O-019

セキュリティとセーフティのリスク管理におけるガイドワードの問題と課題について
Issues and Problems of Guide-word for Security and Safety on Risk Management

五郎丸 秀樹†
Hideki Goromaru

1. はじめに

近年、制御システムはネットワークから切り離された環境下であっても Stuxnet [1]を代表としたサイバー攻撃の対象になり、セーフティだけでなくセキュリティも含めたリスク管理が必要になってきている。リスク管理のガイドワードとして HAZOP [2]や STRIDE [3]をハザードや脅威を見つけるため使うことがあるが、セキュリティとセーフティが混在したシステムでは、既存のガイドワードでは不十分であり、複数のガイドワードの案が出ている。本誌では様々なガイドワードの種類をのべ、ガイドワードの問題点と課題について論じる。

2. ガイドワードの定義

ブレインストーミングを代表とするヒントなしの自由連想とは違い、ガイドワードはヒントで誘導する制限連想の一つであり、自由連想では思いつくことが難しい構成要素間やプロセスでのリスク特定で使われることが多い[4]。国際標準規格では”word or phrase which expresses and defines a specific type of deviation from a property’s design intent”と定義され、その役割は想像力豊かな思考を刺激することである[2]。本稿ではガイドワードとは書かれていない語句（例えば、フレーズ、ヒント、チェックリスト、プロンプトリスト）であってもガイドワードとして使える語句をガイドワードとする。例えば STPA-Sec[5]では” type of unsafe/unsecure control actions”と示された 4 つの語句(例：Stopped Too Soon or Applied Too Long)は定義に従えばガイドワードそのものである。HAZOP ガイドワードでは、No or Not, More, Less, As well as, Part of, Reverse, Other than, Early, Late, Before and After が例として示されている。

3. ガイドワードを使用する意義

我々は、自由連想(ブレインストーミング)でのリスク特定と人的要因リスクを抽出するためにガイドワードによるリスク特定を別々に実施し、マージさせた場合のガイドワードによる新規リスクの割合を調査した。人的要因リスクのガイドワードとして失敗まんだらの原因まんだら（誤判断、不注意、無知等）[6]を使用し、①BLE システム（Bluetooth Low Energy を使用した位置特定システム）、②制御システム（産業用ロボットを使用したシステム）でのリスク特定を実施した。被験者はセキュリティ知識を持った非セーフティ専門家 9 名であり、ガイドワードでは 3 名、自由連想では 6 名に振り分けて実施した。その結果、新規人的要因リスクの割合はリスク全体の約 1/4 となり（図 1）、自由連想では見えてこなかったリスクを特定することができることがわかった。

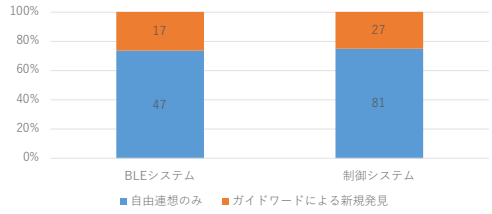

図 1　ガイドワードによる新規発見の割合

4. ガイドワードの適用状況

ここではセキュリティを中心とした、ガイドワードの関連研究について述べる。

4.1 ガイドワードの新規作成

McDermid(1994)ら[7]はコンピュータソフトウェアの解析用に SHARD という手法を考え新たに 5 つのガイドワード(Omission, Commission, Value, Early, Late)を作成した。金ら(2012)[8]は組込み系システムの状態遷移図に着目したガイドワードを作成した。Winther (2001)ら[9]は、security-HAZOP という新たなガイドワード作成方法を提案した。不適切な CIA（機密性・完全性・可用性）の要因に焦点を当て下記のようにガイドワードと属性を組み合わせ新たな脅威を特定する方法である。

- Post-Guideword（例：内部者、技術的な失敗、ウイルス、破損）
- Component（例：ファイヤーウォール、サービス）
- Pre-Guideword（意図的な/意図的でない）
- Attribute（例：開示、操作、停止、汚職）

例えば「内部者によるファイヤーウォールの意図的な操作」という新たな脅威を示すことができる。

4.2 HAZOP ガイドワードと他手法との組合せ

Srivatanakul ら(2005) [10]は UML の一つである Use-case、Raspotnig ら(2012) [11] は CHASSIS（Use-case と Miss Use-case を組み合わせた手法）、Ito (2014) [12] はゴール指向の 1 つである KAOS [13] に HAZOP ガイドワードを適用した。

4.3 自動車業界への適用と STPA の活用

自動車業界でのガイドワードとして、Wei ら(2015)[14]はコンピュータやネットワークへの攻撃語句 [15]を流用し、Macher ら(2016)[16]は HAZOP を改良した機能的観点から特定の特徴に対する潜在的脅威を考慮した手法(THROP)を作成した。Mallya ら(2016)[17]は ISO26262 に STAMP/STPA を適用し、Friedberg ら(2016)[18]は STPA-SafeSec を適用して完全性・可用性における 12 の脅威リストを追加した。Dürrwang ら(2017)[19]は HAZOP を基に SGM という自動車分野の新セキュリティガイドワードを作成しセーフティ知識を持った非セキュリティ専門家に使用してもらった結果、セキュリティ技術者と同じ方法で情報資産と保護目標を特定できるようになることを示した。

4.4 ガイドワードとしての STRIDE の使用

STRIDE[20]はガイドワードとして使用することも多く、金子ら(2018)[21]は STPA-SafeSec に適用した。大久保

†日本電信電話株式会社　Nippon Telegraph and Telephone corporation

Copyright © 2019 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.

(2018)[22]は自動車の自動運転の脅威分析に適用したが Blackhat[23]の報告で STRIDE だけでは不十分であることがわかり新たなガイドワード（不正操作（起動、停止含む）、悪用、のっとり）を追加し、林ら(2018)[24]は STRIDE だけでなく環境要因、機器故障、プログラムのバグ、ヒューマンエラーに関するガイドワードを追加した。

5. 問題と課題

5.1 時代や業界にあわせた変更やカスタマイズ

制御システムとしての自動車業界の自動運転の脅威分析では、SHARD や STRIDE では不十分となり、THROP や SGM など独自追加したガイドワードが出現しており、セキュリティでは新たな脅威に応じて新ガイドワードが必要になる場合がある。新たなガイドワード作成に security-HAZOP[11]を活用することも考えられるが動的に変わる状況に合わせた変更やカスタマイズの方法についてさらに検討が必要である。

5.2 ガイドワード自体の新たな表現

ガイドワード自体が抽象的な用語であるため、初めて使用する場合や慣れていなければ思いつかない可能性がある。また人間の短期記憶（Working memory）の制約により 7±1 または 4±1 の語句しか保持できない[25]。ガイドワードを効率よく運用するには、具体化のための検討や慣れるための仕掛けなど人間の理解能力内で実施について更なる検討が必要である。

5.3 網羅性の弊害

ステークホルダーへの説明のため、ガイドワードに網羅性を求める場合がある。システム構成や実行プロセスを還元主義的に分類しガイドワードとして適用することで網羅性を担保することが考えられる。但し還元主義的な網羅性には限界があり[26]、網羅性に固執しガイドワードの全項目に入力ことに時間をかけすぎたり、項目に１つだけ入力することで満足し思考が止まったりする弊害があり、想像力豊かな思考を刺激する本来の目的とはかけ離れてしまう恐れがある。

6. おわりに

今回セキュリティとセーフティが混在する環境でのガイドワードについて調査を行い、問題や課題が残っていることを確認した。今後は残っている問題や課題を含め検討していきたい。

参考文献

[1] “Five nightmarish attacks that show the risks of IoT security”, http://www.zdnet.com/article/5 nightmarish attacks that show the risks of iot security/ (参照 2019/01/18).

[2] HAZard and OPerability Studies (HAZOP Studies) – Application Guide, IEC 61882:2016.

[3] Shawn Hernan et. al.. Uncover Security Design Flaws Using The STRIDE Approach. MSDN Magazine, 2006.

[4] Risk management – Risk assessment technique, IEC/ISO 31010: 2009.

[5] William Young and Nancy Leveson., Systems Thinking for Safety and Security, ACM, Proceedings of the 2013 Annual Computer Security Applications Conference (ACSAC 2013),2013.

[6] "失敗知識データベースの構造と表現　図 8 原因まんだら", http://www.sozogaku.com/fkd/inf/mandara.html (参照 2019/01/18).

[7] J. A. McDermid and D. J. Pumfrey. A Development of Hazard Analysis to aid Software Design., IEEE, In Proceedings of the Ninth Annual Conference on Computer Assurance (COMPASS '94), Gaithersburg, MD, pp. 17-25, 1994.

[8] 金周彗、松原豊、高田広章, "組込みシステムにおける並列型状態遷移図に基づく安全分析手法", 情報処理学会、組込みシステムシンポジウム 2012,2012.

[9] Rune Winther, Ole-Arnt Johnsen, Bjørn Axel Gran, "Security Assessments of Safety Critical Systems Using HAZOPs", Springer-Verlag Berlin Heidelberg, SAFECOMP 2001, LNCS 2187, pp. 14–24, 2001.

[10] Srivatanakul Thitima Security Analysis with Deviational Techniques [Report] : PhD. Thesis. - York : University of York, Department of Computer Science, 2005. - p. 279.

[11] Christian Raspotnig, Peter Karpati and Vikash Katta, "A Combined Process for Elicitation and Analysis of Safety and Security Requirements", Springer-Verlag Berlin Heidelberg, BPMDS 2012 and EMMSAD 2012, LNBIP 113, pp. 347–361, 2012.

[12] Masao Ito, "Finding Threats with Hazards in the Concept Phase of Product Development", Springer-Verlag Berlin Heidelberg, EuroSPI 2014, CCIS 425, pp. 277–284, 2014.

[13] Emmanuel Letier, Reasoning about Agents in Goal-Oriented Requirements Engineering, Ph.D. thesis, Universite catcholique de Louvain, 2001.

[14] Jingxuan Wei, Yutaka Matsubara and Hiroaki Takada, "HAZOP-based Security Analysis for Embedded Systems: Case Study of Open", IEEE, ECAI 2015 - International Conference – 7th Edition Electronics, Computers and Artificial Intelligence, 2015.

[15] J. D. Howard an T. A. Longstaff, “A Common Language for Computer Security Incidents”, Sandian Nat. Lab., Sandia Rep. SAND98-8867, 1998.

[16] Georg Macher, Eric Armengaud, Eugen Brenner and Christian Kreiner, "A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context", Springer International Publishing Switzerland, SAFECOMP 2016, LNCS 9922, pp. 130–141, 2016.

[17] Archana Mallya, Vera Pantelic, Morayo Adedjouma, Mark Lawford and Alan Wassyng, "Using STPA in an ISO 26262 Compliant Process", Springer International Publishing Switzerland, SAFECOMP 2016, LNCS 9922, pp. 117–129, 2016.

[18] Ivo Friedberg, Kieran McLaughlin, Paul Smith , David Laverty and Sakir Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems", Elsevier Ltd., Journal of Information Security and Applications 34 (2017) pp.183–196, 2017.

[19] Jürgen Dürrwang, Kristian Beckers and Reiner Kriesten, "A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain", Springer Nature, SAFECOMP 2017: Computer Safety, Reliability, and Security pp 305-319, 2017.

[20] Adam Shostack, "Threat Modeling: Designing for security", John Wiley & Sons, Inc., 2014.

[21] 金子朋子、早川拓郎、高橋雄志、大久保隆夫、佐々木良一、"安全性解析手法 STAMP/STPA への脅威分析（＝STRIDE）の適用",情報処理学会研究報告、Vol.2018-DPS-174No.6,2018.

[22] 大久保隆夫, "セーフティ機能のセキュリティ脅威に対する効果の分析", 情報処理学会研究報告, Vol.2018-CSEC-82 No.20, 2018.

[23] "blackhat", https://www.blackhat.com/ (参照 2019/01/18).

[24] 林浩史、高橋雄志、金子朋子、早川拓郎、佐々木良一, "IoT システム向けリスク評価方式と支援ツール SS-Rat の開発", 情報処理学会研究報告, Vol. 2019-GN-106 No.35, 2019.

[25] Nelson Cowan, "The magical number 4 in short-term memory: A reconsideration of mental storage capacity", Cambridge University Press, BEHAVIORAL AND BRAIN SCIENCES (2000) 24, pp.87–185, 2000.

[26] Baruch Fischhoff, Paul Slovic, and Sarah Lichtenstein, "Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation", the American Psychological Association, Journal of Experimental Psychology: Human Perception and Performance 1978, Vol. 4, No. 2, pp.330-344, 1978.

Copyright © 2019 by Information Processing Society of Japan and
The Institute of Electronics, Information and Communication Engineers
All rights reserved.