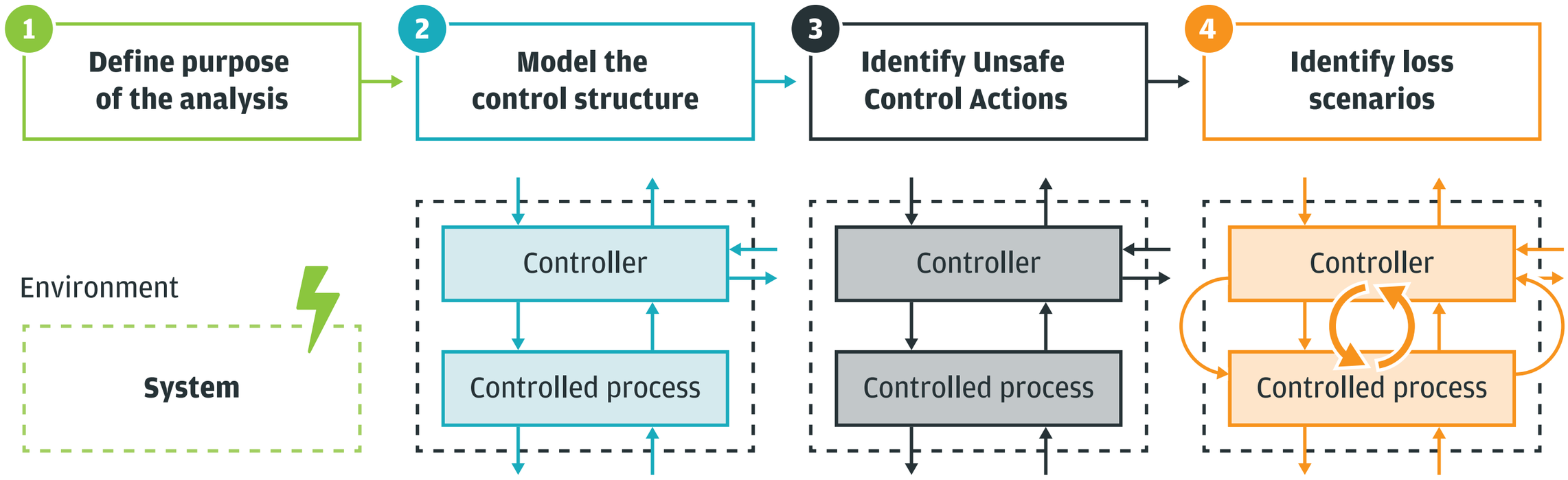
Elektrobit

System-Theoretic Process Analysis – Method overview



- Define system boundary
- Identify **losses**
- Identify **system-level hazards**
- Identify **safety constraints**

“A **loss** involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.”

“A **hazard** is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.”

“A **safety constraint** specifies system conditions or behaviors that need to be satisfied to prevent hazards (and ultimately prevent losses).”

- Model the **control structure**

“A hierarchical **control structure** is a system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behavior of the overall system.”

- Identify **Unsafe Control Actions**
- Identify **controller constraints**

“An **Unsafe Control Action** (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard.”

"A **controller constraint** specifies the controller behaviors that need to be satisfied to prevent UCAs.""

- Identify **loss scenarios**
- Identify scenarios in which control actions are improperly executed or not executed

“A **loss scenario** describes the causal factors that can lead to the Unsafe Control Actions and to hazards.”

elektrobit.com/consulting