EWaSAP

An Early Warning Sign Identification Approach Based on STPA

Dr. Ioannis M. Dokas

John Feehan, Syed Imran

Cork Constraint Computation Centre

University College Cork

Ireland

Early Warning

- The expression ‘early warning’ is used in many fields to mean the provision of information on an emerging dangerous circumstance where that information can enable action in advance to reduce the risks involved

(Basher R. 2006 “Global early warning systems for natural hazards: systematic and people-centred” Phil. Trans. R. Soc. 364, 2167–2182 doi:10.1098/rsta.2006.1819)

Early Warning Signs and Accidents

- Early warning signs precede losses

- “warning signs almost always occur before major accidents”

(Leveson N. 2001,“The Role of Software in Recent Aerospace Accidents” 19 th International System Safety Conference, 10-14 September at Huntsville, Alabama. “http://sunnyday.mit.edu/accidents/issc01.pdf)

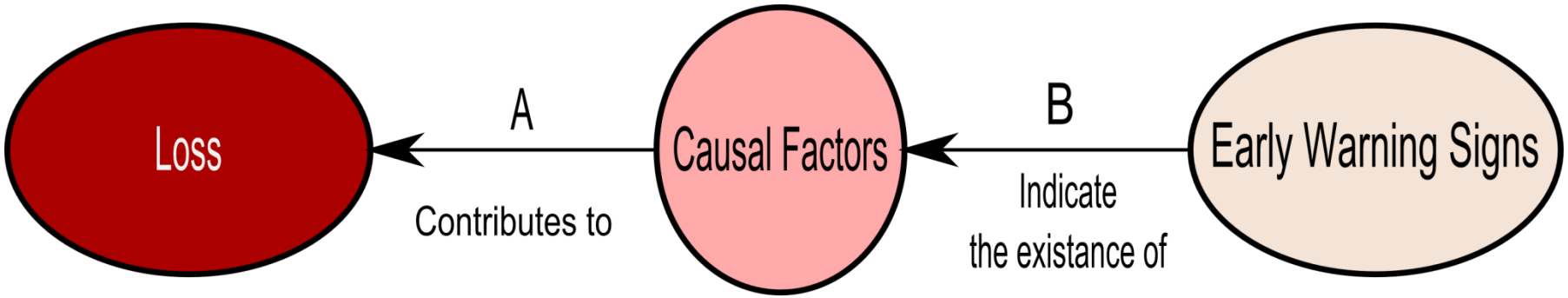
The Problem

- The safety field still lacks the concepts, tools, and measures to recognise warning signs prior to major failure events

(Woods, D. D. (2009), “Escaping Failures of Foresight”, Safety Science, 47(4), 498-501)

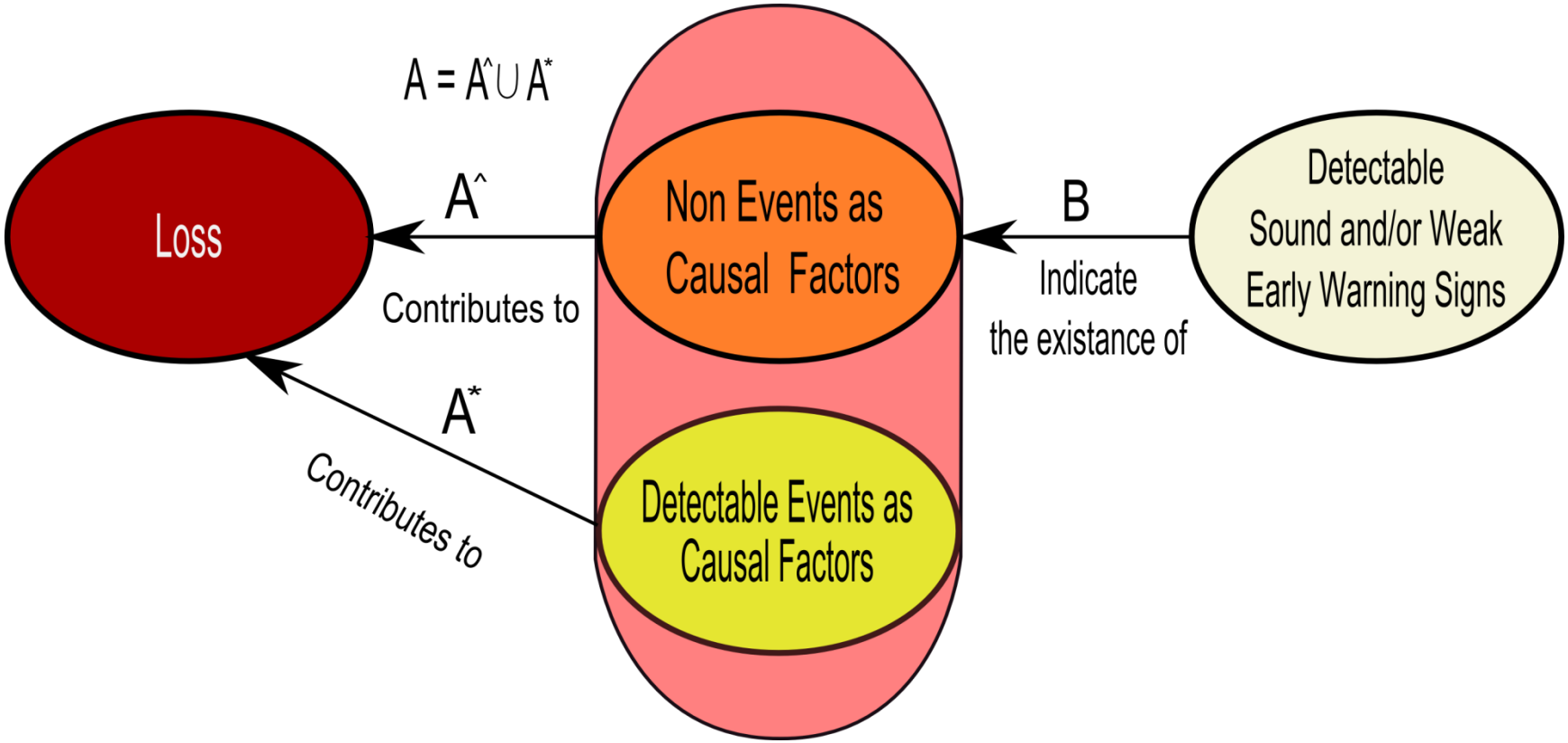
What is Needed

- **PERCEIVE** the signs
- **JUSTIFY** their relations to possible losses



A Simple Early Warning Justification Model

The EWaSAP Justification Model for Early Warning Signs



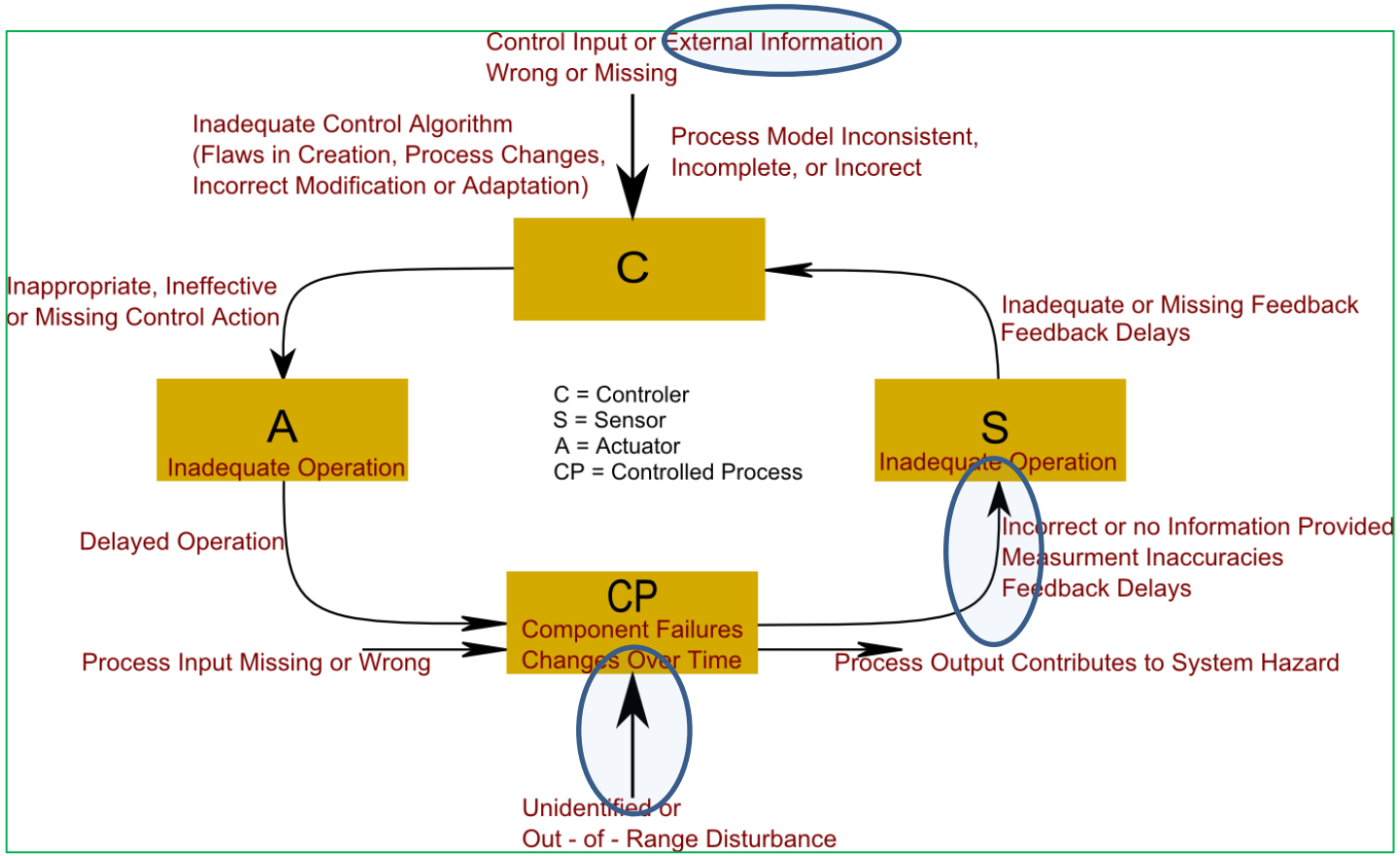
Ideally

- In order to minimize the chance of having controllers within a system with incomplete process models, feedback information **should contain as many early warning signs as possible** so that to be used for justifying the presence of contributing factors to a loss

What Usually Happens

- Due to trade offs and other constraints, the installed services able of providing awareness on internal vulnerabilities are less than those needed to achieve maximum benefit
- False warnings
- Audits
- "Voluntary/Synergetic" early warnings

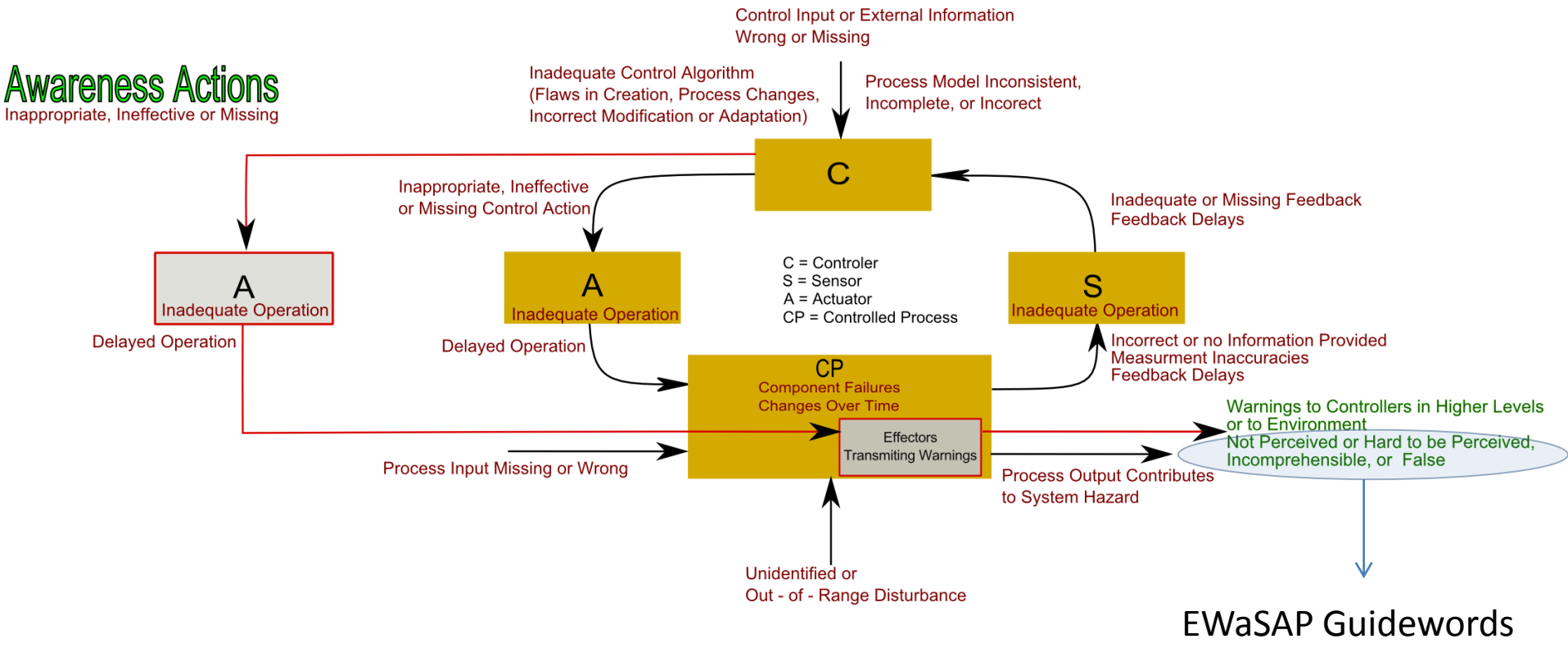
Early Warnings in STPA



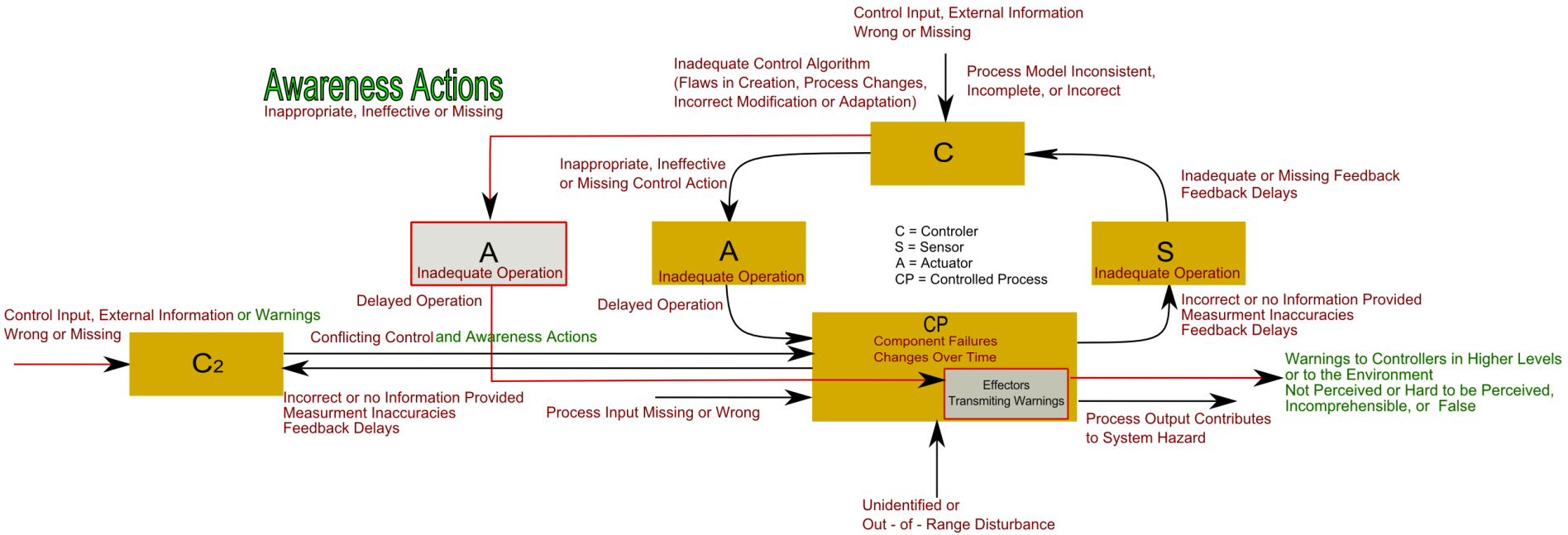
"Feedback is also critical in detecting errors and failures, both errors in the controllers ' own actions **and failures or faults in the controlled system**"

(Leveson N. 2011, "Engineering a Safer World Systems Thinking Applied to Safety ", MIT Press, England, pp 266)

STPA Loop With EWaSAP Awareness Actions and Warnings



STPA Loop With EWaSAP Awareness Actions and Warnings



A possible version of the EWaSAP add on in the multiple controllers case of STPA

Types of Awareness Actions

- Transmit “All Clear” Signs
- Transmit Warnings
- Transmit Alerts (i.e. It has been validated that a hazard occurred)
- Transmit Algedonic signals (i.e. A term originally introduced by S. Beer’s in his VSM model, implying a special transmission to inform the controllers at the highest levels about a serious condition within their organization)

EWaSAP Steps

- Two Groups
  - 1st Establish Synergy
  - 2nd Enforce Internal Awareness Actions

EWaSAP Steps

(STPA steps with Gray - EWaSAP steps with Black and with the EW prefix)

(1) Identify the hazards in the system that may allow accidents to occur. Translate these hazards into top-level safety constraints

EW (1) Decide if there is anyone outside the designed system who needs to be informed about the internally perceived progress of each hazard or of its occurrence (i.e. emergency responders)

(2) a) Create the control structure

b) For each hazard determine the inadequate control actions

1 A required control action to maintain safety is not provided.

2 An incorrect or unsafe control action is provided that induces a loss.

3 A potentially correct or adequate control action is provided too early, too late, or out of sequence.

4 A correct control action is stopped too soon.

c) Restate the inadequate control actions as safety constraints

EWaSAP Steps

EW (2) Identify Useful Sensory Services Outside of the System and Establish Synergy

EW (2.1) Requirements for External Sensory Services

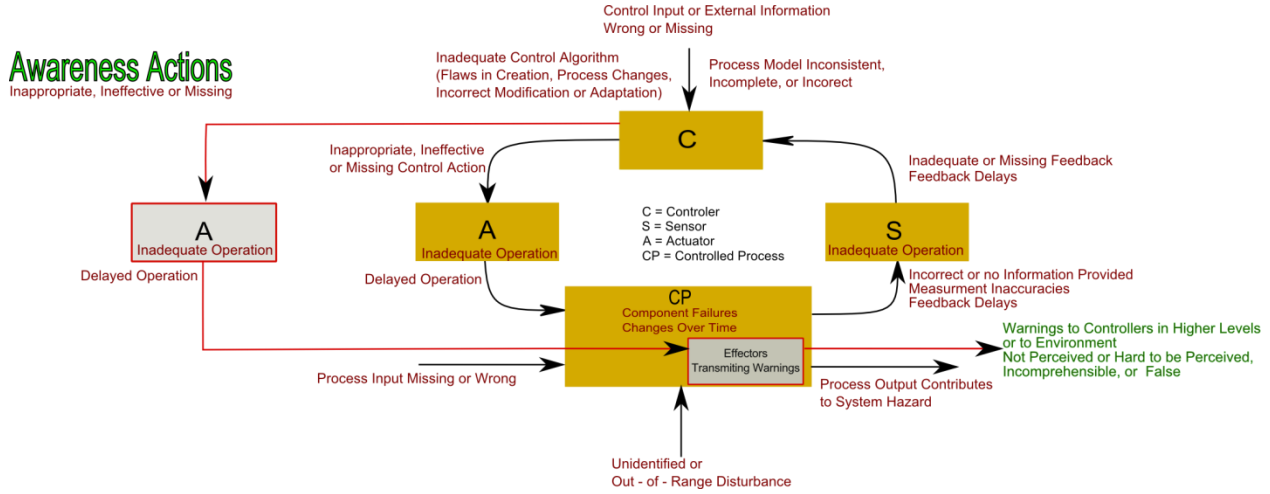
For each top level safety constraint identify the signs which indicate that it has been violated (i.e. identify the signs of the associated hazardous behaviour)

EW (2.2) Assess the Perception Capabilities of the Systems in the Surrounding Environment and Attempt to Establish Synergy

Find systems in the surrounding environment which have sensors able of perceiving the signs defined in the previous step and request to establish synergy. The objective is to agree on enforcing the appropriate awareness actions in their systems, enabling them of transmitting voluntary/synergetic early warnings about your system to the appropriate recipients as per EW(1)

EWaSAP Steps

- (3) Determine how the safety constraints determined in Step (2) could be violated.
- a) Create the process models for each controller .
- b) Examine the parts of the process control loops to determine if they can contribute to or cause system level hazards.



EWaSAP Steps

EW(3) Enforce Internal Awareness Actions

For each flaw in the process control loop do the following:

EW(3.1) Requirements for Internal Sensory Services

Describe what needs to be monitored, and what type of features/capabilities the sensors must have so that to be able to perceive the warning signs indicating the occurrence of the flaw

EW(3.2) Define the Early Warning Signs

After the design trade offs and when it is known which sensors have been selected, define the data indicating the occurrence of the flaw so that to be perceived by the sensor

EWaSAP Steps

EW(3.3): Update the Process Model of the Appropriate Controller(s)

Define appropriate awareness and control actions based on the perceived early warning signs so that to warn about, adapt to, or eliminate the causal factor to the loss which is present in the system

EW(3.4): Define the Meta Data of the Early Warning Signs

For each identified warning sign of the previous step, define its meta-data/attribute values (i.e. how the message will be coded/written by the transmitter) so that to ensure that it will be perceived and ultimately understood by the appropriate controller/s

The High Energy Example

EWaSAP tries to give answers to these questions

What data should be perceived in order to make the appropriate controller aware of the occurrence of these flaws?

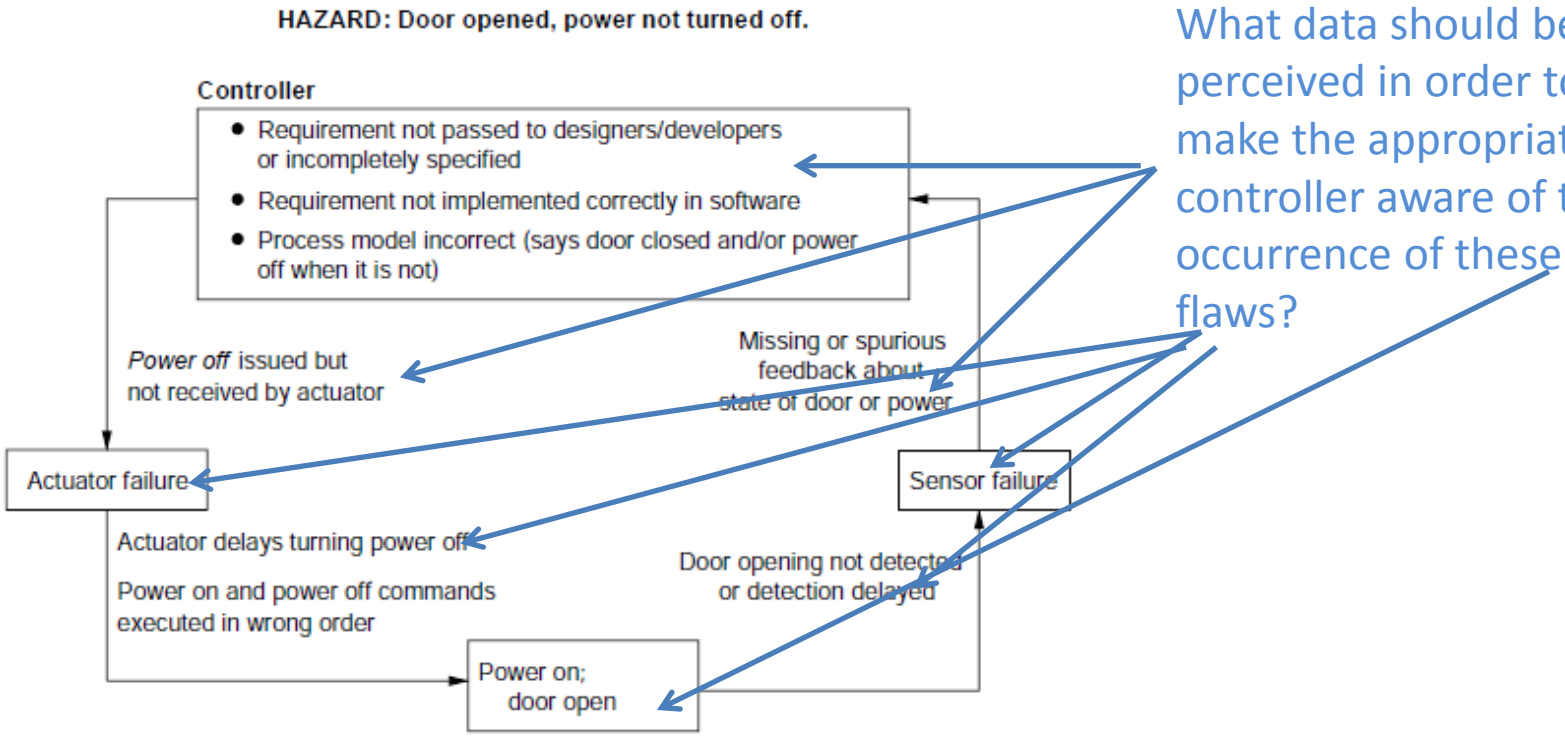
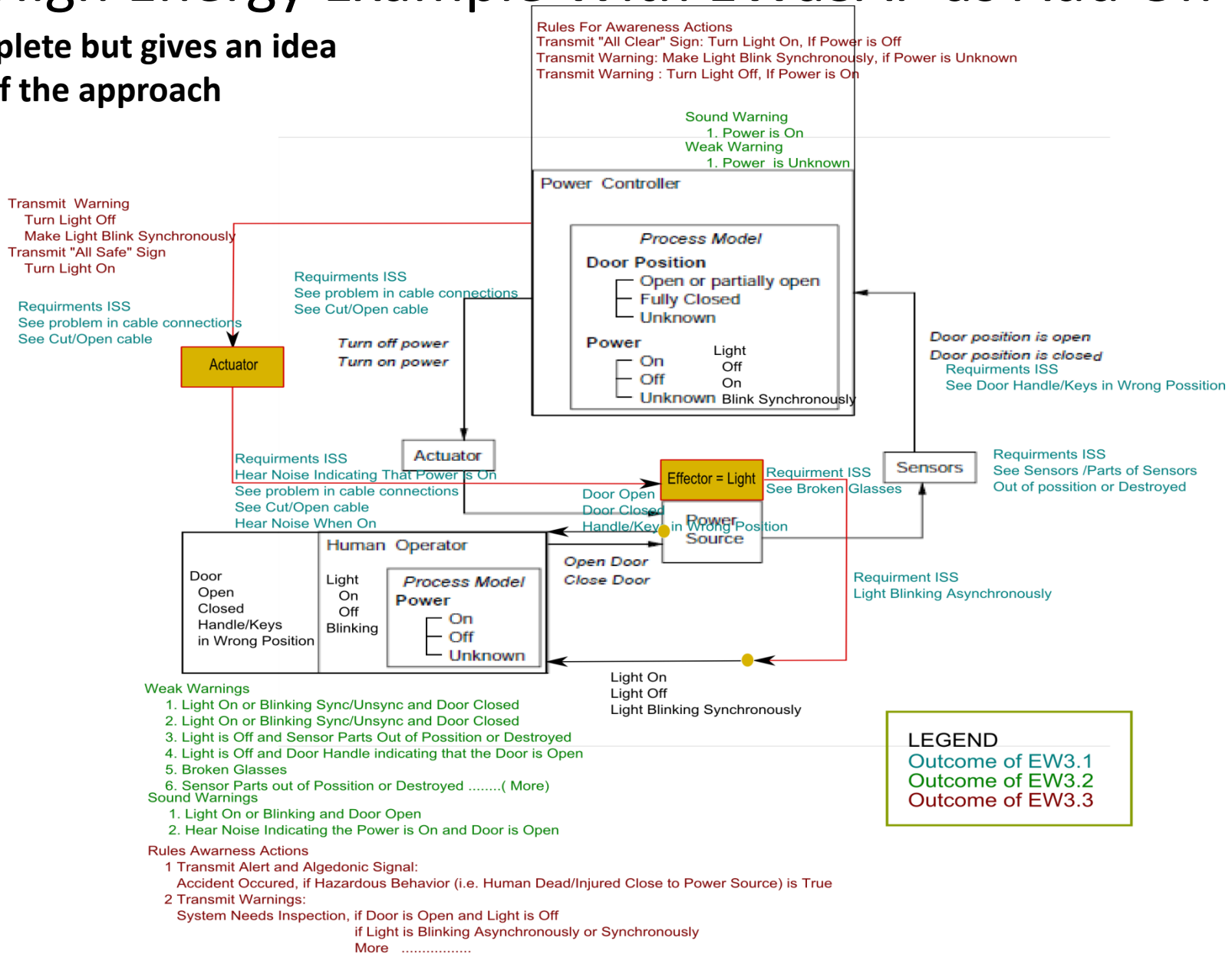


Figure 8.7
Example of step 2b STPA analysis for the high power interlock.

Figure Source:
Leveson N. 2011, "Engineering a Safer World Systems Thinking Applied to Safety ", MIT Press, England)

The High Energy Example With EWaSAP as Add On

Not complete but gives an idea of the approach



Test of EWaSAP

- Case study on the disinfection process of a Drinking Water Treatment Plant
- Aim to compare the early warning signs in the existing safety management system with the signs identified by EWaSAP
- With EWaSAP a significantly larger number of early warning signs were defined

Summary

- EWaSAP is an Add-On to STPA
- Aim: Provide a structure method for the identification of early warning signs
  - and help making controllers are as much as aware as possible about the vulnerabilities in their systems
- Emphasis to Awareness Actions
- First results are positive

Thank you

Dr. Ioannis M. Dokas

e-mail: **i.dokas@4c.ucc.ie**

Cork Constraint Computation Centre

SCEWA
Support To Organizations In Providing Early Warning Services

epa
Environmental Protection Agency