Device Quality Management for IoT Service Providers by Tracking Uncoordinated Operating History

Megumi Shibuya†, Teruyuki Hasegawa† and Hirozumi Yamaguchi‡

†KDDI Research, Inc.
Saitama, JAPAN
e-mail: {shibuya, teru}@kddi-research.jp

‡Osaka University
Osaka, JAPAN
e-mail: h-yamagu@ist.osaka-u.ac.jp

Abstract—**According to the widespread of Internet of Things (IoT) services with a huge number of IoT devices, service providers will face the challenges how to grasp the product quality of the IoT devices by themselves in order to make IoT services highly reliable and dependable. The cumulative failure rate is an important reliability index for evaluating the product quality and service reliability of IoT devices. However, in the horizontal specialization business model, IoT service infrastructure is often operated by multiple players such as service providers and device vendors, and device management information that is necessary to obtain the cumulative failure rate is independently and uncoordinatedly owned by them. In this paper, we propose a method of calculating the cumulative failure rate in such environment. We design an algorithm to aggregate and organize such distributed, uncoordinated information to derive the device operating history, which is fed into the cumulative failure rate calculation formula. Through several simulation experiments, we show the effectiveness of our method in several realistic scenarios, where we also arrange several uncoordinated cases.**

Keywords - IoT; Service reliability; Cumulative failure rate; Operating history; Multiple players; Horizontal specialization business model

I. INTRODUCTION

Recently, the concept of Internet of Things (IoT) has been widely penetrating into our daily lives and IoT device reliability is one of fundamental, technical issues to achieve IoT-enabled world. We have been focusing on such IoT device reliability in reference [1] and this issue enhances the concept of IoT device reliability management for more realistic cases.

According to [2], the number of devices which are available for mobile access is expected to grow to approximately 50 billion units (6.58 units per user) by 2020. In IoT enabled systems, a huge number of *IoT devices* are being interconnected, and such infrastructure becomes more sophisticated and smarter to support our lives. Simultaneously, as it becomes more indispensable, it should be more reliable to achieve sufficient service availability [3]-[5]. This cannot be achieved without high reliability and dependability of IoT devices themselves.

In the research field of reliability engineering, there are several kinds of reliability-indexes such as Mean Time Between Failure (MTBF), Mean Time To Repair (MTTR), Mean Time To Failure (MTTF) and Failure in Time (FIT) [6]. In addition, *cumulative failure rate* is often utilized as a device reliability index [7]. It is a probability of failure occurrence in a certain time period starting from the time when the device becomes in operation. The cumulative failure rate is usually derived using the failure rate for every unit of time, which is defined as a ratio of the number of failed devices to the number of devices being in operation in the unit of time. Here, the devices being in operation may vary at every moment not only due to device failure but also due to operational activities such as new device installation, removal and replacement. Therefore, we need to trace the operating history of each device to calculate accurate cumulative failure rate.

However, in order to obtain the operating history of each device, it is required to obtain the dates of device-associated events such as installation of the device, suspension and resumption of device utilization and failure. If the device manufacturers, simply called *vendors*, themselves provide services (this way of service provision is called *vertically integrated business model* [8]), such information can be obtained easily as everything is managed at a single place. In contrast, in *horizontal specialization business model* [9]-[11] where service providers (simply called *providers*) purchase the devices from vendors and use them (this style is often seen in smart meter services and the Internet access services), device operating history is owned and managed partially and uncoordinatedly by multiple business operators called *players*. Furthermore, by changing business environment around the providers, e.g., the number of IoT devices is dramatically increased and demand for service reliability becomes much more severe, we believe each provider itself is required to expand the quality management of devices which the vendors have been dealing with and responsible for. Accordingly, the possibility of lack of information from the perspective of providers is newly exposed. Therefore, the horizontal specialization business model will causes a significant issue in building a single, consistent view of operating history.

We introduce an example case to explain how and why such a situation is seen in the horizontal specialization business model in the following. In smart meter services, an electric company (i.e., a provider) purchases power meters in bulk from a vendor, lends them to subscribers, and stocks the rest as spares. When a power meter becomes out of order, the provider supports to replace it. Since the provider entrusts the repair service to the vendor, the vendor receives the failed power meter directory from a user and repairs it in order to mitigate the provider's tasks. Then, the vendor is able to manage the product-related information such as the production date and the model number of the meter as well as the failure-related information such as the date and reason of failure and the repair process. However, the device operating status (e.g., operating start date) is not observed by the vendor. Meanwhile, the provider has to manage the subscriber information including the asset information (e.g., the current meter location). Hence, it is not necessary to trace back the information about failure and others. Consequently, in order to obtain a consistent history of meters, it is necessary to design a method of aggregating the management information that are separately and uncoordinatedly managed by multiple players to enable calculation of the cumulative failure rates.

In this paper, we propose a method of calculating the cumulative failure rate, which is an important reliability index that represents device reliability. We assume that services are provided (i) using a large quantity of homogeneous devices and (ii) following the horizontal specialization business model where multiple players are involved and management information are owned separately and uncoordinatedly by them. Then, the method aggregates and analyzes those distributed information to derive the operating history of each IoT device to enable the calculation of cumulative failure rates.

The contributions of this work are four-fold.

- We deal with a significant issue of IoT device management inspired by our business experience on how we grasp and measure the device reliability, which is mandatory to maintain the quality of large-scale IoT service infrastructure operated by multiple players in the horizontal specialization business model.
- We propose a method to obtain the operating history of each IoT device from various types of management information. We would like to emphasize that calculating the cumulative failure rate using complete device history is normally done in device management, but taking into account those devices that are often replaced, repaired and reused at different times and locations is not straightforward.
- We present the experimental result of measuring the accuracy of cumulative failure rates with realistic scenarios where a part of the information is missing. Such a situation often occurs in the real environment.
- To prove wide applicability of our proposed method, we further evaluate the additional but promising uncoordinated case in which additional information elements are added from the middle, i.e., after the service was launched, due to emerging new operational requirements.

This paper is organized as follows. Section II summarizes related work and Section III introduces a service scenario in IoT infrastructure with multiple players. Section IV presents our method and experimental results are shown in Section V. Section VI considers the additional uncoordinated case in which some information elements are added after the service launch. Finally, we conclude this work in Section VII.

II. RELATED WORK

There have been various activities on evaluating product quality and device reliability [6][7][12]-[19] including the research field of reliability engineering [6][7]. Several studies on Operation And Management (OAM) issues of IoT devices in IoT service infrastructure [20]-[27]have also been conducted.

As the reliability terms, based on the methods and procedures for lifecycle predictions for a product, there are several kinds of reliability indexes [6]. Mean Time Between Failure (MTBF) is a reliability term in which the average time form the up time after the repair following a failure to the next failure. Mean Time To Failure (MTTF) is that the average length of time before failure of a device. While MTBF is used for repairable device, MTTF is used for non-repairable device. Mean Time To Repair (MTTR) is the term that the average length of time to repair a failed item. Furthermore, Failure in Time (FIT) reports the number of expected failure per one billion hours of operation for a device. Moreover, cumulative failure rate is often utilized as a device reliability index [7]. It is a probability of failure occurrence in a certain time period starting from the time when the device becomes in operation. The cumulative failure rate is usually derived using the failure rate for every unit of time, which is defined as a ratio of the number of failed devices to the number of devices being in operation in the unit of time.

References [12]-[14] present evaluation methods at the design or production phase of devices, where the cumulative failure rate is estimated by modeling the occurrence of major failures at the component level of devices. Reference [12] focuses on how to calculate the failure rate of N-channel Metal Oxide Semiconductor (NMOS) devices under Hot Carrier Injection (HCI) mechanism and Time Dependence Dielectric Breakdown (TDDB) failure mechanism. The failure rate models and hypothesis test are proposed for each HCI and TDDB. Reference [13] discusses how to determine a new parameter from failure factors observed in the field, e.g., electrostatic discharge inrush current, to integrate it into a conventional estimation method for more accurate cumulative failure rate at the product design phase. Reference [14] proposes how to use the failure statistics to obtain the failure rate of a particular component according to its real conditions. It also demonstrates how the proposed methodologies are applied for failure rate estimation of power circuit breakers. The methodologies can be used for condition-based reliability analysis for electric power networks, in order to obtain an optimized maintenance strategy. Reference [15] proposes an approach to estimating the failure rate for Time-varying Failure Rate (TFR) of the relay protection device with the field data using random failure and aging failure. These approaches assume that all information elements, which are necessary for calculating also the cumulative failure rate, are maintained by the vendor manufacturing the devices, and it is not considered that the number of devices varies by factors other than failures.

The bathtub curve is a common feature of product failure behavior [16]. It is a lifetime of a population of products using a graphical representation. The typical bathtub curve has three phases. The first part is the birth-in period, which is characterized by a high and rapidly decreasing failure rate. The second part is the useful period, when the failure rate remains almost constant. The third part has an increasing failure rate, known as the wear-out period. The bathtub curve can be useful for predicting the device failure if the age of each device is known, however only the characterizations are known.

Reference [17] proposes a one line prognostic algorithm for the power module devices using the operating history of the device to detect the time of failure quickly during operation. Reference [18] proposes the calculating probability of failure using an equipment age model that is relaxed the independence assumption of individual measurements of usage intensity and operating conditions. Moreover, it shows practitioners how to develop a more complete maintenance strategy that allows for both corrective maintenance (CM) and condition-based maintenance model (CBM) using the simple decision routine.

On the other hand, in the telecommunication network, it is difficult to calculate the failure rate accurately by reliability engineering methods because the failure rate is calculated by the number of devices and time differentiation of the cumulative number of failure devices at the given timing of elapsed time. References [19][20] propose evaluation methods for product reliability based on the observation of each device's operation history considering device changes due to non-failure, which is not taken into account in the existing work [7][21]. In reference [19], the instantaneous failure rate of a repairable device for the communication network is calculated as the limit of the average failure rate that is available for the increase and decrease of the number of devices. Namely, the number of cumulative failure rate and the number of devices are estimated as the continuing functions to times. In contrast in [20], they study the applicable condition of the mathematical model for the proposed method.

All the above assume a vertical integration structure in which all the information elements for calculating the cumulative failure rate (or a similar index) are maintained by only one player. In contrast, we are focusing on IoT service infrastructure in which multiple players (e.g., providers and vendors) are collaboratively involved. In such a horizontal specialization structure, which is expected to penetrate the IoT market in the future [11], the followings should be done to manage the product reliability of IoT devices for realizing dependable infrastructure; 1) coordinating the management information provided by each player, 2) extracting and deriving information elements and 3) reconstructing the device operation history from the information elements. As far as we know, this is the first activity focusing on IoT device management with multi-player issues.

Meanwhile, there have been many approaches so far toward IoT device applications [22]-[27], which basically focus on the management and configuration of remote sensor devices over the Internet. For example, Ref. [22] implements IPv6 over 6LoWPAN and RPL and provides CoAP-based control to facilitate sensor device management over the Internet. Reference [23] also takes a remote-management approach where MQ Telemetry Transport is utilized for IoT application and management. In Reference [24], the authors discuss the necessity of wireless sensor network management in a unified manner. They consider that the industrial authorities should be able to provide a network infrastructure supporting various WSN applications and services to facilitate the management of sensor devices, and industrial ecosystem and industrial device management standards have been introduced. Reference [26] is rather unique in the sense that a distributed approach is introduced for IoT device management from a social network point of view, where a social network theory is applied to model the services. Reference [27] discusses cloud-resource management for multi-agent IoT systems, which is also important for entire system coordination. However, they basically focus on the protocol and architecture issues and do not deal with the IoT device management processes and operations.

III. Service Scenario

In this paper, we assume IoT infrastructure with multiple players in the horizontal specialization business model. Under this assumption, we explain the device operating and management information that are separately and uncoordinatedly managed by multiple players. The scenario is based on our own experience, so cases hereafter are likely to be seen in the real world business.

As explained briefly in Section I, we target a service provider such as an electric company or a network provider that purchases the devices in bulk from an IoT device vendor and lends them to subscribers (users). If the IoT device fails, the provider lends an alternative IoT device that is stocked in their warehouse to the subscriber. After receiving it, the user sends the failed IoT device to vendor. As the provider service, it is a common business model that the user lends the device from the provider, such as STB [28].

Figure 1 illustrates the interactions between each player and user. We explain the service provision scenario using this figure.

(1) IoT Device Purchase and Stocking:

The provider purchases IoT devices from the vendor and stocks them as spares. Lending an IoT device from the provider to a user and returning it by the user due to cancellation is conducted via the provider's warehouse. The provider records the *current* location of the purchased IoT devices in asset management information. The vendor records the product-related information such as the shipping date and model number of IoT devices in shipment management information.

(2) Service Startup:

The provider creates the contract-related information for every user and manages it. The provider lends an IoT device to a user, starts the service and records the service start date in user contract information.

(3) IoT Device Failure and Replacement:

When an IoT device fails at a user location, the user contacts the provider to tell his/her device has been failed. The provider sends an alternative IoT device from their warehouse to the subscriber. After receiving it, the user sends it back to the vendor directly using a preprinted address label included with the alternative IoT device for optimizing the physical transport route. The vendor repairs the failed IoT device and records the failure-related information such as date and model number (or send-back date or receiving date as the date of failure). After the repaired IoT device is sent from the vendor to the provider, it is stocked in the warehouse. The provider updates the records related to these two devices (i.e., the current locations of failed and alternative devices). The vendor records the user's location ID from the address label as the evidence for the provider to check whether the user returns the failed IoT device.

(4) Service Cancellation:

When a user cancels its contract, he/she returns his/her IoT device to the provider. The provider re-stocks it in the warehouse and updates the current location information of the IoT device. Furthermore, the service end date of this user is recorded in the contract-related information.

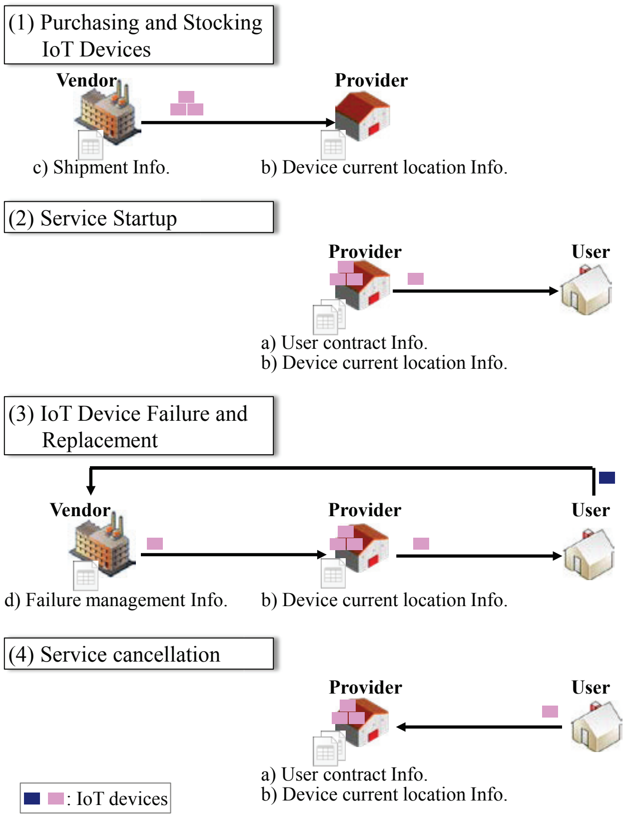


Figure 1. Interaction among multiple players and user.

In summary, the provider maintains a) contract information with users and b) asset management information of IoT devices, the vendor maintains c) shipment-related information of IoT devices and d) the failure-related information. Here, b) is usually sufficient for asset management by the provider. This is because the provider does not care about whether an IoT device was installed at different locations in the past.

On the other hand, as described in Section I, it is required to obtain the occurrence dates of device-associated events such as installation of the device, suspension and resumption of device utilization and failure to calculate the cumulative information such as the service start date and suspension and resumption of the device date in this scenario, and the provider does not observe the information such as the failure date. Therefore, each player cannot collect and build complete device-associated information. This is our motivation to provide a method to build complete operating history of each IoT device from such partial, distributed operating and management information as indicated by the above a) to d).

TABLE I. SERVICE OPERATING AND MANAGEMENT DATA

LIST-A) CURRENT DEVICE LIST (MANAGED BY PROVIDER)

List created date (=Today) (*Tc*) : 2016/09/01

Location (*L*)	Service start date (*T1*)	Current device (*SN*)	Operating start date of current device at *L* (*T4*)
1	2016/01/01	a	-
3	2016/05/01	b	-
4	2016/03/01	c	-
:	:	:	:

LIST-B) FAILED DEVICE LIST (MANAGED BY VENDOR)

Location (*L*)	Failed date (*T2*)	Failed device (*SN*)	Operating start date of failed device at *L* (*T5*)
1	2016/02/01	a	-
3	2016/04/01	a	-
1	2016/04/01	b	-
:	:	:	:

LIST-C) RETURN DEVICE LIST (OUT OF MANAGEMENT BY PROVIDER)

Location (*L*)	Return date (*T3*)	Return device (*SN*)	Operating start date of return device at *L* (*T6*)
3	2016/03/01	c	-
5	2016/06/01	d	-
2	2016/07/01	e	-
:	:	:	:

(: unknown)

Firstly, from a) and b), we try to obtain List-A of Table I with its created date *Tc*. Each pair of the sequence number *SN* and its location *L* can be obtained from b). This *L* is matched with that in a) to associate this pair with the service start date *T1* contained in a). If this device has not been failed since the day of initial installation at a user, we can obtain the history indicating that device *SN* has been working without failure between *T1* and *Tc*, which results in the fact that the operation start date *T4* is *T1* (*T4*=*T1*). Meanwhile, if there was a failure, *T1* is set to the date when an alternative device is started working at location *L*. In this case, *T4*, the operating start date of the original device *SN*, is left *unknown*.

Secondly, we try to obtain List-B of Table I from a) and d). In this scenario, the vendor records the location where the failure occurred (this kind of information is generally useful for such vendors which need some statistics of failure occurrence patterns). Here, we should consider how we will obtain column *T5*, which is the operation start date of each failed device. To do this, we associate date *T2* of failure, the sequence number *SN* and location *L* with contract information of a). Then, we obtain *T5* and the history indicating that device *SN* installed at location *L* had been working from *T5* until *T2* and then failed at *T2*.

In addition, from Figure 1 (3), the provider might maintain the information corresponding to d) that is maintained by the vendor. However, we consider that such information is not necessary for the provider's asset and the provider may not be motivated to maintain it. In other case, the provider might start maintaining it later. However, the information before starting cannot be obtained. Hence, we assume the worst case that the provider does not maintain it.

Moreover, a) contains the service end date *T3* and the service start date *T1*. If we have sequence number *SN* of the device that was returned from location *L*, we can obtain List-C of Table I containing *T6*, the operation start date of the returned device. We note that the provider may not be motivated to record sequence number *SN*. Similarly with the List-A case, from this List-C, we can obtain the history indicating that the returned device *SN* had been working from *T6* until *T3* without failure. Under a certain condition, *T6* is equal to *T1*.

In the next sections, we present how *T4*, *T5* and *T6* are obtained using List-A, B and C, and how the cumulative failure rate is calculated using the history.

IV. Proposed Method

A. Overview

In this section, we explain how to obtain the cumulative failure rate of IoT devices whose management information is maintained separately and uncoordinatedly by multiple players. Our proposed method consists of the following three Steps;

- *Step1*: Reconstructing the operating history of each IoT device,
- *Step2*: Counting the operating days, and
- *Step3*: Calculating the cumulative failure rate.

Specifically, our proposed method basically uses List-A and B for reconstructing the operating history, and List-C as well as (if exists). Note that even without List-C, the method can reconstruct the history but some error may occur because *T3*, and *T6* in List-C are not plotted on the time-sequence diagram (See Figure 2 in Section IV-B). We numerically evaluate the impact of such error in Section V.

B. Design Details

Step1: Reconstruct the operating history of IoT device.

Step1-1) Create time-sequence diagram per location.

(1) First, the time-sequence diagram per location is created as shown in Figure 2 (i) where x- and y-axes are # of days passed (denoted as *T*) from the reference date "0" and location *L* (1, 2, …), respectively. Current date *Tc*, failed date *T2* and return date *T3* in List-A, B, and C are plotted as square boxes on the diagram at (*x*,*y*)=(*Tc*/*T2*/*T3*, relevant *L*), respectively. Note that for easy understanding, in Figure 2, we assign a numeral number *j* to each plot as ID. It is denoted inside the square box corresponding to the plot.

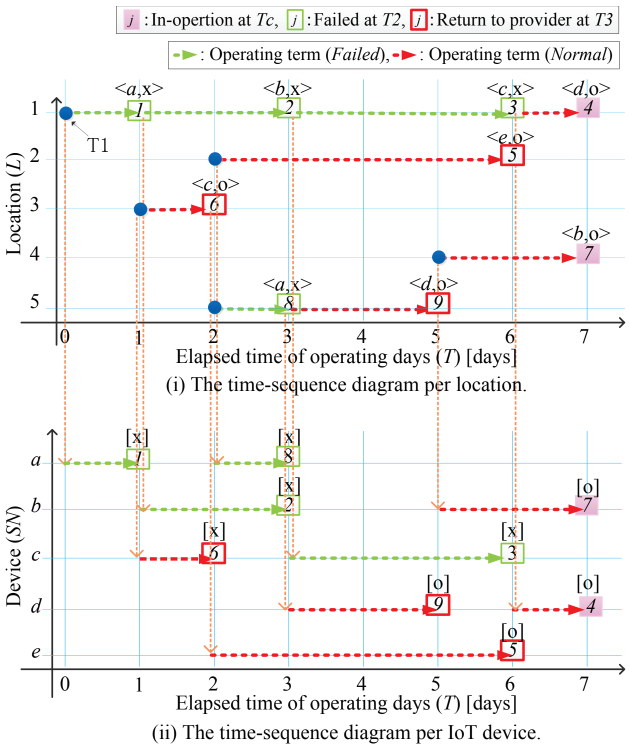


Figure 2. Time-sequence diagrams for reconstructing the operating history of each IoT device.

(2) For each plot *j*, device *SN* and device operating status x="*Failed*" or o="*Normal*" at the relevant date are associated as its attribute. For instance in Figure 2 (i), plot *j*=8 with <*a*,x> (at *T*=3 and *L*=5) means that the device *a* was "*Failed*" at location *L*=5 (then it was sent back to the vendor for repair). Plot *j*=7 with <*b*,o> means that the device *b* was "*Normal*" at *L*=4 (therefore, it is in-operation now (*T*=7)). Plot *j*=9 with <*d*,o> means that the device *d* was "*Normal*" at *L*=5 (because it was returned to the provider without failure due to user cancellation at *T*=5).

(3) Service start date *T1* at location *L* in List-A is plotted on the diagram.

(4) We assume that the failed device is replaced to another device on the same day for non-stop service. Along the time-sequence of each location *L*, the plots on it are traced back from the current date *Tc* (*T*=7) to the reference date (*T*=0) in order to determine the start date (referred to as S_j) of each plot *j* at the location. The date of *j*'s previous plot is regarded as the start date of *j*. For example, the start date of device *b* at plot *j*=2 ((*x*,*y*)=(3,1)) is determined as S_2=1 because its previous plot (*j*=1) is at *T*=1 ((*x*,*y*)=(1,1)).

(5) The operating term for each plot *j* can be extracted as the term from S_j to *T* of plot *j*. For example, device *b* at plot *j*=2 is operated from S_2=1 to *T*=3 so the term is 2 days. As another example, device *b* at *j*=7 ((*x*,*y*)=(7,4)) is operated from S_7=5 to *T*=7 (now in-operation) so the term is also 2 days.

Step1-2) Transform time-sequence diagram per location to per IoT device.

(1) The time-sequence diagram per IoT device (see Figure 2 (ii)) is transformed from Figure 2 (i). At first, each plot *j* in Figure 2 (i) is re-plotted on Figure 2 (ii) according to the device *SN* in its attribute. Note that the device operating status x/o in its attribute is inherited. For instance, plot *j*=2 with <*b*,x> ((*x*,*y*)=(3,1)) in Figure 2 (i) is re-plotted to *j*=2 with [x] ((*x*,*y*)=(3,*b*)) in Figure 2 (ii).

(2) For each plot *j*, the relevant operating term from S_j to *T* of the plot *j* is drawn on Figure 2 (ii). It is easy to obtain each IoT device's operating history by collecting operating terms per device from Figure 2 (ii). For instance, the operating history of device *b* includes two operating terms, i.e., S_2=1 to *T*=3 (*Failed*) and S_7=5 to *T*=7 (*Normal*).

Step2: Counting the operating days.

Two types of operating days are counted per IoT device from the operation histories. The first type is referred as "*Failed days*" (*P*) which is ended with a plot derived from *T2*, i.e., failed date. The second type is referred to as "*Normal days*" (*Q*) which is ended with a plot derived from *T3* or *Tc*, i.e., return or current date without failure. For counting the operating days of each IoT device, an operation term of the device is selected in chronological order and checked whether the term is ended by *T3* or not. If so, the term should be concatenated to the next operating term (if any) as a single piece of operating days. For example in Figure 2 (ii), the device *b* is set *P*=2 and *Q*=2, while the device *c* is set *P*=4(=1+3), and the device *d* is set *Q*=3(=2+1). *P* and *Q* of each device are shown in Table II.

TABLE II. THE OPERATING DAYS FOR EACH *SN* IN FIGURE 2 (ii)

SN	# of operating days (# of terms)	Operating days [days]	
		1st	2nd
a	2 (2)	*P*=1	*P*=1
b	2 (2)	*P*=2	*Q*=2
c	1 (2)	*P*=4 (=1+3)	-
d	1 (2)	*Q*=3 (=2+1)	-
e	1 (1)	*Q*=4	-

Step3: Calculating the cumulative failure rate.

From both *Failure days* and *Normal days* in Step2, the cumulative failure rate is calculated. Let *f*(*x*) denote the failure density function, the failure occurrence probability until time *i* has passed, i.e., the cumulative failure ratio *F*(*i*), is expressed in equation (1) [6].

$$F(i) = \int_0^i f(x)dx \tag{1}$$

We can approximately obtain the following difference equation by differentiating equation (1) and substituting infinitesimal *di* to the unit time (a day).

$$F(i) - F(i-1) = f(i) \tag{2}$$

Here, let $\lambda(i)$ denote the failure rate of *i*-th unit time. Since *f*(*i*) is expressed as

$$f(i) = \big(1 - F(i-1)\big) \cdot \lambda(i), \tag{3}$$

we can obtain the following equation:

$$F(i) = F(i-1) + \big(1 - F(i-1)\big) \cdot \lambda(i), \tag{4}$$

where

$$F(0) = 0, \quad \lambda(i) = \frac{n(i)}{N(i)+n(i)} \quad (i = 1, 2, \dots). \tag{5}$$

Note that *n*(*i*) and *N*(*i*) are the number of failed devices (P = *i*-1) at day *i*, and the number of in-operation devices at the end of day *i*, respectively. From the above discussions, the cumulative failure rate can be calculated from the operating history.

In addition, $m(i)$ denotes the number of returned devices, which is suspended at day i, is given by the following equation:

$$m(i) = N(i-1) - \big(N(i) + n(i)\big). \qquad (6)$$

Assuming that $\lambda(i)$ is the same regardless of the devices, the cumulative failure rate is not affected even if suspended devices exist.

V. EXPERIMENTAL EVALUATION

We verify that the proposed method expressed in Section IV can reconstruct operating histories and calculate the cumulative failure rate. In addition, we evaluate the accuracy of the cumulative failure rate when some information elements are missing.

A. Experimental Setup

In order to validate the effectiveness of our proposal, we develop the simulator implementing the proposed method. The input data set for this simulator consists of List-A, B, and C (if any) without *T4, T5*, and *T6*. From these input data sets, the simulator complements the unknown fields (*T4, T5*, and *T6*), then reconstructs operating histories and calculates the cumulative failure rate. This simulator is a Ruby program with approximately 17,000 lines, executing on a PC whose specification is shown in Table III.

TABLE III. SPECIFICATION OF PC FOR SIMULATION

Parameters		Values
PC	CPU	E5-2650L v2@1.70GHz
	Memory	126GBytes
	OS	CentOS 6.6
Program		Ruby 1.9.3

TABLE IV. PARAMETERS OF CREATING EVALUATION DATA

Parameters	Values
Failed rate *U* [%/day]	0.2, 0.5, 0.8
Return rate *R* [%/day]	0, 0.2, 0.4, 0.6, 0.8, 1.0
The number of simulation days *T* [days]	1,826 (= 5 years)
The number of devices [units]	15,000 ~ 70,000
The number of locations [locations]	100 ~ 10,000

Evaluation data sets as shown in Table IV are arranged with various return rates *R* and failure rates *U*, both of which follow uniform distribution irrespective of *T*. Simulation days *T* is 1,826 days (= 5 years), the maximum number of devices is 70,000 [units], and the maximum number of locations is 10,000. We assume no IoT devices are in-operation at *T*=0, and the replacement of failed device is finished on the same day as the failure occurs. In addition, we assume the followings to simplify the simulation.

- Just after a user cancels his/her contract at location *L*, a new user at Location *L'* starts his/her contract and uses another device.
- Through the simulation, we regard *L* and *L'* are equivalent, i.e., the total number of devices and that of locations are never changed by return events.

TABLE V. VERIFICATION CASES

Case #	List-C management / non-management	unknown data
Case1	Management (=use List-C)	*T4*, *T5*, *T6*
Case2	Non-management (=not use List-C)	*T4*, *T5*, List-C*

**T6*: unknown because of List-C unmanaged

For accurate evaluation results, we arranged 180 data sets in total, because 18 *R*/*U* pairs are specified and 10 random data sets are generated per *R*/*U* pair. Note that these data sets are given as List-A, B and C. At first, a data set consists of all the information elements in List-A, B and C are generated (we call it "reference data set"). Then, an evaluation data set is created from it by omitting unknown fields, i.e., *T4*, *T5* and *T6* or *T4*, *T5* and whole List-C, according to the case in Table V.

B. Verification of proposed method

We verify that the proposed method can complement the unknown fields in List-A, B, and C in Case1 and Case2 by comparing with the reference data sets. We also reconstruct operating histories and calculate cumulative failure rates from all the evaluation data sets.

As a result, we confirm that the simulator successfully completes the above processes for any data sets in any cases. In Case1, all *T4*, *T5* and *T6* of event start dates are completely matched with those in the reference data sets. In contrast, in Case2, *T4* and *T5,* which are operating start dates of failed and current devices respectively, are unmatched from those in the reference data sets due to the lack of List-C. Here, let *K* denote the unmatched rate of start dates. In percentage terms, *K* is given by the following equation:

$$K = ((v1 + v2)/(w1 + w2)) \times 100,$$

where *v1* and *v2* denote the number of unmatched *T4*, *T5*, respectively, while *w1* and *w2* denote the total number of failure events and in-operation events, respectively.

Figure 3 shows the unmatched rate of the start dates *K* where the failure rate *U* varies from 0.2 to 0.8. From this figure, we can easily find that *K* is increased as *R* does, and decreases in proportion to *U*. For example, *K* becomes 77.3%, 62.2% and 52.2% at *R*=1.0 of *U*=0.2, 0.5 and 0.8, respectively. Note that *K* is 0% irrespective of *U* when *R*=0.0 (no return event occurs) because there is no influence due to lack of List-C.

On the other hand, the example computation time to obtain the operating history and the cumulative failure rate are approximately 3 [min] and 1 [min], respectively, in the case of *U*=0.8 and *R*=1.0 with 70,000 IoT devices.

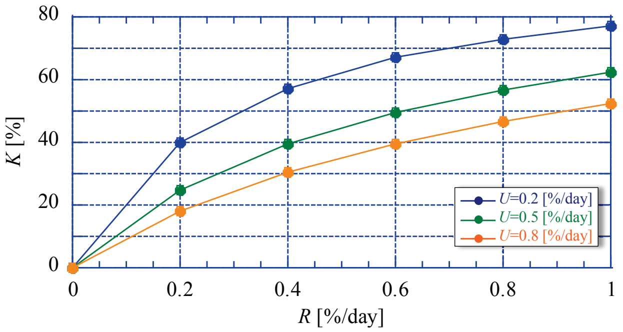


Figure 3. Unmatched rate of start date K vs. return rate R.

C. *Effect of cumulative failure rate by return rate R*

We evaluate the reliability by calculating the cumulative failure rate $F(i)$ various rerun rate R. Figure 4 shows the cumulative failure rate $F(i)$ in each failure rate U where the return rate R varies from 0.0 %/day to 1.0 %/day at 0.2 %/day intervals. Each plot indicates the average of $F(i)$ values individually calculated from 10 random data sets arranged per R/U pair.

It is clear in Figure 4 that $F(i)$ increases in proportion to R irrespective of U and that the larger R becomes, the more rapidly the cumulative failure rate $F(i)$ increases. As for the errors of $F(i)$ (referred to as α) between R=0.0 and 1.0, α =0.143 at i=400, α=0.138 at i=159, and α=0.130 at i=105, respectively. So the error α decreases with increase of U.

Figure 4 also indicates that our method conservatively underestimates the cumulative failure rate. In the case hat List-C is unmanaged, the operating terms of return events, such as device d at S_9=3 to T=5 and device c at S_6=1 to T=2 in Figure 2 (ii), are lost. As a result, $N(i)$ in equation (5) can be smaller so that $F(i)$ in equation (4) tends to be increased in a short time as R increases. From the provider's perspective, the calculated rate can be still useful when the provider discloses it to the vendor for encouraging more improvement on the product quality and reliability of IoT devices.

However, in the reverse direction from the vendor to the provider, such underestimation may mislead the vendor, e.g., vendor may consider he need not do anything next. Conversely, the vendor should recognize that the actual failure rate may be higher. Meanwhile if multiple vendors exist, the cumulative failure rate can be still used as an important index for comparing device qualities between these vendors.

Therefore, the calculated failure rate should be interpreted carefully according to the player's role.

VI. Additional Uncoordination Case

Practically there could be wide variations on what management information is maintained by each player. In the scenario described in Section III, we assume that each player is dedicated to playing his role and does not have any incentive to maintain extra management information beyond his role. However, in the real world, it is probable that players may add some management information due to emerging new operational requirements after the service starts. For example, similar service infrastructures and their providers are often unified in real cases.

Here, we qualitatively discuss how to handle such management information change, especially in the case that some useful information elements can be obtained after a certain date. For example, in Sec. III, it is considerable that the service is started with a very small number of users and it is not so important for the provider to improve product reliability of IoT devices at this moment. However, the number of IoT devices increases as the service grows, and the provider wants to improve the product reliability of IoT devices so that the provider starts maintaining List-C on a certain date (T=Y).

In such a case, return date $T3$ in List-C is on and after the date Y and there are no previous records before it, i.e., from $T=0$ to $Y-1$. For calculating the cumulative failure rate, we can choose one of the following three options.

Option 1)

The calculation is conducted using recorded $T3$ ($T3 \geq Y$) only, assuming that no return event (service cancelation), occurs at any T where $T<Y$.

Option 2)

The calculation is conducted after complementing $T3$ at T ($T<Y$) based on R calculated from recorded $T3$ ($T3 \geq Y$).

Option 3)

The calculation is conducted without List-C.

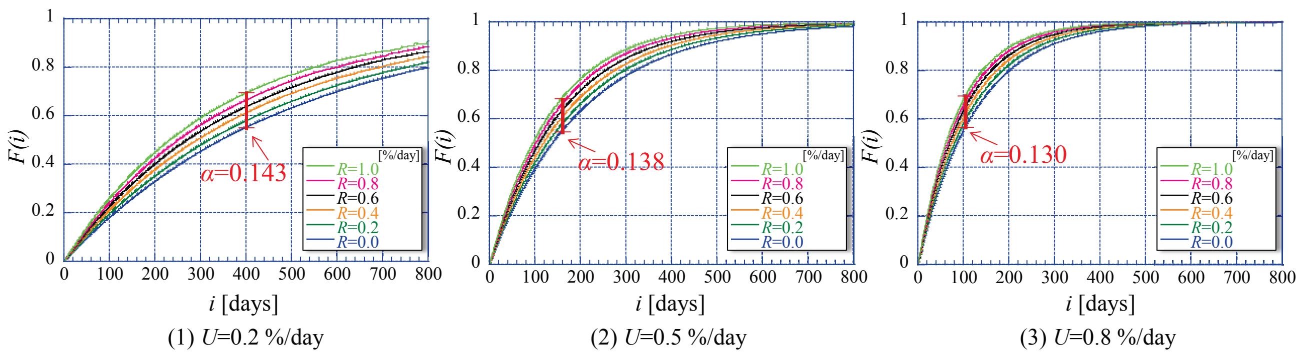


Figure 4. Cumulative failure rate $F(i)$ vs. operating days i with different return rates R.

Among above three options, Option 3 is equivalent to the result of $R=0.0$ in each U in Figure 4. According to the results in Figure 4, it is expected qualitatively that the cumulative failure rate $F(i)$ in Option 2 is the most increasing trend, i.e., seems the worst product quality, followed in order by $F(i)$ in Option 1 and $F(i)$ in Option 3. Hereafter, we describe it as "Option 2 > Option 1 > Option 3".

To verify the above qualitative analysis, we conduct the quantitative evaluation of the three options. At each option, the evaluation data are emulated as follows, then the cumulative failure rate $F(i)$ is calculated.

Option1)
Return events occurring at $T<Y$ are deleted from reference data. Then, the start dates of all events (return, failure, and current) are calculated.

Option2)
Return events occurring at $T<Y$ are deleted from reference data, and return rate R' at T ($T\geq Y$) is calculated. Then, the return events are inserted at T ($T<Y$) based on R'. Finally, the start dates of all events are calculated.

Option3)
All the return events are deleted. Then, the start dates of all events are calculated.

Evaluation data sets are arranged with different return rates R (0.2, 0.5, and 0.8) and failure rates U (0.0 to 1.0 at 0.2 intervals), and other parameters are set as shown in Table IV. In addition, Y is set to 365, 730, 1,095 or 1,460 [days] considering one year as a unit. For accuracy of evaluation results, we arrange 1,620 data sets in total. Concretely, 72 $R/U/Y$ sets are specified and 10 random datasets are generated per $R/U/Y$ sets in Options 1 and 2. In Option 3, 18 R/U pairs are specified and 10 random data sets are generated per R/U pairs. Note that at Option 3, the calculation is conducted without List-C regardless of T.

TABLE VI. MAXIMUM ERROR RATE (ABSOLUTE VALUE) OF R' IN OPTION 2 AT EACH Y

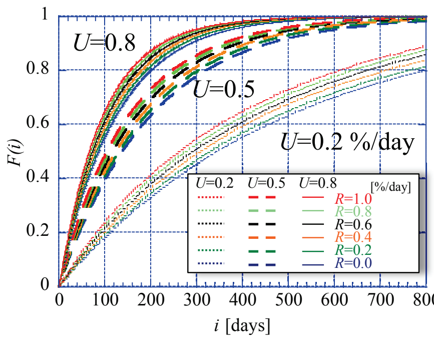
Y [days]	365	730	1,095	1,460
Max. $\|R'-R\|/R$	0.023	0.029	0.026	0.028

Before presenting the evaluation results, we confirm the error rate of the estimated return rate R' to the ground truth at each Y in order to verify whether or not R' was given accurately when the data sets of Option 2 are created. The maximum error rates (absolute values) of R' for different Y's in 24 data sets are shown in Table VI. Consequently, the errors are between 0.023 and 0.029, which are negligibly small. Hence we conclude that R' can be regarded as R in Option 2.

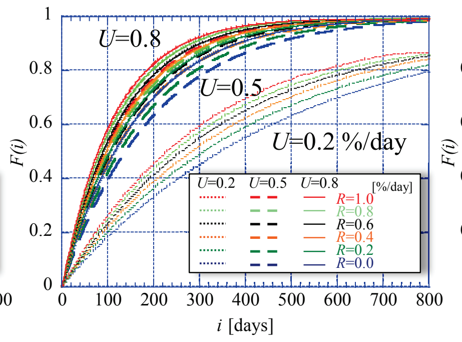
Figure 5 shows the cumulative failure rate $F(i)$ in each option, where failure rates U are 0.2, 0.5 and 0.8 and return rates R are between 0.0 and 1.0 at 0.2 %/day intervals. We note that only $F(i)$ in Y=730 case is shown in Figure 5 for better visualization. In all options, $F(i)$ increases rapidly as U becomes larger. In Options 1 and 2, $F(i)$ increases proportionally to R. On the other hand, in case of Option 3, $F(i)$ is almost same[i] for the different R values.

Next, we evaluate the cumulative failure rate $F(i)$ in each option quantitatively. $F(i)$ where return rates R are 0.0 and 1.0 at Y=730 is shown for each U in Figure 6. It is clear in each case of U, the cumulative failure rate $F(i)$ at R=1.0 increases rapidly where the increasing rates of three options are: Option 2 > Option 1 > Option 3. As for the errors of $F(i)$ between Options 2 and 1 (referred to as β) and between Options 2 and 3 (referred to as γ) where the values of U are 0.2, 0.5, and 0.8, we obtain β=0.05, 0.04 and 0.03, γ=0.13, 0.13 and 0.12, respectively.

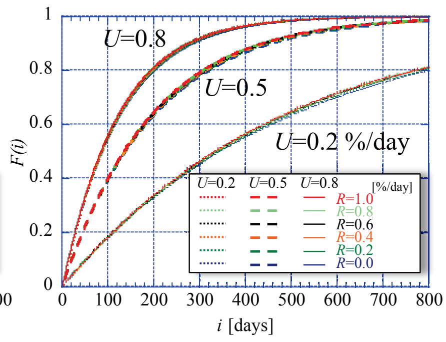
[i] Only negligible difference caused by failure events generated randomly in each data set is observed.



(1) Option 1

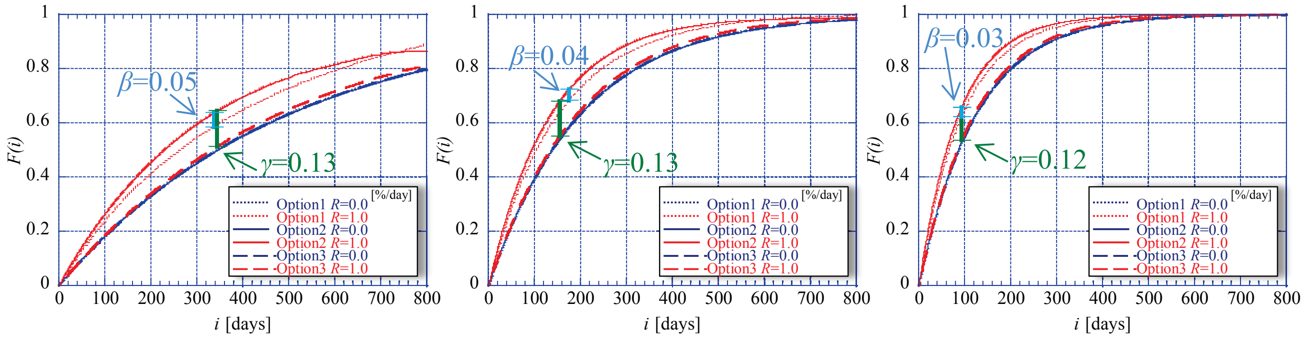


(2) Option 2



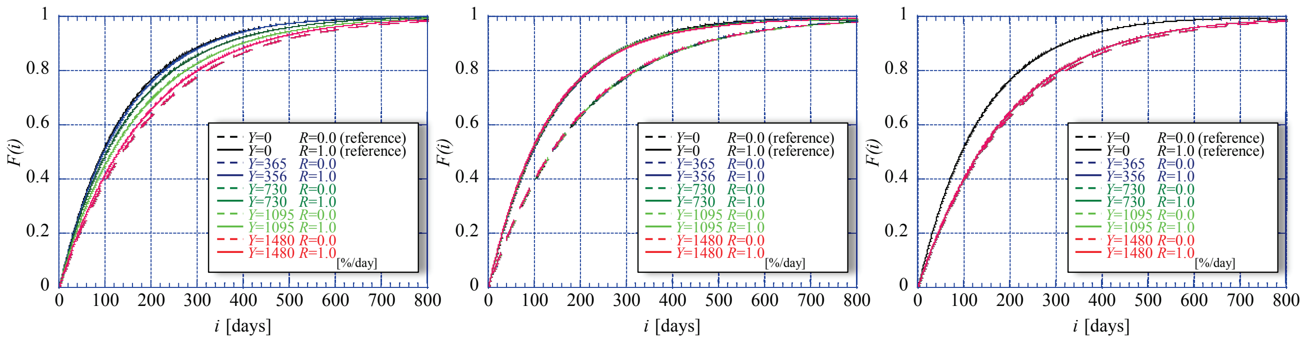
(3) Option 3

Figure 5. Cumulative failure rate $F(i)$ vs. operating days i with different return rate R and failure rate U in each Option (Y=730).
(thin dot, thick dot and solid lines correspond to U=0.2, 0.5 and 0.8 cases, respectively)



(1) U=0.2 %/day (2) U=0.5 %/day (3) U=0.8 %/day

Figure 6. Cumulative failure rate *F(i)* vs. operating days *i* with differenet Option/*R* pairs in each *U* value (*Y*=730).



(1) Option 1 (2) Option 2 (3) Option 3

Figure 7. Cumulative failure rate *F(i)* vs. operating days *i* with different *Y*/*R* pairs in each Option (*U*=0.5).

Furthermore, we confirm the impact of starting the maintenance of List-C at Y on the cumulative failure rate $F(i)$. Figure 7 shows $F(i)$ at each Y when U is 0.5. For comparing the results, in all figures, we plot Y=0 (black solid and dotted lines) as the references in which List-C is maintained from the beginning as well as List-A and List-B. In Option 2 at R=1.0, $F(i)$ is almost the same irrespective of Y. On the other hand in Option 1, $F(i)$ becomes larger as Y decreases. In addition, $F(i)$ at Y>0 is smaller than that at Y=0. Furthermore, as for comparison of Options 1 and 2, $F(i)$ in Option1 is smaller than that in Option 2 at Y=365 (the smallest value of Y in this evaluation).

These results prove the correctness of our qualitative expectation for the cumulative failure rate $F(i)$, i.e., Option 2 > Option 1 > Option 3 (see Section VI). Note that the above order is not changed irrespective of Y, the date for starting the maintenance of List-C.

VII. CONCLUSION

In this paper we proposed a method of calculating the cumulative failure rate in IoT service infrastructure operated by multiple players such as service providers and device vendors in the horizontal specialization business model. According to changing business environment around providers such as massive numbers of IoT devices and strenuous demand on its service availability, we believe each provider itself is also required to expand the quality management of devices instead of or together with vendors.

We revealed the possibility on lack of information from the provider's perspective, and proposed the method which aggregates and analyzes distributed information to derive the operating history of each IoT device to enable calculation of cumulative failure rates. We also verified that the proposed method can derive operating histories and calculate the cumulative failure rate. In addition, we evaluated the accuracy of the derived cumulative failure rates when some information about device operation are missing. From the experimental evaluation, our method conservatively underestimates the cumulative failure rate. So, the calculated failure rate should be interpreted carefully according to the player's role. Even if such underestimation exists, from the provider's perspective, it is considered to be useful because it becomes some evidence to encourage the vendor to improve the product quality and reliability of IoT devices more.

Furthermore, to prove wide applicability of our proposed method, we also evaluated the additional but promising uncoordinated case in which additional information elements are added after the service was launched, due to emerging new operational requirements. We quantitatively analyzed the cumulative failure rate using three types of options for calculating methods.

We are now planning to apply our method to further different cases. We believe that we have shown the applicability of our method by introducing well-seen, representative cases in this paper, but examination of our approach in a variety of scenarios is part of our future work.

REFERENCES

[1] M. Shibuya, Y. Hasegawa, and H. Yamaguchi, "A Study on Device Management for IoT Services with Uncoordinated Device Operating History," Proc. International Conference on Networks (ICN 2016), pp.72-77, Feb. 2016.

[2] Cisco Systems Inc., "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html, accessed Jan. 8, 2016.

[3] M. Ahamad, "Reliability Models for the Internet of Things: A Paradigm Shift," Proc IEEE International Symposium on Software Reliability Engineering Workshops, pp.52-59, Nov. 2014.

[4] M. Ahamad, "Designing for the Internet of Things: A paradigm Shift in reliability," Proc. Electribuc Cioibebts & Technology Conference, pp.1758-1766, May 2015.

[5] M. N. Sahana, S. Anjana, S. Ankith, K. Matarajam, K. R. Shobha, and A. Paventhan, "Home energy management open IoT protocol stack," Proc. IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp.370-375, Dec. 2015.

[6] S. Stanley, "MTBF, MTTR, MTTF & FIT Explanation of Terms," http://imcnetworks.com/wp-content/uploads/2014/12/MTBF-MTTR-MTTF-FIT.pdf, accessed Sep. 16, 2016.

[7] W. Zheng, W. Zengquan, and W. A-na, "Failure Rate Calculating Method of Components Based on the Load-strength Interference Model," Proc. IEEE Industrial Engineering and Engineering Management (IEEM 2010), pp.783-787, Dec. 2010.

[8] OPS rules, "Vertical vs. Horizontal Integration: Which is a better Operations Strategy?," Sep. 2012, http://www.opsrules.com/supply-chain-optimization-blog/bid/241648/Vertical-vs-Horizontal-Integration-Which-is-a-Better-Operations-Strategy, accessed Jan. 8, 2016.

[9] Z. Yu, "IT, Production Specialization, and Divison of Labor: A Smith-Ricardo Model of International Trade," Carleton Economic Paper, Jun. 2003, http://carleton.ca/economics/wp-content/uploads/cep03-06.pdf, accessed Jun. 8, 2016.

[10] R. Suoranta, "New Directions in Mobile Device Architectures," Proc. Euromicro Conference on Digital System Design (DSD'06) , pp.17-26, Aug. 2006.

[11] Fujitsu Limited, "Management Direction Briefing," Oct. 2015, http://pr.fujitsu.com/jp/ir/library/presentation/pdf/en/md-20151029note.pdf, accessed Aug. 8, 2016.

[12] Z. Zhou, X. Liu, Q. Shi, Y. En, and X. Wang, "Failure Rate Calculation for NMOS Devices under Multiple Failure Mechanisms," Proc. International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), pp.362-365, Jul. 2013.

[13] T. Tekcan, G. Kahramanoglu, and M. Giinduzalp, "Determining Reliability by Failure Rate Estimation via a New Parameter," Proc. Reliability and Maintainability Symposium (RAMS), pp.1-7, Jan. 2012.

[14] J. Pan. Z. Wang, amd D. Lubkeman, "Condition Based Failure Rate Modeling for Electric Network Components," Proc. Power Systems Conference andExposition (PSCE '09), pp.1-6, Mar. 2009.

[15] R. Wang, A. Xue, S. Huang, X. Cao, Z. Shao, and Y. Luo, "On the Estimation of Time-Varying Failure Rate to Protection Devices Basedon Failure Pattern," Proc. Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), pp.902-905, Aug. 2011.

[16] Q. Duan and J. Liu, "Modelling a Bathtub-Shaped Failure Rate by a Coxian Distribution," Proc. IEEE Transactions on Reliability, vol. 65, issue 2, pp.878-885, Jun. 2016.

[17] P. James and A. Forsyth, "Real time, on line, age calculation of IGBT power modules," Proc. Power Electronics, Machines and Drives (PEMD 2010), pp.1-4, Apr. 2010.

[18] A. J. Henry and J. A. Nachlas, "An equivalent age model for condition-based maintenance," Proc. Reliability and Maintainability Symposium (RAMS), pp.1-6, Jan. 2012.

[19] H. Funakoshi and T. Matsukawa, "A failure Rate Estimation Considering the Change in the Number of Equipments," IEICE Trans. B Vol. J93-B No.4, pp.681-692, 2010 (in JAPANESE).

[20] H. Funakoshi and T. Matsukawa, "A Failure Rate Estimation Considering the Change in the Number of Equipments - Applicable condition of mathematical model for proposed method -," IEICE NS2009-17, pp.1-6, 2009 (in JAPANESE).

[21] M. Xie, Y. Tang, and T. N. Goh, "A modified Weibull extension with bathtub-shaped failure rate function," Reliability Engineering and System Safety, 2002, 76(3): 279-285.

[22] Z. Sheng, H. Wang, C. Yin, X. Hu, S. Yang, and V. C. M. Leung, "Lightweight Management of Resource-Constrained Sensor Devices in Internet of Things," in IEEE Internet of Things Journal, vol.2, no.5, pp.402-411, Oct. 2015.

[23] C. Zhou and X. Zhang, "Toward the Internet of Things application and management: A practical approach," in IEEE WoWMoM 2014, pp.1-6, 2014.

[24] S. N. Han, S. Park, G.M. Lee, and N. Crespi, "Extending the Devices Profile for Web Services Standard Using a REST Proxy," in IEEE Internet Computing, vol.19, no.1, pp.10-17, Jan.-Feb. 2015.

[25] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT," in IEEE Access, vol.3, pp.622-637, May 2015.

[26] G. Chen, J. Huang, B. Cheng, and J. Chen, "A Social Network based Approach for IoT Device Management and Service Composition," Proc. IEEE World Congress on Services 2015, pp.1-8, Jun. 2015.

[27] B. Manate, T. Fortis, and V. Negru, "Infrastructure Management Support in a Multi-Agent Architecture for Internet of Things, " Proc. Modelling Symposium (EMS), pp.372-377, Oct. 2014.

[28] Freepress, "That Box Your Cable Company Forces You to Rent," May 2016, http://www.freepress.net/blog/2016/05/20/box-your-cable-company-forces-you-rent, accessed Nov. 22, 2016.