

STRUCTURAL RELIABILITY ANALYSIS OF A STAR STRUCTURED COMPLEX ELECTRONIC SYSTEM

Georgiev, Anton Slavchev, Technical University – Varna, georgiev_an@tu-varna.bg

Nikolov, Nikolay Ivanov, Technical University – Varna, nikolay.nikolov@tu-varna.bg

Abstract: This article concerns reliability modeling and analysis of network structured complex electronic systems. A brief overview of common network topologies is presented. Reliability models of a star structured complex electronic system in SCADA application as fault tree and reliability block diagram are presented and analyzed. A structural reliability system analysis is performed.

Keywords: system reliability, complex electronic systems.

АНАЛИЗ НА СТРУКТУРНАТА НАДЕЖДНОСТ НА СЛОЖНА ЕЛЕКТРОННА СИСТЕМА СЪС СТРУКТУРА ТИП ЗВЕЗДА

Георгиев, Антон Славчев, Технически университет - Варна, georgiev_an@tu-varna.bg

Николов, Николай Иванов, Технически университет - Варна, nikolay.nikolov@tu-varna.bg

Абстракт: Статията е посветена на моделиране и анализ, касаещи надеждността на сложни електронни системи с мрежова структура. Направен е кратък обзор на най-често срещаните мрежови топологии. Представени и анализирани са модели от гледна точка на структурната надеждност, като дърво на отказите и блокова схема на надеждност, по отношение на сложна електронна система със структура тип звезда, предназначена за управление и сбор на данни. Направен е анализ на структурната надеждност на системата.

Ключови думи: надеждност на сложни системи, сложни електронни системи.

INTRODUCTION

A complex electronic system (CES) usually comprises a large number of functional units and blocks interconnected in such a way that the system is able to perform a set of required functions including its basic system function as well as all auxiliary functions. These are elements of the system. The system and its elements have operational modes including normal operating modes, test modes and contingency modes induced by failures, faults or operator errors [1].

The system elements, together with the links between them form the structure of the system. Nowadays computerization of the industry causes a typical approach to design and composition of complex electronic systems. Often the CES layout is shaped in line with topologies, borrowed from computer networks. First of all these are cases when the links between elements are bidirectional and most of system elements are similar, equal or identical in their design and functions. A brief overview of common network topologies will be given below.

In reliability perspective each particular CES structure determines system reliability characteristics. This is the reason why each typical CES structure requires thorough reliability

analysis for basic dependences to be identified, necessary to be known in case when the reliability of a specifically structured CES have to be analyzed.

This article is intended to analyze a typical centralized star structured CES. The analysis methods applied are fault tree analysis, reliability block diagram analysis and logical analysis.

COMMON NETWORK TOPOLOGIES

Network topology is the layout or organizational hierarchy of interconnected nodes of a (computer) network [7]. The common network topologies are presented on *Fig. 1*. These are listed and briefly discussed below:

- A chain network (see *Fig. 1a*): all nodes are connected consecutively one by one. This kind of topology is not proper for CES design, because the manner of connections between nodes limits the systems functionality. This is suitable for network of CES (e.g. wireless and radio-relay lines)
- A bus network (see *Fig. 1b*): all nodes are connected to a common medium along this medium. This topology is applicable to CES design. In many aspects this is similar to the star topology and can be analyzed as such.
- A tree network (see *Fig. 1c*): nodes are arranged hierarchically. This topology is more suitable for network of CES (e.g. wireless networks) than for CES design.
- A ring network (see *Fig. 1d*): each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. This topology is more applicable to network of CES (e.g. radio-relay lines) than to CES design.
- A star network (see *Fig. 1e*): all nodes are connected to a special central node. This is a topology, frequently followed in the design of CES, mostly in cases when CES are composed as hierarchical and centralized ones.
- A mesh network (see *Fig. 1f*): each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other. Such topology is used for design of a CES which comprises a number of elements, totally different in functions performed by them within the system[8].
- A fully connected network (see *Fig. 1g*): each node is connected to every other node in the network. This topology is not proper for design of CES because of links redundancy.

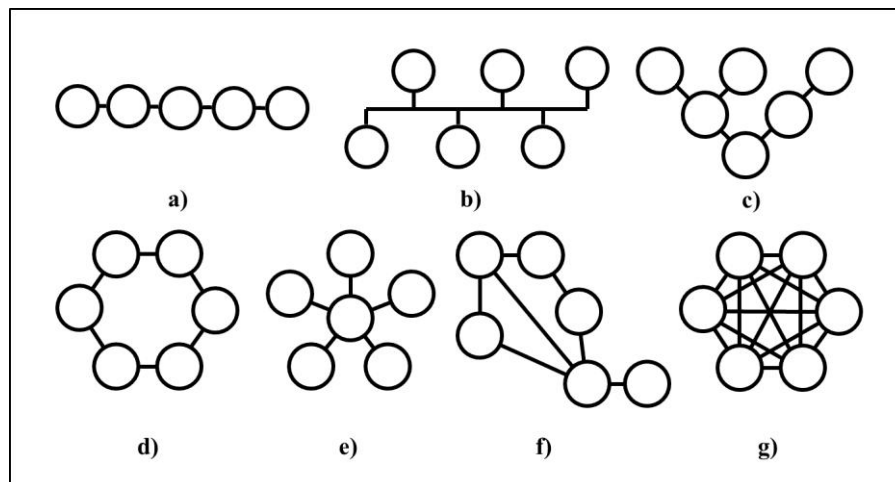


Fig.1. Common network topologies.

When the design of a CES follows a network topology, this is mostly in regard to the physical system structure. In a physical sense the nodes of the systems topology are electronic subsystems, blocks and units, i.e. elements of CES.

The reliability analysis presented in this article is concerned to the reliability of technical components and systems and will not deal with the software reliability and/or the human factor.

One of the network topologies is most suitable to be followed when compose a CES. This is the centralized star topology.

STAR STRUCTURED CES (SSCES)

Consider a CES which is built up in line with a centralized star topology. This is a system, intended to control a power substation or a knot station within the electricity distribution grid. This CES is functioning as a lowest (local) level subsystem of a SCADA (Supervisory Control and Data Acquisition) system, developed over a number of sites but is also capable to work independently [4],[5],[7]. The topology of such system is shown on *Fig. 2a*) and its simplified block diagram is presented on *Fig. 2b*). The system structure is hierarchical and three different hierarchic levels can be distinguished. These are the lowest system level containing all local end points, the center of the structure and also the upper SCADA system level. The latter will not be considered during the analysis below. Only the link to it will be taken into consideration.

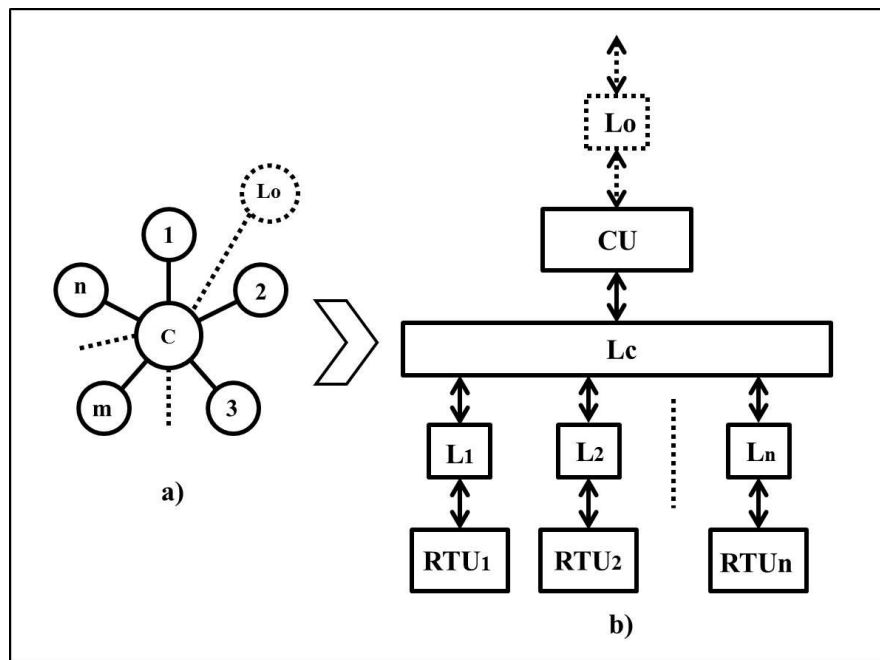


Fig.2. a) Centralized star topology; b) Centralized star structured CES – SCADA subsystem.

The system comprises a known number (n) of end points and a central point. The end points are equipped by Remote Terminal Units (RTU) intended to control the power switches. The RTUs are identical or similar in regard to their design and perform identical functions. This gives the reason to be assumed that their reliability characteristics are also identical. The central point is equipped by a central unit (CU) supervising the system. The data acquired at the end points are transmitted to the central point.

The control signals generated or retransmitted by the central point are distributed to the end points. All links between central point and each of the end points are bidirectional in order to ensure proper functioning of the system. Being a subsystem of a larger SCADA system, this CES is equipped by an interface module (dashed line block on *Fig. 2b*) marked as L_0 , which connects the system to the upper SCADA level.

The linking modules of each end point are marked respectively as L_1, L_2, \dots, L_n . These include interface equipment and also the lines if any. The common interface unit at the central unit is marked as L_c .

RELIABILITY MODELING OF SSCES

During its operation a CES needs of a technical support usually performed by a maintenance team conducting reliability-centered maintenance (RCM). The purpose of the maintenance process is to keep the system available, i.e. able (under combined aspects of its reliability, maintain ability and maintenance support) to perform its required functions at a stated period of time [1].

During CES operation there might be occurred failures of the systems elements. Nevertheless that all systems elements are assessed in most cases as repairable items they may also be treat as non-repairable ones by the maintenance team.

The most important task at the start of any systems reliability analysis is this for systems failure modes identification. For the CES under analysis there are different approaches:

- The first of it is to asses the system as completely failed in case when the system function is not performed anymore for all end points together. This does mean that eventual failure which causes problem in system function performance regarding one or several end points will be assessed as partial system failure if at least one end point is still working properly.
- The second one is to asses the system as completely failed in case when the system function is not performed anymore even in regard to only one end point.

The former approach leads to overassessment of the systems reliability. In contrast, the latter leads to underassessment of this. Both of it are extreme and therefore not acceptable for practical application. This issue will be clarified during the analysis below.

FAULT TREE OF SSCES

The fault tree approach is a typical one to reliability analysis of CES. The fault tree of the system studied can be seen on *Fig. 3*. Its structure is strictly corresponding to the system design.

The fault tree presented is a logic diagram which comprises $n+1$ OR gates and one Voting OR gate. These are logic operators used here in reliability aspect[3]. The fault tree also takes into consideration $2n+3$ input events. They are marked as a_{01}, a_{02}, a_{03} and $a_{i,j}$ respectively, where $i = 1, 2, \dots, n$ and $j = 1, 2$. In reliability sense the input event a_{i1} denotes failure of the respective RTU $_i$ but a_{i2} denote failure of link equipment at the respective end point. The input event a_{01} denotes failure of the CU as well as a_{02} denotes failure of the common interface unit. The input event a_{03} denotes failure of the equipment linking the system to the upper system level. All input events are considered to be basic ones as each of it can cause a complete system failure directly or under some conditions given. In logical aspect occurrence of an input event means appearance of a logic state “1” at the respective input of the fault tree diagram. Absence of failure is equal to a logic state “0” at the respective input.

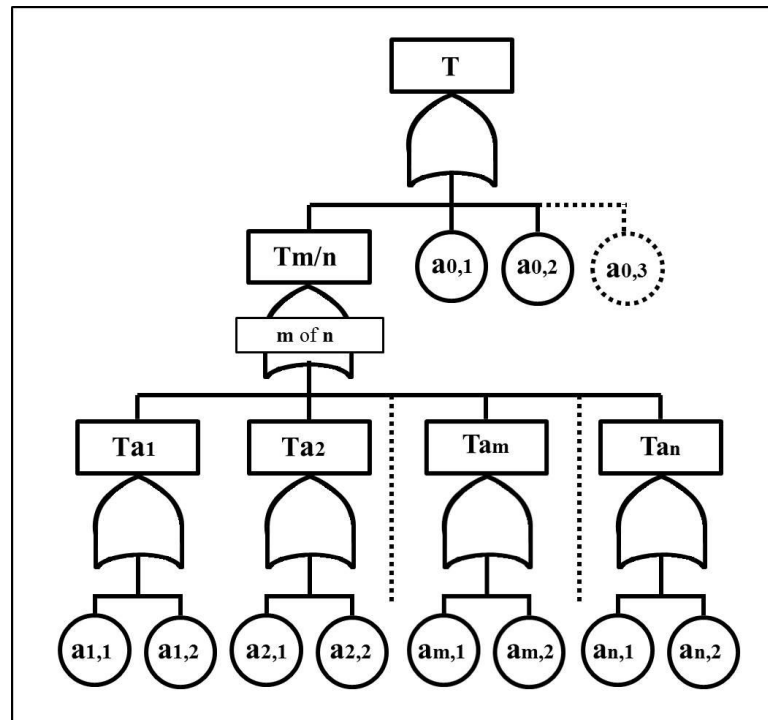


Fig.3. Fault tree of SSCES.

In reliability aspect the top event, marked as T denotes a complete system failure. The events marked as $T_{a1}, T_{a2}, \dots, T_{am}, \dots, T_{an}$, are failures of equipment at the respective end point $1, 2, \dots, m, \dots, n$. From reliability point of view occurrence of each of these events denotes a partial system failure at the respective end points. In logical aspect this means appearance of logical state “1” at the respective logic gate output. The event $T_{m/n}$ is occurred when the condition “ m out of n ” is fulfilled. This condition requires more detailed explanation because of its importance in reliability perspective. As it was clarified above the system comprises a number of n end points containing sets of equipment. At the start of system reliability estimation one have to set a requirement about how many end points have to become failed (usually this number is less than n) before to announce the entire system as a completely failed one. In reliability aspect this is a kind of a threshold level marked as a given number m and its announcement is equal to identification of the system failure mode.

If the number of events T_{ai} occurred remains less than m then the entire system is assessed as still functioning. Otherwise, if their number becomes equal to or bigger than m then they all together cause occurrence of the event $T_{m/n}$, which causes a complete system failure (back to diagram: because the condition “ m out of n ” is fulfilled and at the output of the logic gate Voting OR appears logic state “1” which trough the logic gate OR causes appearance of a state “1” at its output and this means occurrence of the top event T - complete system failure). This way the input events $a_{i,j}$ may cause a complete system failure under condition explained above. In contrast the input events a_{01}, a_{02}, a_{03} can cause the same directly through the logic gate OR. Occurrence of each of these events is equal to appearance of a logic state “1” at the input and then at the output of it. This means again occurrence of the top event T - complete system failure. In case when it is correctly constructed and relevant to the CES the fault tree gives the basis for reliability estimation in regard to failures and faults of the system and its elements.

There is another typical approach there to system reliability analysis applicable especially to structural system reliability analysis. This is the reliability block diagram approach.

RELIABILITY BLOCK DIAGRAM OF SSCES

Conducting a reliability analysis it is also possible the structure of the system to be presented and analyzed by a reliability block diagram (RBD). This is another typical approach to reliability analysis of CES. RBD is a success-oriented network, describing the function of the system. It displays the logical connections of the components, needed for the system function to be fulfilled [2]. The RBD of SSCES is presented on Fig. 4. RBD strictly corresponds to the system layout and includes all system elements relevant to the system reliability. Each element of the system is displayed as a block which has two end points. If there is a connection between them then the element is functioning.

The RBD of SSCES also corresponds to the SSCES fault tree presented above. This is built up by conversion of SSCES fault tree. Because of that the diagram blocks and their labels strictly correspond to the initial events in the fault tree. The diagram layout also so strictly corresponds to the logic gates of the fault tree.

The main difference between RBD and the fault tree here is that the label in the fault tree denotes an event that could be eventual failure of the respective element (logic state “1”) or absence of failure (logic state”0”), but the same label in RBD denote the respective element which could be in workable condition (logic state”1”) or in condition of failure (logic state”0”), as the RBD is a success-oriented structure.

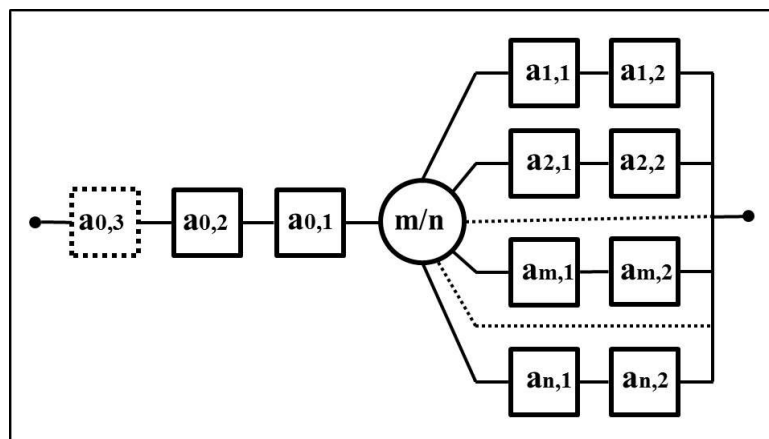


Fig.4. Reliability block diagram of SSCES.

When there is a connection between the right end point and the left end point of the RBD the system function is considered as fulfilled. A passable route from the right to the left end point has to be ensured by chain of blocks in workable condition (elements in state “1”).

STRUCTURAL ANALYSIS OF SSCES

The system studied is composed of $2n+3$ components. Obviously the system is coherent as all its components are relevant and the structure function is non-decreasing. The state of each component can be described by a binary variable, as follows

$$a_{ij} = \begin{cases} 1 & \text{if the element is functioning} \\ 0 & \text{if the element is failed} \end{cases}, \quad (1)$$

where $i = 1, 2, \dots, n$ $j = 1, 2$.

The same is a truth also for a_{01} , a_{02} and a_{03} .

The state of the entire system described by a binary function has the form

$$\varphi(a) = \varphi(a_{01}, a_{02}, a_{03}, a_{11}, a_{12}, \dots, a_{ij}, \dots, a_{n1}, a_{n2}), \quad (2)$$

where

$$\varphi(a) = \begin{cases} 1 & \text{if the system is functioning} \\ 0 & \text{if the system is failed} \end{cases} \quad (3)$$

In order to simplify the analysis we will introduce a number of $n+2$ auxiliary binary functions. The first of them are

$$T_{a_i} = a_{i1} \cdot a_{i2}, \quad (4)$$

where $i = 1, 2, \dots, n$.

In reliability perspective these functions denote functioning or failure of the equipment at the i -th end point. An other auxiliary function is $T_{m/n}$ for which is valid

$$T_{m/n}(T_i) = \begin{cases} 1 & \text{if } \sum_{i=1}^n T_i \geq m \\ 0 & \text{if } \sum_{i=1}^n T_i < m \end{cases}, \quad (5)$$

The reliability meaning of (5) is that at least m out of n chains of elements (at the respective end points) at the right side of the RBD have to be in workable condition for knot marked as “ m/n ” to become passable from right to left. Here m is the threshold level discussed above but its meaning is opposite to this in the fault tree. In RBD a complete system failure will be occurred when the number of end point branches in workable condition becomes equal to or less than $m-1$.

Following RBD the system function can be determined as

$$\varphi(a, T) = a_{01} \cdot a_{02} \cdot a_{03} \cdot T_{m/n} \quad (6)$$

This formula is suitable for a transition to reliability indices by direct substitution, but the function $T_{m/n}$ is still not determined by functions of elements.

For illustration of the approach to this we will study the simplest case, when $n=3$, and $m=2$, [2][6]. Then for the function $T_{2/3}$ is valid

$$T_{2/3}(T_i) = T_1 \cdot T_2 \cup T_1 \cdot T_3 \cup T_2 \cdot T_3 = 1 - (1 - T_1 \cdot T_2)(1 - T_1 \cdot T_3)(1 - T_2 \cdot T_3) \quad (7)$$

After transformations

$$T_{2/3} = T_1 \cdot T_2 + T_1 \cdot T_3 + T_2 \cdot T_3 - 2T_1 \cdot T_2 \cdot T_3 \quad (8)$$

Considering (4), (6) and (8) the system function can be expressed as

$$\varphi(a) = a_{01} \cdot a_{02} \cdot a_{03} (a_{11} \cdot a_{12} \cdot a_{21} \cdot a_{22} + a_{11} \cdot a_{12} \cdot a_{31} \cdot a_{32} + a_{21} \cdot a_{22} \cdot a_{31} \cdot a_{32} - 2a_{11} \cdot a_{12} \cdot a_{21} \cdot a_{22} \cdot a_{31} \cdot a_{32}) \quad (9)$$

As this expression is worked out upon the base of RBD which is success-oriented, it is suitable for transition to reliability indices by direct substitution of elements functions by its reliability functions $P_{01}(t)$, $P_{02}(t)$, $P_{03}(t)$, $P_{ij}(t)$. The result will be the reliability function of the entire system $P(t)$. For simplification the functions will be presented without “(t)”. Hence

$$P = P_{01} \cdot P_{02} \cdot P_{03} (P_{11} \cdot P_{12} \cdot P_{21} \cdot P_{22} + P_{11} \cdot P_{12} \cdot P_{31} \cdot P_{32} + P_{21} \cdot P_{22} \cdot P_{31} \cdot P_{32} - 2P_{11} \cdot P_{12} \cdot P_{21} \cdot P_{22} \cdot P_{31} \cdot P_{32}) \quad (10)$$

CONCLUSIONS

The star structure is typical for a large class of CES. For specific application of CES as SCADA systems this appears to be a basic one. Both fault tree approach and RBD approach are applicable to SSCES reliability analysis. They provide the analysis with different points of view to the CES reliability. An adequate set up of a threshold level (m) is of a high importance for correct estimation of the SSCES reliability indices in SCADA applications.

References

- [1] GEORGIEV A. Sl. New concept for increase in operative reliability of electronic systems. Monography, Aquaprint Ltd., ISBN 978-954-92824-6-7, Varna, 2013. (Bulgarian)
- [2] RAUSAND M. System reliability theory. John Wiley & Sons, Inc., ISBN 0-471-47133-X, New Jersey, 2004.
- [3] HRISTOV Hr., TRIFONOV, V. Reliability and security in communications. ISBN 954-9315-43-6, Sofia, 2005. (Bulgarian)
- [4] SVENSSON S., SPIRA, D. Framework to enable reliability analysis of SCADA solutions. Elforsk. 2012.
- [5] SCADA Systems. White paper. Motorola Inc. 2007
- [6] LLOYD E., LEDERMAN, W., Handbook of applicable mathematics. Volume 4. New York, 1997.
- [7] PETERSON L., DAVIE, B. S., Computer Networks: A Systems Approach, Fifth Edition, Elsevier, 2011.
- [8] GEORGIEV A., T. PAPANICHEV, D. KOVACHEV, Evaluation of Technical Condition of a Radar with Redundancy, International Journal of Engineering and Innovative Technology (IJEIT), Vol. 4, Issue 6, Dec. 2014, pp. 185-192, ISSN: 2277-3754