Analysis of Resilience of a Digital Substation Using an Event Tree

Irina Kolosok and *Elena* Korkina

Energy Systems Institute by L.A.Melentiev, Siberian Branch of Sciences, Irkutsk, Russia

Abstract. A digital substation is an example of a cyber-physical system that is a sophisticated system consisting of two closely interrelated subsystems: physical (technological) and information-communication ones. Sophistication and vulnerability of an information-communication subsystem that performs functions of management becomes comparable to those of a physical subsystem. In the latest years the studies have been focused on the problems of cyber attacks against information-communication subsystems as potential external disturbances of present-day cyber-physical systems. Resilience is ability of an informational system to survive in the conditions of continuous cyber attacks. The proposed here approach to assessment of digital substation resilience using an event tree can serve as expert's assistance in ensuring the digital substation resilience.

1 Introduction

A substation is a unit for the process control in the Russian Federation National Power Grid. An electric substation (SS) is a facility within the electric power system (EPS) that is intended for power reception, conversion and distribution. It consists of transformers and other power converters, control devices, switchgears, and auxiliary devices. The main functions of a substation include process-related communication and data transfer; relay protection and automatic (RPA) equipment; control over automatic protective devices; automatic process control system (APCS); power consumption accounting using an automatic system for commercial accounting of power consumption. Until recently RPA and APCS of a substation dwelled on the facility independence and isolation, which ensured reliability of communication within a substation and facilitated the use of internal protocols.

Transition to automation and control systems for a substation of a new generation is performed based on the standards and technologies of a digital substation (DSS). They include IEC 61850 Standard, intelligent electronic devices, digital metering transformers, and data transfer using fiber optic. IEC 61850 Standard covers the relay protection systems engineering, substation control and management, as well as development of secondary circuits of substations. A peculiar feature of DSS is data transfer via a specifically adjusted network with Ethernet packages switching (a process bus and station bus), which allows use of digital communication between electronic current/voltage transformers or merging devices, and such connecting devices as protection relays, controllers and power meters on the connected lines.

The process of computer resources integration into physical facilities within implementation of the "Cyber-Physical System" (CPS) concept has the following peculiar features:

- High degree of computerization, data exchange via a network, including via Internet;
- Availability of an automatic control center that ensures systems independence and reduction of their dependence on the operator;
- Control of physical components using controllers, and integration of a technological process with adaptive control;
- Robustness under disturbances and at cyber attacks.

A digital substation is a typical example of a Cyber-Physical System. It is obvious that any cyber attack causes certain damage to a Cyber-Physical System and timely analytical approach to CPS cyber security enhancement is a prerequisite of DSS normal operation. With introduction of IEC 61850 Standard, all the data of the upper automation level of SS may become targets of cyber attacks, should appropriate measures be not taken. Data transmission via Ethernet network using a process bus and a bus of a substation raises DSS vulnerability to cyber attacks as security threats for a 'conventional' substation (software or equipment failure, low competence of personnel) are complemented by threats of interference into the bus operation and into time synchronization process.

Under the impact of factors aimed at destabilization of normal operation, DSS shall remain robust even in case of partial functionality loss. Section 2 considers issues of informational security and resilience of energy facilities. Section 3 uses an event tree technology for

understanding the DSS processes. Results of studies are summarized in Section 4.

2 Informational security of CPS. Cyber security.

There have been a sufficiently large number of cyber attacks on energy facilities. Data attacks are the most common group of cyber attacks threatening the energy system security [2]. There are three main types of attacks on the data: False Data Interference (FDI), Load Redistribution Attacks (LRA), and Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks. FDI attacks on the optimum power flow module (OPF) may cause transmission line overloading, interruptions in power supply, and physical damage of EPS equipment. There are two approaches to LRA attacks: immediate (maximization of ES procedures cost right after the attack) and delayed (gradual overloading of transmission lines to maximize cost of operations at a certain time after the attack). DDoS attack is initiated by several attackers simultaneously such that suspension of actions of one attacker does not stop the attack and it is practically impossible to distinguish between technological and adverse requests for servicing.

The existing methodology for ensuring the informational CPS security is based on the conventional protection means for cyber attacks detection. They include security analysis of the network infrastructure, means for detection of adverse software, etc. Security of sophisticated commercial cyber-physical systems can be ensured by control over access to finite devices and detection of malfunctions by analysis of messages from terminal devices. Present-day facilities use a number of cyber security measures. From the technical standpoint they are firewalls, virus-protection programs, installation of licensed hardware and software, etc. From the standpoint of personnel discipline it implies strict observance of guidelines on access to the local network of an energy facility, veto on entering the external network and on use of external information storage medium that have no relation to production activity, etc.[3].

In the latest years the studies have been focused on the problems of cyber attacks as potential external disturbances for information-communication subsystems of present-day CPS [2,4,5, et al.]. For analysis of CPS ability to resist cyber attacks and recover after them the term 'resilience' has been offered. The most thoughtful interpretation of 'resilience' term is given in [6] where it is defined as a property of a system to withstand any changes or interrupted events by reducing their initial negative impact and mitigating the consequences for the system (absorbing capacity), self-adaptation of a system to those changes and events to mitigate consequences (adaptation capacity), and system recovery by appropriate controlling actions in the minimum time possible (recovery capacity). According to [7], resilience is a property of an informational system to survive in the conditions of continuous cyber attacks.

Depending on the adaptation, self-organization and recovery capacity, different options of recovery are possible: 1) by mode that does not differ from the pre-fault state (robust behavior); 2) incomplete recovery with weakened mode parameters (flexible behavior); 3) transition to a non-operable state (destructive behavior); 4) with mode parameters exceeding the pre-emergency condition (recovery with adaptation). Ref. [6] presents a time graph (Fig. 1) of productivity decline options of some system under the impact of destabilizing factors, and productivity recovery under availability of certain capabilities (technical, functional, organizational, etc.).

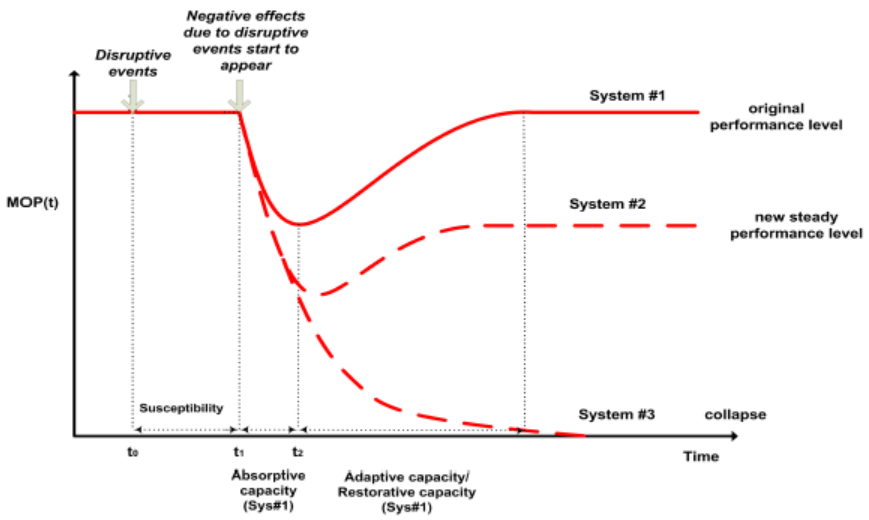

Fig. 1. Main regularities of robust and non-robust behavior of the system [6].

Thorough analysis of threats to an informational system allowed the equipment designers and manufacturers to develop a number of approaches to DSS resilience enhancement. Thus, Ref. [8] offers a cluster principle in the DSS structure that provides for: functional backup; backup with degradation; a displacement reserve, when a

high-priority function replaces low-priority one, and others. For cyber security of DSS hardware and software, Ref. [9] prescribes strict observation of communication security protocols; use of basic components of the information system of Russian manufacture only (microchips of a central processor and a controller of periphery interfaces, a basic input/output circuit, an operational system, application software); advanced testing of coding and cryptoprotection algorithms in-built into every intelligent device, RPA terminals, and interface devices for their adequacy to RF GOSTs (State Standards). Technological abilities of microprocessor devices of RPA shall allow their control from a dispatching center and from a Network Dispatching Center [10]. Ref. [11] ascertains that higher transfer capability of a process bus, IEC 61850-9-1 Protocol and a fiber optic link can ensure 100% cyber security.

Study of resilience of an information-communication-technological system (ICTS) of a corporate network is given in monograph [12]. For the purpose of study a number of cyber attacks (Technical Computer Intelligence (TCI), intrusion of adverse software, information theft and destruction, denial of service (DoS), re-direction of the network traffic) are presented as cyber-threat trees. Modeling of the listed above cyber attacks allowed their rating and assessment of vulnerability of all the valuable ICTS components to those cyber attacks. RAM memory of personal computer/DB servers/Email servers/web-servers turned out to be most vulnerable to TCR attacks and intrusion of adverse software, whereas a switchboard (its MAC address, ports, commutations matrix) are most vulnerable to DoS cyber attacks.

Detailed description of cyber attacks types and analysis of ICTS components vulnerability allowed us to conclude that mechanisms of cyber attacks on any facility with similar hard- and software and similar system of information subsystem control are identical. Therefore, an information system of a digital substation can be subjected to cyber attacks similar to those described in [12]. DSS productivity level under the effect of negative factors will be declining but can be recovered, should there be appropriate protection means.

As to recovery of CPS workability, Ref. [13] considers four states: pre-emergency – emergency – recovered – predicted ones. Emergency CPS state may be caused both by failure of a physical component, and of a cyber component. Unlike a physical component whose workability has two features (operable/non operable), a cyber component is additionally characterized by a new state, namely, by 'delay', i.e., a cyber component itself is in operable state, but data transfer is delayed, which leads to failure of other CPS components.

Ref. [14] considers three modes of CPS cyber security: normal mode (control of all the physical and logical connections to an information network); emergency mode (automatic transition to the mode of workability maintenance of the main components of an information network of a control system under loss of secondary functions); recovered mode (return of a control system to initial state). In case of cyber incidents, they propose to adhere to the concept of controlled degradation of a control system that consists in what follows. For enhancing the resilience of present-day informational systems of automation and control they have excessive functional redundancy that can be partially neglected in the conditions of attacks. Term 'degradation' implies temporary return to positions of lower functionality to secure the main functions: first degradation level means disconnection of a secondary system (that is not responsible for technological process) from the local network, and segmenting the local network for narrowing the medium of cyber attack development; second level of degradation is independent mode of RPA microprocessor devices; and, in case of heavy incidents it implies manual mode of control.

Fig. 2 (similarly to Fig. 1) gives a schematic diagram of differences in approaches [13] and [14] in terms of period of impact of destabilizing factors affecting the extent of DSS functionality loss, and period of impact of factors contributing to its recovery at cyber attacks..

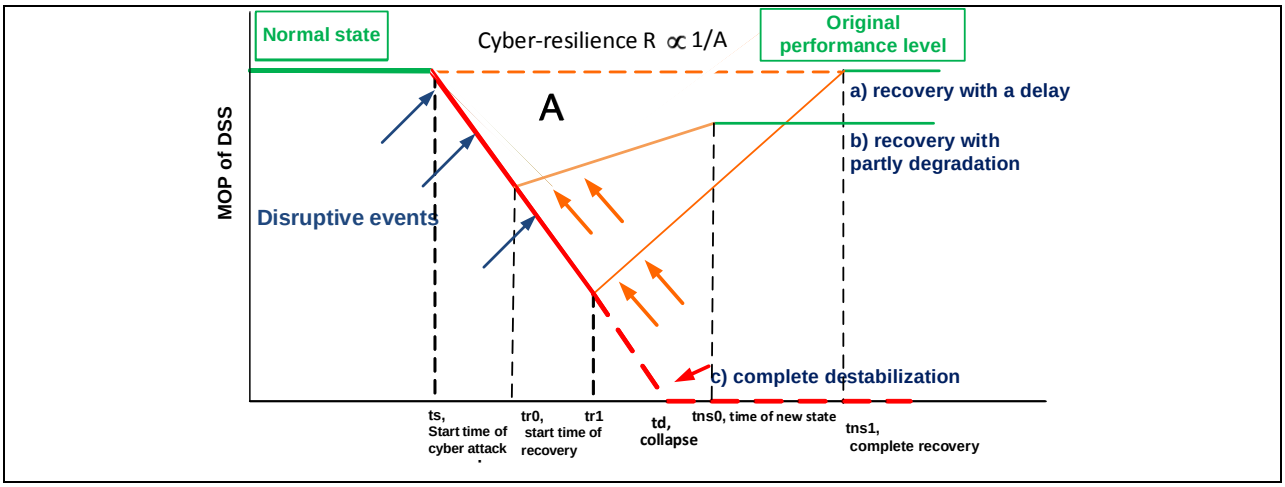

Fig. 2. DSS resilience: a) recovery with a delay [13]; b) recovery with degradation [14]; c) complete destabilization [13].

Industry's requirements to a local computing network become more severe while APCS takes over a larger scope of functionality and data loss may case heavy consequences. For example, if data from sensing devices do not timely come to RPA terminal, it may cause short circuit propagation to adjacent sections of an electric network that would cause more severe losses than those in case of timely disconnection of a sort-circuited section. For this reason the energy projects often pose a requirement of "Recovery time less than 1 ms". Relative to the above said, development of events [13] may follow two different scenarios: a) or c) (Fig. 2)

3 Analysis of resilience of a digital substation using an event tree

Object stability under the effect of destabilizing factors is defined based on cause-effect chains of arguments complemented by probability characteristics [15]. A cyber attack is a cause that may lead to different consequences for the energy facility under consideration.

Construction of an event tree is a graphic method of monitoring the sequence of events leading to an unfavorable outcome. A tree trunk (an incident) is in the left-hand part of the figure. Tree branches are possible ways of the incident consequences development. Every technical system has elements of protection, i.e., methods, devices, attachments securing the system from emergencies and catastrophes. After an incident the event to follow either occurs or does not occur, depending on the operation or failure of protecting elements of the system. Upper tree branches reflect development of events under protection operation. Those are branched of actuation. Lower branches are branches of failures.

Fig. 3 presents a tree of events for a remote reconnaissance cyber attack [12] that undertakes an effort of penetrating into some information system starting from searching for technical documentation on the system configuration. If documentation is accessible, an attacker may use it for preparing a real attack on the network. If documentation is not accessible, the attacker starts 'eavesdropping' the network in order to identify addresses of network devices (topology), location of routers and switchgears (network scanning), and types of the data transfer protocols.

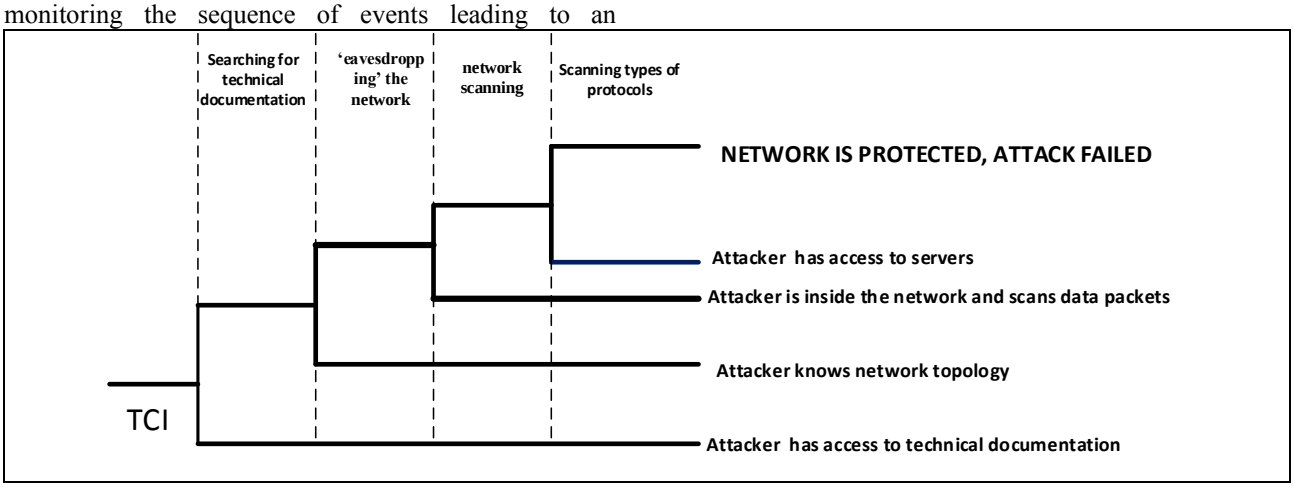

Fig. 3. An event tree for a cyber attack "Technical Computer Intelligence" (TCI).

DSS productivity depends on the failure-free operation of both physical components (relay protection and automatic (RPA) devices; automatic protective devices; teleautomatic and synchronized vector measurements, recorders of emergencies) and on information-communication components (a data acquisition and transmission system, an automatic system for commercial accounting of power consumption, an automatic process control system, communication and channel equipment, server equipment, software of different purpose). In order to get the DSS resilience curve similar to that in Fig. 1, resilience of separate DSS components can be preliminarily analyzed using an event tree. If statistical data on failures due to cyber attacks are available, then the numerical information can be presented on the 'Productivity' axis. Numbers in Fig. 4 have been taken arbitrarily.

As a result of TCI cyber attack (Fig. 3), five outcomes are possible, but the attack failed in one case only, whereas in four other cases the intelligence objectives of an attacker were a success. Let us take two extreme cases out of those five: "Network is protected. Attack failed", and "Attacker possesses documentation". Now we draw envelope curves and color them green and red, accordingly (Fig. 5).

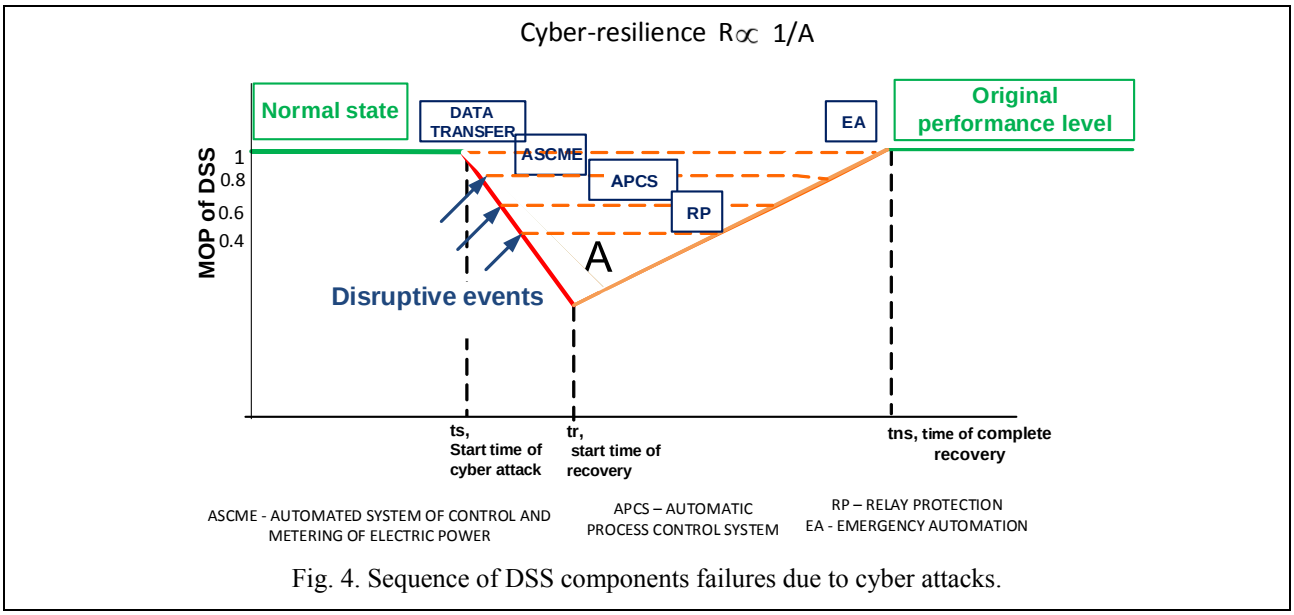

Fig. 4. Sequence of DSS components failures due to cyber attacks.

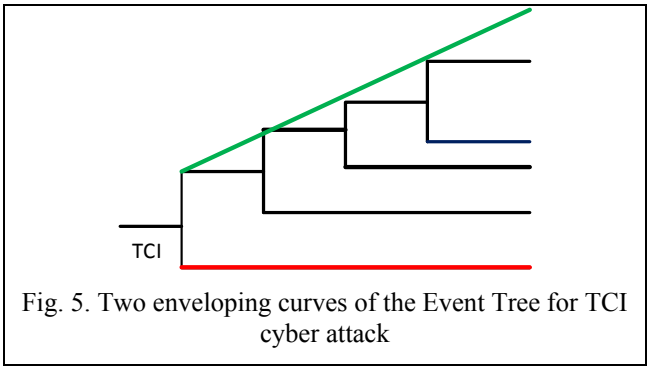

Fig. 5. Two enveloping curves of the Event Tree for TCI cyber attack

Preliminary conclusions on the impact of destructive factors can be made under the lack of numerical information. For that purpose a graph with enveloping curves of TCI cyber attack overlaps the DSS resilience graph (Fig. 6), and an enveloping curve corresponding to the failed attack means that the system is resilient. Therefore, it is advisable to align its direction with a line of normal DSS productivity. Then the second enveloping curve that means a successful attack shows a trend of DSS productivity decline

.

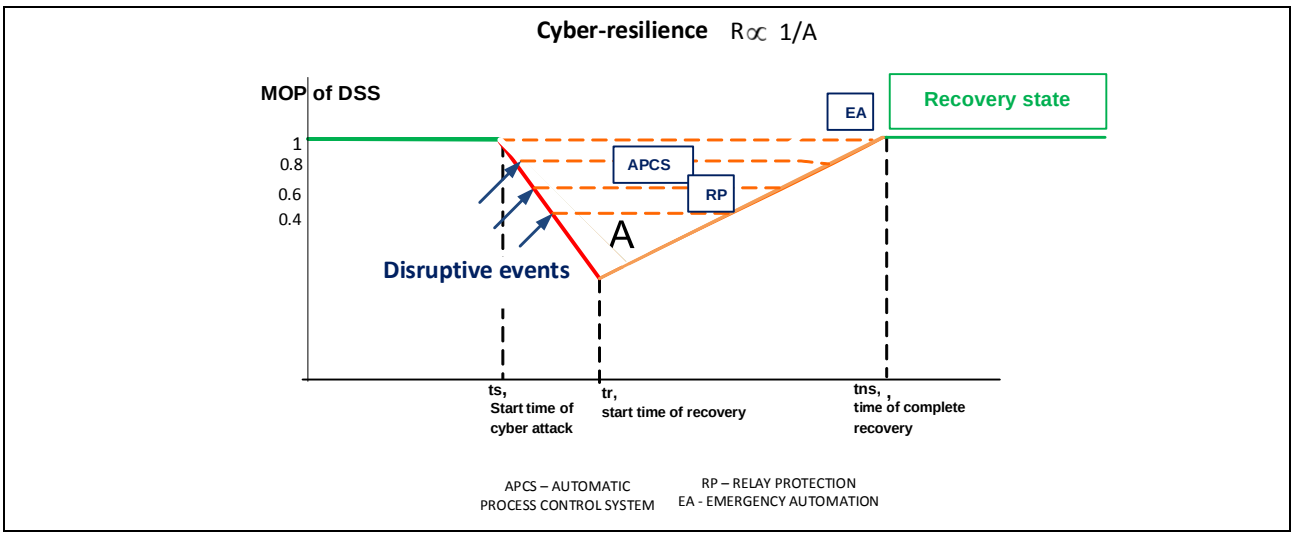

Fig. 6. An Event Tree on the DSS resilience graph for TCI attack

How the extent of threats to DSS cyber-attacks can be estimated? Scaling the calculations of undertaken cyber threats given in [12], we can demonstrate the extent of effect of some or other attacks on DSS operation. A temporary productivity decline curve (Fig. 1) is proposed to be presented by two separate but interdependent curves, the first one being a cyber subsystem (ICS), and the second one - a physical (technological) one (Fig. 7).

Figure 7 shows that intelligence cyber attacks (started at the moment ts1) have no effect on the DSS technological process. But from the moment td2 any subsequent cyber attack (intrusion of adverse software, information theft and destruction, denial of service (DoS), re-direction of the network traffic) to some or other extent reduce the productivity of automatic DSS operation to the extent of DSS failure.

.

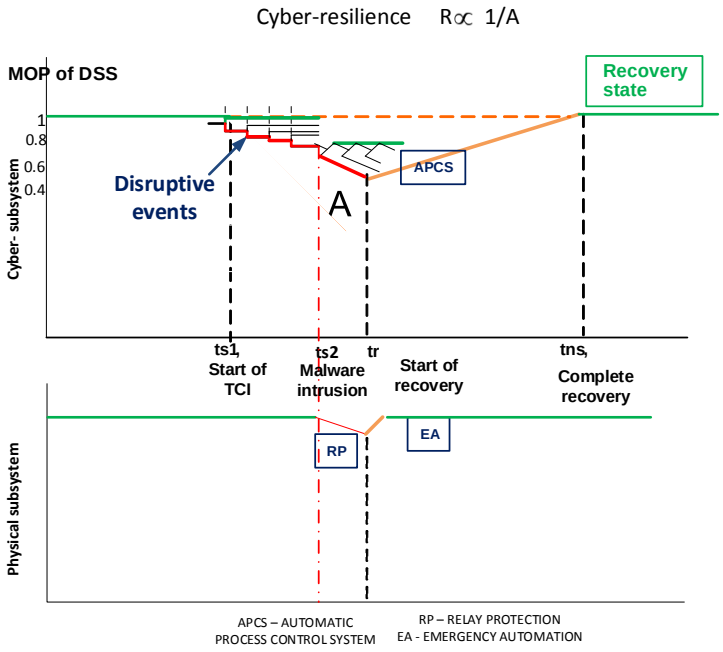

Fig. 7. Interdependence of destabilizing processes in the cyber and physical subsystems.

4 Conclusions

Lack of a complete set of components of DSS technical solutions, experience of engineering, adjustment and operation, do not give grounds for DSS projects replication. Numerical indicators of failures of physical components due to cyber attacks can be obtained during cyber attacks modeling, since there is no official statistical data. A real base for assessing the DSS resilience is division of its cyber-physical structure into layers. The proposed here approach to DSS resilience assessment using an event tree can serve as expert's assistance in ensuring the DSS resilience.

References

1. I. Kolosok, E. Korkina. Analysis of resilience of a digital substation using an attack tree. Releishchik, **2** (2018)
2. S. Mehrdad, S. Mousavian, G. Madraki, Yu. Dvorkin. Cyber-physical resilience of electrical power systems against malicious attacks: A review. // Current Sustainable /Renewable Energy Reports, https://doi.org/10.1007/s40518-018-0094-8 (28.06.2018)
3. N. Voropai, I. Kolosok, E. Korkina. Problems of enhancing the digital substation resilience. Relay protection and automatic equipment, **34**, 1 (2019)
4. I. Kolosok, E. Korkina, L. Gurina. Reliability analysis of results of state assessment using PMU data at WAMS cyber attacks. (Methodological issues of studying reliability of large energy systems. Vyp. 66 Minsk: BNTU, 2015).
5. B. Papkov, A. Kulikov, V.Osokin. *Cyber threats and cyber attacks in electric energy industry.* (Nizhny Novgorod: NIU RANHiGS, 2017).
6. C. Nan, G. Sansavini, W. Kröger, and H.R. Heinimann. A Quantitative Method for Assessing the Resilience of Infrastructure Systems. PSAM (2014).
7. A. Lukatsky Cyber resilience and cyber survivability, cyber robustness, cyber continuity. https://www.securitylab.ru/blog/personal/Business_without_danger/342751.php (12.03.2018)
8. M.A. Vlasov, A.S. Kirillov, A.A. Kuzmin, A.E. Nazarovskiy, S.A. Peregudov, A.A. Serdtsev. Cluster digital substation with flexible dynamic architecture. (The International Conference "Digital substation. IEC 61850 standard" Moscow, 2017)
9. A. Kulikov, V. Zinin, A. Petrov. Cyber security of a digital substation in the "Digital Substation" technology with account of import substitution. (Relay protection and automatic equipment for energy systems, St.-Petersburg, 2017)
10. A. Ivanchenko. Management and maintenance of substations of National Power Grid. (Energetik (Annex). -M.: Energoprogress, 2018).
11. F. Levshin, M. Shurdov. Cyber secure DSS. Elektroenergiya. Transmission and Distribution. **4** (2018)
12. M. Kotsynyak, I. Kuleshov, A. Kudryavtsev, O.Lauta. Resilience of an information-communication network. (SPb: Boston-spektr, 2015)

13. D. Obychaiko, V. Shikhin. Development of a combined method for assessing the operating reliability of cyber-physical systems. (Proc. of XI All-Russia Conference “IT in power engineering”, 2018)
14. M.V. Nikandrov, L.A. Slavutsky, D.V. Suslov, I.G. Nazarov. A complex for ensuring the controlled degradation of a control system of an energy facility at cyber attacks. (Proc. of XI All-Russia Conference “IT in power engineering”, 2018)
15. Horia-Nicolai L. Teodorescu. Defining resilience using probabilistic event trees. sci-hub.se/10.1007/s10669-015-9550-9.