Drawbacks in Using the Term "System of Systems"

Nancy Leveson
Technical Report, System Safety Research Lab,
MIT
December 2012

A few years ago, a new term, "system of systems," was invented and has become quite popular. I've puzzled over this term because it doesn't make any sense to me with respect to systems theory and systems engineering. Let's start by reviewing some basic definitions in systems theory.

A system can be defined as a set of components that act together as a whole to achieve some common goal, objective, or end. The components are all interrelated and are either directly or indirectly connected to each other. The system state at any point in time is the set of relevant properties describing the system at that time. The system environment is a set of components (and their properties) that are not part of the system, but whose behavior can affect the system state. The existence of a boundary between the system and its environment implicitly defines inputs or outputs as anything that crosses that boundary.

It is important to understand that a system is always a model—an abstraction conceived by the viewer of the system. Systems and their boundaries do not exist in reality but only in the view of the beholder. One viewer may see a very different system than another in terms of where the boundaries are drawn, the relevant system properties and components, and even the purpose of the system.

Abstractions are useful in that they help humans deal with complexity. One useful abstraction in understanding complex systems is to view them as hierarchical structures. A model of a complex system can be conceived in terms of a hierarchy of levels of organization, each more complex than the one below. Each level of the hierarchy can be thought of as a system, which is made up of components at a lower level. Each of these components (or subsystems) can itself be made up of subsystems, and so on. Figure 1 shows a depiction of a system labeled A (level 1 of the hierarchy) composed of three subsystems A1, A2, and A3 at level 2 of the hierarchy, which of which is made up of other components (level 3 of the hierarchy). Note that the term "system" is recursive in that a subsystem is itself a system, which is made up of subsystems and so on. The difference is only at what level of the hierarchy ("granularity") the system is currently being viewed. The subsystems A1, A2, and A3, when viewed by themselves, is each a "system" with its own subsystems.

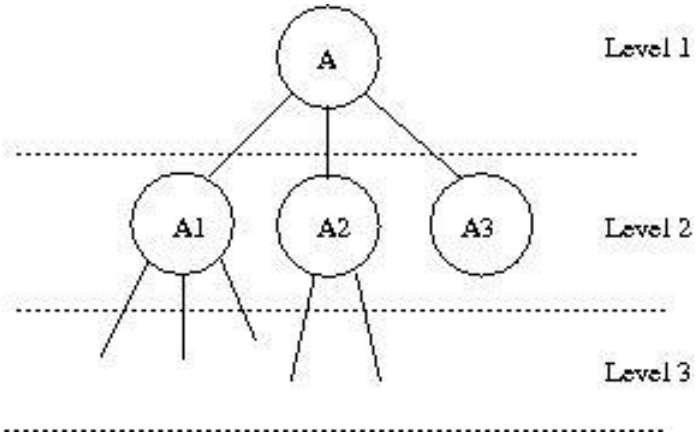

Figure 1: System **A** is composed of three subsystems **A1**, **A2**, and **A3**. Each of these subsystems may themselves be composed of other subsystems (components).

A system can also be viewed as part of a larger system. Figure 2 views system A as part (a subsystem or component) of a larger system AB, which has two components or subsystems A and B. There is no difference between considering AB as a system with components (subsystems) labeled A and B, or as a "system of systems" or a "system of subsystems" or whatever other term one wants to invent. All these terms are identical in what they represent and there is no need for a new term that seems to imply that it is a different thing and can or must be treated differently. I've heard people claim that the difference is that a "system of systems" is made up of already existing systems. But almost all systems are made up of existing subsystems. When creating a new system, rarely does anyone create everything from scratch, down to the screws and bolts. But even if they did, it does not negate the second basic concept in systems theory, which is emergence.

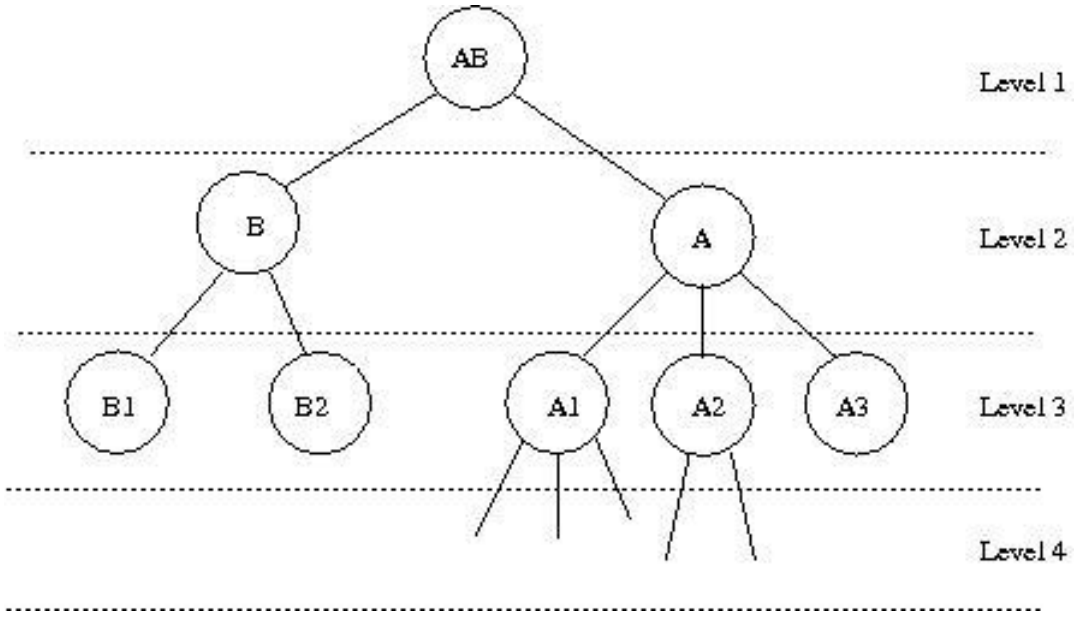

Figure 2: System A is here viewed as a component (subsystem) of a larger system AB

Each level of a system hierarchy is characterized by having *emergent properties*. The concept of emergence is that, at any level of complexity, some properties characteristic of that level (emergent at that level) are irreducible. They arise through interactions among the components at a lower level of complexity (a lower level of the hierarchy). Such properties do not exist at the lower levels in the sense that they are meaningless in the language appropriate to those levels. For example, the emergent property *shape* of an apple, although eventually explainable in terms of the cells of the apple, has no meaning at the individual cell level. As another example, consider the property of *gridlock* in traffic. Looking at an individual car, the concept of gridlock has no meaning. Gridlock as a property *emerges* only when the highway system is viewed as a larger system where many cars, along with a particular design of a roadway and other components of the highway system and its environment, interact. Emergent properties arise from the interaction of lower level components in the hierarchical system structure.

Now what does all this have to do with safety of medical devices? Safety is an emergent property. It is possible for individual system components to have hazards, for example sharp edges, flammable parts, or unsafe individual operation such as an infusion pump overdosing a patient. These hazards usually are not affected by putting these individual systems together into a system, although they could be.

But other hazards arise (emerge) only when components are considered together within a larger system where they interact either directly or indirectly. Analyzing the safety of only one individual component of that system does not and cannot consider the emergent safety problems (hazards) that arise when putting two or more components together. Usually, the hazards that need to be considered at the system level are different than those at the component level, but even if the hazards are the same, the causes are very different as the role of the interaction of the components comes into play as a potential cause of the hazard.

Let's consider some simple examples. The potential hazard of alarm overload can be associated with a single medical device but the problem arises in a different way when multiple devices, all with alarms, can sound at the same time or interfere with each other. The system level problem of alarm overload requires more than simply looking at an individual medical device or even several devices. It requires looking at all the devices that can sound alarms as well as considering the characteristics of the system components (probably humans) that must respond to the alarms and any ways that one alarm might interfere with another. As another simple medical example, a system-level hazard for a hospital patient might be a nurse connecting the wrong lines together, for example, connecting a feeding tube to an intravenous tube.[1] When considering only the intravenous feeding system, this hazard does not arise and, in fact, is not visible. It emerges only when all the lines into a patient are considered. System hazards exist only at the system level, although it is usually necessary to inspect the design of the individual system components to identify potential causes of the system hazards.

At the AAMI meeting on interoperability, I was surprised at the number of presentations that seemed to assume that safety analysis can be performed on individual components and then the components can be put together into a system that will be safe. Because safety is an emergent property, this assumption violates the most basic concepts in systems theory and systems engineering. This is where talking about "systems of systems" becomes dangerous because it somehow assumes that a "system of systems" is different than a system. It is not—the terms "system" and "system of systems" have the exact same meaning and the same top-down system engineering techniques have to be applied. Bottom-up approaches cannot be used to analyze or assure safety in a complex system, even if one calls it a "system of systems." Specifically, doing independent hazard analyses on individual components and then assuming those analyses can be combined in some way to handle system hazards will not be effective.

Consider an aerospace example[2], this time where the components interact with each other. Suppose a flaps control system communicates information to another aircraft system that uses the information provided by the flaps controller. That information is in the form of a variable (value) the flaps controller puts onto the data bus indicating whether the flaps are extended or not. Without understanding how the flaps controller determines whether the flaps are extended, the FLAPS EXTENDED word on the data bus could be interpreted in any of the following ways:

1. Both left and right trailing edge flap surfaces have been detected in the "1" or greater flap detent[3].

---

[1] It is surprising how often this occurs even though simple techniques to eliminate the problem were identified decades ago by the aircraft industry to eliminate wiring errors. The medical industry has resisted using these techniques.

[2] Gregg Bartley and Barbara Lingberg, Certification Concerns of Integrated Modular and Avionis (IMA) Systems, *27th Digital Avionics Systems Conference*, Oct. 26-30, 2008

[3] A detent is a device used to mechanically resist or arrest the rotation of a wheel, axle, or spindle.

2. Both left and right trailing edge flap surfaces have been detected **not** in the "UP" flap detent.
3. Flap Lever Handle detected in the "1" or greater flap handle detent.
4. Flap Lever Handle detected **not** in the "UP" flap handle detent.

All four of these possibilities may have different implications for the user of the variable. Baker provides the following examples: Once the trailing edge flaps begin to move, the logic that determines "flaps not in the UP position" will be satisfied almost immediately. In reality, however, the flaps may take five to ten seconds to fully reach the "flaps detected in the `1' detent" position. In addition, the FLAPS EXTENDED variable may also exhibit different characteristics during failure conditions. If the flap surfaces will not respond to a valid command due to a hydraulic system failure, for example, the *flap level position* will no longer reflect the true position of the flap surfaces once they are moved out of the UP detent.

The lesson is that how the signal is computed can have a major impact on the safety of the system as a whole when other system components use that signal and assume that it indicates the true state of the flaps at the time they receive the signal.

The users also assume that the component generating that signal does not change its logic (design). But what if it does? Let's say that the flap system designers discover a problem during flight test that requires a change in the internal logic that calculates a flight deck alert. They decide that one way to address this problem is to compute the FLAPS EXTENDED variable using the *flap lever position* instead of the actual *flap surface position*, which was the original design. Note that this change does not require any change in the actual interface between the two subsystems (the one generating the position indicator and the one using it): the content of the variable has not changed nor has the way the variable is transmitted on the bus. But the actual meaning of the variable is now technically different than it was before the change. The impact of this change on safety cannot be determined without being analyzed at the system and subsystem level.

To summarize, the change in one component of the system may impact the safety of the system when that component interacts with other components in the system. Merely calling this a "system of systems" and assuming these "systems" are independent and can be designed, analyzed, and changed independently does not solve the problem. Even when systems are composed of existing components, the need for an integrated system safety analysis remains. This fact implies more information is required about the design of the independent components than simply their external interfaces—in the case of the flaps position example, more is needed than simply the name and content of the shared or exchanged information.

Safety is a system property. It must always be analyzed top-down and for the system as a whole. When putting two or more existing components ("systems") together, the emergent properties must be analyzed for the integrated system. Calling that larger system a "system of systems" may be misleading by implying that emergent properties can be treated differently than any other system or different system engineering techniques can be used.