Details of the Trustworthiness Calculator:

In this section we analyze the trustworthiness of a whole system made out by an arbitrary number of assets (components), each one characterized by its individual trustworthiness level for each quality attribute of interest. As we describe next, the attribute under investigation and the system structure are the basic parameters affecting the system's trustworthiness computation formula. This means that the exact formula to be used for each trustworthiness attribute will depend on the particular system structure. Thus the Trustworthiness Calculator will be able to identify whether the system can be represented as a series or a parallel structure and select the most appropriate formula for each attribute from the metric database. This will allow the System Trustworthiness Architect to test several structures and, if alternative components are available, examine several combinations of components for each structure. In this way she will be able to achieve the desired level of trustworthiness.

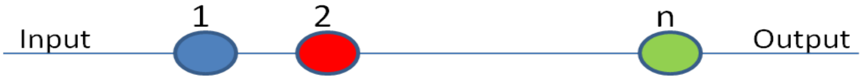
In what follows, we present the trustworthiness quantification for the *reliability* attribute and two fundamental structures, i.e., the series and the parallel sequence of components.

Let r_s , stand for the system's reliability, while r_i represents the reliability of each individual component "i", i.e. the probability that performs its required functions under stated conditions for a specified period of time. As described in D3.1, reliability is related to asset dependability.

Additionally, let $X = (x_1, \dots, x_n)$ stand for the components' state vector, with x_i denoting the state of component , i.e., $x_i = 1$ if component i functions and $x_i = 0$ in the opposite case. Following the notation above, $x_s(X)$ is the whole system's state with respect to the state vector.

Series structure: In this case, each component implements a different operation, meaning that the data flow (from left to right) results to the desired outcome, if and only if all the components work properly.

Graphically:



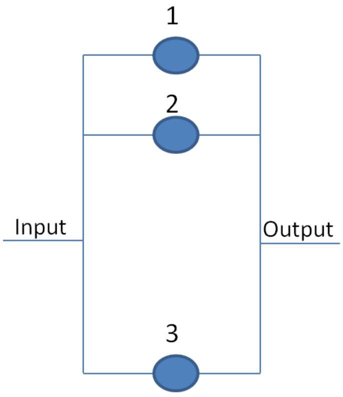
Thus the state of a system in series structure may be expressed as: $x_s = \min(x_1, \dots, x_n)$

and the computation formula for the its reliability attribute is as follows:

$$r_s = P\{x_s = 1\} = \prod_{i=1}^{n} r_i$$

Parallel structure: In this case, all the components implement the same operation, meaning that only one properly operating component is sufficient for the whole system to achieve the desired outcome.

Graphically:



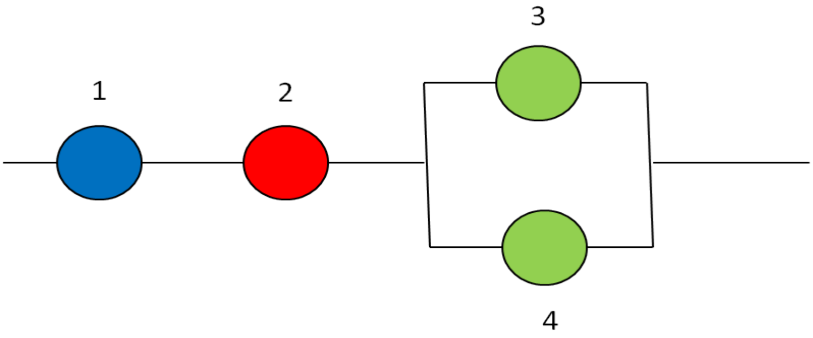
Thus the state of a system in parallel structure may be expressed as: $x_s = \max(x_1, \dots, x_n)$

and the computation formula for its reliability attribute is as follows:

$$r_s = P\{x_s = 1\} = 1 - \prod_{i=1}^{n}(1 - r_i)$$

Example: Combination of series and parallel structure over a four components system. This system works properly if components 1 and 2 and at least one of components 3 or 4 functions.

Graphically:



Thus the state of a system in this combinatorial structure may be expressed as:

$$x_s = \min(\mathrm{x}_1, \mathrm{x}_2, \max(x_3, x_4))$$

and the computation formula for its reliability attribute is as follows:

$$r_s = P\{x_s = 1\} = P\{x_1 = 1, x_2 = 1, \max(x_3, x_4, x_5) = 1\}$$

$$= P\{x_1 = 1\}P\{\, x_2 = 1\}P\{\max(x_3, x_4, x_5) = 1\}$$

$$= r_1 r_2[1 - (1 - r_3)(1 - r_4)]$$

The ***k* out of *n*** System: This kind of system functions properly, if at least k of the total n components are doing so ($k \le n$). Note that a series or a parallel system may be expressed as special cases of a k out of n system, where the series is the n out of n case, while the parallel the 1 out of n.

Example 1: In the case that all the components have equal reliability values ($r_i = r, \forall i$), then the reliability of the system is described by a binomial distribution, i.e.:

$$r_s = P(x_s = 1) = P\left\{\sum_{i=1}^{n} x_i \ge k\right\} = \sum_{i=k}^{n} \binom{n}{i} r^i * (1-r)^{n-i}$$

Example 2: The 2 out of 3 system in the general case of unequal reliability among the components.

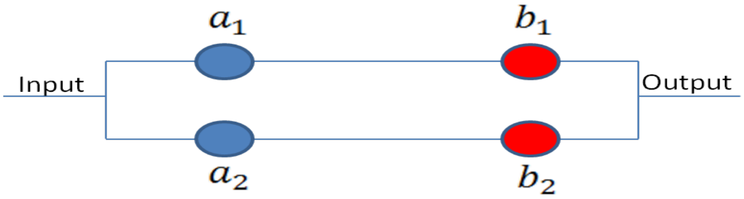
$$r_s = P(x_s = 1) =$$

$$P\{X = (1,1,1)\} + P\{X = (1,1,0)\} + P\{X = (1,0,1)\} + P\{X = (0,1,1)\} =$$

$$r_1 r_2 r_3 + r_1 r_2 (1 - r_3) + r_1 (1 - r_2) r_3 + (1 - r_1) r_2 r_3$$

Example: Following this analysis, we can support decision making processes, where we aim to achieve the maximum possible trustworthiness with respect to the system's structure and subject to monetary cost constraints. For instance, consider an integrator building up a series system, consisting of two different types of components (a and b), which are characterized by equal level of reliability, e.g., $r_i = r = \frac{1}{2}, \forall i$. Additionally, suppose that the budget constraints restrict the number of desposable components to two for each type. The integrator has to decide among two possible choices considering the structure. Should she build two identical systems, or duplicate each component? Notice that the monetary cost in both cases is equal, as the integrator utilizes exactly the same components. Finaly, we assume that all components are interoperabale, e.g., these use standardised interfaces that allow combining assets of different functionality (such as a_1 and b_2).

Case 1: Two identical systems

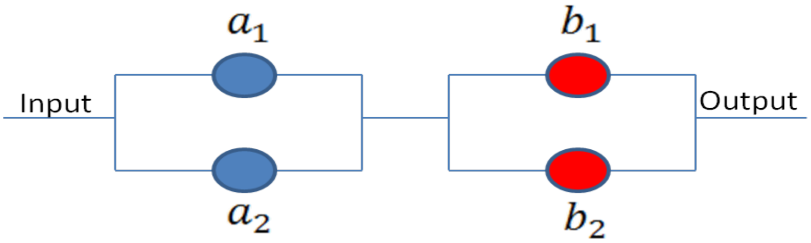


In this case, we achieve a properly working system, if (a_1 AND b_1) OR (a_2 AND b_2) are doing so.

Thus, we fomulate and calculate the systems's reliability as follows:

$$r_s = 1 - \prod_{i=1}^{2} (1 - r_{s_i}) = 1 - (1 - r_{a_1} * r_{b_1}) * (1 - r_{a_2} * r_{b_2}) = {}^{7}/_{16}$$

Case 2: Duplicate the components



In this case, we achieve a properly working system, if (a_1 OR a_2) AND (b_1 OR b_2) are doing so. Thus, we fomulate and calculate the systems's reliability as follows:

$$r_s = r_a * r_b = \left(1 - \prod_{i=1}^{2}(1 - r_{a_i})\right) * \left(1 - \prod_{i=1}^{2}(1 - r_{b_i})\right) = {}^{9}/_{16}$$

From comparison, it becomes obvious that the integrator should choose the second alternative.