http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 6 Issue 6, Nov. 2017, ISSN: 2288-0003

Editor-in-Chief

Prof. Thomas Byeongnam YOON, PhD.

Global IT Research Institute

Journal Editorial Board

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

- **How to submit your Journal paper and check the progress?**

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume. 6 Issue. 6

1 A Detailed Large-Scale Radio Propagation Characteristics Approaches with Time and Spatial Ratio 1060

Jinhyung Oh, Young Jun Chong

Radio Resource Research Institute, Electronic Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea

2 A Process-Aware Drone-Equipped 3D Engine and Wireless Control Measurement Platform for Integrated Management of SOC Facilities 1067

Young-Geol Lee*, Younlae Lee**, Yeonyi Jang***, Minjae Park*

**Department of Computer Software, Daelim University, South Korea*
***R&D Center, KGI, LTD., South Korea*
****Department of Applied Information Technology and Security, Ansan University, South Korea*

3 Metric of Vulnerability at the Base of the Life Cycle of Software Representations 1073

Mikhail Buinevich*, Konstantin Izrailov*, Andrei Vladyko*

*The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint Petersburg, Russia

A Detailed Large-Scale Radio Propagation Characteristics: Approaches with Time and Spatial Ratio

Jinhyung Oh, Young Jun Chong

Radio Resource Research Institute

Electronic Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea

jinhyung@etri.re.kr, yjchong@etri.re.kr

***Abstract*—The 3.5GHz band was determined as the mobile communication frequency in IMT-2020. Basically, TD-LTE in small cell environment and supplementary downlink in hotspot area will be used in 3.5GHz band. In addition, the frequency resources are becoming insufficient over time due to the explosive increase in the radio equipment. If we use frequency resources in a time and space based sharing manner, it is expected that we will be able to efficiently use the scarce frequency resources. According to recent trends, the channel sounder for the 3.5GHz band consists of a universal device such as NI equipment for baseband and transceiver and its own modules which are high power amplifier, RF switch, timing module and antenna. In this paper, we introduce the channel sounder and have verified various measurement parameters such as path loss, delay spread, K-factor and channel capacity for actual radio measurements through this channel sounder in urban and suburban areas in the 3.5GHz band. Additionally, we show the result of the path loss modelling with time and space rate using this system.**

***Keyword*—Channel sounder, Radio propagation, Time and spatial ratio, Frequency sharing**

I. INTRODUCTION

RESEARCH on radio wave propagation characteristics and development of propagation models has become an indispensable research area for the design, introduction, performance analysis and verification of new radio communication systems. The studies on the propagation characteristics and modeling for the sub-6GHz band have been continuously studied for stable positioning of the new communication system in major countries [1]-[3]. The international standards organizations such as ITU, IEEE, 3GPP, and WINNER propose standard analysis methods and modeling results. In recent years, major domestic and international standards organizations are examining 5G wireless communication systems operating in various sub-6GHz bands such as 400MHz, 700MHz, 4GHz and 5GHz. From the viewpoint of radio propagation characteristics, radio wave characterization and the development of new radio models, the consensus and dedication of major international standards organizations is more important than individual countries. The reason is that the acquisition and use of the spectrum and its impacts are not merely affecting individual countries. We will now explain why the 3.5GHz band is important for radio measurement. First, the 3400-3600MHz band was selected as the mobile communication frequency in IMT-2020 along with the 1427-1518MHz band [4]. The second is that major companies such as Qualcomm are claiming to use the 3.5GHz band for small cell TD-LTE services [5]. Finally, the 3.5GHz band is likely to be used as a downlink supplemental link due to the explosion of frequency resources [6]. Because of these many reasons, the 3.5 GHz band is considered to be an important frequency resource for future mobile communication environments. When many communication devices and systems are going to use the 3.5 GHz band, the best and most efficient way is to share frequency resources in space and time. If a particular frequency band is not always used temporally or spatially, then each communication device and system will be able to share frequency resources. Therefore, in this paper, we introduce the 3.5GHz band radio propagation measurement system and analyze the measurement result of the corresponding band using this system to confirm the temporal or spatial propagation characteristics according to frequency sharing.

II. SYSTEM SPECIFICATION

In this section, we introduce the specification of our developed radio measurement system. As shown in Fig. 1 below, our radio measurement system consists of five main components: baseband digital signal processing module, RF transceiver module, timing module, antenna, monitoring panel and storage module.

Manuscript received September 2, 2017. This work was supported by the ICT R&D program of MSIP/IITP [No.2017-0-00066, Development of time-space based spectrum engineering technologies for the preemptive using of frequency] and a follow-up of the invited journal to the conference paper of the 19th International Conference on Advanced Communication Technology (ICACT2017).

Jinhyung Oh is with radio resource research group, Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea (phone: +82-42-860-5275; fax: +82-42-860-5199; e-mail: jinhyung@etri.re.kr).

Young Jun Chong is with radio resource research group, Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea (e-mail: yjchong@etri.re.kr).


Fig. 1. System Total Shape

TABLE I
IMPLEMENTATION PARAMETERS FOR RADIO MEASUREMENT SYSTEM

Parameters	Specification
Frequency	400MHz-4GHz
Bandwidth	5MHz-130MHz
Channel Impulse Response	68dB (below 10ns resolution, above 65dB)
Transmit Power	Max 7dBm
Receive Auto Gain Control (AGC)	Min -70dBm
File Save and Replay	Receive data save and replay possible
Transmit and Reception Filter	0.1-1 (SRRC Filter, roll-off factor variable)

A. Baseband Digital Signal Processing Module

The baseband digital signal processing module is basically developed using universal NI PXI modules and the output signal is generated as direct sequence spread spectrum(DSSS) BPSK with 100Mcps. In baseband digital signal processing module, it consists of PXI 8135 for the computing function, NI 5792 for the receiving adapter module, NI 5793 for the transmitting adapter module and PXIe 7966 for the FPGA module.

B. RF Transceiver Module

The RF transceiver module is also made up of NI universal modules which are Tx/Rx IF modules and RF up/down converter. The RF upconverter raises the signal with the variable IF frequency below 3GHz to the RF frequency of 5GHz. And the RF downconverter serves to lower the signal having an RF frequency of 5GHz to an IF frequency of 3GHz. And the high power amplifier(HPA) utilizes RFHIC RUM43020 commercial product with output powers of up to 20 watts.

C. Timing Module (TIMU)

To produce the synchronized timing signal on the RF module and baseband, a rubidium oscillator with a 10MHz reference signal is utilized. To keep the time synchronization between the transmitter and the receiver of the radio measurement system, an RF cable is connected between the transmitter's TIMU and the receiver's TIMU. The clock signal is also inserted to the RF and baseband modules from the TIMU.

D. Antenna

The antennas used in the radio measurement system are developed to operate in the band between 3.5GHz and 3.7GHz. The antenna spacing is lambda(=85.7mm@3.5GHz) and the antenna gain is designed around 4-5dBi to obtain additional HPA output. The horizontal antenna pattern of the antenna is omni-directional, and the vertical antenna gain is designed to be distributed within the upper and lower 45 degrees.

E. Monitoring Panel and Storage Module

In the monitoring panel, key measurement data such as power level, spectrum mask, I/Q data and channel impulse response(CIR) are displayed. As shown in the Fig. 2-a below, the left side of the monitoring screen is configured to change the frequency, bandwidth, transmission power, receive auto gain control(AGC) and filter roll-off factor for operation of the radio wave measuring system. The measurement system operating parameters and current measurement status monitoring screens are implemented in NI LabVIEW and can be modified if functional modifications are required. Because measurement data is stored every second, a huge amount of measurement data accumulates on NI hard RAID system which is a massive storage device and a PCI express interface is built between NI PXI and NI hard RAID system for fast data storage and processing. The detailed parameters of our radio wave measurement system are shown in Table 1.

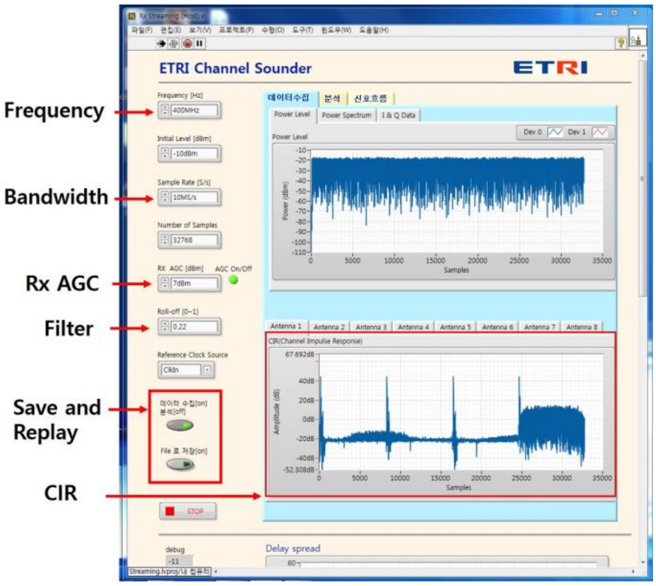


Fig. 2-a. Receiver Display

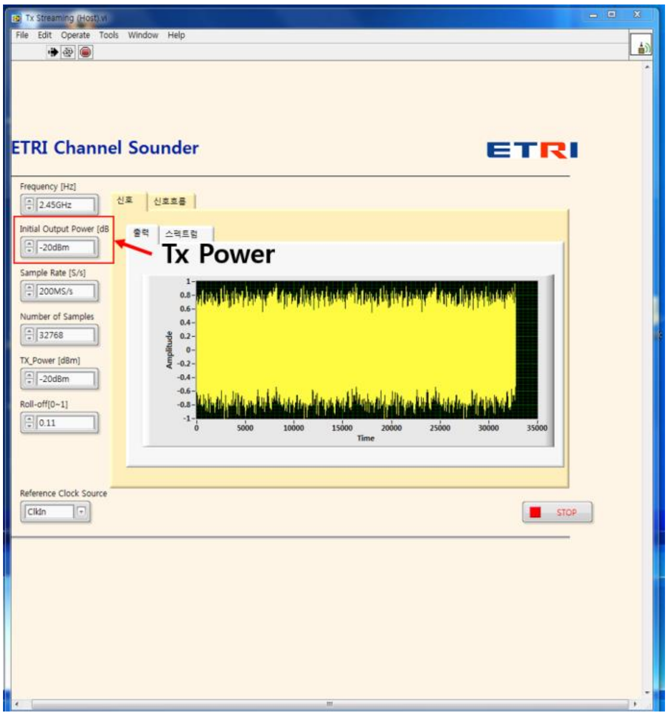


Fig. 2-b. Transmitter Display

F. Transmit Signal Generation and Receive Signal Processing Procedure

Fig. 3 shows the procedure for generating the transmit signal. The length of the PN sequence is 4096, and this sequence is oversampled twice using zero padding. To remove the adjacent signal from the transmitter, a squared root raised cosine filter with a roll-off factor 0.22 is used. The oversampled PN sequence is upconverted to IF frequency with a 200MHz sampling rate.

As shown in the Fig. 4, the received signal through the wireless channel performs A/D conversion at a sampling rate of 200MHz. After generating I/Q data, DC offset and I/Q phase offset should be removed. Next, the received signal is cross-correlated with a previously known PN sequence after processing the squared root raised cosine filter.

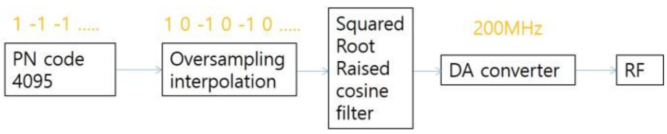


Fig. 3. Transmit Signal Generation Procedure

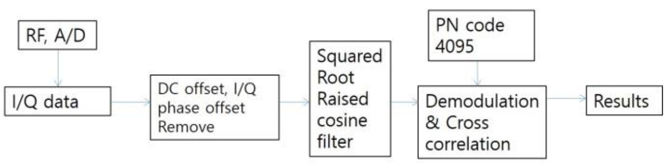


Fig. 4. Receive Signal Processing Procedure

III. MEASUREMENT

A. Synchronization

In order to perform cross-correlation between the received signal and the known PN sequence before measuring the propagation environment with the system introduced in this paper, time synchronization should be established between the transmitter and receiver. The magnitude and time delay of the received signal can be checked through cross-correlation between the received signal and the known PN sequence. The resolution of the time delay is closely related to the bandwidth of the signal. For example, a signal with a bandwidth of 100MHz has a time delay resolution of 10ns, so it can be detected up to 10ns in a multipath signal.

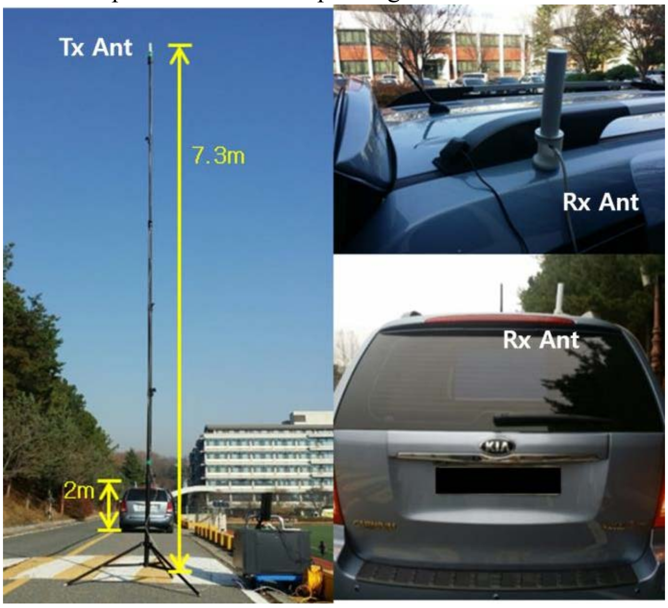


Fig. 5. Transmission and Receiving Antenna Configuration

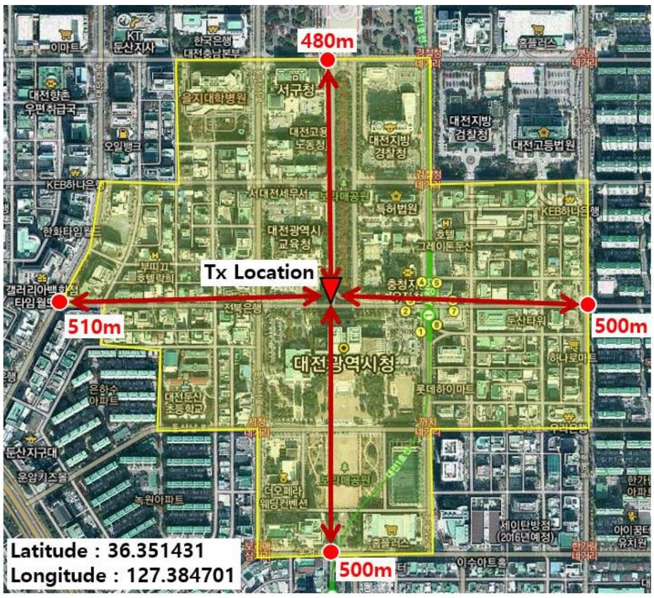


Fig. 6. Measurement Location and GPS Information of the Tx Location

B. Scenario

In this subsection, we briefly describe the measurement environment and scenarios. As shown in Fig. 5, the transmission antenna is installed on a pole with a height of 7.3m and the receiving antenna is installed on a vehicle with a height of 2m. Measurement are carried out near the Daejeon Metropolitan City Hall to analyze the propagation environment in the small cell urban environment. The location of the measurement area and the GPS information of the transmission point are shown in Fig. 6. The measurement scenario depends on the time and space rate measurement, and the detailed measurement contents according to the time and space rate will be described below.

1) Time Ratio Measurement Scenario:

Since the measurement of the radio wave according to the time rate is performed by fixing the position of the transmitter and receiver, the transceiver is arranged as shown in Fig. 7. The measurement time is conducted for seven and half hours from 11:30 a.m. to 19:00 p.m., considering lunch and work time.

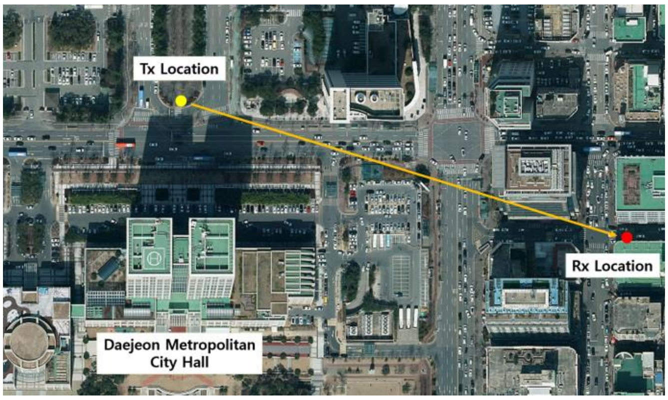


Fig. 7. Radio Measurement Map for Time Ratio

2) Spatial Ratio Measurement Scenario:

The radio wave measurement is carried out while driving near the Daejeon Metropolitan City Hall. The transmitter is placed in the same point as the time rate measurement, and the receiver is installed in a moving vehicle. Most of the measurement areas are high-rise buildings and large-scale transportation corridors. The measurement results are stored every one second while the vehicle carrying the receiver is travelling within an area of approximately 0.5km from the transmitter. The moving path of the receiver-equipped vehicle for the measurement of the space rate is shown in Fig. 8.

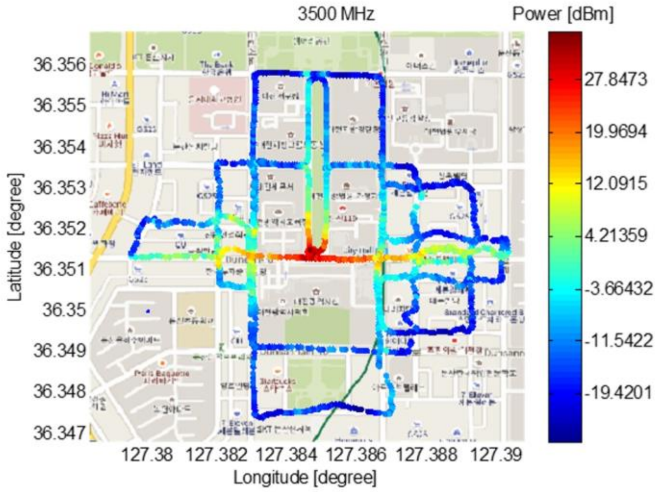


Fig. 8. Radio Measurement Map for Space Ratio

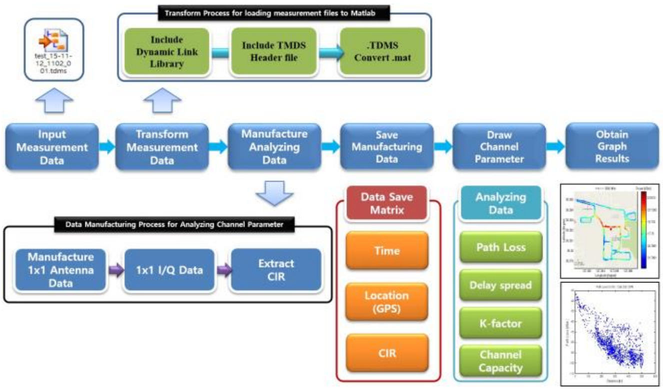


Fig. 9. Detailed Steps for Measurement Data Analysis

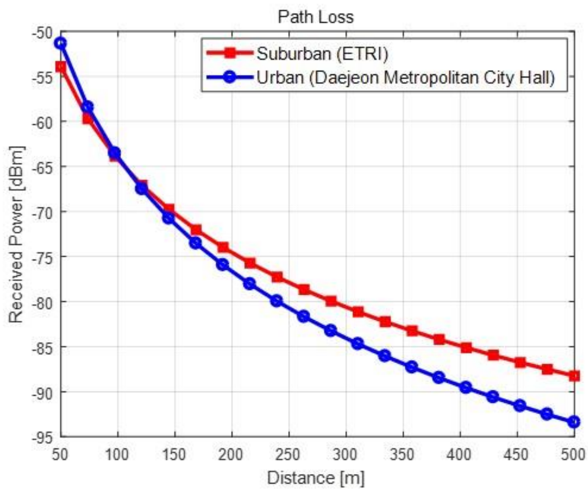


Fig. 10. Path Loss Result

IV. Performance Results

As can be seen in Fig. 9, there are several steps to analyze the radio wave measurement results. In the transform measurement data step in Fig. 9, because our measurement and analysis program is based on MATLAB, we convert the files stored in the TDMS file format which is saved in NI HDD RAID system to the MAT file format that can be read by MATLAB. In manufacture analyzing data step after file transforming, among the measured PN sequences that are repeatedly stored four times, the first and fourth PN sequences that may have been contaminated at the receiving process are removed, and only the PN sequences at the second and third positions are selected to analyze. Through the measurement time, location from the GPS and the channel impulse response(CIR) stored in our radio measurement system, we can derive radio wave measurement parameters such as path loss and delay spread, etc.

A. Radio Wave Parameter Analysis

1) Path Loss:

We derive path loss results as shown in Fig. 10. This graph shows the results inside the ETRI which is a suburban area, and the results near the Daejeon Metropolitan City Hall area, which is an urban area. The path loss measured in the urban area near the Daejeon Metropolitan City Hall is larger than that in the suburban area as the distance increases. This is because there is a higher and denser building in the urban area. In (1), there are several variables to express the path loss formula. In urban area, L_0 is 20.06, n is 4.204 and X_σ is

8.91dB. In suburban area, L_0 is 4.367, n is 3.431 and X_σ is 11.26dB.

$$\text{Path Loss} = L_0 + 10n\log_{10}\left(d/d_{ref}\right) + X_\sigma \qquad (1)$$

2) Delay Spread:

Figure 11 shows the results of CDF in terms of time delay. The results in the blue graph, urban area, show a large distribution in the case of long time delay compared to the result in the red graph. Because there are a lot of high buildings in the urban area, many reflection waves are occurred. So, the large time delay results are relatively happened in the urban area. In (2), A is 0.0186 and B is 0.88 in suburban. In urban area, A is 0.3611 and B is 0.3593 in (2).

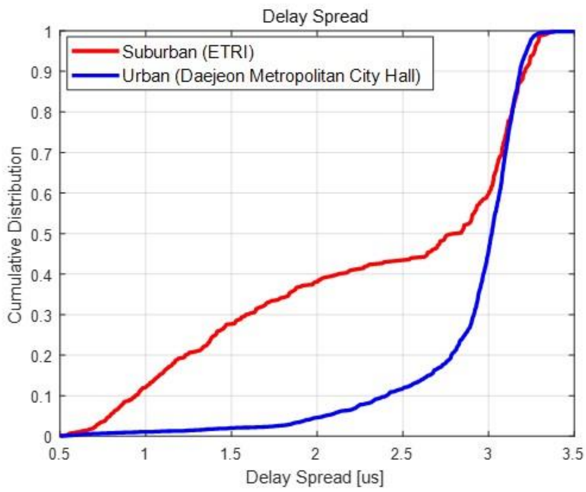


Fig. 11. Delay Spread Result

$$\text{Delay Spread} = A \cdot d^B \qquad (2)$$

B. *Performance Results for Time Rate*

The measurement results for the time rate are shown as below figures.

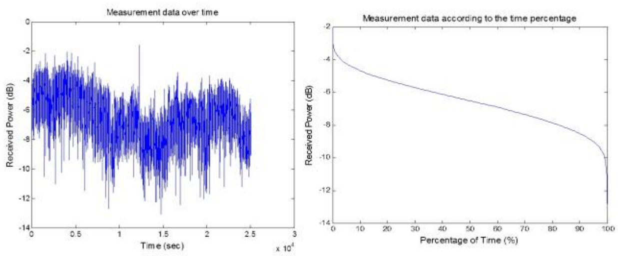


Fig. 12. Measurement Results for Time Ratio and Receiving Values according to Time Ratio

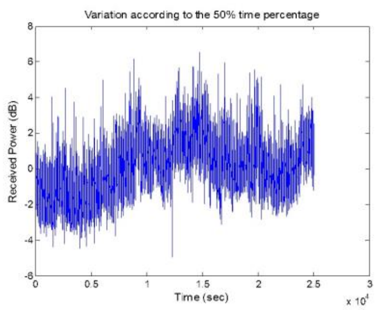


Fig. 13. The Variation Value for Signal according to the 50% Time Percentage

The time rate refers to the statistical properties of the field strength measured at a fixed location and indicates how much more than a few dB have been measured in the corresponding percentage of the total measurement time. The graph on the left side of Fig. 12 shows the strength of the received signal according to the total measurement time. As shown on the right graph of Fig. 12, the received signal strength values according to the 10%, 50% and 90%-time rate are -4.86dB, -6.19dB and -8.07dB, respectively. And Fig. 13 is a graph representing the magnitude of the received signal when the 50%-time ratio is assumed.

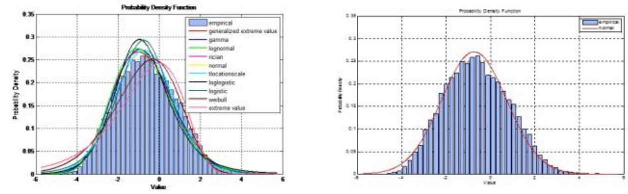


Fig. 14. The Variation Value for Signal according to the 50% Time Percentage

We show the probability distributed function (pdf) graph according to the strength of the received signal and search the distribution with similar tendency to the derived measurement result pdf graph. As shown in the right side of Fig. 14, a graph having similar distribution to the measurement results is derived, and its distribution is a normal distribution with a standard deviation of 1.47. Table 2 shows the path loss results according to the time rate application.

TABLE II
MEASUREMENT ENVIRONMENT CONSTANT VALUE

$PL(d) = L_0 + 10n\log_{10}(d/d_{ref}) + X_\sigma + \Delta T$(CORRELATION FACTOR)							
Measurement Condition			Path Loss			ΔT	Std
f	h_b	h_m	L_0	n	X_σ		
3.5	7	2	20.06	4.204	8.91	$N^{-1}(p)*\sigma$	1.47

C. *The Performance Results for Spatial Ratio*

The result of the path loss due to the mobile measurement is shown in Fig. 14 below.

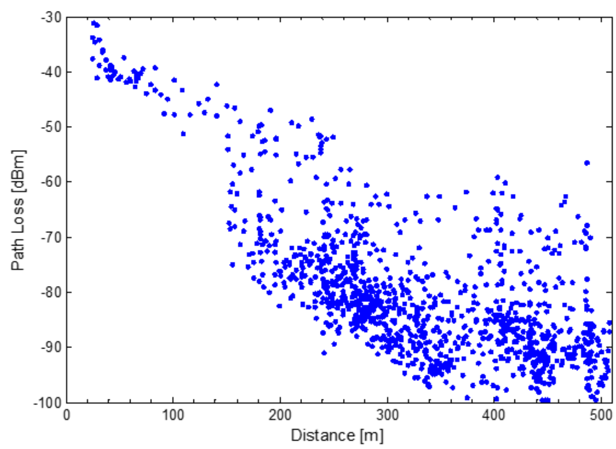


Fig. 15. Measurement Data with Mobile Vehicle

To analyze the measurement results related to the spatial rate, we should divide the results in Fig. 15 into the LOS and NLOS regions. The LOS signal distribution is shown in Fig. 16, and the curve fitting formula is expressed in (3).

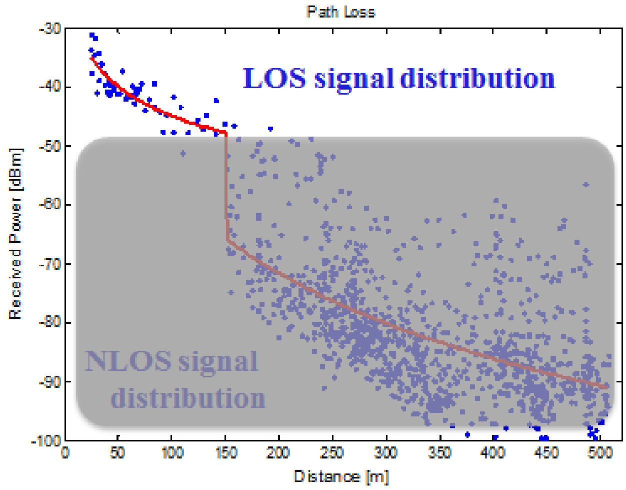


Fig. 16. LOS Signal Distribution for Spatial Ratio

$$L_{LOS} = 99.89 - 31.65\log_{10}(f) - 16.31\log_{10}\left(\frac{d}{d_{ref}}\right) \quad (3)$$

To verify the distribution of the signal with spatial rate, we obtain the difference of the LOS path loss model of equation (3) from the LOS actual measurement value. The distribution of the results is shown in Fig. 17.

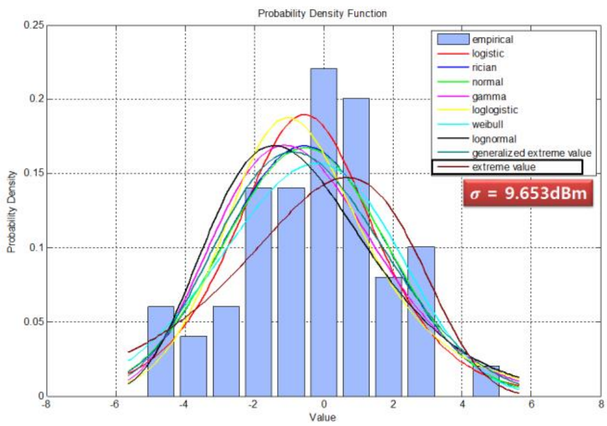


Fig. 17. Inference for LOS Signal Probability Distribution

From Fig. 17, we have obtained the LOS signal pdf and confirmed that extreme value distribution has the most similar distribution to our measurement results. The path loss model equation of NLOS is obtained from the actual measured data curve fitting, and the graph and equation are shown in Fig. 18 and formula (4). From Fig. 18 and equation (4), we confirm the pdf result and the most similar distribution function is t-location scale function as shown in Fig. 19. Based on the above results, we obtain path loss results according to the spatial rate as shown in Fig. 20. We can confirm the path loss value for 10%, 50% and 90% spatial ratio is -46dBm, -49dBm and -78dBm, respectively, when the distance between transmitter and receiver is about 200m. And we can check that the path loss is increased as the spatial rate increases from 10% and 90%.

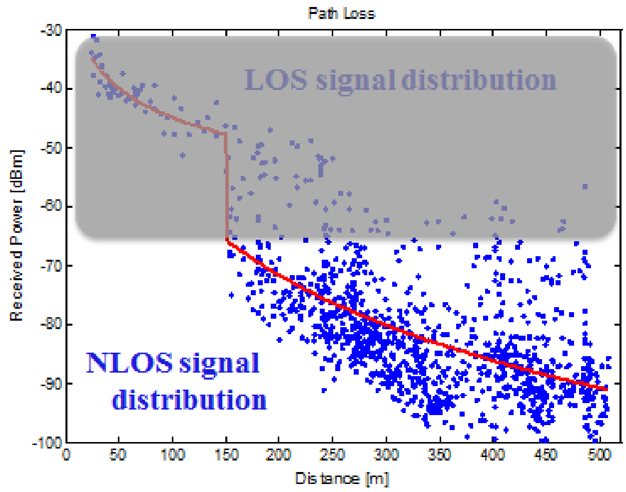


Fig. 18. NLOS Signal Distribution for Spatial Ratio

$$L_{LOS} = 20.55 + 5.109\log_{10}(f) - 47.93\log_{10}\left(\frac{d}{d_{ref}}\right) \quad (4)$$

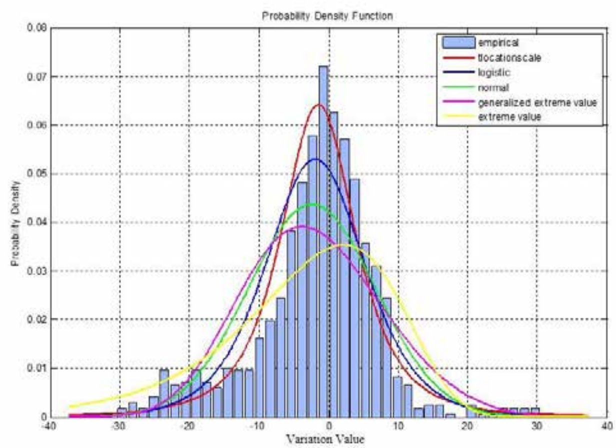


Fig. 19. Deduction for NLOS Signal Probability Distribution

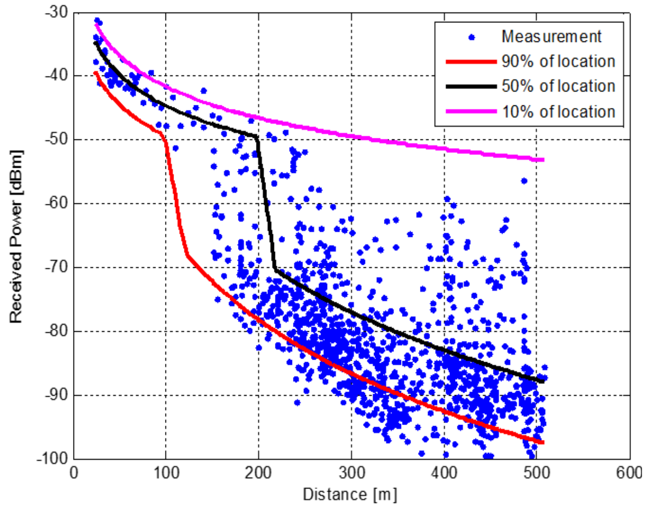


Fig. 20. Path Loss Results according to the Spatial Ratio

V. Conclusions

In this paper, we describe the results of measurement analysis in our radio measurement system and 3.5GHz band small cell environment. We measured the actual environment through the system we developed and derived a path loss model based on time and space ratio. Due to the short measurement period, the reliability of the analysis of measurement results may be somewhat insufficient. However, the tendency of analyzing the whole measurement result is well confirmed. In the future, we will try to get more accurate results by drawing sufficient measurement results.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.2017-0-00066, Development of time-space based spectrum engineering technologies for the preemptive using of frequency)

References

[1] Sun Kun, Wang Ping and Li Yingze, "Path loss models for suburban scenario at 2.3GHz, 2.6GHz and 3.5GHz," *Antennas, Propagation and EM Theory, 2008. ISAPE 2008. 8th International Symposium on, Kunming, 2008*, pp. 438-441.

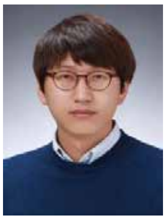
[2] M. Rizwan and S. A. Abbas, "Median path loss, fading and coverage comparison at 3.5GHz and 700MHz for mobile WiMax," *Multitopic Conference, 2008. INMIC 2008. IEEE International, Karachi, 2008*, pp. 266-271.

[3] Shanjian Liu, Yan Zhang, Yanhua Rui, Chunhui Zhou, Shidong Zhou and Tingchang Wang, "5.8GHz broadband channel characteristic analysis using measurement data," *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on, hangzhou, China, 2006*, pp. 1-4.

[4] http://www.dcenr.gov.ie/communications/en-ie/spectrum/Pages/Agenda-Item-1.1-results.aspx

[5] https://www.qualcomm.com/media/documents/files/lte-tdd-the-globalsolution-for-unpaired-spectrum.pdf

[6] http://www.fiercewireless.com/tech/story/verizon-qualcomm-andericsson-partner-field-trials-35-ghz-spectrum-sharing/2014-07-13



Jinhyung Oh received his B.S degree in Electrical Communications Engineering from Korea Advanced Institute Science and Technology (KAIST), Daejeon, in 2008 and M.S. degree in Electrical and Electronic Engineering from Korea Advanced Institute Science and Technology (KAIST), Daejeon, in 2010. In 2010, he joined the Electronic and Telecommunications Research Institute (ETRI) where he is a researcher of the Radio Technology Department. His research interests include wireless communications, interference analysis and digital beamforming.

Young-Jun Chung received the B.S. degree from the Jeju University, Jeju Island, Korea, in 1992, and the M.S. degree in electronics engineering from Sogang University, Seoul, Korea in 1994, and Ph.D degree in Electronic Engineering from Chungnam National University, Daejeon, Korea in 2005.
Since 1994, he has been with ETRI, Daejeon, Korea, where he is a leader of spectrum engineering research and section principle member of the research staff of the Radio Technology Department. His research interests include RF circuit, RF systems, and spectrum engineering.

A Process-Aware Drone-Equipped 3D Engine and Wireless Control Measurement Platform for Integrated Management of SOC Facilities

Young-Geol Lee*, Younlae Lee**, Yeonyi Jang***, Minjae Park*

**Department of Computer Software, Daelim University, South Korea*

***R&D Center, KGI, LTD., South Korea*

****Department of Applied Information Technology and Security, Ansan University, South Korea*

yglee@daelim.ac.kr, candy143@daum.net, isnowi@ansan.ac.kr, mjpark@daelim.ac.kr

***Abstract*— Disasters such as earthquakes, floods, landslides, and bridge collapses are socially costly. We intend to integrate facilities management to effectively manage the incidents of these disasters effectively. In order to utilize and automate various IoT technologies at this time, we propose a process-aware drone-equipped 3D engine and wireless control measurement platform for integrated management of SOC facilities.**

***Keyword*— Process-Aware System, SOC, IoT, Sensor, Drone, 3D Engine**

I. INTRODUCTION

In recent years, large-scale earthquakes have been increasing in Korea, and they can cause huge loss of life and economic loss in a wide area when an earthquake occurs, and can cause national disaster such as paralysis of the national neural network. Due to the large scale of disasters, new and complex disasters, the overall disaster risk of society has increased, and the scale of damage has also become larger, and the public's interest in disaster and safety has become very high. The Republic of Korea has established and implemented a 'Comprehensive Plan for Disaster and Safety Technology Development' in order to promptly respond to and recover from disasters and other accidents such as national protection, disaster, accident prevention, and damage, data, etc., there is not enough integrated management system for systematic management and utilization. In addition, it is required to develop interworking technology that collects and analyzes various types of regular and non - disaster data in order to collect the increasing disaster response strategies and to solve the problems. In order to manage various SOC facilities, it is necessary to provide detailed infrastructure information at the member level as well as simple facilities information, which can be solved through the combined virtual space information technology combining 3D model shape information and sensor information. In order to maintain the accurate and efficient facility maintenance, it is necessary to automatically construct a 3-D facility model by using the drone so that it can manage the three-dimensional position in the facility in connection with the field measurement equipment.

Fig. 1 Various Types of Disaster Situations

We propose a smart maintenance management integrated platform for process-aware 3D facility management that can be automated by combining IoT technology with surveillance system (image information, measurement equipment, etc.) for disaster preparedness.

Manuscript received on August 1, 2017. This research was supported by a grant(code17CTAP-C129818-01) from Technology Advancement Research Program (TARP) funded by Ministry of Land, Infrastructure and Transport of Korean government.

Youn-Geol Lee is with Department of Computer Software, Daelim University, 29, Imgok-Ro, Dongan-Gu, Anyang-Si, Gyeonggi-Do, 13916, South Korea (first author, phone: +82-31-442-4423, fax: +82-31-442-4428, e-mail: yglee@daelim.ac.kr)

Yoonlae Lee is with R&D Center, KGI CO. LTD., 129, Gaetbeol-ro, Yeonsu-gu, Incheon-Si, Gyeonggi-Do, 21999, South Korea (co-author, e-mail:candy143@daum.net)

Yeonyi Jang is with department of Applied Information Technology and Security, Ansan University, 155, Ansandaehak-ro, Sangnok-gu, Ansan-si, Gyeonggi-do, 15328, South Korea (co-author, isnowi@ansan.ac.kr)

Minjae Park is with department of Computer Software, Daelim University, 29, Imgok-Ro, Dongan-Gu, Anyang-Si, Gyeonggi-Do, 13916, South Korea (corresponding author, phone: +82-31-442-4434, fax: +82-31-442-4428, e-mail: mjpark@daelim.ac.kr)

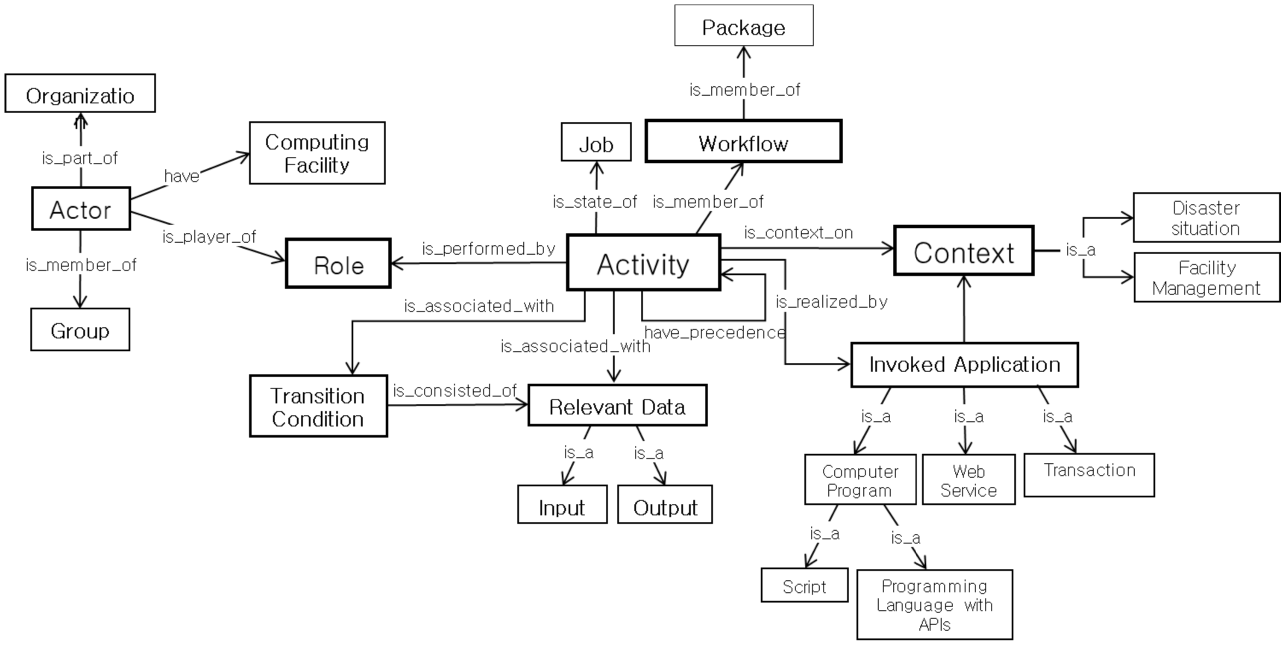


Fig. 2 Process Meta-Model for Proposed Platform

II. RELATED WORKS

Our research is based on researches related to drone, wireless and process management technologies. Recently, interest in drones and IoT is very high, and there are many related studies. In particular, [1, 2, 3] are drone studies related to the disaster directly related to this study. [1] is a study that responds to disaster situations. [2] is a study that is for drone applications for supporting disaster management. [3] is a study that is for data management of drone-based 3D model reconstruction of disaster site. We focus on drone-equipped 3D engine for drones, and there are differences from other studies. And, some studies[4, 5, 6] have attempted to extend the application of the workflow model. [4] is a workflow model for data-intensive workflow processing. [5] is a workflow model for IoT processing. [6, 7] are a fairly classic studies with color and fragment concept workflow models that can add new information to workflow models. Based on these various previous studies[4, 5, 6, 7], we will describe an extended workflow model tailored to the disaster situation. In the area of facility management, interest in facility management is very high, and conceptual and experimental researches[8] on the remote facility monitoring field have been continuously carried out. [9] was implemented in a segmented manner with respect to the history and current status of specific facility facilities. Especially, the real-time monitoring part is not able to realize the complete system due to the communication cost problem and performance limit. Facility monitoring[10] that needs to take precautionary measures is difficult to utilize positively by checking the status of fragmentary situation and there is no possibility of data sharing and it is very likely to be expanded to complex accidents and disasters. Therefore, we will try to overcome these problems.

III. A PROCESS-AWARE DRONE-EQUIPPED 3D ENGINE AND WIRELESS CONTROL MEASUREMENT PLATFORM

We propose a process-aware drone-equipped 3D engine and wireless control measurement platform. Its core is process-aware platform, drone-equipped 3D engine, and wireless control measurement platform, each of which can be described as follows.

A. *Process-Aware Platform*

We propose a platform that introduces process management technology. The platform supports drone-equipped 3D-engine and wireless control measurements. The platform has expanded its process management technology to support those functions. The most important feature of this process management technology consists of modeling technology and execution technology. Because this platform needs the model specific to IoT environment, we want to extend existing workflow model. We will extend ICN[11, 12, 13] among well-known workflow representation methods. In addition, we extend BPMN 2.0[14, 15, 16, 17] standard method for actual system execution.

Process-aware platform technologies
- model: modeling methodologies (ICN, BPMN 2.0)
- process management: process/workflow engines

Fig 2 represents an extended ICN(Information Control Nets) meta-model for disaster management automation. It can be defined by adding new elements for disaster management and facility management automation to original elements. We add context information for disaster situations and situation handling for facility management to appropriately handle invoked applications for execution in the components and components of the main workflow process. And BPMN 2.0, the standard modeling method, can also be extended. BPMN classifies and divides tasks by type to perform unit activities. We can implement this task by adding a task for the proposed situation to this generalized type.

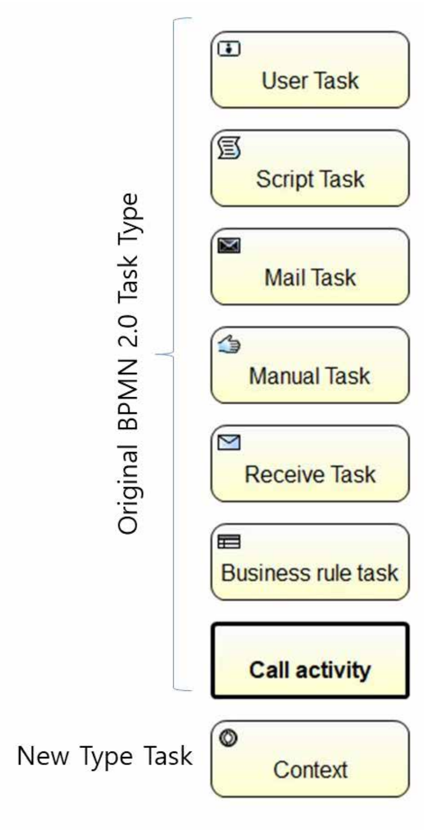


Fig. 3 Extended BPMN Task Types

In order to design processes for proposed platform, we can use a new type task or activity. The defined process is transformed to an executable language in the form of xml for automated execution. An example of a BPMN process and its conversion to an executable language is described in Fig 4.

The defined process model can be executed by the process management system. A process-aware platform is basically split into two phases for its definition and execution. The first is the process model described earlier, and the second is the management of the defined process model. The process of creating a model can be divided into build-time, and the process of managing is run-time. The two-step process is described in Fig. 5. The process in build-time means defining the process, and the process in run-time means that the defined process is executed and monitored.

B. Drone-Equipped 3D Engine

Drone-Equipped 3D Engine is a mobile mapping platform which multiple sensors and measurement systems have been integrated to provide three-dimensional near-continuous positioning of the platform's path inspace and simultaneously collected geo-spatial data.

Current drone application techniques are used for a brief topographic survey. In the future, 3D image acquisition technology for management facilities based on drone is a necessary element technology in next generation spatial data scanning field, and it is highly possible to utilize it in various creative ways.

In the case of linear facilities (levees) or large facilities (roads, bridges), it is not possible to perform accurate management using only the GPS location information of facilities. In case of embankment, the distance between starting point and ending point is long and it is not a straight line. Therefore, the 3D engine technology using the drone is essential for accurate maintenance and diagnosis as well as the location of the facilities in the facilities. In the present study, the application part of the drones was developed not only to manage the points of the facility but also to manage the three-dimensional position of the facilities such as the line and the area,

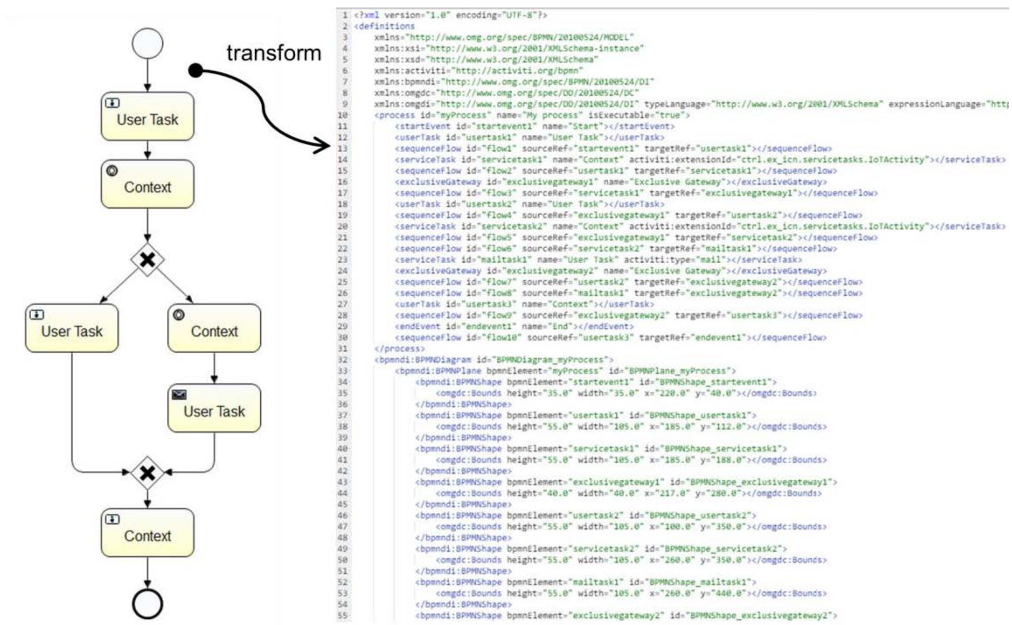


Fig. 4 A BPMN Model Example with Context Type Task and Its Executable Language

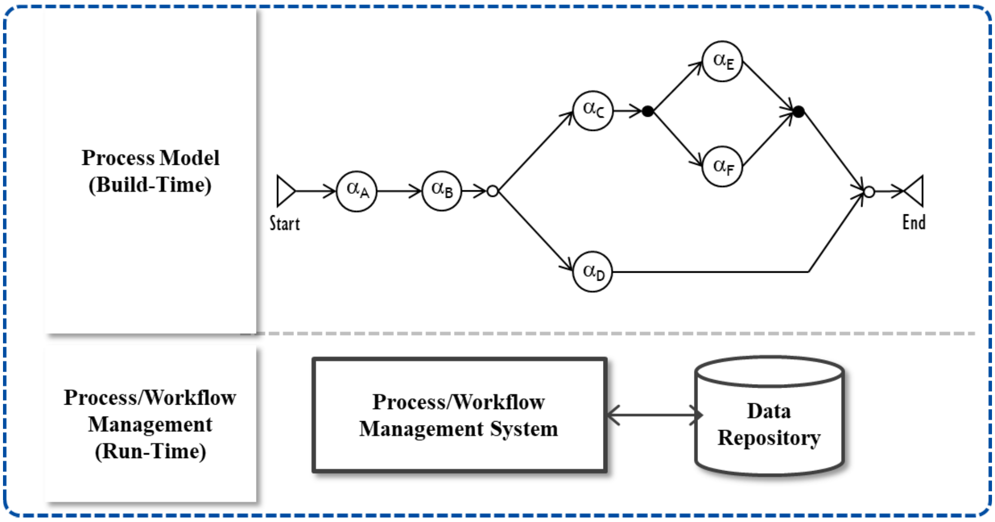


Fig. 5 A Process-Aware Platform Concept

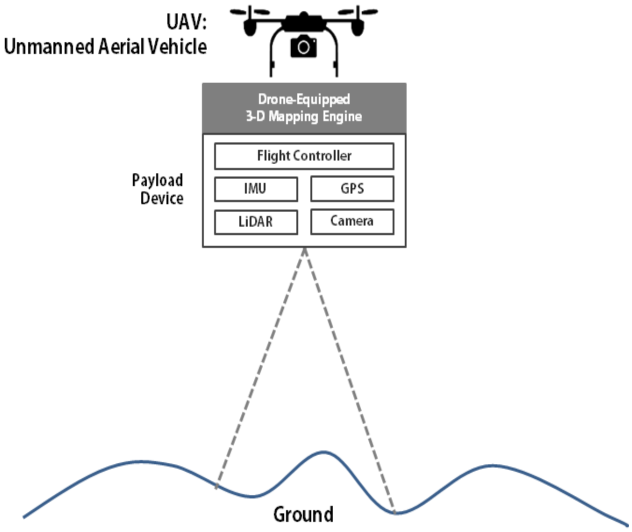


Fig. 6 Drone-Equipped 3D Engine

C. *Wireless Control Measurement*

Drone-Equipped Wireless Control Measurement is a software system with data-centric language for sensing, capturing and detecting of remote point of interest or sensor device using unmanned aerial vehicle's autonomous and programmable functions.

Data dissemination system that can share the data needed for social safety in real time in relation to the status and status of SOC facilities is also helpful for national safety management. In addition, new applications can be created in conjunction with climate, social phenomena, and traffic. In order to easily and flexibly apply the network structure for real-time control and measurement in various fields, a standard interface is devised so that various facility management subjects can utilize it, and various information can be extracted from a single view through sharing. This technology is interworking with the wireless control metering sensor based on the information from the drones based 3D engine which can manage the position of the sensor information. It is the basic technology for establishing smart integrated maintenance system of SOC facilities. With this

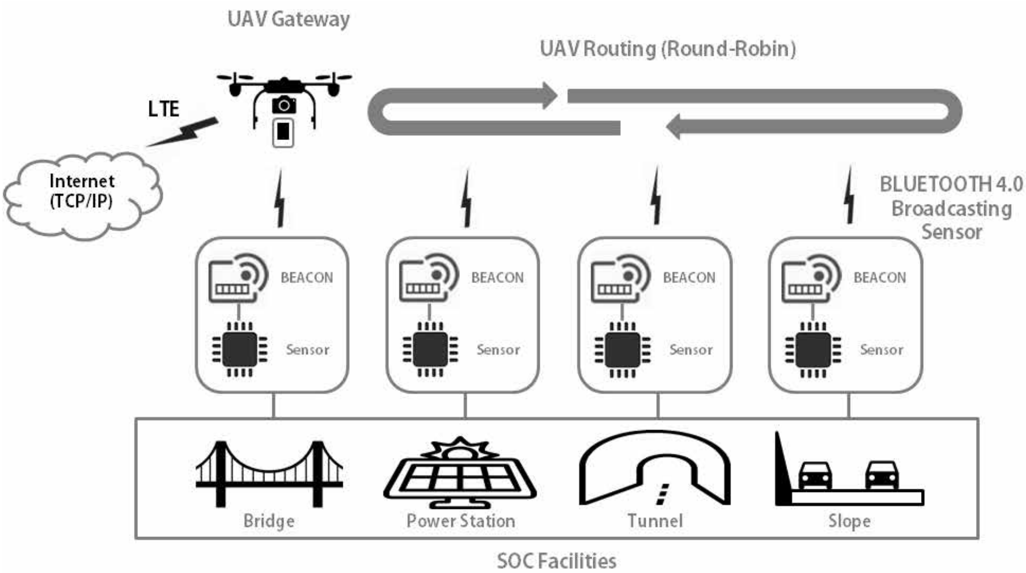


Fig. 7 Wireless Control Measurement

technology, it is possible to make an accurate and quick judgment on a disaster site, and minimize disaster damage.

D. A process-aware drone-equipped 3D engine and wireless control measurement platform

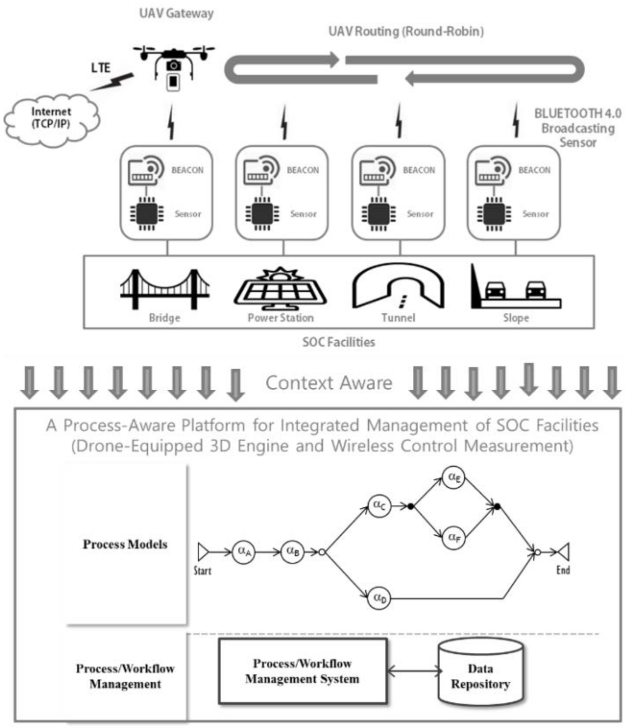


Fig. 8 A Process-Aware Drone-Equipped 3D Engine and Wireless Control Measurement Platform

By changing the recovery-oriented disaster management system into a preventative management system, and by providing a risk definition tool that can author a risk prediction model, especially in the private and public sectors, various facility managers can predict disasters and risks in advance. It can also be automated and processed using process management techniques.

Based on the technology described above, this technology can automate the judgment of a disaster site. Of course, the disposal of the facility management section for the disaster site is divided into unit tasks, and the definition and management can be made flexible because it can be partially or totally automated. Since the contents of the unit work are extended by using the process model defined above, information about the situation is considered now. However, as technology develops in the future, it is possible to have information processing using technologies such as a new artificial intelligence.

IV. Conclusions

In this paper, we propose a process-aware platform that supports drone-equipped 3D engine and wireless control measurement. We have described a drone-equipped 3D engine and wireless control measurement capabilities and process management functions to automate it partially or fully. Although it is approach from a conceptual point of view, it seems to be meaningful in that it provides the basis of possibility of automated drone-equipped 3D engine and wireless control measurement technologies.

In the future, we will specifically study in detail the core function of the drone-equipped 3d engine, and we need the research on the processing technology for the wireless control measurement. And we will try to automate it using process management technology. It will be scenarioized, one case study will be created, and the completed platform will be applied to the disaster scene.

We strongly believe that this platform will handle the disaster scene quickly and efficiently.

Acknowledgment

This research was supported by a grant(code17CTAP-C129818-01) from Technology Advancement Research Program (TARP) funded by Ministry of Land, Infrastructure and Transport of Korean government.

References

[1] DANIEL, Kai, et al. AirShield: A system-of-systems MUAV remote sensing architecture for disaster response. *In: Systems conference, 2009 3rd Annual IEEE. IEEE,* 2009. p. 196-200.

[2] RESTAS, Agoston. Drone applications for supporting disaster management. *World Journal of Engineering and Technology*, 2015, 3.03: 316.

[3] KIMA, C.; MOON, H.; LEEA, W. Data Management Framework of Drone-Based 3d Model Reconstruction of Disaster Site. *ISPRS-International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 2016, 31-33.

[4] Park, Minjae, et al. "A scientific workflow model designer based on scientific information control nets." *Advanced Communication Technology (ICACT), 2015 17th International Conference on. IEEE*, 2015.

[5] Kim, Meesun, et al. "Modeling process-aware Internet of Things services over an ARDUINO community computing environment." *Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE*, 2017.

[6] JEONG, Woo-Jin; KIM, Kwang-Hoon. A Colored Workflow Model for Business Process Analysis. *Journal of Internet Computing and Services*, 2009, 10.3: 113-129.

[7] KIM, Hyung-Mok; KIM, Kwang-Hoon. A Cooperative Workflow Modeling Methodology Using Fragment-ICNs. *Journal of Internet Computing and Services*, 2005, 6.6: 107-115.

[8] Ok Hyun and Kim Seong-Jin, "Application Method of Remote Site Monitoring in Public Road Construction Projects," *Journal of the Korea Academia-Industrial cooperation Society*, Vol. 14, No. 12 pp. 6550-6557, 2013

[9] Kyoon-Tai Kim, "Development of a Mountainous Area Monitoring System based on IoT Technology," *Journal of the Korea Academia-Industrial cooperation Society*, Vol. 18, No. 3 pp. 437-446, 2017

[10] Dong-wook Lee, Hyun-byung Chae, Soo-kwon Chae, "A Study on the Development of Remote Sensing System for Rectangular Sewer Duct to Prevent and Respond to Disasters," *J. of Korean Society of Environmental Technology*, Vol. 18, No. 2, April 2017, pp. 103-114

[11] ELLIS, Clarence; MALTZAHN, Carlos. The Chautauqua workflow system. In: System Sciences, 1997, *Proceedings of the Thirtieth Hawaii International Conference on. IEEE*, 1997. p. 427-436.

[12] KIM, Kwanghoon; ELLIS, Clarence A. ICN-based Workflow Model and its Advances. *Handbook of Research on Business Process Modeling*, 2009, 34-54.

[13] ELLIS, Clarence A.; NUTT, Gary J. Modeling and enactment of workflow systems. *In: International Conference on Application and Theory of Petri Nets*. Springer, Berlin, Heidelberg, 1993. p. 1-16.

[14] SILVER, Bruce; RICHARD, Bruce. BPMN method and style. *Aptos: Cody-Cassidy Press*, 2009.

[15] WHITE, Stephen A. Introduction to BPMN. *IBM Cooperation*, 2004, 2.0: 0.

[16] WHITE, Stephen A. BPMN modeling and reference guide: understanding and using BPMN. *Future Strategies Inc.*, 2008.

[17] RODRÍGUEZ, Alfonso; FERNÁNDEZ-MEDINA, Eduardo; PIATTINI, Mario. A BPMN extension for the modeling of security requirements in business processes. *IEICE transactions on information and systems*, 2007, 90.4: 745-752.

Young-Geol Lee is a full professor of computer software at Daelim University, South Korea. He received B.S., M.S., and Ph.D. degrees in computer science from Inha University in 1993, 1995, and 1999, respectively. His research interests include Database, Spatial Database, Geographic Information System, Spatial Warehousing, Data-centric Constraint Language and Process-aware facility management systems.

Younlae Lee is the director of KGI Corp., the South Korea Software Development Co. He received B.S. degrees in physics from Inha University and M.S. degrees in civil engineering from Kangwon University. He developed BlastAZ, the blasting simulation program. And his Research interests include 3D modeling and Imaging processing, Simulation systems, IOT(Internet of Things) and location-based infrastructure maintenance systems.

Yeonyi Jang is an assistant professor of Applied Information Technology and Security at Ansan University, South Korea. She received Ph.D. degrees in Advanced Imaging Science Multimedia, and Film from Chung-ang University in 2011. Her research interests digital image processing, 3D-Modeling and Information Security.

Minjae Park is an assistant professor of computer software at Daelim University, South Korea. He received B.S., M.S., and Ph.D. degrees in computer science from Kyonggi University in 2004, 2006, and 2009, respectively. His research interests include groupware, workflow systems, BPM, CSCW, collaboration theory, process warehousing and mining, workflow-supported social networks discovery and analysis, process-aware information systems, data intensive workflows, and process-driven Internet of Things and process-aware factory automation systems.

Metric of Vulnerability at the Base of the Life Cycle of Software Representations

Mikhail Buinevich*, Konstantin Izrailov*, Andrei Vladyko*

*The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint Petersburg, Russia

bmv1958@yandex.ru, konstantin.izrailov@mail.ru, vladyko@sut.ru

***Abstract*— This article investigates the problem of the origin of software vulnerabilities in terms of their life cycle. For this purpose, the process of creating a software by a person is examined in detail and partially formalized with in philosophical categories – «Form vs Essence». There is proposed main representations of life cycle and intermediate stages of the transformation between it. As an example there's hypothetical comparison of two software transformations with a graphical interpretation of the security level of each of final representations. This article is a author's works continuation on the fundamental research of the security problems of the software domain.**

***Keyword*— information safety, machine code, software representation, vulnerability, methodology, metric, life cycle**

I. Introduction

Current problem of information security is existence of vulnerabilities in the software (further – SW). It is necessary for effective counteraction to vulnerabilities all-round studies of properties of this object, thus not only static, but also dynamic. Last define lifetime of vulnerabilities according to a scale of process of creation of a SW. So, the analysis of points of appearance of vulnerabilities will allow to evaluate the current security level of a product and to make its forecast for different variations of development process. The analysis of points on a scale where vulnerabilities can be guaranteed found, will allow to construct the systems of their neutralization more effectively.

As process of creation SW is interactive and step-by-step, and points of emergence of vulnerabilities have to correspond to steps of interaction of the person with him – at the same time vulnerabilities can possess various degree of premeditation from the person. It will allow to create typification of vulnerabilities on points of their emergence and prerequisites to it.

Processing of a program code automatic means can be considered an analog of interaction of the person with a code as the rules put in them are also created by the person – for disposal of monotonous work. The set of steps of interaction in this case will be similar.

II. Areas of Life of Vulnerabilities in Submissions of the Software

The research of dynamic properties of vulnerabilities begun in author's article [1] is under construction on states SW in certain points of life cycle. Such states can be described by means of the philosophical categories reflecting interrelation of two parties of everyone representations of a program code (further – Representation): his form (external manifestation – the flowchart [2], a programming language, etc.) and essence (inner meaning – logic of use of elements of schemes, operators of language, etc.). In fact, the form is only one of possible reflections of essence within the current environment (in particular it is various for the person – the text and images, and machine – a binary code). Justification of the chosen division into states it is possible to find possible use at construction SW appropriate design means: experts of a certain profession and the standard automating programs (further – Utilities). Each of means according to own mission carries out transformation of Representation from previous to the subsequent (and with application a reverse engineering and in the opposite direction [3, 4, 5, 6], for example, for the benefit of search of vulnerabilities). Offered in above to the mentioned author's article of Representation, describing the creations SW typical process for telecommunication devices, and involved for this means, are given in Table 1.

TABLE 1.
Representations Software and Design Means for Their Transformations

Order №	Initial representations	Project tool for transformation Name	Type
	---	Creator	Specialist
1	Main idea	Concept developer	Specialist
2	Concept model	Design architect	Specialist
3	Architecture	Algorithmist	Specialist
4	Code algorithms	Coder	Specialist
5	Source code	Compiler	Utility
6	Assembler code	Assembler	Utility
7	Machine code	Linker	Utility
8	Image file	---	---

Note. The first Representation arises only owing to activity of the creator, and the last finishes process of creation SW.

It should be noted that a profession the algorithmist and the coder extremely seldom meets in modern practice, though it

Manuscript received data is October 13, 2017. This work is a follow-up of the invited journal to the accepted conference paper of the 18th International Conference on Advanced Communication Technology.

M. V. Buinevich is with The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, Saint-Petersburg, 22-1 Prospekt Bolshevikov (e-mail: bmv1958@yandex.ru).

K. E. Izrailov is with The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, Saint-Petersburg, 22-1 Prospekt Bolshevikov (corresponding author to provide phone: +7(921)555-2389; fax: none; e-mail: konstantin.izrailov@mail.ru).

A. G. Vladyko is with The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, Saint-Petersburg, 22-1 Prospekt Bolshevikov (e-mail: vladyko@sut.ru).

was demanded at initial stages of development of the region of programming. In current state of IT area they are united by a profession the programmer, leading to the fact that experts of the last are forced to be engaged in transformation of two Representations with various appointment at once (see No. 3 and No. 4 in Table 1). Authors consider that such situation is caused by purely economic reasons and hypothetically is the indirect source of vulnerabilities influencing quality (in sense of safety) the final product.

Considered in [1] states point to significant jumps between forms and essence SW, lowering details of transformations between the next Representations. And as states in itself are completely static – any changes without participation of design means (from Table 1) are impossible – that cognitive stages of transformations between Representations are of special interest as in them new vulnerabilities ([7, 8]) can appear.

III. Representation transformation stages

According to the interpretations of form and essence entered above, reflection of any Representation in the objective (physical) world can be created by means of only his form which is obviously consisting of the system of others, smaller – elementary forms. In the subjective (mental) world, Representation has an appearance of the complete essence consisting also of the system of elementary essence. And as the structure and properties of forms of various Representations are, as a rule, essentially various and don't give in to external regularity, it is possible to make transformation only consciously and only through their essence storing all communications lacking for this purpose. A rare exception are transformations between extremely similar Representations by means of trivial rules (for example, the translation of a binary code from hexadecimal Intel HEX in binary record). We will repeatedly note that in case of use of Utilities the situation essentially doesn't change as though the last and make a transfer automatically, however generally these means will transform an entrance form to own internal representation – i.e. work with essence, and then generate the last according to an output form.

We will consider abstractly separate taken transformation of Representation of i to the subsequent Representation of $i+1$ (further – Representation of j) which is carried out by a certain project tool. The essence of work of any such tools comes down to three fundamental phases: analysis of Representation of i, its processing and synthesis of Representation of j.

As an example we will use conversion of algorithms of a program code (Representation of i) to the source code (Representation of j) the coder (the expert – project means for creation of the code implementing the given algorithm). So, the coder studies the given algorithm (for example, it has flowchart appearance), realizes its sense, selects a suitable programming language (if it is not set in advance) and implements on it a necessary functionality. Obviously, the coder shall the be sign, both with the form of the flowchart of an algorithm, and with a paradigm of a programming language and its syntax; also his abilities and experience shall allow to work with the corresponding essence of Representations.

A. Phase 1. Analysis

The phase of the analysis of Representation by the person consisting in his understanding is rather difficult and debatable; nevertheless, the existing researches (in particular, in the field of Text Comprehension [9]), allow to allocate the following stages of this process.

Stage 1. Perception

At this stage of people makes initial recognition of a form of Representation of i by means of sense organs (as a rule, sight). As it isn't possible to person to capture all form of Representation entirely (as though the flowchart consisted of the only graphic element), his breakdown on elementary forms is made. At the same time the elementary sense (or in terms of the entered categorial couple – essence) compared to each such elementary form remains not certain so far. Representation of i from area of the physical world passes into own world of the subject studying him. So, the coder, studying the flowchart, obtains initial visual information on her elements and their communications.

Stage 2. Understanding

At this stage of person compares the received elementary forms to certain elementary essence according to own thesaurus (the system of comparisons of terms and their concepts). Representation of i acquires a certain semantic essence, though rather separate. So, the coder begins to perceive elements of flowcharts with a condition (a symbol – the Decision) as conditional transitions to elements with data processing (a symbol – Process).

Stage 3. Interpretation

At this stage person synthesizes the uniform essence of Representation of i which is the coordinated whole in a brain, using the elementary essence understood by him. At the same time, as a rule, the total sense of Representation is much more difficult, than summation of separate semantic elements from the previous stage – classical synergetic effect. Judgment of Representation by semantic interpretation of the understood forms is in this way made. This way a coder understands the general sense of work of an algorithm.

B. Phase 2. Processing

As Representations of i and j are based on own unique elements of essence (corresponding to the missions), between the last the corresponding converting is necessary. The phase of processing of representation in working memory of the person [10] consisting of the only stage is for this purpose intended.

Stage 4. Re-comprehension

The stage can be considered the most difficult and the least studied – at it the sense SW constructed on elements of essence of Representation of i in identical sense on elements of essence of Representation of j will be transformed. The stage is similar to modeling process where the essence of Representation of i has an appearance of a certain internal model in a brain of the person which then is investigated for the purpose of receiving (or transformations in her) the new model corresponding to the essence of Representation of j. So, the coder, using own cognitive skills, not just finds unambiguous compliance of steps of an algorithm to programming language designs, namely will transform them in more difficult way. At the same time the rule «one in one» doesn't work as the flowchart of an algorithm already is 2D (the unidirectional count with cycles), and a program code – 1D (a set of lines with own structure). The situation many times becomes complicated if the algorithm corresponds to one paradigm of programming (for example, imperative), and the required programming language – another (for example, functional).

C. Phase 3. Synthesis

The synthesis phase following a reconsideration phase has to construct his form on the essence of Representation of *j* – to transfer Representation from the subjective world of the person to objective surrounding. Thus, the phase reasonably can consist of the stages belonging to an analysis phase, but which are carried out upside-down. There are even utilities with the close purposes and the principles of work (for example, SWIM [11]).

Stage 5. Shaping

At this stage person breaks the uniform essence of Representation on elementary, ready for reflection in the physical world. There is a certain structure of maintenance of Representation of *j* though without any specification concerning her form. So, the coder from conscious sense of work of an algorithm (step-by-step) receives the scheme of performance according to a programming paradigm (in this case, imperative).

Stage 6. Exposition

At this stage person compares to each elementary essence the same elementary form. The return thesaurus (the system of comparisons of concepts and their terms) is for this purpose used. Programming language forms are compared to semantic elements of Representation of *j*. So, the coder presents the scheme of performance in the form of set of designs of language.

Stage 7. Decoration

At this stage person makes concrete entry of Representation of *j* strictly in the required look – graphic, text, binary and so forth. Representation has a uniform consistent form. So, the coder makes the end result of the activity – writes down a program code of an algorithm.

Stages can be considered intuitive and logical on a set of examples. The structure of phases and stages and also graphic interpretation of their work in categories of a form/ essence is given in the Fig. 1. Zone 1, 2 and 3 correspond to conditional degree of sensibleness of essence by the person for each of Phase and Stage of transformation of Representations.

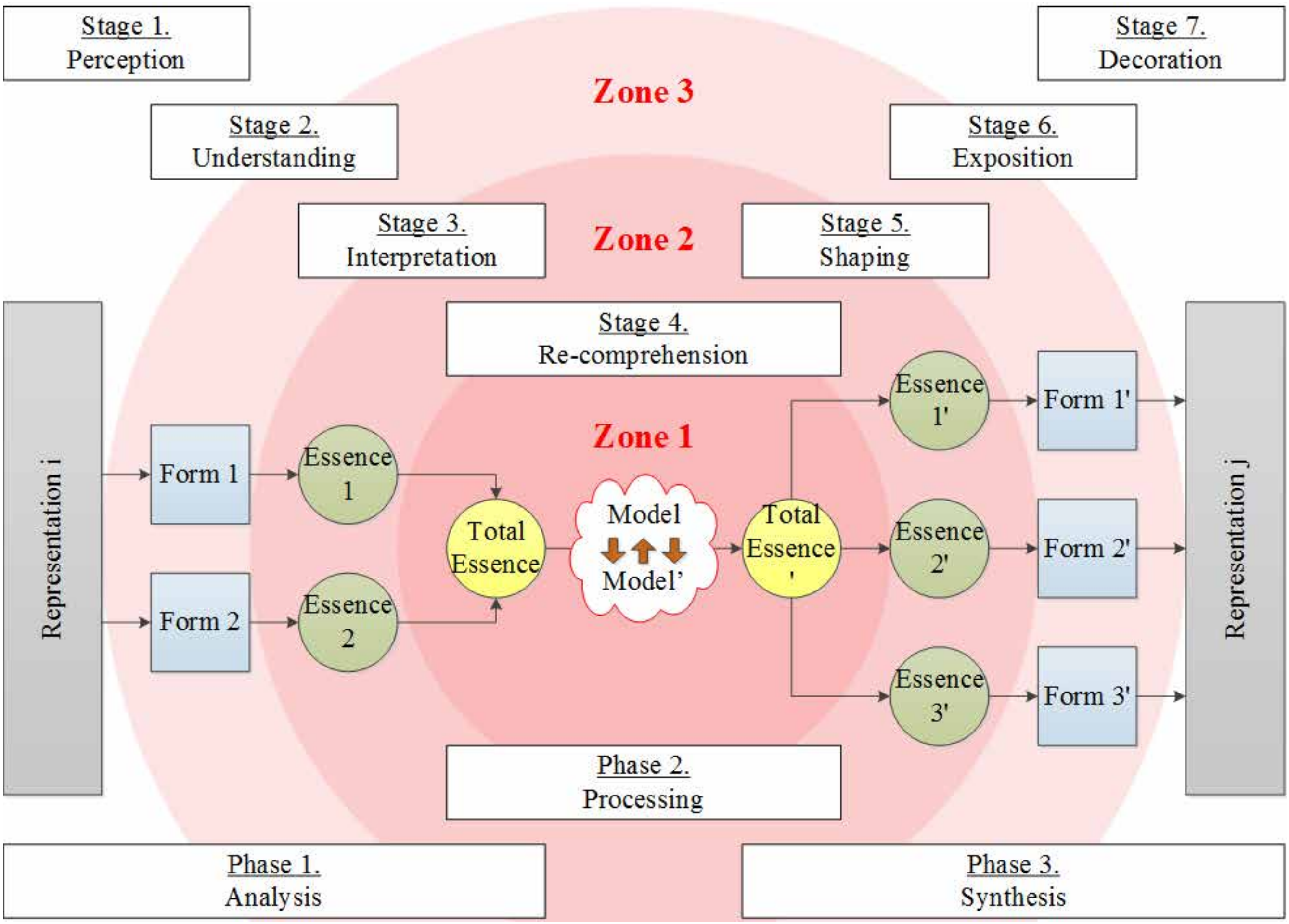
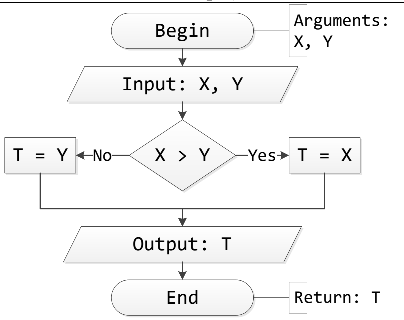


Fig. 1. Scheme of transformation of Representation and its graphic interpretation

Explanations to the diagram in the Fig. 1 for the example consisting in creation of the source code of function of a choice maximum of two numbers according to the given flowchart of an algorithm are provided in Table 2.

TABLE 2.
EXPLANATIONS TO THE SCHEME OF TRANSFORMATION OF REPRESENTATION AND EXAMPLE OF CODING

№	Result of transformation	Elements of the scheme of transformation (for example)
	Submission of the flowchart of an algorithm (Representation *i*)	
1	Visual elements of the flowchart of an algorithm (Form 1, 2)	«Begin» with receiving two variables: X and Y; «Decision» on transition (conditional branch) with a condition of comparing of two variables «X > Y»; two «Processes», each of which appropriates to temporary variable T one of two X and U variables; «End» with return of a variable T; unidirectional connectors of all elements;
2	Sense of elements of the flowchart of an algorithm (Essence 1, 2)	Obtaining value of the X and Y variables; comparing of the X and Y variables; if X > Y, then assignment of a variable T of variable X value , else – value variable Y; resetting of variable T value;
3	Sense of all algorithm (Total Essence)	Comparing of values of the X and Y variables and resetting maximum of them through variable T value;
4	Sense of the source code implementing the algorithm (Total Essence') received by the intermediate models (Model, Model')	Determination of function with arguments X and Y returning the value, maximum from them; use for storage of result of temporary variable T;
5	Sense of elements of the source code (Essence 1', 2', 3')	Targeting a signature of function with arguments of X and Y; comparing values of the X and Y variables of construction IF-ELSE; depending on result of comparing locating in temporary variable T of one of values of the X and Y variables; resetting from function variable value T;
6	Constructions of the source code according to a language syntax (Form 1', 2', 3')	Function title with two arguments X and Y; beginning and end of a function body; declaration of temporary variable T; conditional GOTO statement for «X > Y»; branches of the conditional branch on the separate units of a code containing assignment of a variable T of the X or Y variables; return statement from function of a variable T;

7	Representation listing of the source code (Representation *j*)	`int funct(int x, int y) {`
		`    int t;`
		`    if (x>y) {`
		`        t = x;`
		`    } else {`
		`        t = y;`
		`    }`
		`    return t;`
		`}`

<u>Note.</u> First column «№» means order number of Stage.

IV. TYPIFICATION OF VULNERABILITIES WHEN TRANSFORMING REPRESENTATION

As it was specified, vulnerabilities can appear in the course of change of Representations (incremental and step by step), it is expedient to enter their typification in the place in which they appeared – i.e. to the stage initiating vulnerability. So, the erratic understanding the coder on Stage will lead 2 senses of an element of the conditional branching (for example, the incorrect sign of comparing) to incorrect interpretation of a sense of all algorithm and, as a result, to writing of the incorrect source code (for example, returning the minimum number instead of maximum) even if all remained stages were executed absolutely truly.

The premeditation level corresponding to a conscious participle of the person to vulnerability appearance can be additional typification reasonably. The following can be such types of premeditation for the given stages:

- unwitting – shown in the mistakes made by the person not consciously i.e. owing to its physical or psychological state, or because of external factors;
- malicious – based on conscious entering of mistakes into Representations, for example, owing to personal ambitions, the order or the compelled reactions.

It is obvious that if the casual nature of vulnerabilities is inherent with different degree in all stages of transformation of Representations, then malicious can belong only to a stage of reconsideration and the next to him. It follows from the fact that around a stage there is sufficient degree of sensibleness of essence by the malefactor (corresponding to zones in the Fig. 1); at all other stages person just tries to understand sense of Representation through perception, and then to describe it.

V. ASSESSMENT OF SAFETY OF TRANSFORMATION OF REPRESENTATION

We will consider process of receiving each new Representation of safety change, previous from a position. We will enter the level of safety of Representation of i as density of his essence without vulnerabilities (or the relation of «volume» of essence without vulnerabilities to general «volume») and we will designate him the S_i parameter. It is obvious that for Representation without vulnerabilities of S_i=1. Safety of the following Representation *j* is defined by S_j; at the same time $S_j < S_i$ condition will be always met. Equality of $S_j = S_i$ is possible only at automatic transformation by the entrusted Utilities and won't be considered here. The situation when $S_j > S_i$ meaning that as a result of transformation, a part of vulnerabilities has disappeared and in general is extremely improbable (though some Utilities of assembly can signal about use of unsafe operations and offers options of their correction).

We will consider features of each of the specified SW development process stages and also types of vulnerabilities from the point of view of premeditation. For this purpose we will compare coefficient of increase in level of insecurity of Representation with each stage – $K_N^p(t)$, corresponding to probability of emergence of vulnerability like P (U – Unwitting, M – Malicious) at the Stage *N* (from 1 to 7) in timepoint of t (a point on a scale of performance of stages). The value of coefficient can lie in the range *[0..1]*. Then coefficients influence the level of safety of Representation as:

$$S_j = \prod_{N=1..7} \left(1 - K_N^P(t)\right) \times S_i.$$

Thus, each stage due to «nonzero» probability of emergence of vulnerabilities inevitably reduces safety of new Representation.

The coefficient $K_N^P(t)$ has dependence on timepoint because of stages aren't carried out instantly, and have a certain duration in process of which (from the beginning of a stage before its end) vulnerabilities can appear with various speed (the corresponding derivative from $K_N^P(t)$ in a certain timepoint of t_0). Such assumption is competent as at some stages of vulnerability practically don't appear (because of simple subconscious work of a human brain), on some have the increased intensity (because of need to the person to work with the large volume of memory), and on some have growth rate, time-dependent (because of complex processing by a brain both the initial, and constantly obtained new information). We will consider coefficient $K_N^P(t)$ for each of a stage and type of premeditation of vulnerability.

For definition of a temporary type of coefficient of increase in level of insecurity we will use the simplified reasoning – but, nevertheless, reasonable logic and experience as definition of an exact formula for $K_N^P(t)$ demands carrying out a full-fledged research on a set of statistics (and its processing) concerning places and types of emergence of vulnerabilities on each of stages of transformation of Representations. Also we will divide a type of conversion within each stage from the point of view of topology into 4 groups:

– «one to one» (further, «*1:1*») or the transformation of one element to other element;

– «one to several» (further, «*1:N*») or the transformation of a uniform element to a set of other elements;

– «several to one» (further, «*N:1*») or the transformation a set of one elements in a uniform element;

– «several to several» (further, «*N:N*») or the transformation a set of one elements to a set of other elements.

VI. Influence of subjective components of the person

The Stage 1 is defined by consecutive perception of elementary forms of Representation of *i* from a uniform form and is carried out by the person with good degree of automaticity, though in the form of «*1:N*». As essence by the person is still not understood, emergence only of casual vulnerabilities is possible. Thus, the stage can be characterized by the average value of coefficient having a linear appearance:

$$\begin{cases} K_1^U(t) = k_1^U \times t \\ K_1^M(t) \equiv 0 \end{cases}.$$

The Stage 2 is defined by consecutive understanding of elementary forms of Representation of *i* by their «replacement» by the corresponding elements of essence, i.e. in the form of «*1:1*». As the understanding of elementary essence doesn't give a full picture of sense an Idea, emergence only of casual vulnerabilities is possible. Thus, the stage can be characterized by low value of coefficient and have a linear appearance:

$$\begin{cases} K_2^U(t) = k_2^U \times t \\ K_2^M(t) \equiv 0 \end{cases}.$$

The Stage 3 is defined by consecutive interpretation of elementary essence of Representation of *i* in uniform essence which is carried out by the person with good degree of automaticity, though in the form of «*N:1*». As the person at the end of a stage already has an idea of full essence, besides casual vulnerabilities emergence of rare malicious vulnerabilities is possible. Thus, the stage can be characterized by average value of coefficient for casual and very low for malicious vulnerabilities and have a linear appearance:

$$\begin{cases} K_3^U(t) = k_3^U \times t \\ K_3^M(t) = k_3^M \times t \end{cases}.$$

The Stage 4 is defined by transformation of sense of Representation of *i* to sense of Representation of *j* (by their essence) which is made by the person most consciously. Transformation is similar to process of «the solution of a task» – poorly studied creative action. Nevertheless, the approximate type of coefficient of K_4^P can be received as a result of the following reasonings. Firstly, the stage isn't consecutive (on extremely measure, in the same degree as others) since there is no uniform algorithm of the decision any tasks – it is creative with emergence of Insight. Secondly, though transformation is also similar to a look «*1:1*», nevertheless, because of their dimensions of keeping of people is capable to work only with their parts that leads to a type of «*N:N*». And, thirdly, standard feature of work with non-standard tasks is existence of a step of assessment i.e. as far as the decision has come or has achieved the objectives. Thus, it is possible to assume that generally the stage will gradually transform one parts of essence of Representation *i* to other parts of essence of Representation *j*, checking at the same time each new received part for coordination both with initial, and with already received from the point of view of proximity to a goal.

According to the made assumption, with each transformation of a part of essence the number of the made actions increases by one – because of need of coordination of each following part for a limit with all previous. The last corresponds to the arithmetic sequence (which sum of members is equal: $1 + 2 + \cdots + n = \frac{(n+1)\times n}{2}$) and directly influences emergence of casual vulnerabilities.

As the person has complete idea of the essence of Representations, this stage is most preferable to the vulnerabilities introduced by the malefactor; at the same time, their addition can be carried out in process of transformation. Thus, the stage can be characterized by coefficient with the high value for casual vulnerabilities having a square appearance and an average for malicious vulnerabilities and to have a linear appearance:

$$\begin{cases} K_4^U = k_4^U \times t^2 \\ K_4^M = k_4^M \times t \end{cases}.$$

The Stage 5 is defined consecutive decomposition of uniform essence of Representation of *j* in elementary essence which is carried out by the person with good degree of automaticity, though in the form of «*1:N*». As the person at the beginning of a stage still operates with full essence, besides casual vulnerabilities emergence rare malicious is possible. Thus, the stage can be characterized by average value of coefficient for casual and very low for malicious vulnerabilities and have a linear appearance:

$$\begin{cases} K_5^U(t) = k_5^U \times t \\ K_5^M(t) = k_5^M \times t \end{cases}.$$

The Stage 6 is defined by consecutive formation of elementary forms of Representation of *j* by «replacement» of the corresponding elements of essence with them, i.e. in the form of «*1:1*». As work with elementary essence doesn't allow to operate with full sense of Representation, emergence only of casual vulnerabilities is possible. Thus, the stage can be characterized by low value of coefficient and have a linear appearance:

$$\begin{cases} K_6^U(t) = k_6^U \times t \\ K_6^M(t) \equiv 0 \end{cases}.$$

The Stage 7 is defined by the consecutive description of a uniform form of Representation of *j* from elementary forms which is carried out by the person with good degree of automaticity, though in the form of «*N:1*». As the person have completely departed from the essence of Representation, emergence only of casual vulnerabilities is possible. Thus, the stage can be characterized by average value of coefficient and have a linear appearance:

$$\begin{cases} K_7^U(t) = k_7^U \times t \\ K_7^M(t) \equiv 0 \end{cases}.$$

It is expedient to write down the level of insecurity of Representation a two-component vector which elements set density of each of types of vulnerabilities (casual and malicious): $S_i \equiv [S_i^U, S_i^M]$. The general deterioration in safety in this case and also according to the entered coefficients, will be defined by the equation $[S_j^U, S_j^M] = M \times [S_i^U, S_i^M]$, where M – a metrics (in the form of a single matrix) increases in insecurity when transforming Representations. The metrics is defined how:

$$M \equiv \prod_{N=1..7} \left(\begin{bmatrix} 1 - K_{0N}^{\ U} & 0 \\ 0 & 1 - K_{0N}^{\ M} \end{bmatrix} \times [S_i^U, S_i^M] \right),$$

where $K_{0N}^{\ P}$ – coefficient of increase in level of insecurity on the termination of a stage *N* for type of premeditation of vulnerability of U or M. Thus, the metrics doesn't depend on time and her components are calculated as number. Unlike existing (diverse and specialized for own tasks, for example [12, 13, 14, 15]), the entered metrics at rather high level of abstraction sets safety of the gained Impression on everyone a stage of interaction of people code. At the same time, the metrics allows to predict safety level in the future as it depends only on the chosen life cycle of creation SW.

In case of more real reflection of safety the matrix of *M* won't be single since unwitting and malicious vulnerabilities exert impact at each other on each of stages of transformation of Representations. Formalization of this situation is more difficult and demands carrying out additional researches.

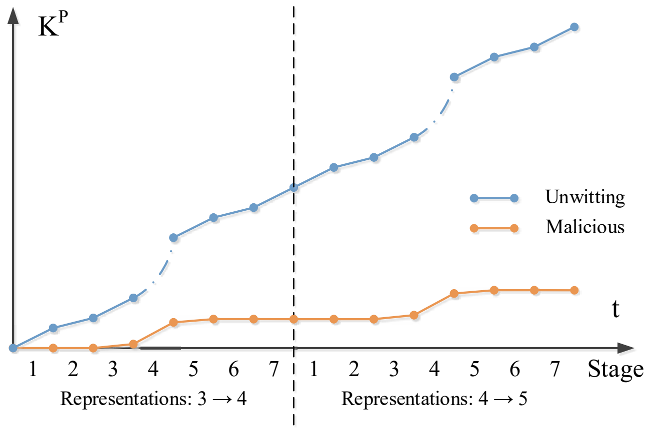
Graphic interpretation of coefficient $K_N^P(t)$ for various stages and types of vulnerabilities, illustrating their distinctions and features, has the following stylized appearance (Fig. 2):

Fig. 2. Graphic interpretation of coefficient of increase in level of insecurity of Representations for each phase

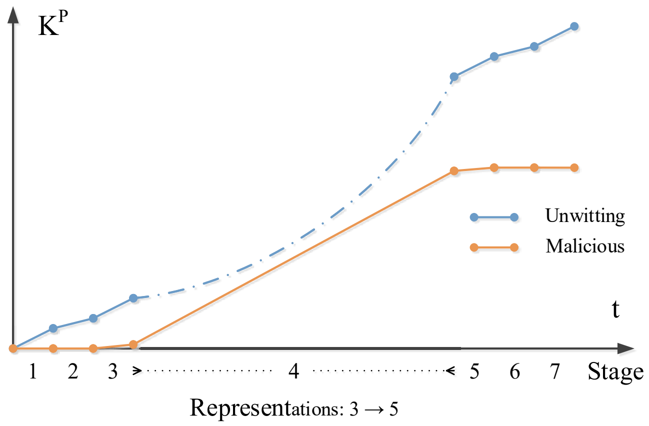
VII. Comparison of Safety of Transformation of Representations for Standard Scenarios of Software Development

As an example of potential applicability of the explained approach to assessment of safety we will make hypothetical comparing of two methods of creation of a program code (Representation 5) on its architecture (Representation 3) – with use of the intermediate algorithmized representation (Representation 4) and without it. In the second case the programmer receives the essence of Representation of algorithms of a code implicitly in the course of reconsideration of essence of Representation of architecture in Representation of the source code, passing thereby phases of synthesis of algorithmized Representation, its explicit processing and the subsequent analysis.

With sufficient degree of convention, but without loss of sense, change of the general coefficient of increase in level of insecurity of Representations $K^P(t)$ (as compound of $K_N^P(t)$ on each phase N) for both types of vulnerabilities ($P = \{I, M\}$) in a case from use of algorithmized Representation (further – Case 1) and without him (further – Case 2) is shown on the following schedules (Fig. 3).



a) transformation through Representation 4 (3→4→5)



b) transformation without Representation 4 (3→5)

Fig. 3. Graphic interpretation of the general coefficient of increase in insecurity when transforming Representations 3 in 5

At the Fig. 3 the dashed line has shown coefficient $K^P(t)$ with square dependence on t time. Units of measurements of schedules and the scale of Stage 4 on graphics 3b are conditional, designed to reflect the general behavior of coefficient and difference between him for two options of transformation.

The analysis of graphics 3) and 3) in the Fig. 3 allows to draw the following conclusions. First, in Case 1 using of intermediate Representation 4 means emergence of additional Stages 5, 6, 7 (for transformation of Representations 3 → 4) and Stages 1, 2, 3 (for transformation of Representations 4 → 5) that inevitably leads to accumulative increase in insecurity of Representation 5 because of casual vulnerabilities. Secondly, in Case 2 the refusal of use of intermediate Representation 4 means increase in Stage 4 twice that leads to a bigger increase in insecurity of Representation 5 because of casual vulnerabilities (because of a square type of coefficient $K_4^U(2t)$). Thirdly, existence in Case 2 twice of smaller quantity of Stages 3, 4, 5 having not zero $K_N^M(t)$ leads to smaller increase in insecurity of Representation 5 because of malicious vulnerabilities, than in Case 1.

According to the above-mentioned analysis, it is possible to claim that the choice of each of the described ways of creation SW results in various probability of emergence of vulnerabilities in Representation, at the same time the quantity of their one type can increase, and another to go down.

VIII. Conclusion

The described approach to safety assessment SW for various stages of his creation allows to create the formalized mathematical apparatus, as for assessment of current state of safety SW, and his forecasting (for example, as in [16]). The last one helps to make the reasonable choice among different variations of SW development, calculating at the same time potentially dangerous places. Collecting expert opinions and statistical data which will allow to set necessary invariant parameters of the device is necessary for transformation of a theoretical research into practical tools. The future of development of a research can develop into full processing of all process of creation SW – removal of one of his representations, addition of others, modification of the third – that will allow to receive final SW set safety level. Also, adaptation of process of creation safe SW under the field of its application, such for example as telecommunication devices is possible.

Reference

[1] M. Buinevich, K. Izrailov, A. Vladyko, "The life cycle of vulnerabilities in the representations of software for telecommunication devices," in Proc. 8th IEEE International Conference on Advanced Communication Technology (ICACT), South Korea, PyeongChang, 2016, pp. 430-435.

[2] K. Xinogalos, “Using flowchart-based programming environments for simplifying programming and software engineering processes,” IEEE Global Engineering Education Conference (EDUCON), Germany, Berlin, 2013, pp. 1313-1322

[3] M. Buinevich, K. Izrailov, A. Vladyko, "Method for Partial Recovering Source Code of Telecommunication Devices for Vulnerability Search," in Proc. IEEE 17th International Conference on Advanced Communication Technology (ICACT), South Korea, PyeongChang, 2015, pp. 76-80..

[4] M. Buinevich, K. Izrailov, A. Vladyko, "Method and Prototype of Utility for Partial Recovering Source Code for Low-Level and Medium-Level Vulnerability Search," in Proc. IEEE 18th International Conference on Advanced Communication Technology (ICACT), South Korea, PyeongChang 2016, pp. 700-707.

[5] M. V. Buinevich, K. E. Izrailov, "Method and utility for recovering code algorithms of telecommunication devices for vulnerability search," in Proc. IEEE 16th International Conference on Advanced Communication Technology (ICACT) , South Korea, PyeongChang, 2014, pp. 172-176.

[6] P. Tripathy, K. Naik. “Reengineering,” Software Evolution and Maintenance: A Practitioner's Approach, 2014, pp. 133-186.

[7] R. Aliyev, L. Peñalver, "Analyzing Vulnerability Databases," in Proc. 10th IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 2016.

[8] A. Fedorchenko, I. Kotenko, A. Chechulin, "Design of Integrated Vulnerabilities Database for Computer Networks Security Analysis," in Proc. 23rd Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Turku, Finland, 2015, pp. 559-566.

[9] M. Gernsbacher, M. Kaschak. “Text Comprehension,” The Oxford Handbook of Cognitive Psychology, 2013, pp. 462-474.

[10] M. Yeari, “The role of working memory in inference generation during reading comprehension: Retention, (re)activation, or suppression of verbal information?,” Learning and Individual Differences, 2017, Vol. 56, pp. 1-12.

[11] M. Raghothaman, Y. Wei, Y. Hamadi. "SWIM: Synthesizing What I Mean – Code Search and Idiomatic Snippet Synthesis", in Proc. IEEE 38th International Conference on Software Engineering (ICSE), USA, New York, 2016, pp. 357-367.
[12] J. Knight, B. Rodes, K. Wasson, "A security metric based on security arguments," In Proc. 5th International Workshop on Emerging Trends in Software Metrics, USA, New York, 2014, pp. 66–72.
[13] X. Cheng, N. He, M. Hsiao, "A New Security Sensitivity Measurement for Software Variables," In Proc. IEEE Conference on Technologies for Homeland Security, USA, Waltham, 2008, pp. 593-598.
[14] Metrics and measurement of trustworthy systems // Military Communications Conference (MILCOM). IEEE. 2016. pp. 1237-1242.
[15] J. Cho, P. Hurley, S. Xu "Metrics and measurement of trustworthy systems," in Proc. IEEE 35th Military Communications Conference (MILCOM 2016), Baltimore, United States, 2016, pp. 1237-1242.
[16] M. Buinevich, P. Fabrikantov, E. Stolyarova, K. Izrailov, A. Vladyko "Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast," in Proc. IEEE 11th International Conference on Application of Information and Communication Technologies (AICT), Moscow, Russia, 2017, pp. 293-297.

Mikhail Buinevich received the D.Sc degree in Engineering from the Naval Institute of Radio Electronics, St. Petersburg, Russia, in 2010.
He has 20 years of experience in research and development in IT security. Now he is a Professor at The Bonch-Bruevich Saint-Petersburg State University of Telecommunications and supervises post graduates.
Prof. Buinevich is the Editor-in-chief of "Proceedings of Telecommunication Universities" scientific journal.

Konstantin Izrailov defense his degree of PhD at The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russia in 2017. Now he is an Associate Professor at that University.
Mr. Izrailov interests include: Information & Network Security; Software-Defined Networking; Internet of Things.

Andrei Vladyko (IEEE member (M'14)) acquired his degree of PhD at Komsomolsk-on-Amur State Technical University, Russia in 2001.
At present he is a head of R&D department of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.
Mr. Vladyko major interests include: Information & Network Security; Software-Defined Networking; Internet of Things; Wireless Sensor Network.

Volume 6 Issue 6, Nov. 2017, ISSN: 2288-0003

ICACT-TACT JOURNAL

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591

Business Licence Number : 220-82-07506, Contact: secretariat@icact.org Tel: +82-70-4146-4991