

 POLITECNICO DI MILANO



Logical Methods: GTST-(D)MLD

Prof. Francesco Di Maio
Dipartimento di Energia
Via La Masa 34, B12

francesco.dimaio@polimi.it



Logical Methods: Goal Tree Success Tree – Dynamic Master Logic Diagram (GTST – DMLD)



- Goal-oriented approach based on hierarchical framework.

AIM:

1. Comprehensive knowledge of a complex system.
2. Quantitative analysis (evaluation of system performance and recovery).



FAILURE-ORIENTED APPROACHES



“bottom-up” perspective



Consequences of events on system functionality are inferred by **cause-effect logic**, requiring the definition of failure scenarios



Car accident caused by:

- Flat tyre;
- Breaks malfunctioning;
- Spark plug burnt;
- ...



FAILURE-ORIENTED APPROACHES

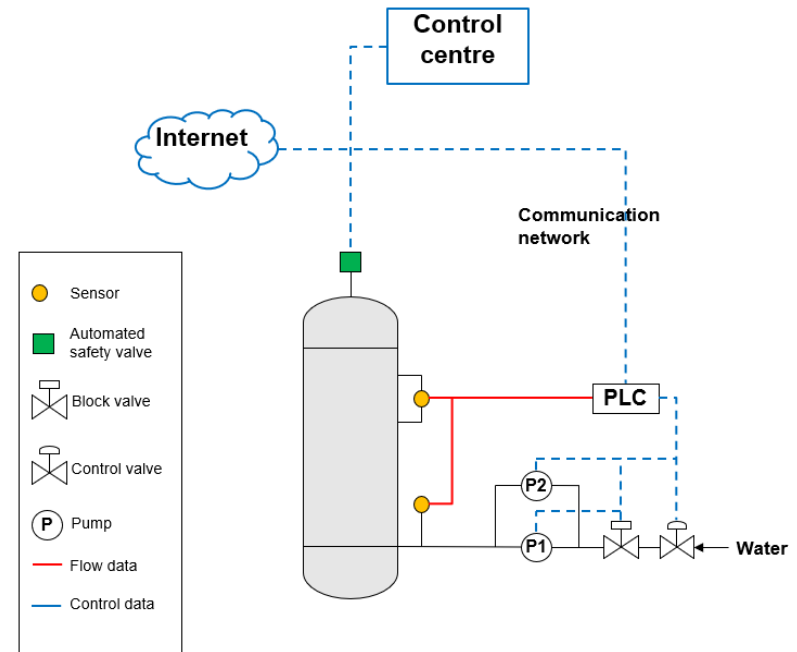


“bottom-up” perspective



Consequences of events on system functionality are inferred by **cause-effect logic**, requiring the definition of failure scenarios

Attack Tree Bow Tie (AT-BT) of a chemical reactor [2]



[2] H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, “A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie –combining new version of attack tree with bowtie analysis”, 2018, computers & security 72 175–195



Attack Tree Bow Tie (AT-BT) of a chemical reactor [2]

FAILURE-ORIENTED APPROACHES



“bottom-up” perspective



Consequences of events on system functionality are inferred by **cause-effect logic**, requiring the definition of failure scenarios

Reactor explosion



FAILURE-ORIENTED APPROACHES

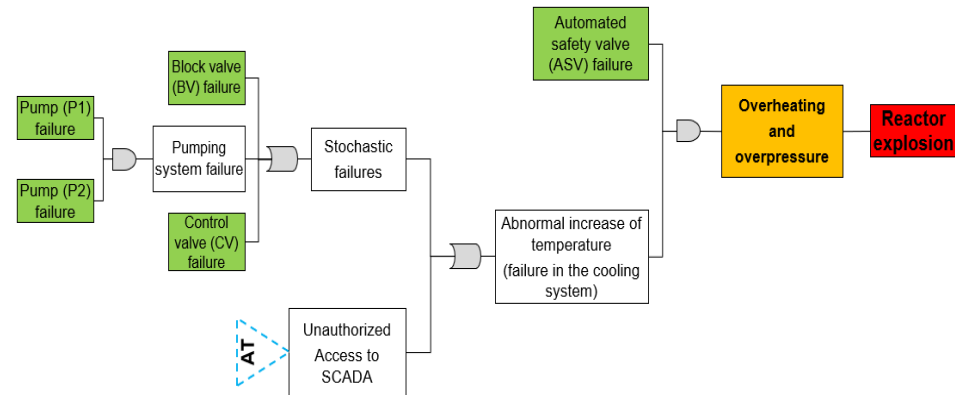


“bottom-up” perspective



Consequences of events on system functionality are inferred by **cause-effect logic**, requiring the definition of failure scenarios

Attack Tree Bow Tie (AT-BT) of a chemical reactor [2]





FAILURE-ORIENTED APPROACHES

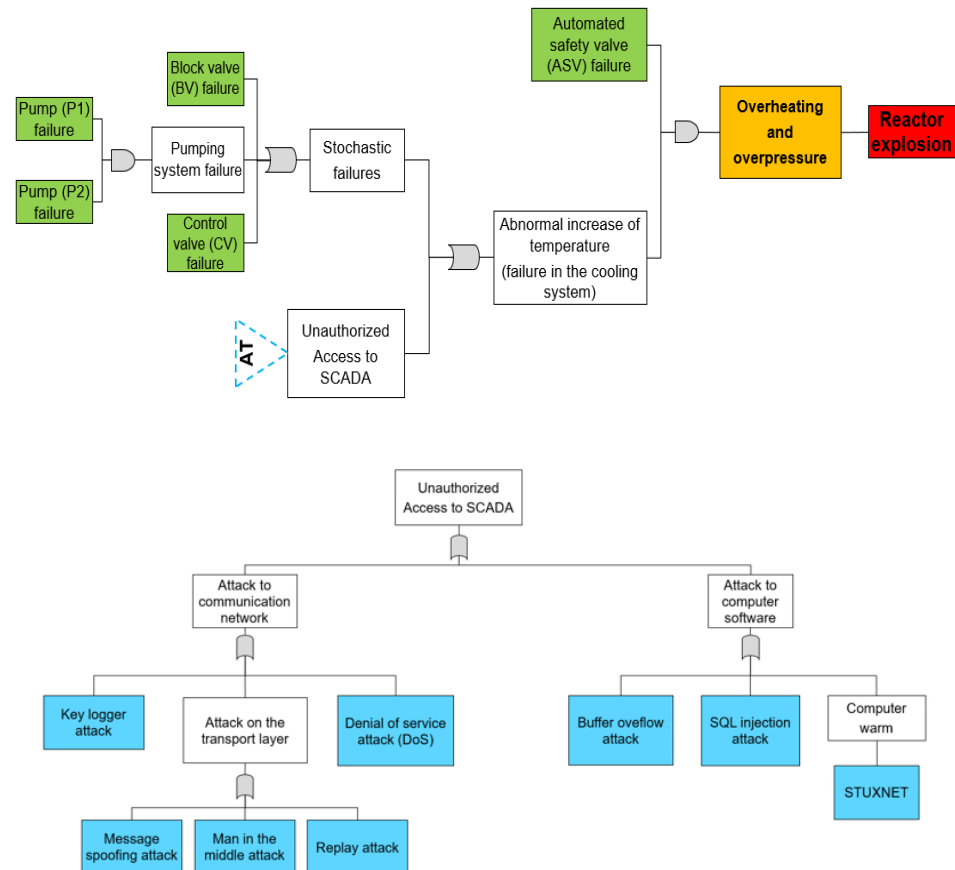


“bottom-up” perspective



Consequences of events on system functionality are inferred by **cause-effect logic**, requiring the definition of failure scenarios

Attack Tree Bow Tie (AT-BT) of a chemical reactor [2]





FAILURE-ORIENTED APPROACHES



“bottom-up” perspective



Consequences of events on system functionality are inferred by **cause-effect logic**, requiring the definition of failure scenarios

LIMITATIONS:

- Impossibility to enumerate all **failure scenarios** [1].
- Difficulty in defining all the events probability (in particular, of security-related events) [3].



- Car accident is avoided if:
 - Flat tyre signalling;
 - Air bags;
 - ABS;
 - ...

GOAL-ORIENTED APPROACHES

“top-down” perspective

Goals of the system, rather than failure modes, are identified and components/systems that can guarantee their fulfillment are enumerated



GTST – DMLD construction



Goal Tree Success Tree – Dynamic Master Logic Diagram

Goal Tree Success Tree
(GTST)

+

Master Logic Diagram
(MLD)



Goal Tree Success Tree - Master Logic Diagram
(GTST - MLD)

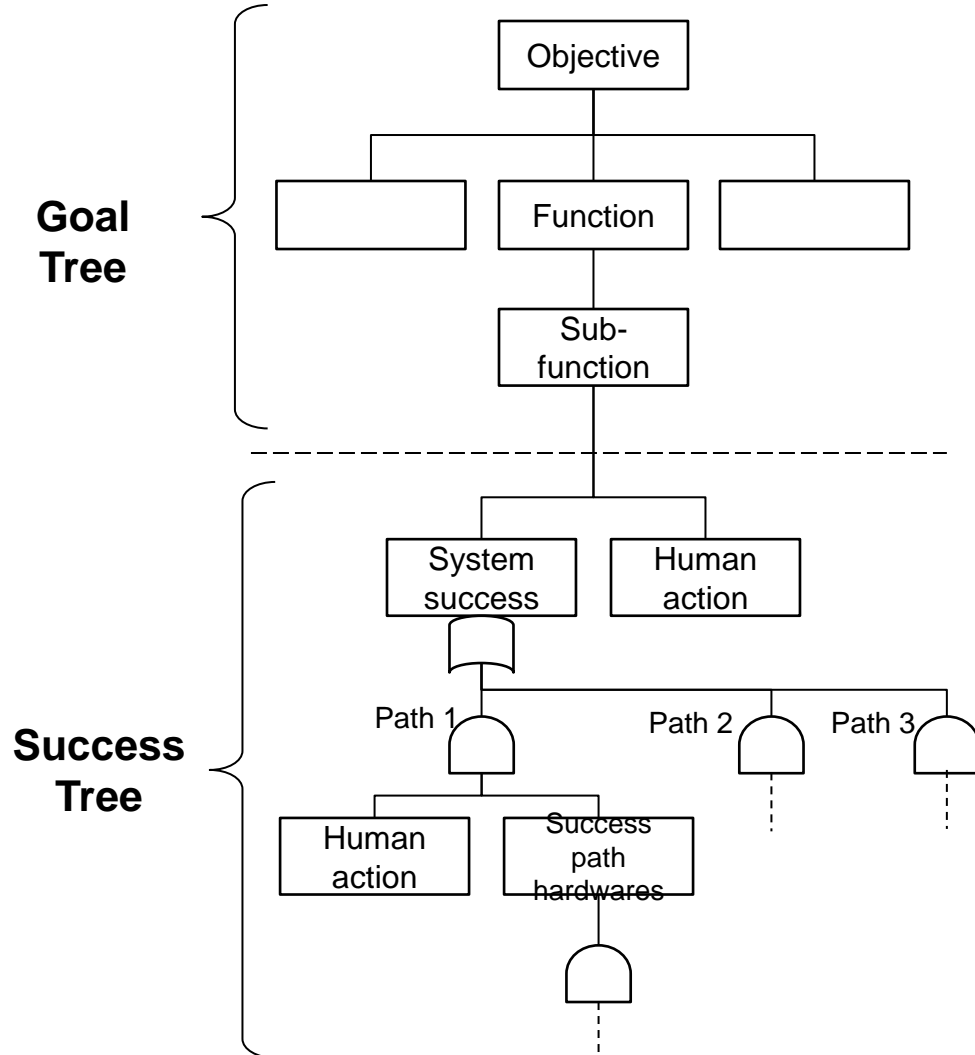
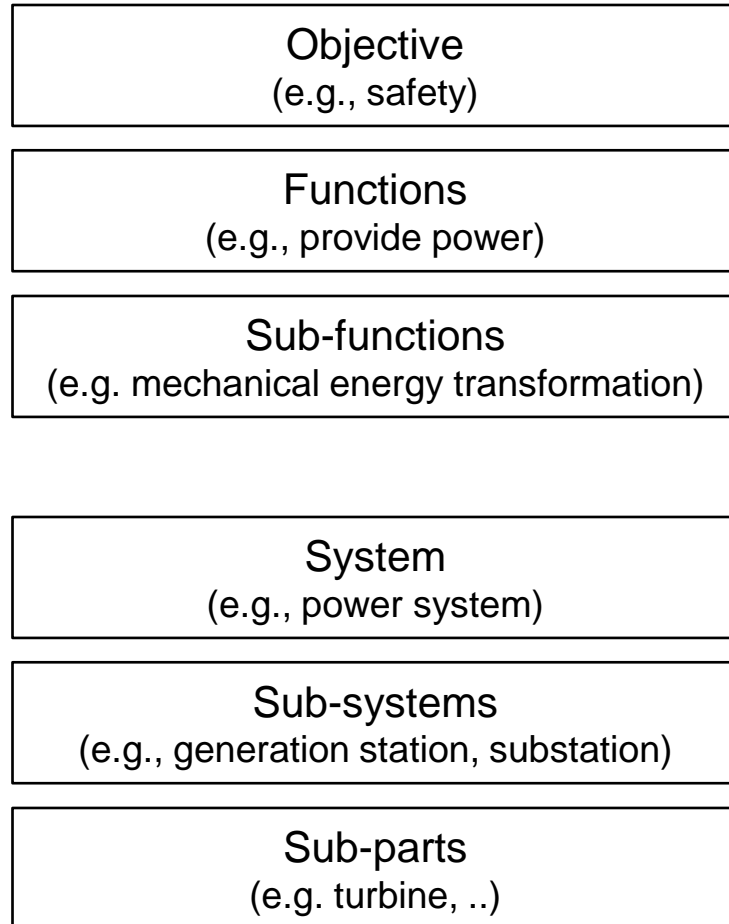


+ dynamic behavior

Goal Tree Success Tree – Dynamic Master Logic Diagram
(GTST – DMLD) (or DMLD)



Goal Tree Success Tree

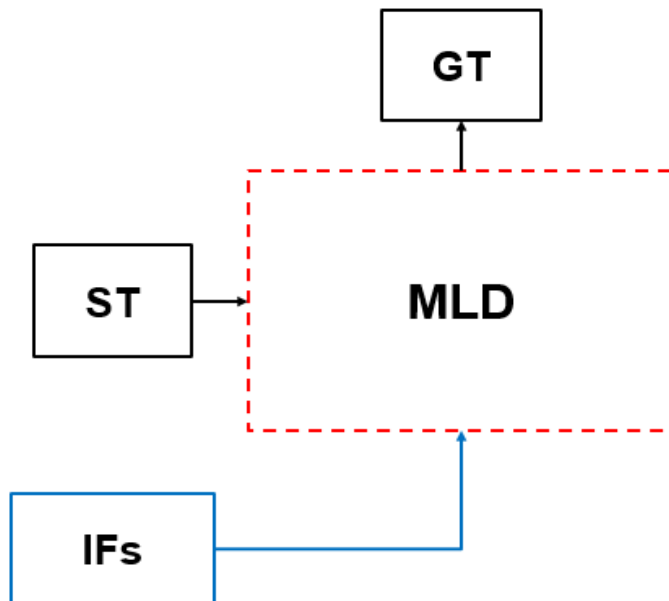


[Kim and Modarres, 1987]



The GTST-MLD approach (2)

GOAL-ORIENTED APPROACHES

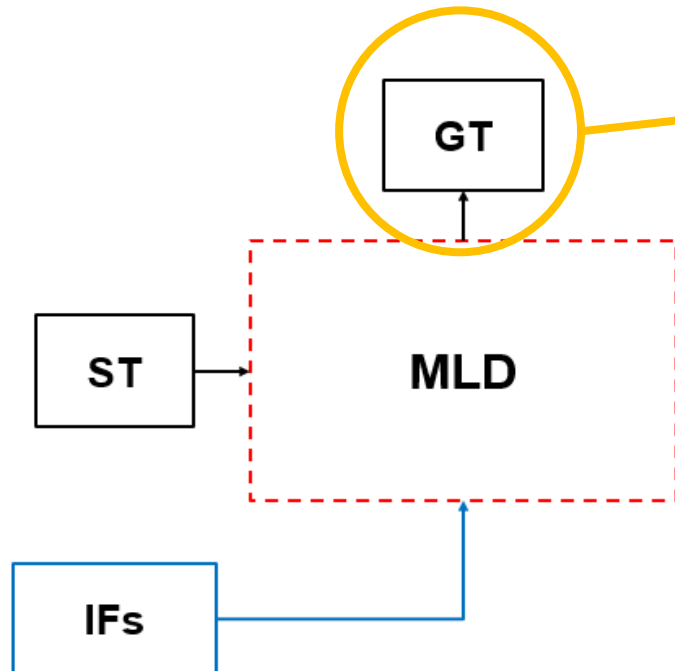


“top-down” perspective

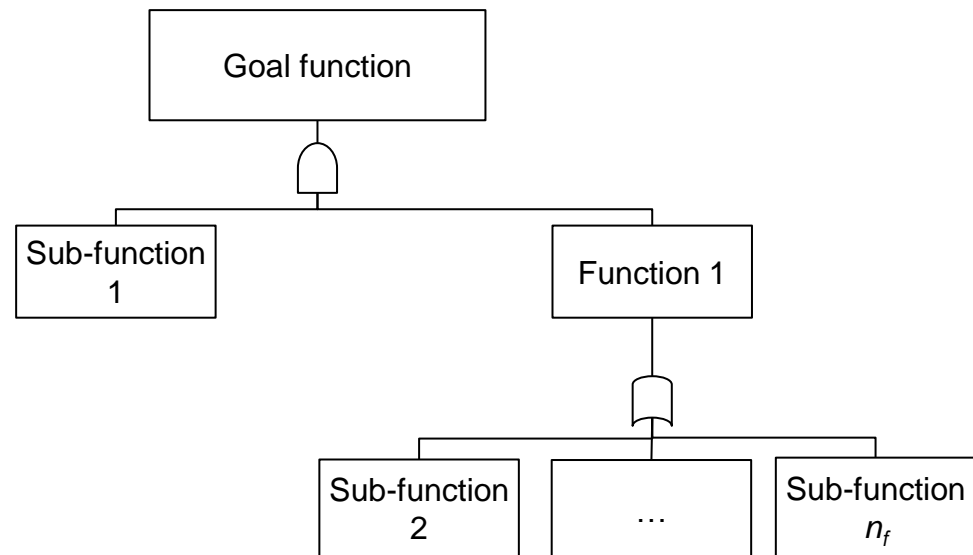
Goals of the system, rather than failure modes, are identified and components/systems that can guarantee their fulfillment are enumerated



The GTST-MLD approach (2)

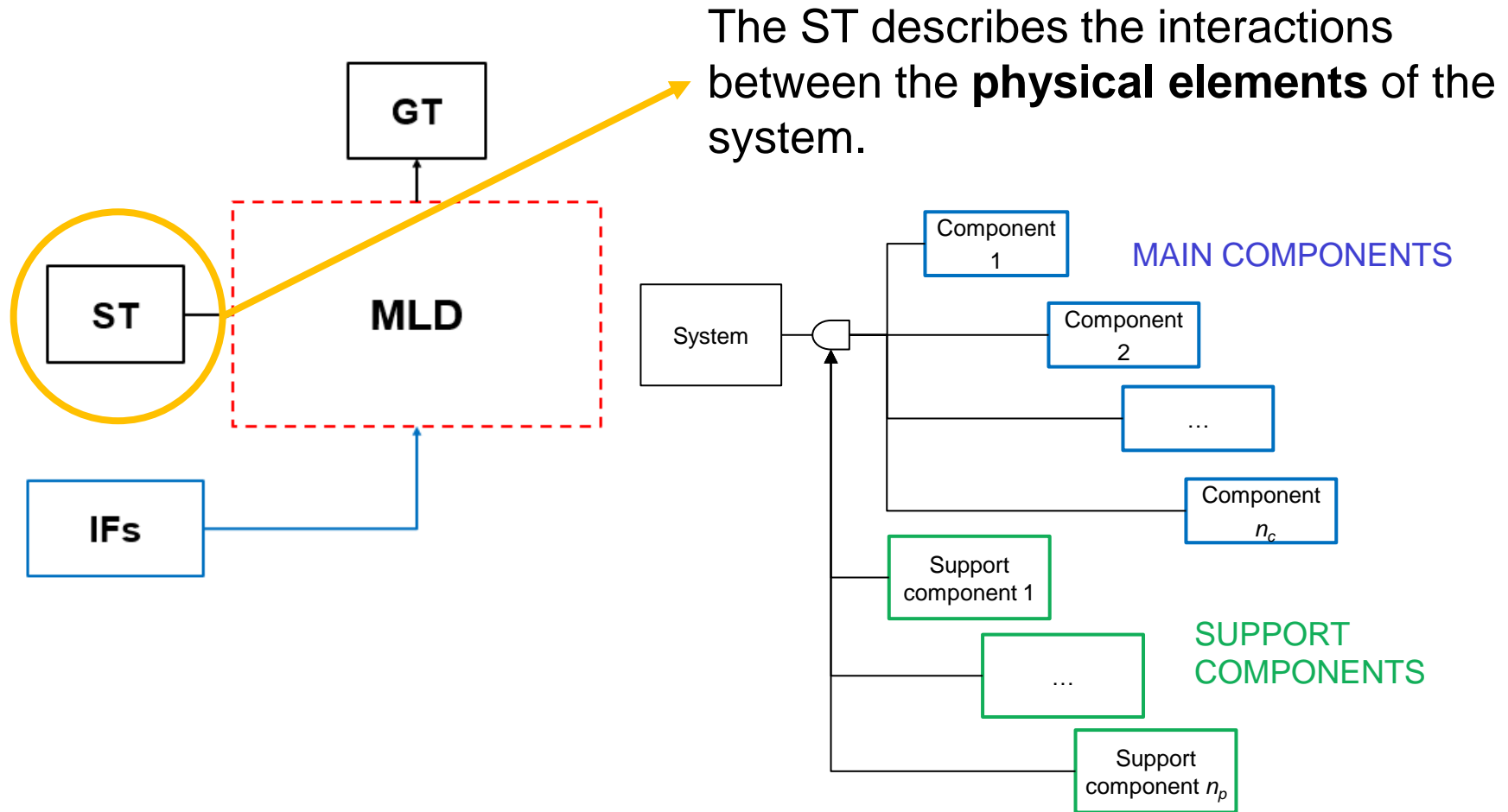


The Goal Tree (GT) hierarchically decomposes the system safety **goal function** into n_f sub-functions.



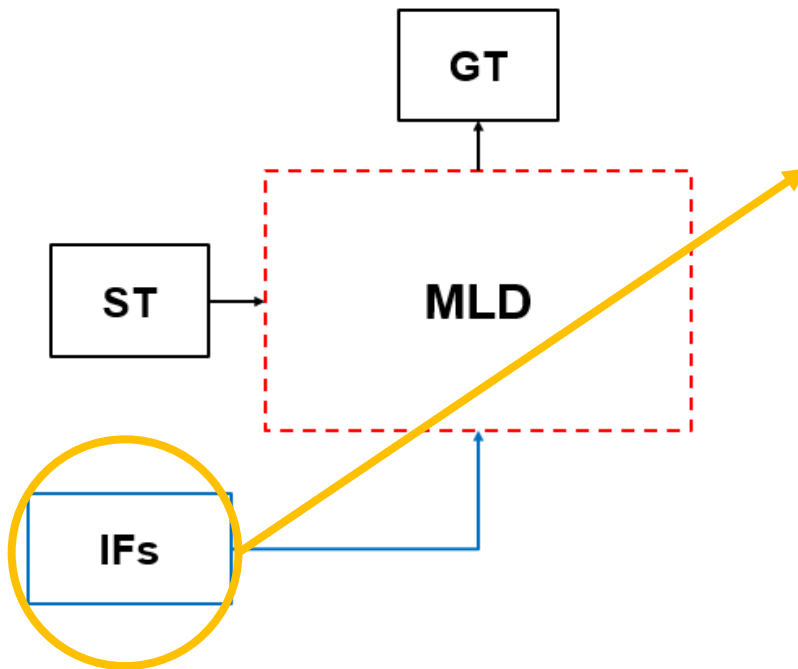


The GTST-MLD approach (3)





The GTST-MLD approach (4)



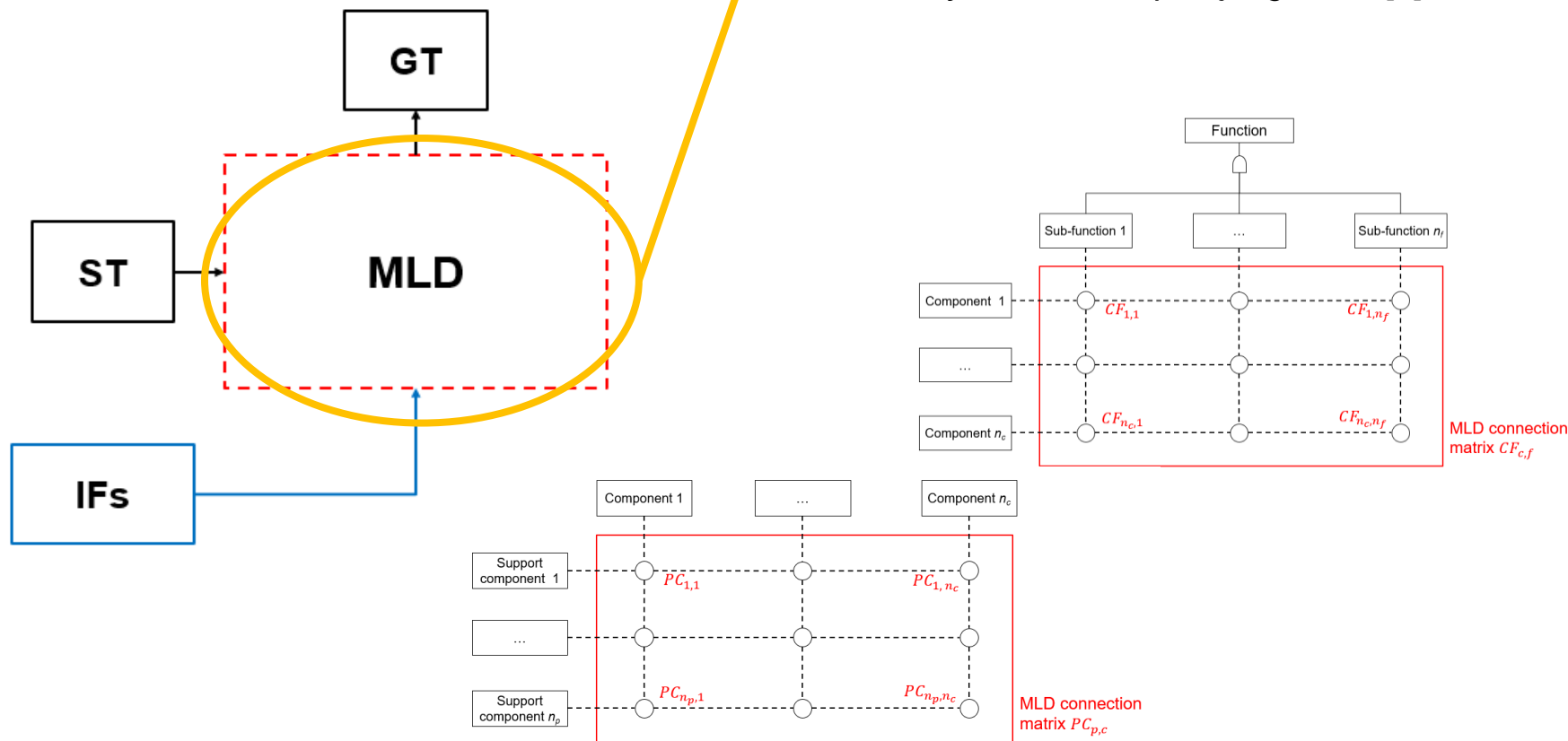
The Influencing Factors (IFs) are the **dysfunctional aspects** that can prevent the system to achieve the goal function.



The GTST-MLD approach (5)

The **relationships** between GT, ST and IFs are represented by the Master Logic Diagram (MLD).

Traditionally based on expert judgement [4].



[4] E. Ferrario, E. Zio, "Goal Tree Success Tree–Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems", 2014, Engineering Structures 59 411–433



GTST – MLD

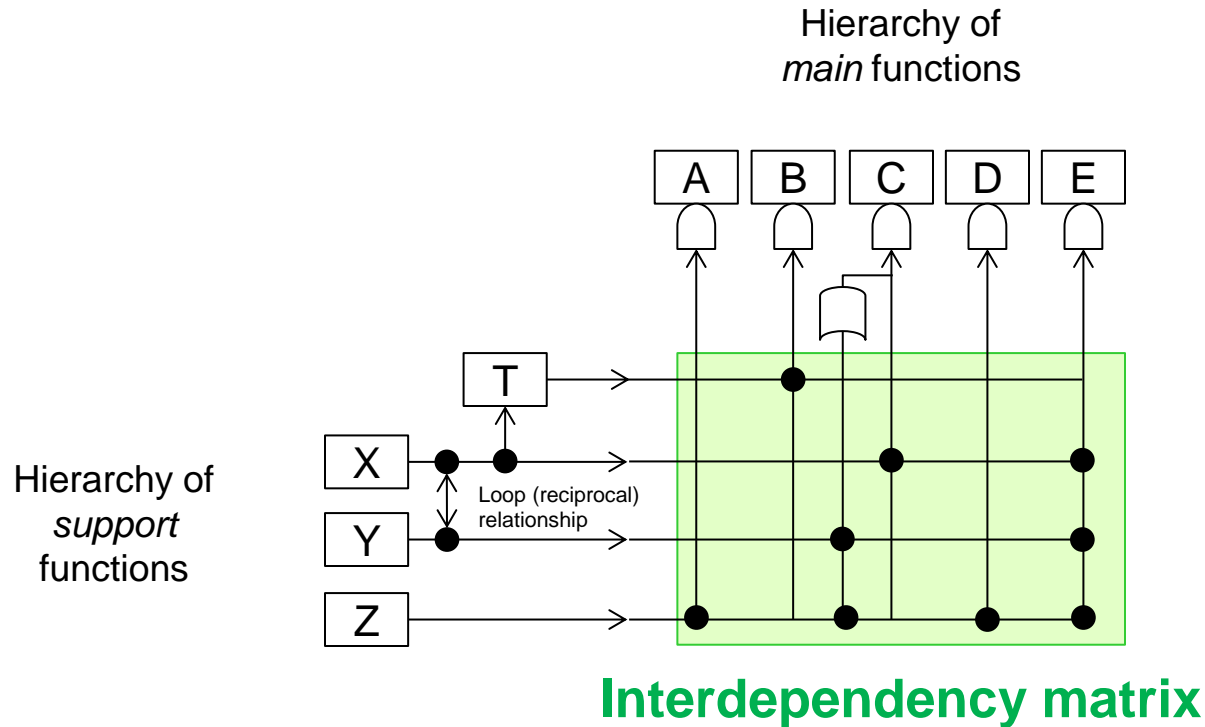
quantitative analysis



Master Logic Diagram

MLD clearly shows the dependencies among the independent part of the systems, including the *support items*. It is developed and displayed hierarchically.

[Modarres 1999]

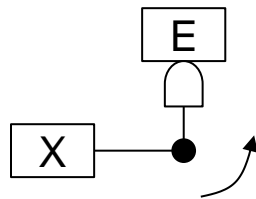




Master Logic Diagram

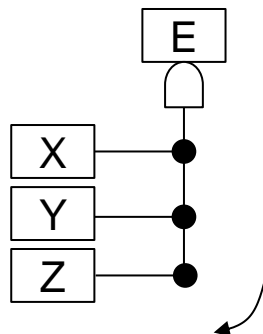
It describes causal effects of a failure. There are two important causal relations:

1. To know the ultimate effect of a failure



Failure of X causes failure of E

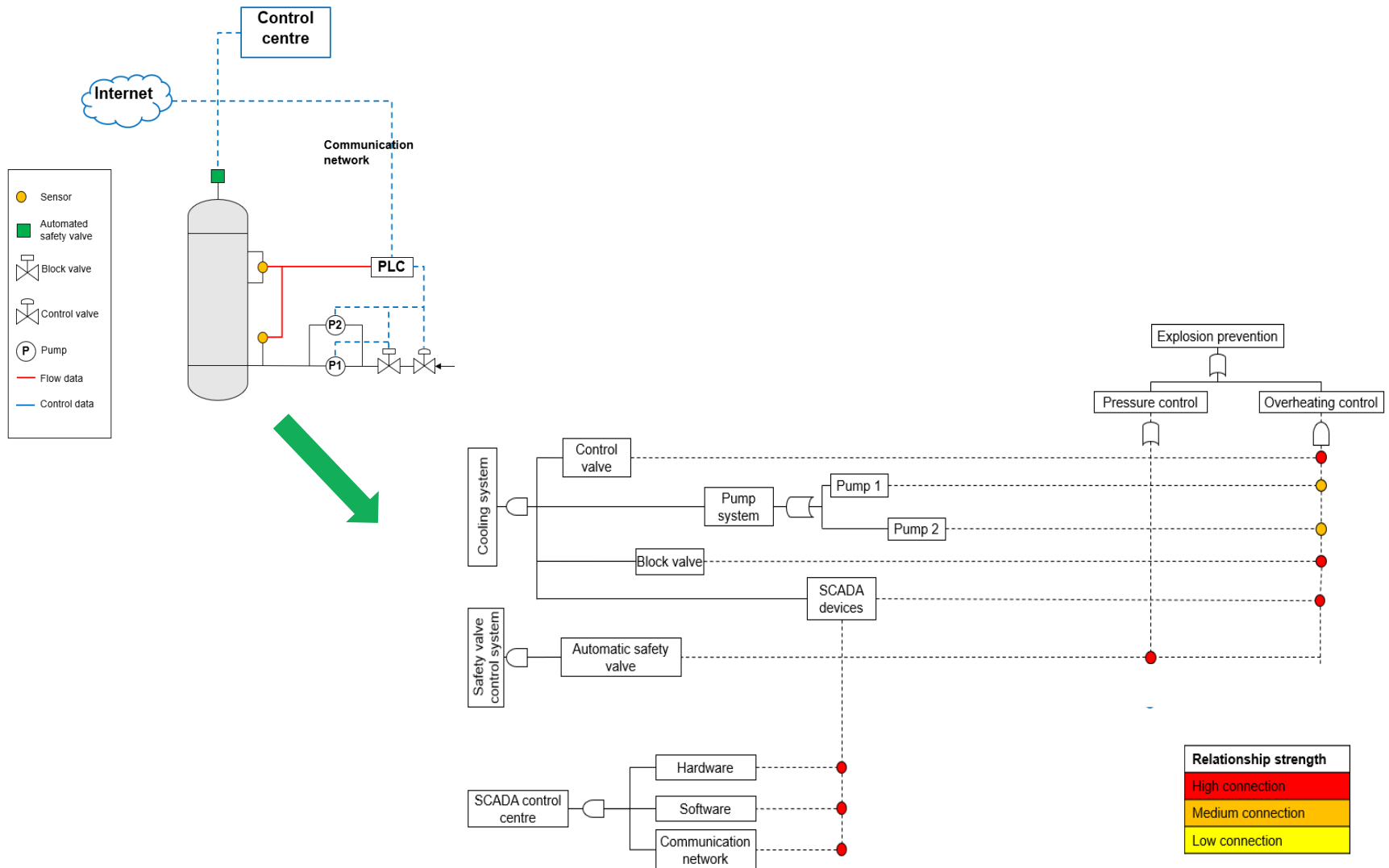
2. To determine the ways that a function can be achieved (a system would successfully work)



Success of E requires success of X, Y and Z



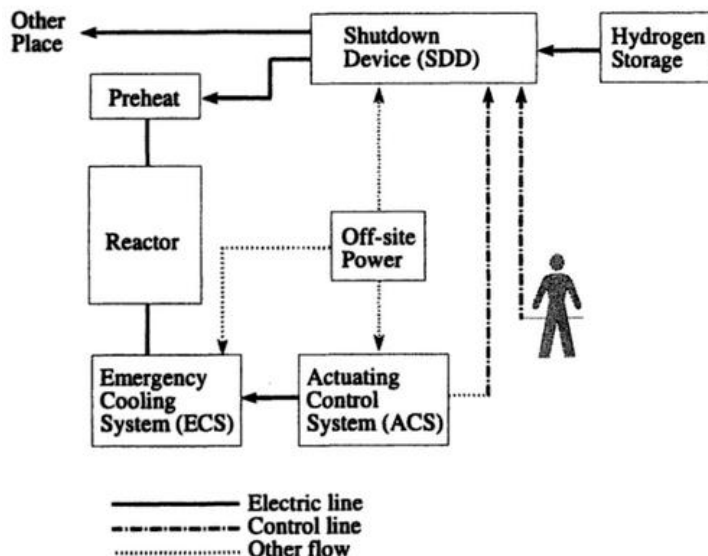
Example 1: Chemical Reactor





Master Logic Diagram: example of the H-Coal process

In case of an emergency, a shutdown device (SDD) is used to shut down the hydrogen flow. If the reactor temperature is too high, an emergency cooling system (ECS) is also needed to reduce the reactor temperature. To protect the process plant when the reactor temperature becomes too high, both ECS and SDD must succeed. The SDD and ECS are actuated by a control device. If the control device fails, the emergency cooling system will not be able to work. However, an operator can manually operate (OA) the shutdown device and terminate the hydrogen flow. The power for the SDD, ECS, and control device comes from an outside electric company (off-site power-OPS).



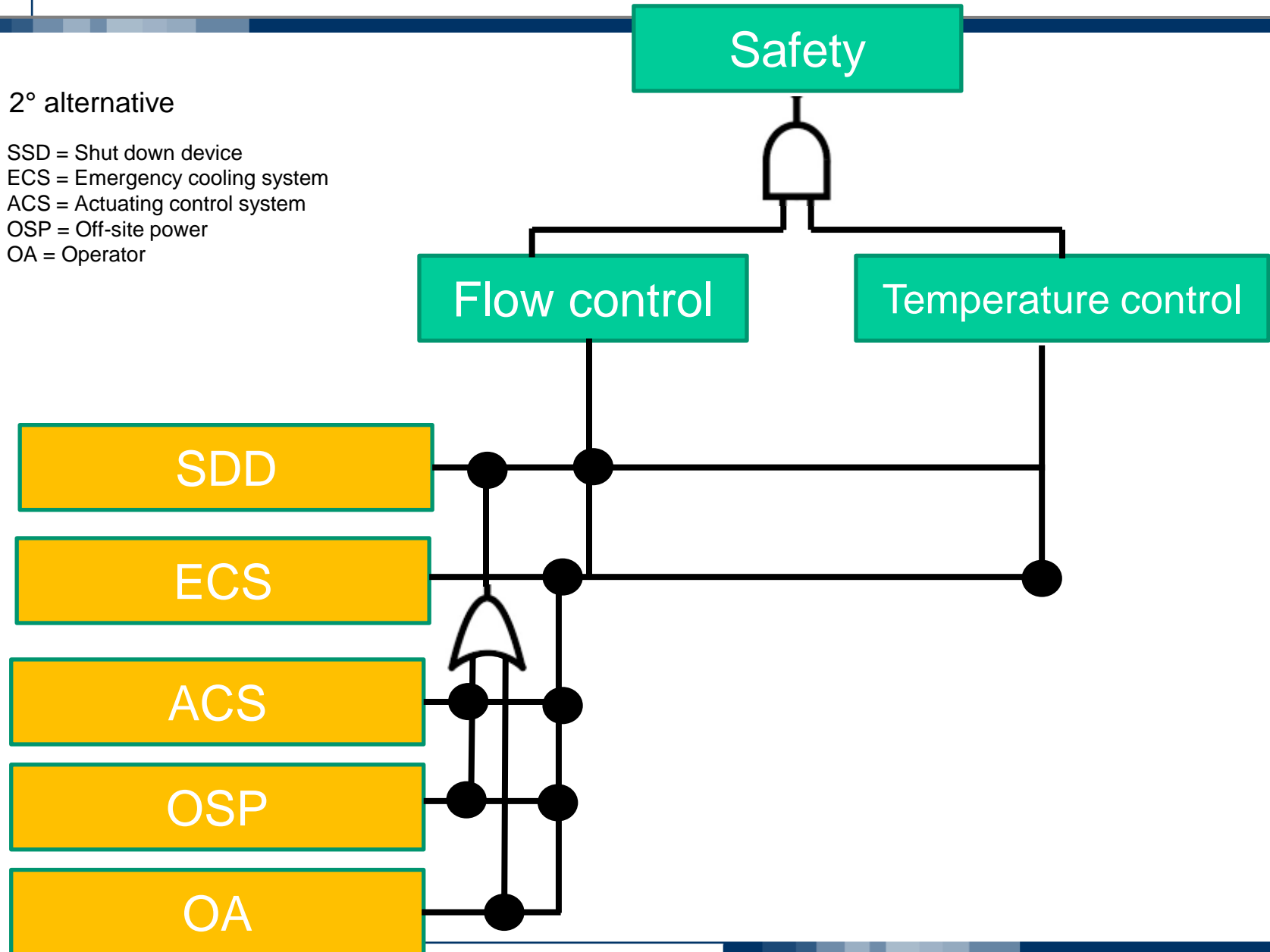
[Modarres et al. 1999]



Master Logic Diagram: example of the H-Coal process

2° alternative

SSD = Shut down device
ECS = Emergency cooling system
ACS = Actuating control system
OSP = Off-site power
OA = Operator

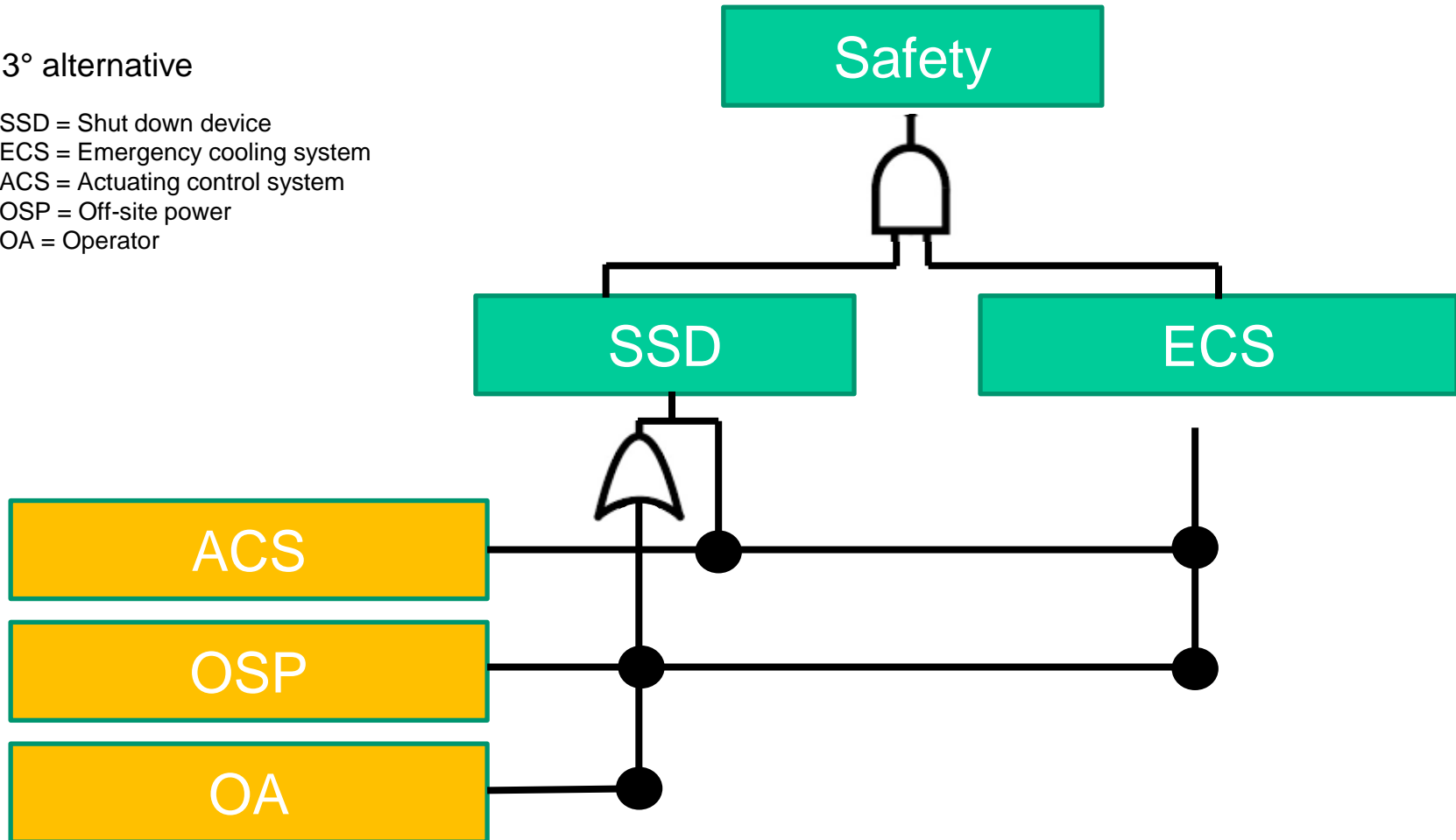




Master Logic Diagram: example of the H-Coal process

3° alternative

SSD = Shut down device
ECS = Emergency cooling system
ACS = Actuating control system
OSP = Off-site power
OA = Operator





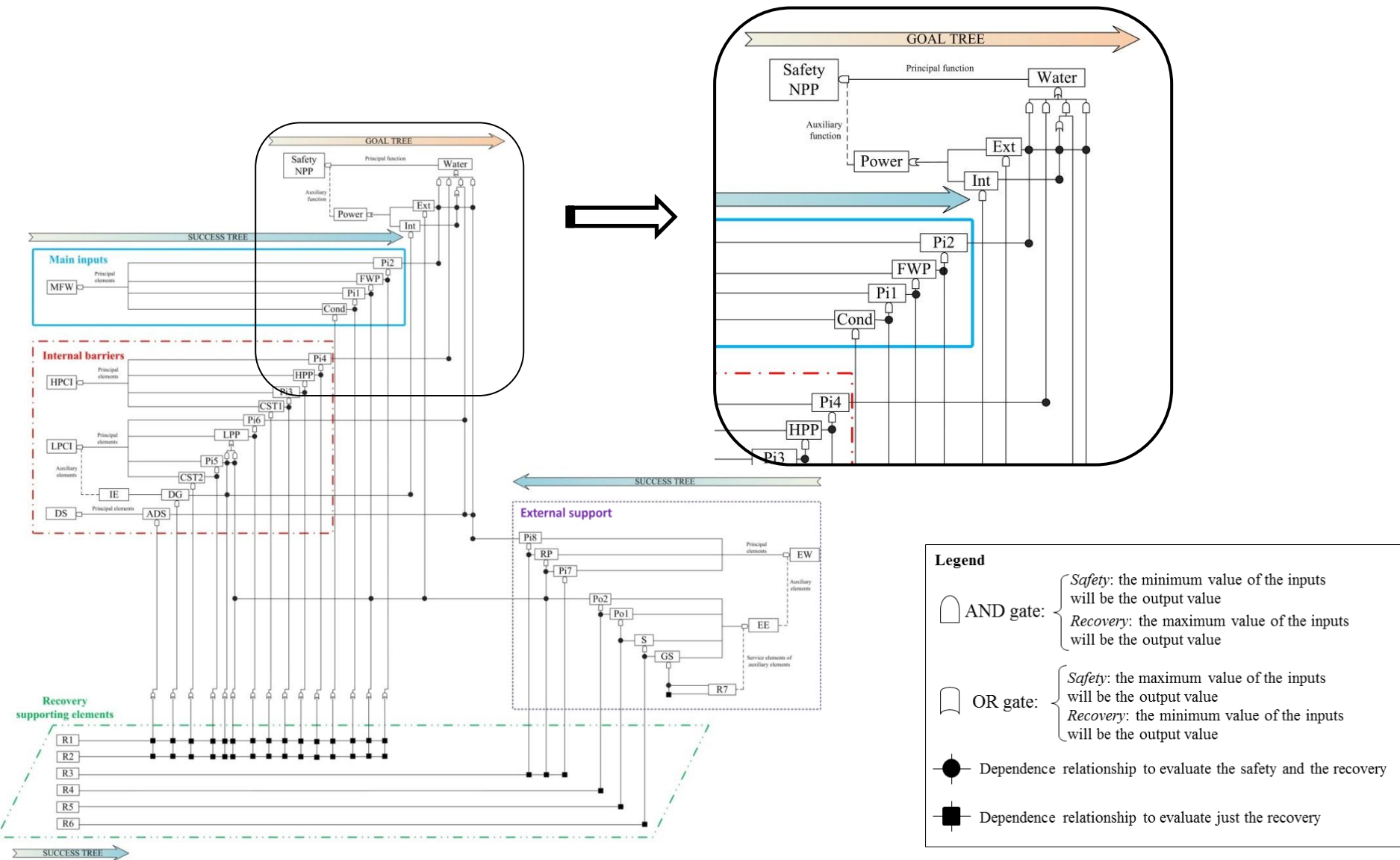
- **Main Feedwater system**

- **Water systems:**
 - High Pressure Coolant Injection (HPCI) System
 - Low Pressure Coolant Injection (LPCI) System
- **Depressurization system:**
 - Automatic Depressurization system (ADS)
- **Power system:**
 - Diesel Generator (DG)

- **Water system:**
 - Water from the river
- **Power system:**
 - Offsite power

- **Road transportation system:**
 - Road access (R)

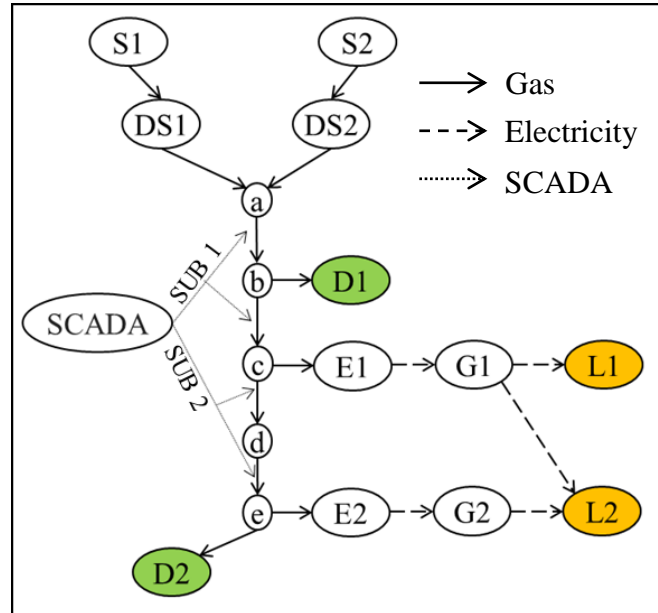






GTST – DMLD example: Critical Infrastructures

Example: graph of interconnected gas and electricity networks



[Nozick et al., 2005]

Input arcs:

- S1_DS1 and DS1_a
- S2_DS2 and DS2_a

Goals:

- D1 and D2 (gas)
- L1 and L2 (electricity)

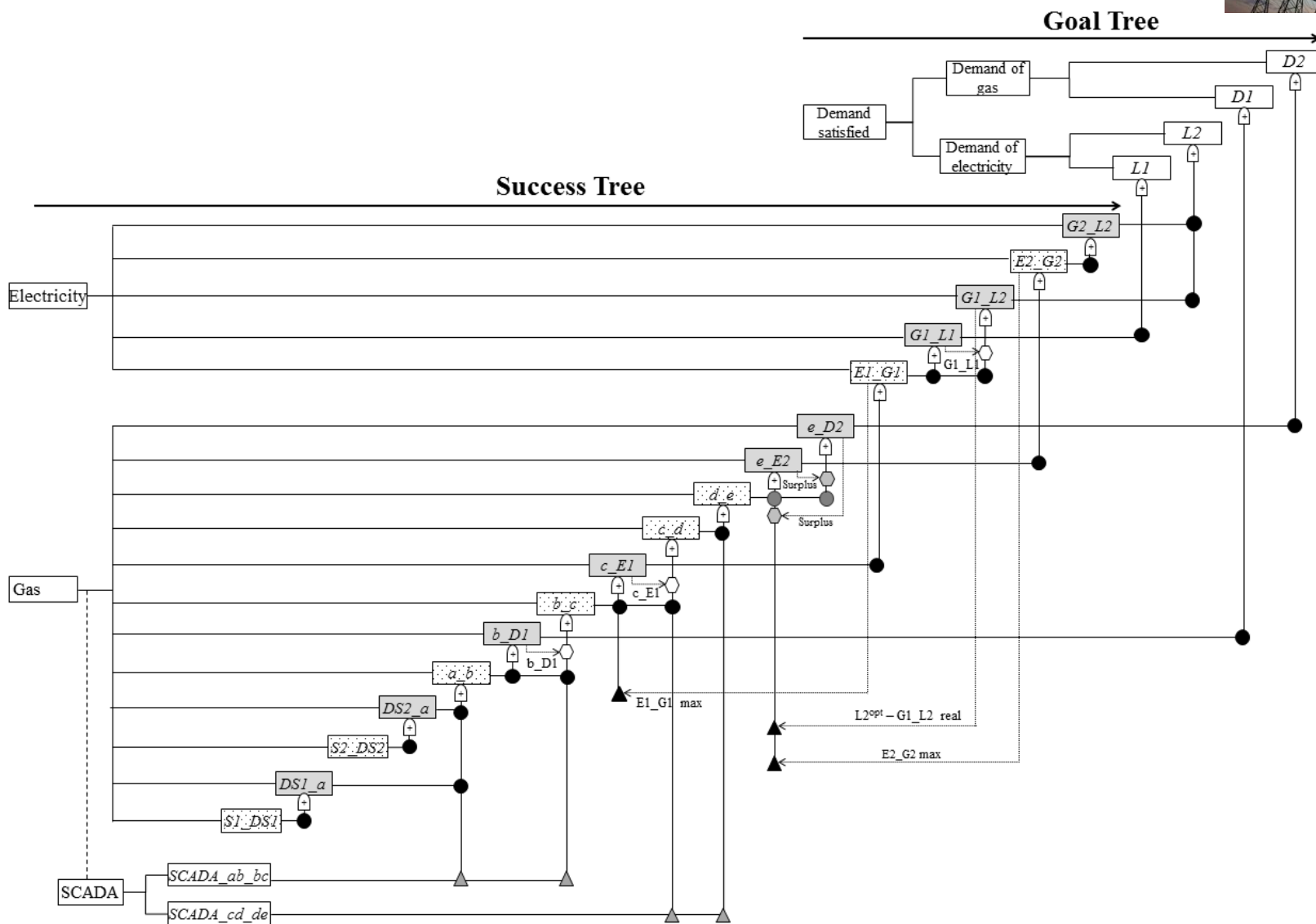
Transmission arcs:

- a_b, b_c, c_d, d_e, e_D2, b_D1, c_E1, E1_G1, G1_L1, G1_L2, e_E2, E2_G2, G2_L2

- **Input arcs** that inject flow (product) in the system
- **Demand nodes/goals** that require a given amount of product
- **Transmission arcs** that transfer the product to other components in the system



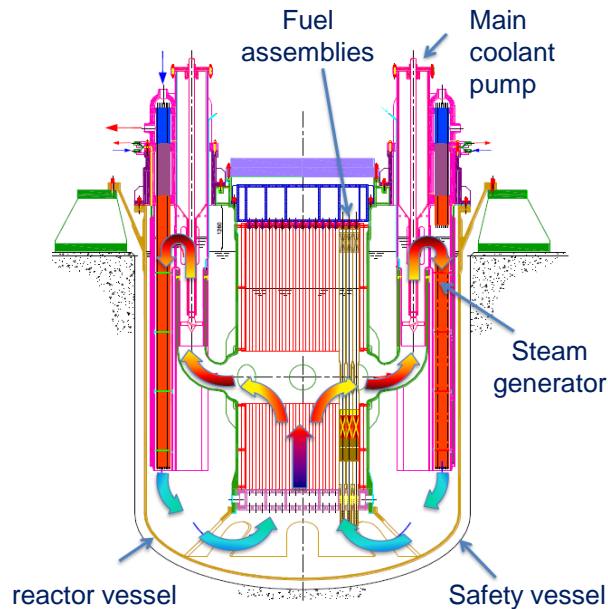
GTST – DMLD example: Critical Infrastructures



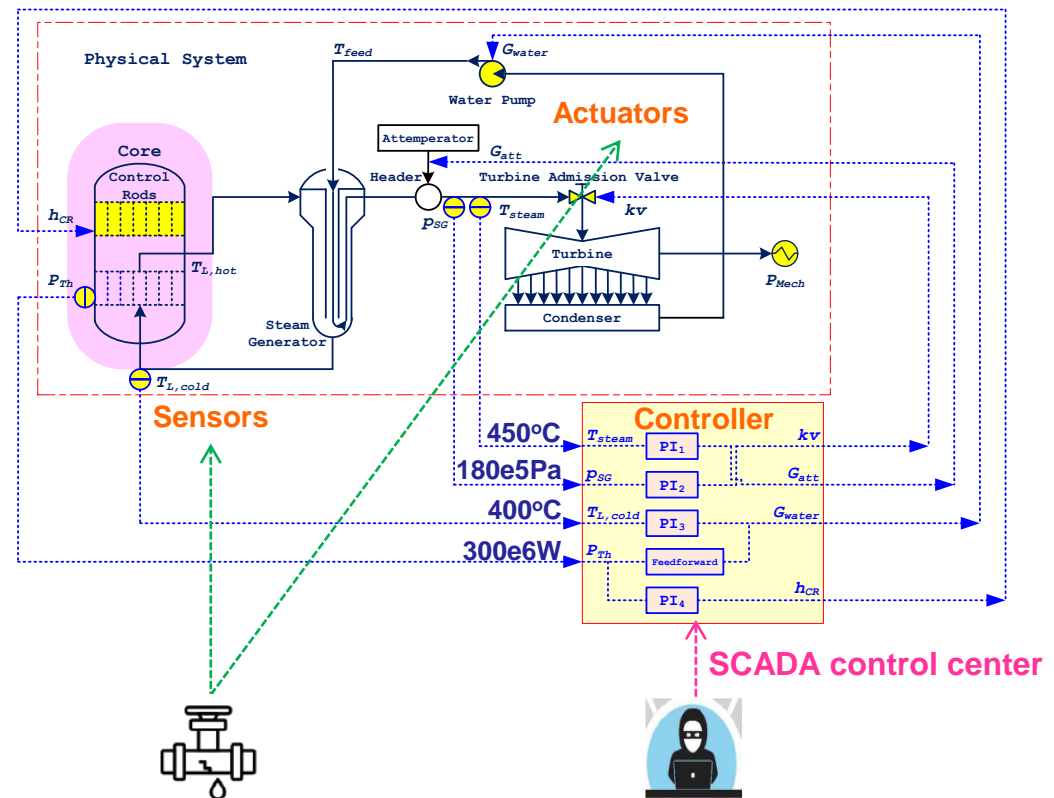


GST-MLD example: The Advanced Lead-cooled Fast Reactor European Demonstrator (ALFRED)

ALFRED primary system layout
small-size (300 MW) pool-type LFR



ALFRED multi-loop control scheme
4 Single-Input-Single-Output control loops

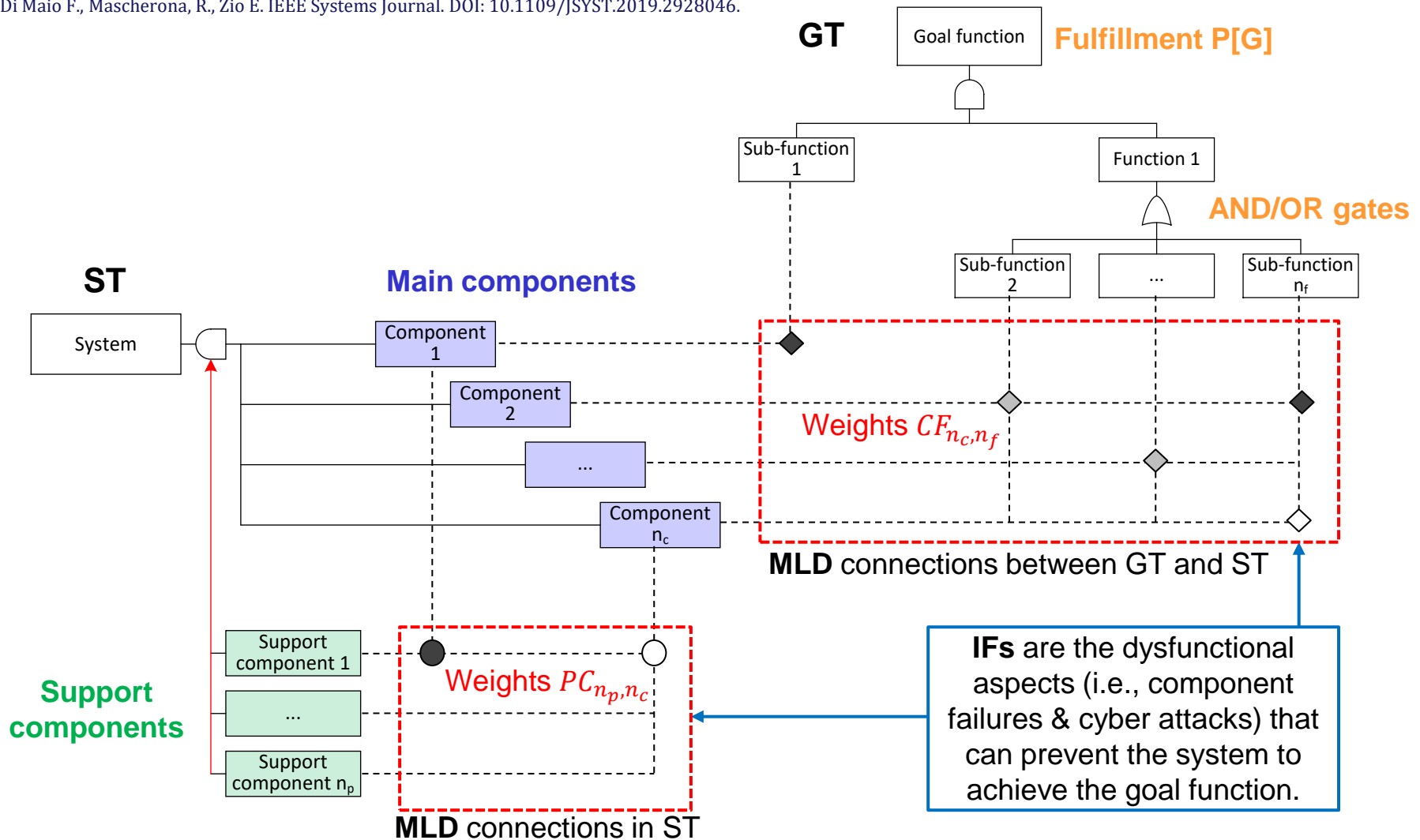


Component failures (Malicious) external events



Available Modeling Solution: GTST-MLD for Risk Analysis of CPSs

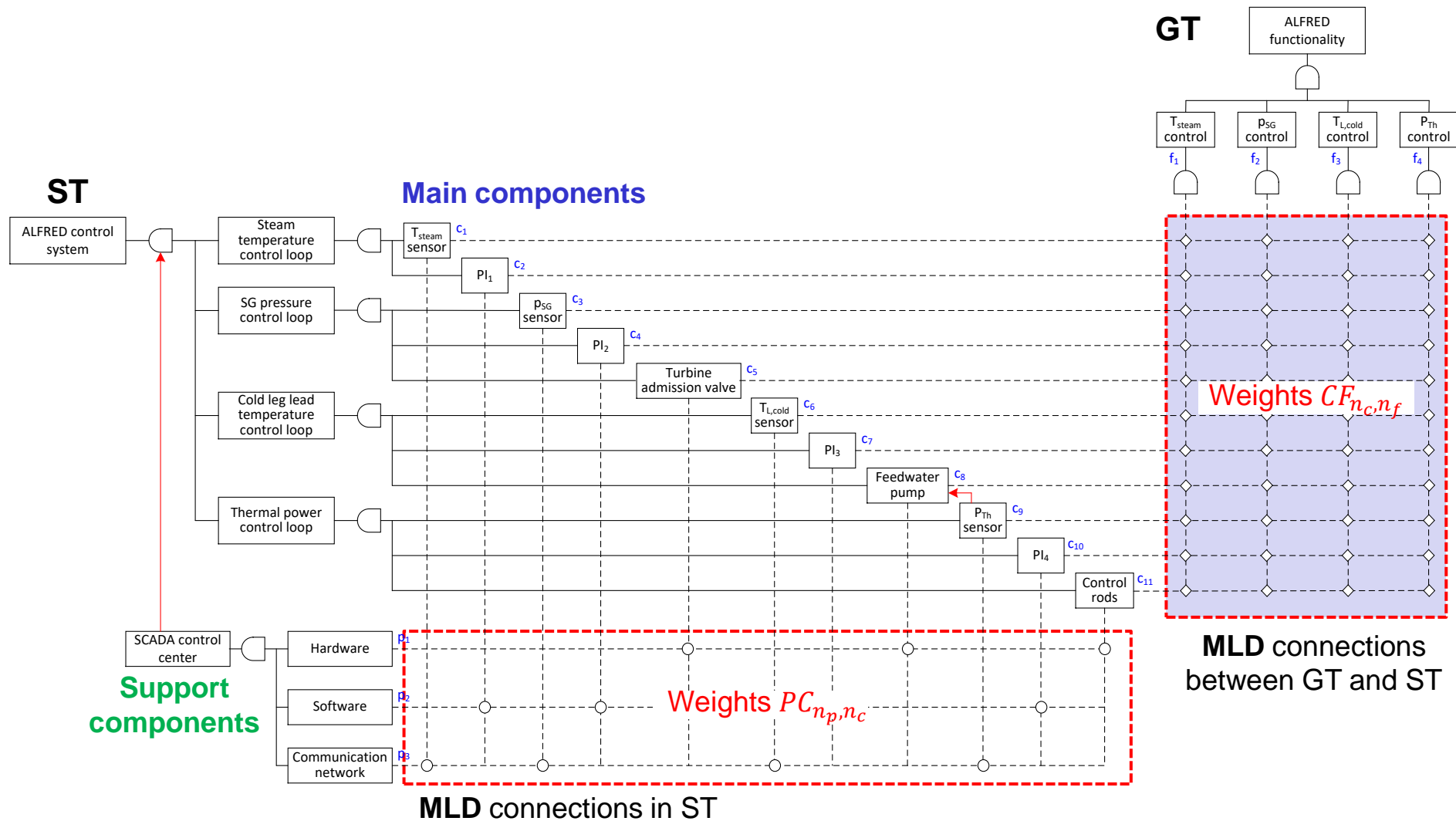
[J] Di Maio F., Mascherona, R., Zio E. IEEE Systems Journal. DOI: 10.1109/JSYST.2019.2928046.



Challenge: expert-dependent weights assignment



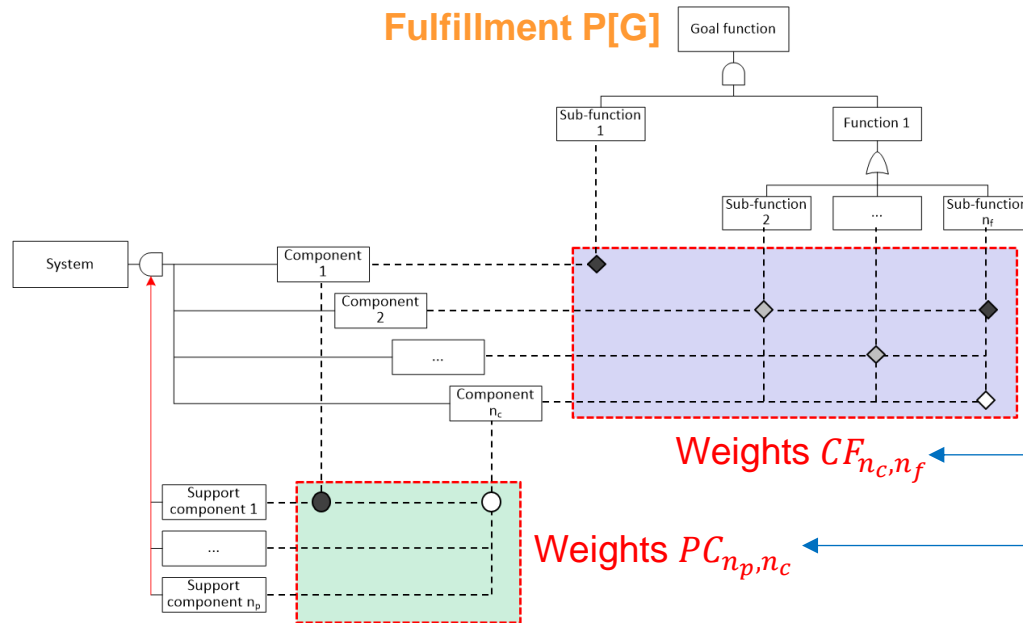
The GTST-MLD Model of the ALFRED





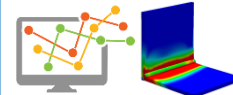
Proposed Solution: Simulation-based GTST-MLD for Weights Setting

Fulfillment $P[G]$



Weights CF_{n_c, n_f}

Weights PC_{n_p, n_c}

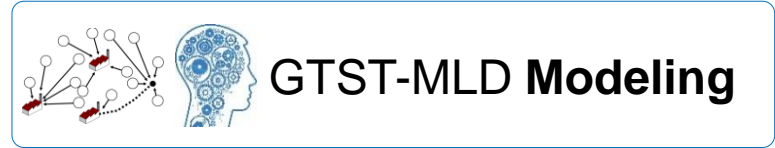
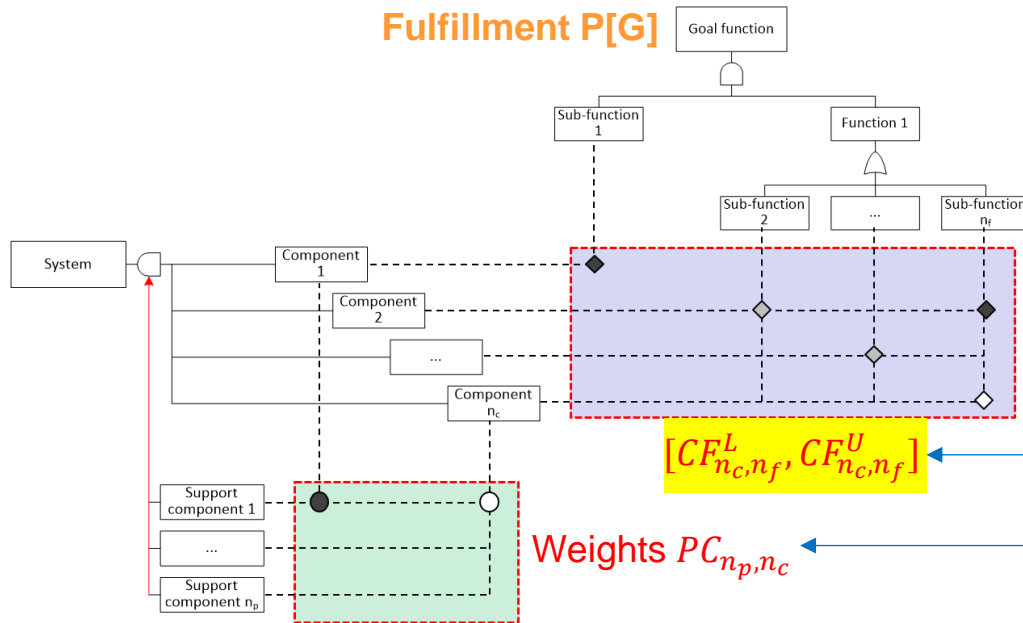


Simulation for assigning weights by integrating the heterogeneous sources of knowledge, information and data.

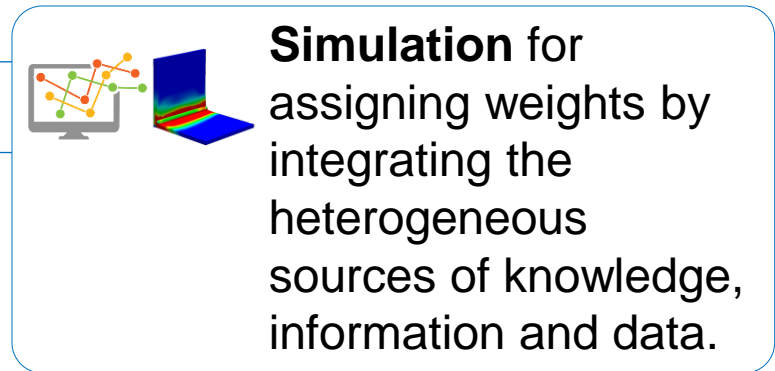


Proposed Solution: Simulation-based GTST-MLD for Weights Setting

Fulfillment $P[G]$



&



Monte Carlo simulation for propagating uncertainties through the GTST-MLD to the system unreliability estimates $F_{GTST}(t) = 1 - P[G](t)$, overcoming the expert-dependent weights assignment.



GTST-MLD Weights Setting: Monte Carlo Engine for Accidental Scenarios Injection

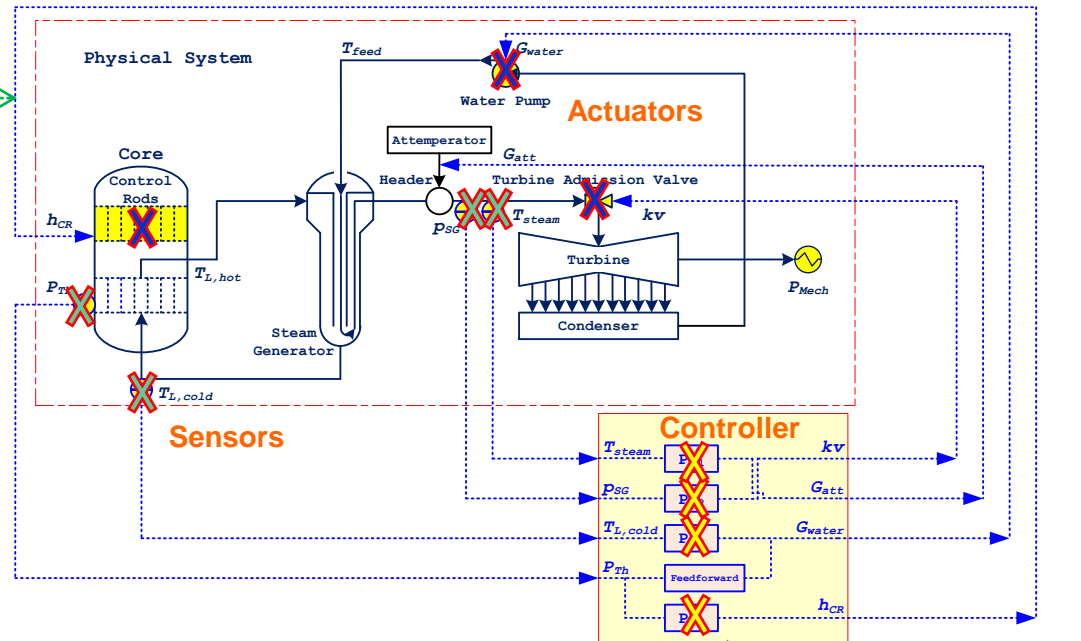


Component failures

 **Sensors** bias, drift, wider noise, freezing

 **Actuators** fail stuck

 **PI controllers** proportional gain change, integral gain change, set point change



Malicious cyber attacks
mimicking component failures

- Doorknob rattling;
- STUXNET virus;
- Key logger;
- Man in the middle;
- Denial of Service;
- Message spoofing;
- Replay;
- Buffer overflow.



SCADA control center

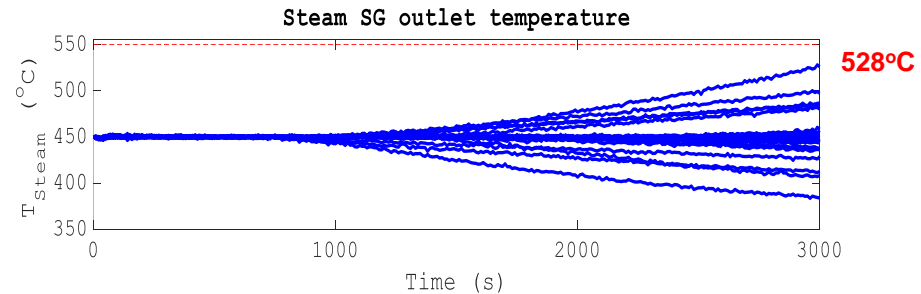


GTST-MLD Weights Setting: Monte Carlo Engine for Accidental Scenarios Injection

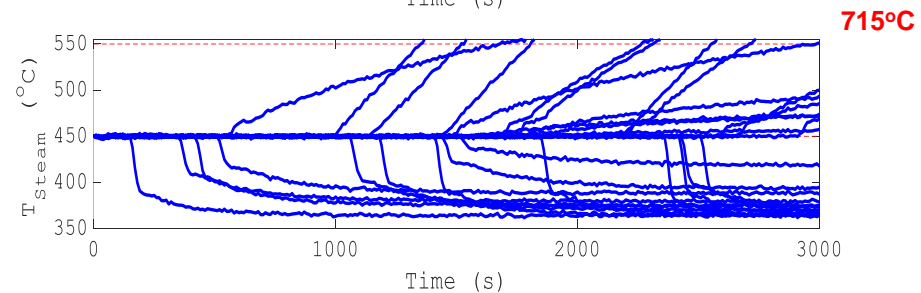
[J] Wang W., Cammi A., Di Maio F., Lorenzi S., Zio E. Reliability Engineering and System Safety 175 (2018) 24-37.

Safety parameters responses to different accidental (cyber attacks) scenarios:

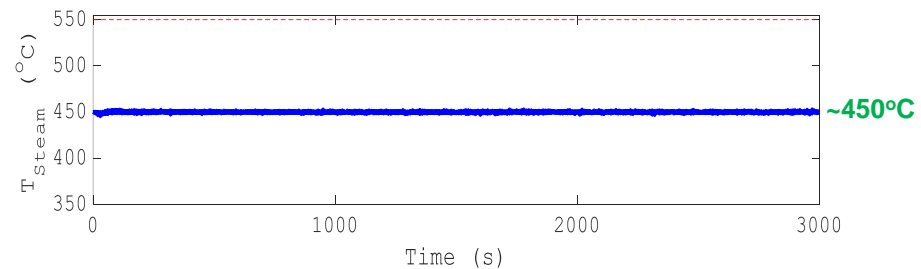
✗ DoS attack freezes $T_{L,cold}$ sensor



✗ Water pump fails stuck



✗ Cyber attack to K_p gain value of PI_1





Estimated GTST-MLD Weights

Bounds of CF_{n_c, n_f} considering different cyber attack scenarios

Three-level risk metric for ranking the strengths of the weights estimates

Strength	Weight estimate
Low	[0.0, 0.2)
Medium	[0.2, 0.8)
High	[0.8, 1.0]

CF_{n_c, n_f}	$f = 1$	$f = 2$	$f = 3$	$f = 4$
$c = 1$	0	0	[0, 6.03E-265]	0
$c = 2$	0	[0.70, 0.85]	[1.06E-30, 4.95E-22]	[5.77E-45, 4.39E-23]
$c = 3$	[0.26, 0.37]	[0.63, 0.72]	[1.54E-5, 2.20E-3]	[0.12, 0.15]
$c = 4$	0	[0.46, 0.51]	[0.02, 0.07]	[0.74, 0.88]
$c = 5$	0	0	[0, 1.69E-307]	0
$c = 6$	0	[0.09, 0.18]	[0, 3.09E-258]	0
$c = 7$	[6.36E-8, 6.12E-5]	[1.95E-17, 2.05E-12]	[2.23E-5, 8.66E-4]	[3.39E-6, 5.10E-4]
$c = 8$	0	0	0	[2.50E-3, 0.02]
$c = 9$	[0.05, 0.21]	[0.62, 0.73]	[1.05E-14, 1.55E-8]	[0.90, 0.98]
$c = 10$	[0.40, 0.44]	[0.31, 0.34]	[3.08E-5, 1.10E-3]	[0.42, 0.45]
$c = 11$	[6.17E-8, 0.07]	[0.52, 0.59]	[0, 4.91E-22]	[0.01, 0.08]



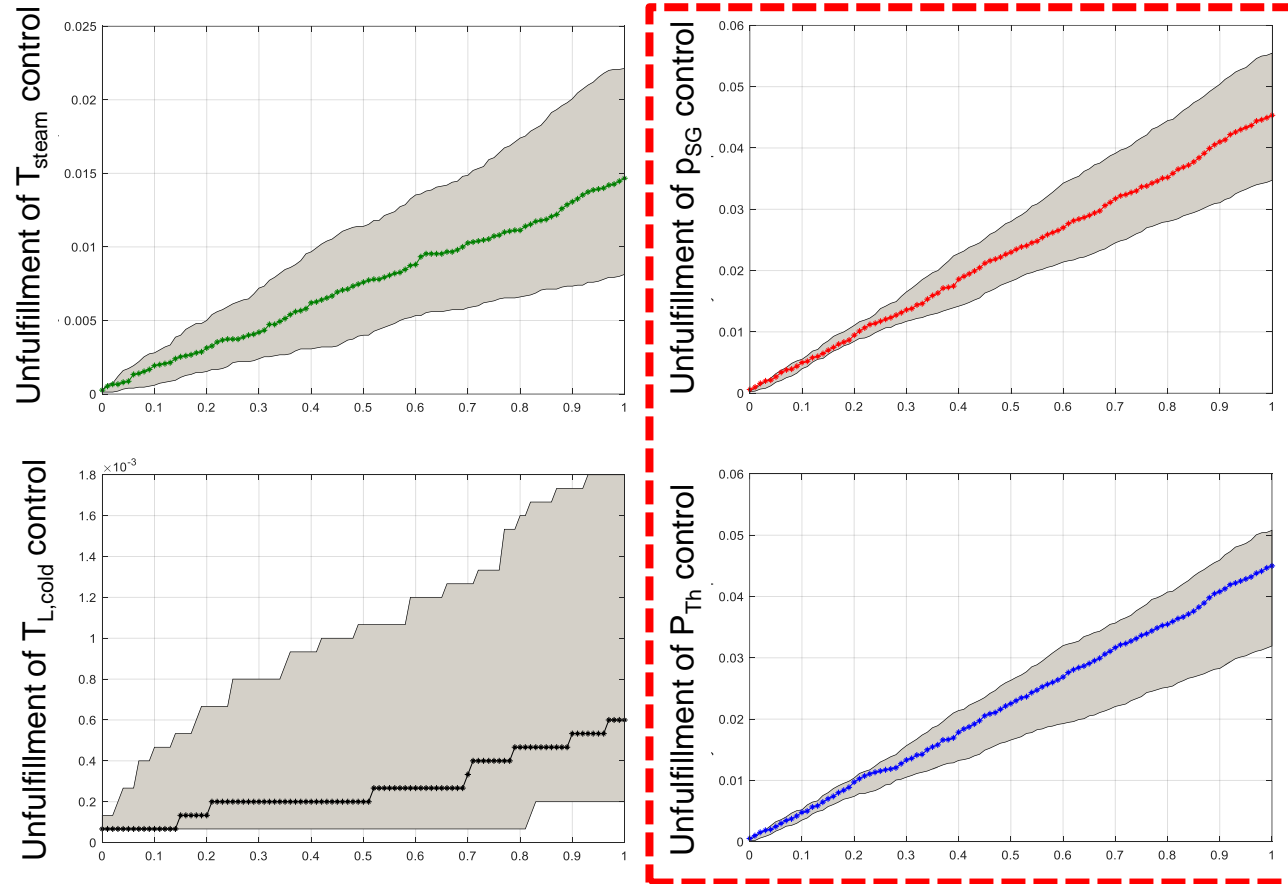
Most vulnerable functions:

- P_{Th} ($f = 4$) control;
- p_{SG} ($f = 2$) control;
- T_{steam} ($f = 1$) control.



Risk Analysis of the ALFRED by Simulation-based GTST-MLD

Bounded probabilities of sub-functions unfulfillment

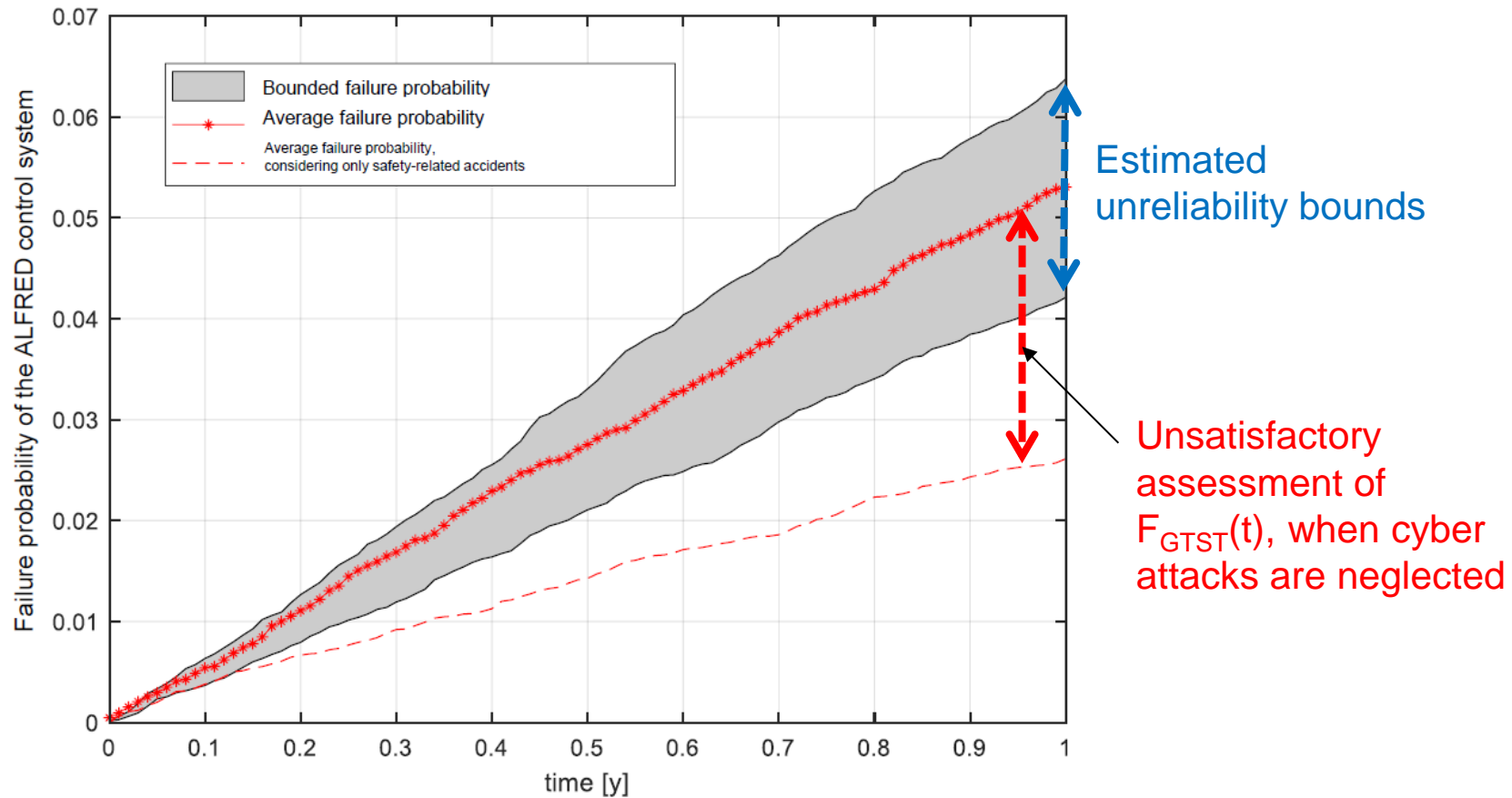


The main components failures are more likely to have adverse impacts on the p_{sg} ($f=2$) control and P_{Th} ($f=4$) control fulfillments.



Risk Analysis of the ALFRED by Simulation-based GTST-MLD

Failure probability of the ALFRED control system






What?

Novel goal-oriented framework based on GTST-MLD for risk analysis of CPSs

Why?

- 1) CPSs show a tight **combination** of (and **coordination** between) **physical** and **cyber** domains.
- 2) Risk analysis has to consider **both** (**stochastic**) components failures and (**intentional**) **cyber-attacks** to provide reliable risk estimates.

How?

- **Simulation-based inference method for assigning the weights of a GTST-MLD** model for performing the risk analysis of CPSs jointly treating safety and security aspects;
- 
- **Identification of the most vulnerable functions**



GTST-DMLD: Advantages

1. Comprehensive knowledge of the system in terms of functions, objects and their relationships.
2. Good understanding of the system structure.
3. Representation of dependencies and interdependencies.
4. Dynamic behavior modeling.
5. Cause-effect reasoning.
6. Possibility to be combined with other representation methodologies.
7. The flow can be partitioned in the system according to different priorities of the demand nodes.



1. Difficult to build and manage hierarchies for large-scale systems.
2. Unclear representation when a sequential (geographical) importance of the demands is not considered.
3. Computer-aid tools are required to handle the creation and reasoning of complex GTST-(D)MLD.



References

- [Curtois 1985] Courtois, P. J. (1985). "On Time and Space Decomposition of Complex Structures." *Communications of the Acm*, 28(6), 590-603.
- [Hu and Modarres 1999] Hu Y.S., Modarres M. (1999) Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modeling. *Reliability Engineering and System Safety* 64; 241–269.
- [Kim and Modarres 1987] Kim I.S., Modarres M. (1987) Application of Goal Tree Success Tree model as the knowledge-base of operator advisory systems. *Nuclear Engineering and Design* 104, 67-81.
- [LaRocca et al. 2011] La Rocca, S., Guikema, S. D., Cole, J., and Sanderson, E. (2011). "Broadening the discourse on infrastructure interdependence by modeling the "Ecology" of infrastructure systems." *Applications of Statistics and Probability in Civil Engineering*, M. Faber, J. Köhler, and K. Nishijima, eds., London, 1905–1912.
- [Modarres 1999] Modarres M. (1999) Functional modeling of complex systems with applications. *IEEE Proceedings Annual Reliability and Maintainability Symposium*.
- [Modarres et al. 1999] Modarres, M., Kaminskiy, M., and Krivtsov, V. (1999). *Reliability engineering and risk analysis: a practical guide*, CRC press, New York.
- [Nozick et al. 2005] Nozick, L. K., Turnquist, M. A., Jones, D. A., Davis, J. R., and Lawton, C. R. (2005). "Assessing the performance of interdependent infrastructures and optimising investments " *International Journal of Critical Infrastructures*, 1(2-3), 144-154.
- [Sanderson 2009] Sanderson, E. (2009). *Mannahatta: a natural history of New York City*, Abrams, New York.
- [Zio 2007] Zio, E. (2007). *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific Publishing Co. Pte. Ltd.