Title	システム安全設計の質と伝達性を向上させる表記法の提案
Sub Title	Proposal for notations to improve quality and transferability of system safety design
Author	吉岡, 奈紗(Yoshioka, Nasa) 白坂, 成功(Shirasaka, Seiko)
Publisher	慶應義塾大学大学院システムデザイン・マネジメント研究科
Publication year	2015
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2015年度システムエンジニアリング学 第217号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40002001-00002015-0058

修士論文　　2015 年度

システム安全設計の質と伝達性を向上させる表記法の提案

吉岡 奈紗

（学籍番号：81433535）

指導教員　白坂 成功

2016 年 3 月

慶應義塾大学大学院システムデザイン・マネジメント研究科
システムデザイン・マネジメント専攻

論　　文　　要　　旨

学籍番号	81433535	氏　名	吉岡 奈紗

論 文 題 目：

システム安全設計の質と伝達性を向上させる表記法の提案

様々なシステムは人間によって設計されており、その安全性もまた人間が担保していくものである。昨今、そのシステムの膨大化や複雑化、またその影響でシステムに関わる人間も多様化してきている。そんな中、システムに関わる人間同士のコミュニケーションやノウハウの伝承に関しても様々な課題が存在する。例えば、ISO26262 などの制度でシステムの安全性を第三者に説明する義務が発生していたり、ノウハウが伝承されていなかった事によって今後安全に運用できないかもしれないシステムが存在し始めている。このように、安全を担保する際のコミュニケーションに関する課題は多く存在する。更に、設計者自身にスポットを当てると、新たな課題が見えてくる。人間はある決定に至る思考の各段階で様々な選択を重ねている。それを結節点に見立てて"ノード"と呼ぶなら、意思決定のプロセスとは、それらのノードをツリー状に描くことによって図式化できるものである。ここで決定の目的を安全担保とし、思考のスタートを保証したい事柄とすると D-Case という議論を見える化する手法となる。また、思考のスタートを起こってほしくない事柄とすると、Fault Tree Analysis（FTA）というハザード分析の手法となる。

本研究は様々なシステムの設計に多用されている FTA に、ある 1 つの考慮の要素を加える事で、FTA をより意味のある書記法とすることを目指した。ここでいう、「より意味のある」やり方とは①決定のプロセスが網羅的で後から辿れるトレーサビリティーを持ち②誰もが理解でき③後から来る人達にも伝わる方法である。また、①～③を満たし、本来の目的である安全の確保に資する手法として、新たに筆者の創案になる拡張された D-Case の有用性を主張し、その活用を推奨しようとするものだ。

そこで、D-Case の新しい記載ルールとして、安全設計者が設計中に考えたことを D-Case に反映させるための Reason Node と D-Case 上で関係文書や文書内の整合性・追跡性を担保するための Document Node を提案する。また、FTA の新しいルールとして、D-Case に既存する上位概念を具体化する際にその軸を表す Strategy Node と前提条件や制約条件を示す Context Node、新しい概念である Reason Node を追加して、D-Case の網羅性や追跡性、伝達性を向上させて新たに整合性や伝承性を追加する。FTA に関しては、網羅性を向上させ、追跡性や整合性を追加したり FTA を介して議論しやすいようしたりにする。

研究の流れとしては、提案する表記を実際のロケット開発に適応して、再度上記の課題を確かめた上で自身の提案の有用性を実感した他、28 名の方に協力してもらって六種類、十の方法の検証を行った。各検証では基本的に安全設計を行う設計者として D-Case または FTA の記載を、またその安全のロジックを共有する立場として既に作られた D-Case または FTA を読むということをしてもらった。

結論として、D-Case に Reason Node を追加したことで、設計者自身の思考整理に役立った他、より目的に沿った D-Case 記載の可能性も見られた。また、設計者の意図が見える化されて安全のロジックに関する伝達性や設計のポイントの伝達性が向上した。また Document Node の追加によって、システムの安全設計に関する文書間や文書内の関係性が見える化され、それぞれの整合性確保の簡易化が達成された。更に、文書や項目間で追跡性や整合性が向上したことによって、ある設計の影響する範囲が機械的に洗い出せるようになった。また、FTA に Strategy Node、Context Node、Reason Node を追加したことで、上位のハザード要因をより細かく分割する際の視点が一点に固定され、明確になることで以前よりも網羅性が向上しただけでなく、追跡性や整合性、ロジックやノウハウの伝達性も向上した。

キーワード（5 語）
システムアシュアランス, アシュアランスケース, D-Case, FTA, 安全設計

SUMMARY OF MASTER'S DISSERTATION

Student Identification Number	81433535	Name	Nasa Yoshioka

Title

Proposal for Notations to Improve Quality and Transferability of System Safety Design

Various systems have been designed by human, and also their safety has been designed by human. Recently the system become huge and complex. And also the relationship between the human who has relationship with the system become complex. Therefore various problem also exists with the communication between human involved in the system or knowledge transfer. For example, the obligation to explain the detail of system safety to a third party in the system because of ISO 26262. There is another example. The system which has the possibility not to operate safety begins to exist because the know-how of operation has not been handed down. In addition, when we focus on the engineers, the human always piled a various choice at each stage of decision making. If that would be called as "Node", the process of decision making can be drawn graphically as a tree. Now if the propose of decision would be Safety Assurance and the starting point of thinking would be the event to assure, that becomes "D-Case" which is the tool to visualize the discussion. And also if the starting point of thinking would be the event which is not wanted to occur, that become Fault Tree Analysis (FTA) which is the tool of analyzing the hazard.

This study aim to be the tool which would be more meaningful than existing FTA frequently used in the various design by adding the three Nodes. Referred to here, "more meaningful" means ① the process of decision making has tradability and much covering, ②everyone could understand, ③ successor can also understand. And also by meeting ① to ③, the D-Case which has new Node extended by this study is tried to recommend to use.

For achieve these purpose, two new Node are added to D-Case. One is "Reason Node" which shows us the reasons which the engineers thought during the design. Another is "Document Node" which shows us the name of the concerned documents. And also new three Nodes are added to FTA. One is Strategy Node which is already existed in D-Case shows us the viewpoint to divide the upper event to lower event. The other is Context Node which is also existed in D-case shows us the assumption. The last one is Reason Node which is explained above.

The verification and validation which are six types and ten ways are done by 28 people who have a various background. They tried to stand both position which are the safety engineers and the stakeholder or the successor of the system.

In conclusion, Reason Node helps the engineer to make a logic of the safety design and draw the D-Case according to the purpose more than before. And also the process of decision making during the safety design is visualized so the transmissibility of the know-how and logic of the safety design. Document Node helps the engineer to maintain the consistency between the documents. And also the coverage of influences by modifying the safety design can be visualized. So the coverage can be washed out automatically. Moreover the comprehension of FTA is improved by adding Strategy Node. Context Node and Reason Node because the viewpoint to divide the upper event to the lower is fixed. So the viewpoint become clear. Therefore not only the coverage has been improved but also the traceability, consistency are also improved. The new functions which are logic and know-how transfer can be also added.

Key Word(5 words)
System Assurance, Assurance Case, D-Case, FTA, System Safety