Toward Safety of Systems of Systems — an Entropic Approach

Thomas V. Huynh

Department of Systems Engineering
Naval Postgraduate School, Monterey, CA

E-mail: thuynh@nps.edu

ABSTRACT

Leveson [1] put forth an assumption that “systems will tend to migrate toward states of higher risks,” and “such migration is predictable and can be prevented by appropriate systems design or detected during operations using leading indicators of increasing risk.” Demetrius and Manke [2] establish that network entropy is positively correlated with robustness. In this work, we use this positive entropy-robustness correlation and the risk growth rate introduced herein to validate the assumption by establishing that lower entropy corresponds to higher risk and that a system or a system of systems will tend to migrate toward states of lower entropy. Our exploratory work can form a basis for the development and implementation of safety measures (to prevent higher risk) for systems of systems operations.

KEYWORDS: System safety; robustness; network entropy; fluctuation rate; risk growth rate; similarity; systems of systems.

1. INTRODUCTION

A current research area of interest is the development and implementation of safety measures (to prevent severe risk of losses — human or systems) for systems of systems (SoS) operations. An SoS is a composite system that is comprised of component systems that are interconnected to fulfill the unique purpose of the SoS; each of the component systems serves organizational and human purposes and may be locally managed and optimized independently, or nearly so [3-5]. By SoS operations it is meant the collective and collaborative executions of tasks by the component systems of the SoS.

An SoS can be represented as a network with its component systems (or constituent elements) as nodes connected via links representing their connectivity [6, 7]. The nodes can be connected by physical or logical means and can communicate with each other. Network connectivity is realized by the connections of the nodes and thus affected by the success or failure of their connections. Two connected nodes are said to be interoperable with each other if they effectively interface with each other (i.e., to effectively exchange and process information and data and to effectively execute established procedures and rules). Network interoperability is realized by the interoperability of the nodes. Two nodes of a network are said to be similar if they are connected and interoperable with each other. They are rendered dissimilar if any factor, operational or environmental, adversely affects their connectivity and/or interoperability.

The concept of nodal similarity is related to the similarity principle for an SoS (stated in Section 5), which is an extension of the Similarity Principle for a mixture of chemical species [8]. Not only does the work in [8] inspire the development of a general methodology to derive requirements on architecting an SoS to provide sustainable delivery of value [9], but it also encourages an investigation of a connection between SoS safety and its entropy. As discussed later in this paper, the concept of similarity of the components of a system, the component systems of an SoS, or the nodes of a network is related to the safety of the system, SoS, or
network and to the entropy of these entities. Hereinafter, the component systems of an SoS and the nodes of a network are synonymous and thus used interchangeably.

When a system or an SoS is in a state in which it is free from the risk of self-damage or injury to people and property, then the system or SoS safety is said to have been achieved [10]. A system is in an unsafe state if it has a high probability of being subject to such a risk. During the operation of a system or an SoS, it is desirable or sometimes necessary to detect its unsafe states of the system (using “safety detectors” as opposed to “unsafety detectors” coined by Ning et al. [11]) so that certain measures can be taken in advance to prevent it from reaching unsafe states. Furthermore, to maximize the probability of a system, product, or an SoS being safe, it is also necessary to design safety into it from the beginning, including designing and implementing these safety detectors. (A future paper will address system safety design and implementation.) The “safety detectors” do not have to be only physical. They can also be logical, in the sense that outputs from them point to an impending disaster to an SoS itself as well as to others external to it. An example of such output is SoS or network entropy.


Our work is inspired by the work in [8], Leveson’s treatment of system safety [1], the work on complexity and demographic stability in population models by Demetrius et al. [16], the work on a class of robust networks by Aldana and Cluzel [17], and the work on robustness and network evolution by Demetrius and Manke [2]. In the latter, the network entropy characterizes the structure and ergodic behavior of a dynamical system operating on a network. It is found to be positively correlated with robustness. Furthermore, maximal values of entropy arise as robustness increases, and minimal values of entropy arise as robustness decreases [2].

A robust system is one which performs in an acceptable manner in the presence of expected variations in certain parameters as well as unexpected variations in unknown parameters [18]. When the robustness of a system or an SoS diminishes, resulting ultimately in its fragility and hence in a high risk state, the system or SoS moves toward a state of being unsafe. In a new paradigm of system safety, Leveson [1] enunciates a new assumption that “systems will tend to migrate toward states of higher risks,” and “such migration is predictable and can be prevented by appropriate systems design or detected during operations using leading indicators of increasing risk.”

In this paper, focused on system safety and entropy, we validate the assumption by proving that lower entropy corresponds to higher risk and that an SoS (or network) and systems will tend to migrate toward states of lower entropy. (In a future paper we will address the question as to what are some leading indicators, if any, to warn of increasing risk of a system of systems in operation.)

Toward this goal, we represent an SoS as a network and define its connectivity and interoperability; apply the concept of nodal similarity; connect network (SoS) safety to network entropy; make use of the positive correlation between network entropy and network robustness; invoke the Similarity Principle to establish a corollary for systems; and finally convert Leveson’ assumption to two propositions.

The rest of the paper is organized as follows. The concept of nodal similarity is elucidated in Section 2. Section 3 captures the 1994 U.S. air-to-air friendly fire accident [1] and points out
dissimilarity of the participants. Section 4 discusses network entropy and robustness; the result in this section underlines the establishment of the propositions. Section 5 discusses network entropy as it is related to the Similarity Principle [8]. Section 6 captures the main result, namely, the establishment of the propositions and the corollary. The paper then ends with some concluding remarks.

2. SIMILAR NODES IN A NETWORK

In this section, we represent an SoS (in fact a system as well) as a network, briefly discuss the quantitative aspect of network connectivity and interoperability, and elucidate the concept of similar nodes in a network. A detailed elaboration of the quantitative aspect of network connectivity and interoperability can be found in [6, 7].

Consider a network in which every pair of nodes is assumed to be connected with some probability of connection. The mean number of links supported by a node of the network is then a measure of connectivity of the network. It is also known as the average degree of the network [19, 20]. The interoperability measure of the network is defined as the mean number of interoperable nodes in the network.

Two nodes are said to be similar if they are connected and interoperable with each other. They are rendered dissimilar if any factor, operational or environmental, adversely affects their connectivity and/or interoperability. Two factors that can affect nodal similarity are nodal behavior (component system behavior) and nodal interactions. A node becomes dissimilar if it interacts in a dysfunctional manner with the nodes to which is it connected — for example, if it fails to communicate with those nodes (e.g., via communication channels) or if it fails to exchange accurate information with those nodes for a successful execution of a task. Parenthetically, the phrase ‘dysfunctional interaction’ in the system safety context is coined by Leveson [1]. Likewise, a node also becomes dissimilar if its behavior (referred to in [1] as failed physical process) or action is not rule compliant or detrimental to the safety of others or its own — that is, it violates safety constraints as referred to in [1]. Numerous instances of safety-constraints-violating nodal behavior and dysfunctional interactions are exhibited in the 1994 U.S. air-to-air friendly fire accident discussed in Section 3.

3. U.S. AIR-TO-AIR FRIENDLY FIRE ACCIDENT

This air-to-air friendly fire (FF) accident involving U.S. aircraft is treated in detail in [1]. The information pertaining to this accident that is used in our work comes entirely from [1]. The purposes of discussing this accident are to (i) illuminate the concept of nodal similarity or dissimilarity, (ii) use it as a concrete example to demonstrate that the network or SoS entropy decreases as the SoS moves toward unsafe states, and finally (iii) suggest a need for safety detectors.

On April 15, 1994, while patrolling the Tactical Area of Responsibility (TAOR), which is the Iraqi territory above the 36th parallel, two U.S. Air Force F-15s shot down two U.S. Army Black Hawk helicopters, mistaking them for Iraqi Hind helicopters, killing 26 people (15 U.S. citizens and 11 others) onboard the Black Hawks. Whereas the Operation Provide Comfort (OPC) structure as an SoS is extensive, for the purpose of illustration we focus on a reduced OPC SoS shown in Fig. 1. We refer to this reduced SoS as the network. It nodes are the Mission Director, Airborne Warning and Control System (AWACS) with its members, the F-15s/Pilots and Black Hawks/Pilots.
pilots, and the Black Hawk pilots. The links or interactions among these nodes are shown by the solid double-headed arrows. The dashed double-headed arrow implies a link that should have existed via communications channels but did not actually exist because of adverse environmental factors and a flawed control structure.

As pointed out in Section 2, a node becomes dissimilar if its behavior violates safety constraints (called detrimental behavior hereinafter) and/or its interactions with other nodes become dysfunctional. In this FF accident, the detrimental behaviors of each node in Fig. 1, which are extracted from [1], are now enumerated. The F-15 lead pilot performed inadequate visual identification (ID) pass (no second visual ID pass); misidentified the Black Hawks as Iraqi helicopters (Hinds); did not conform to hostile alert; did not report to the Airborne Command Element (ACE), representing the commander in the AWACS; acted with undue haste; acted without ACE’s approval; did not wait for positive ID from the wing pilot; did not question vague response from the wing pilot; violated altitude restrictions; deviated from the mission to protect the AWACS; poorly adhered to radio discipline; and acted with a competitive motivation rooted in rivalry with F-16 pilots.

The F-15 wing pilot also poorly adhered to radio discipline; acted with a competitive motivation rooted in rivalry with F-16 pilots; performed inadequate visual ID pass; did not report lack of ID; continued to engage despite the lack of ID; used inaccurate models of helicopters; used an inaccurate model of the Rules of Engagement (ROE); and used an inaccurate model of airspace occupants.

The Black Hawk pilots entered the TOAR before sanitized; did not change to the TAOR frequencies; believed the Airspace Control Order restriction on entry into the TAOR did not apply to them; thought being tracked by the AWACS; and thought the AWACS using the Delta Point system (providing code names for real locations).

The Mission Director failed to issue command to cease targeting the Black Hawks; was unaware of the presence of the Black Hawks; and was unaware of the F-15s engaging an aircraft.

The ACE did not provide control commands to the F-15 pilots with respect to following the ROE and engaging aircraft; failed to issue command to cease engaging the Black Hawks; was unaware of presence of the Black Hawks in the TAOR; did not know what ‘engaged’ means; did not consider helicopters part of its responsibility; understood the ROE differently from the F-15 pilots; and thought the Black Hawks conducting standard operations in the Security Zone and had landed.

The AWACS members display behavior adverse to safety. The enroute controller did not tell the Black Hawk pilots to change to the TAOR frequencies. The enroute controller did not hand off control of the Black Hawks to the TAOR controller. The enroute controller did not monitor the course of the Black Hawks while in the TAOR. The enroute controller did not use the Delta Point system to determine the Black Hawks flight plan. The TAOR controller did not monitor the course of the Black Hawks in the TAOR. Nobody alerted the F-15 pilots before they fired that the helicopters they were targeting were friendly. Nobody warned the F-15 pilots that friendly aircraft were in the area. Nobody tried to stop the engagement. Nobody told the Black Hawk pilots that they squawked a wrong IFF (Identification Friend or Foe) code. The Mission Coordination Center (monitoring operations and operational control of the Black Hawk helicopters) did not relay information that was not on the Air Tasking Order about the helicopters during the morning briefing. The shadow crew was not monitoring activities. There was confusion in the AWACS over who was tracking the helicopters, the responsibilities of surveillance and weapon directors, and who had authority to initiate engagement. No one was assigned the responsibility for monitoring helicopter traffic in the No-Fly Zone. The helicopters were in fact thought to only go to Zakhu (in the Security Zone).

The dysfunctional interactions occurred at every level in the OPC control structure [1]. In this paper, only the following dysfunctional interactions confined to the reduced OPC SoS are mentioned. No Mission Director’s control commands were provided to the ACE. No report from the ACE was sent to the Mission Director. The AWACS provided inaccurate JTIDS (Joint Tactical
as it is related to network safety, is addressed in Section 6. As in [2, 16], the fluctuation decay rate, \( R \), is defined according to

\[
R := \lim_{t \to \infty} \left[ -\frac{1}{t} \ln P_\epsilon(t) \right]
\]

in which \( P_\epsilon(t) \) denotes the probability that the sample mean of the observable deviates by more than \( \epsilon \) from its unperturbed value at time \( t \).

As observed in [2], “large values of \( R \) entail small deviations of the observable from the steady-state condition and small values of \( R \) correspond to large fluctuations around its mean value.” Furthermore, as proved in [16],

\[
\Delta H \cdot \Delta R > 0
\]

where \( \Delta H \) and \( \Delta R \) describe changes in \( H \) and \( R \), resulting from a change in the network parameters. If \( R \) changes from a large value to a small value, i.e., the network changes from being stable to being unstable, its entropy decreases. That is, if \( R \) is getting small, then robustness is diminishing. Eq. 3 is known as the fluctuation theorem [16], which states, “The rate of decay of fluctuations to the steady state is positively correlated with entropy.”

5. ENTROPY AND THE SIMILARITY PRINCIPLE

In [8] Lin enunciates the Similarity Principle for a mixture of chemical species:

“If all the other conditions remain constant, the higher the similarity among the components is, the higher value of entropy of the mixture (for fluid phases) or the assemblage (for a static structure or a system of condensed phases) or any other structure (such as chemical bond or quantum states in quantum mechanics) will be, the more stable the mixture or the assemblage will be, and the more spontaneous the process leading to such a mixture or an assemblage or a chemical bond will be.”

The state of maximal entropy is the state of maximal similarity (or indistinguishability) [8].

An SoS can be viewed as mixture of the component systems [9]. Adopting the Similarity
Principle espoused by Lin [8], the similarity principle for an SoS enunciated in [9] is:

The higher the similarity among the systems of an SoS is, the higher the value of the entropy of the SoS will be, the more stable the SoS will be.

As a corollary (applied to systems),

A system (or an SoS) whose components (or component systems) cannot stay similar forever unless their deviations in time are rectified will tend to migrate toward lower entropy.

As discussed in Section 2, similarity of an SoS/network has to do with the similar ability of each system to perform in a safe manner. If the component systems migrate toward dissimilarity, the SoS migrates toward higher risk and its entropy decreases.

Although respectively arrived at from two different perspectives — Li’s Similarity Principle [8] and Leveson’s new paradigm of system safety [1], the corollary is equivalent to Proposition 2 stated in Section 6. Their proof is now provided.

6. ENTROPY AND SYSTEM SAFETY

As aforementioned, in a new paradigm of system safety, Leveson [1] suggests that “systems will tend to migrate toward states of higher risks” and, furthermore, “such migration is predictable and can be prevented by appropriate systems design or detected during operations using leading indicators of increasing risk.” Based on this suggestion (or “new assumption” as termed by Leveson [1]), we state the following propositions.

**Proposition 1.** Lower entropy corresponds to higher risk.

**Proposition 2.** Systems and systems of systems tend to migrate toward states of lower entropy.

As mentioned in Section 4, the observable of interest is the number of similar nodes in the network. Accordingly, \( P_t \), introduced in Section 4, is the probability that the mean number of similar nodes at time \( t \) deviates by more than \( \varepsilon \) from the number of similar nodes required for safe operations. Such deviations are indicative of risk of unsafe operations, and the rate of change of the deviations implies the rate of risk growth. Large values of \( R \) entail small deviations, hence a small rate of risk growth and a stable network. Small values of \( R \) entail large deviations, hence a large rate of risk growth and an unstable network. These correlations motivate the definition of the risk growth rate of the network, \( \rho \), as

\[
\rho := \lim_{t \to \infty} \left( -\frac{1}{t} \ln \left[ 1 - P_t(t) \right] \right). \tag{4}
\]

It follows from Eq. 2 and Eq. 4 that

\[
\Delta \rho \cdot \Delta R < 0, \tag{5}
\]

where \( \Delta \rho \) describes changes in \( \rho \).

Combined with Eq. 3, Eq. 5 yields

\[
\Delta H \cdot \Delta \rho < 0 \tag{6}
\]

in which, again, \( \Delta H \) describes changes in \( H \).

Thus, if \( \rho \) changes from a large value to a small value, the network entropy increases. That is, if \( \rho \) is getting small, then robustness is augmenting. Increasing risk corresponds to decreasing entropy. Eq. 6 thus implies that the rate of risk growth is negatively correlated with entropy. Proposition 1 is thus established.

The proof of Proposition 2 now follows. Assume each node in an \( N \)-node network can be in one of the two states (as defined in Section 2): similar (if its degree is at least equal to 1 and it is interoperable with the nodes to which it is connected) and dissimilar (if otherwise). That is, \( M = 2 \).

Suppose the \( N^{th} \) node is in a dissimilar state with a probability \( p_{N2} \) at some time \( t \) after the network operation begins at time \( t = 0 \). Then \( p_{N2} = 1 - p_{N1} \), where \( p_{N1} \) is the probability the \( N^{th} \) node is in a similar state at time \( t \). Then Eq. 1 can be written as
\[ H(t) = -\sum_{i=1}^{N-1} \sum_{j=1}^{M} p_{ij} \ln p_{ij} - p_{N1} \ln p_{N1} + (1 - p_{N1}) \ln(1 - p_{N1}) \]

\[ = -\sum_{i=1}^{N-1} p_{N1} \ln p_{N1} - (p_{N1} \ln p_{N1} + (1 - p_{N1}) \ln(1 - p_{N1})) \]

\[ H(t) = H_0 + (p_{N1} \ln p_{N1} + (1 - p_{N1}) \ln(1 - p_{N1})) < H_0 \]

where \( r_1 = r_2 = r \) for simplicity and \( s = 2e^{rt} - e^{2rt} \).

As shown in Fig. 2, with \( N = 10 \) and \( r = 1 \) per unit time, the network entropy decreases with time as the failing nodal behavior (component system behavior) and dysfunctional nodal interactions remain undetected and uncorrected. This example shows that the SoS and systems whose dissimilarity remains undetected and uncorrected tend to migrate toward states of lower entropy.

7. CONCLUSIONS

This exploratory work is part of our on-going research in the development and implementation of safety measures (to prevent severe risk of losses—human or systems) for systems of systems (SoS) operations. The principal result of this work is the establishment of the two propositions in Section 6 and the feasibility of using entropy (SoS entropy) as a metric for SoS or network safety assessment or tracking.

The significance of the result is that the SoS entropy (or any other entropy-based metrics) could be used as a leading indicator to aid in preventing safety collapse such as the air-to-air friendly fire accident.

Our on-going research investigates such leading indicators and the concept and the implementation of safety detectors and algorithms to process their outputs.

REFERENCES


