Eternal Systems (EtSy) - Ultra Large-Scaled(ULS-) Systems:

Eternal Systems run for ever - e.g. for repair, they cannot simply be switched on or off - and they surround us and our life every day.

The Notion of EtSy - also called Ultra-Large-Scaled Systems - in 2006 became invented by the DoD-study on ULS-Systems undertaken by the "Software Engineering Institute (SEI)" of the Carnegie Mellon University" [Pittsburgh PA 15213-3890].

SEI defines an ULS-System as a "system of systems", i.e. a "Socio-Technical Ecosystem (STE-System)" that requires "breakthrough research ... in design and evolution, orchestration and control, monitoring and assessment".

With the advent of the Cyber-Hyper Ventilation, EtSys are sometimes called Cyber Physical Systems, since they combine Physical Parts, e.g. Energy, Rail, with Cybernetic Parts, e.g. Data Sensor Networks, into an Integrated Hybrid System.

A better notion is the concept of 'Critical Infrastructures', that has been invented by [BMBF - German Ministry for Education and Research] and is called 'KRITIS', which comprises actually 8 combinations of physical systems with I&C Technologies, such as:

1. Nutrition Services Infrastructure;
2. electrical Energy Distribution Infrastructure, e.g. Smart Grid, Smart Metering Systems;
3. Information & Telecommunication Infrastructure, e.g. 3GPP, WiFi, ...
4. Health Care Services Infrastructure;
5. Transportation and Traffic Control Infrastructure;
6. Media, Social Communication & Culture Infrastructure;
7. Freshwater Services Infrastructure;
8. Finance & Insurance Services Infrastructure;

By the former definitions the system aspects are being focussed, i.e. systems are considered that adopt smart space technologies, in order to do its anticipated business better or to optimize certain aspects, e.g. to improve its performance, to scale its configuration with respect to changed requirements by using "knowledge" about computing, networking, distributing, transporting, managing (logistics) etc.

The EtSy Reference Model comprises three "Onion Peels", i.e. *stratospheres* of system constraints:

1. the most inner kernel strato is business oriented and comprises the stakeholders, business assets and goals to be safeguarded and achieved during doing business by actors of the system. (Notice: actors may operate on a platform. In that discourse the notion of system is synonymously used to the notion of platform.);
2. the intermediary strato is the embedding Eco Strato to the kernel and is constraint oriented. The Eco Strato embeds the business into lawful, social, safe, secure and privacy regulations and constraints;
3. the outer strato is implementation oriented, that provides the Man-Machine Interactions and interfaces (MMI) comprising hardware, software and firmware, i.e. the platform of operation.

From the EtSy Reference Model you may derive the observation that, e.g security, privacy, safety or other wishful system aspects is in-between of business and any implementing technology.

And indeed that is true! E.g. consider system security, as it is defined by [Security Evaluation.ETSI TVRA] that is measured by the effort of countermeasuring that has been taken into account to the anticipated level of vulnerability to certain system assets - in other words the "hardness of countermeasures" to fortify these assets against an attacker.

So, an attacker most-probably will use the outer strato, providing the MMI, to penetrate the system such that the attacker gains access to some of the kernel strato's assets.

However, system theory teaches us that any probed system is a System under Change (SuCh). A changing, i.e. an operating system is always vulnerable. Consequently and in order to secure the system it must be changed to a System under Control (SuCo) or at least under supervision.

A controlled system is less sensitive against unintentional "uncertainties" from the outer strato, but more sensitive against intentional countermeasures from the kernel strato's actors. The reason is that the outer uncertainties are unknown and as such simply "overlay" the output, i.e. the intentional behaviour of the actors but not their decision-takings at the input so-to-say.

Hence Systems under Control can make the difference between decision-taking by actors and the effects from decision-taking to somebody else or to a system service or component.

Speaking in terms of system engineering artifacts, then decision-taking is the input data to a steering component used by the actor, and the anticipated effects are the output data from the steering component fed into the system. Fortunately only the "output" is observable from outside strato, i.e. the attacker's strato as well.

Thus security testing means the adoption of the role of the "advocatus diaboli", i.e. the attacker's role, but not adopting of a role of one the business stakeholders!

Why Advocatus Diaboli role? Because it is assumed that the attacker is external to the system and thus not a decision-taking stakeholder from inside the system. So he can observe effects of decision-taking but he cannot take part of the internal process of decision-taking.

The latter is very important, because it means inside attackers cannot be defended at all! Inside attackers can destruct any - even a secured - system!

When decision-taking rooms, spaces or processes and decision-taking actors and the business assets of a system or enterprise are strictly be certified and security constraints be set, deployed and are enforced as well very strictly -->

Then the system can operate resiliently against attackers only overlaying with possible attacks of generating system penetration probes, testing the effects of decision-taking to the system. The latter must be strictly hidden to any outsider.

Consequently, the system never can be put under control by an attacker from outer strato, although it can be tested, or penetrated by probes!

An EtSy Reference Model dealing with an approach of a type of Security Architecture must be structured as follows:

1. the Outer Stratosphere System Components are observable at its input and output interfaces. The input to the system comprises "steering commands" in order to generate anticipated effects or results by that system. The system output is also called system state[1].
2. the User and Consumer Stakeholders' Environment - i.e. the Application - is strictly to be separated from the open system components by implementing the security notion of a Security Perimeter - as it is defined by the Common Criteria – surrounds the Application.
3. The Security Perimeter must include all Assets of strategic requirements, decision-taking and signaling, i.e. the operating business stakeholders, - the application's steering engine - to provide forward-control to the outer strato system components.
4. The application steering engine consists of a decision-taking component coupled with a signaling component; and finally a component that provides feed-back measurements of the system state in order to support application stakeholders in decision-taking, which closes the cycle of secured system control operation.

[1] The (Eternal) System ist - according to the Common Criteria – the Target of Evaluation (ToE), but is outside the control components of the Security Perimeter – since the System has open interfaces to everybody!