compared with the V-model built for the software engineering process, we have decided to take a rather inductive approach, instead of trying to clearly define what systems engineering is.

In our approach, we first gathered the information of actual complex system development projects conducted in Japan that failed as well as those that turned out to be successful, analyzed these cases, and formulated a set of key failure and success scenarios. These scenarios can be considered as an integral part of the systems engineering approach that should be widely shared among the Japanese companies across industries to improve the success rate of their complex system development projects.

In the field of system safety analysis, it is also becoming important to adopt more system-oriented approach. Prof. Nancy Leveson of MIT has proposed the new system-oriented accident causality model and hazard analysis technique named STAMP, Systems Theoretic Accident Model and Processes. This is one of the contemporary approaches that is effective in addressing the challenges we face today in increasingly complex systems.

We recognize that STAMP is extremely effective to analyze and design the system safety used in the SoS environment. So we are aiming at developing and disseminating the system-oriented safety analysis model based on STAMP that has been tailored to facilitate its implementation by Japanese companies across industries.