Understanding STAMP/STPA through a daily life example

Rodrigo Martins Pagliares, Francisco Lemos, Celso Massaki Hirata

Fourth STAMP Workshop, MIT - Massachussets Institute of Technology

March 26, 2015.

Authors

- **Rodrigo Martins Pagliares**
  - Instituto Tecnológico de Aeronáutica, **ITA**, São José dos Campos, SP, Brazil.
  - Universidade Federal de Alfenas, **UNIFAL-MG**. Alfenas, MG, Brazil.
  - pagliares@bcc.unifal-mg.edu.br

- **Francisco Lemos**
  - Instituto de Pesquisas Energéticas e Nucleares, **IPEN**, São Paulo, SP, Brazil.
  - flemos@ipen.br

- **Celso Massaki Hirata**
  - Instituto Tecnológico de Aeronáutica, **ITA**, São José dos Campos, SP, Brazil
  - hirata@ita.br

Agenda

1. Introduction
2. Example
3. Step 1
4. Step 2
5. Discussions

Application of STAMP/STPA

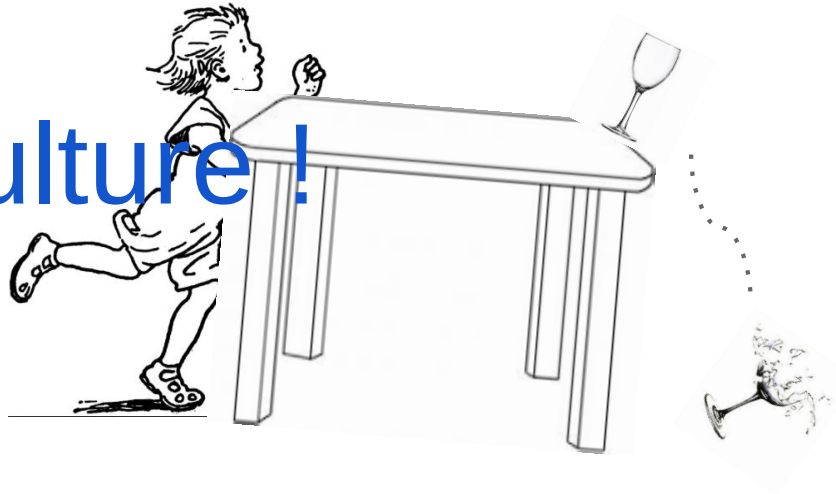
- The application of **STAMP/STPA** is not an easy task
  - Even **experienced professionals** have difficulties to apply some STAMP/STPA **principles** and **concepts**.

- One **possible reason** is that it requires a **different way** of understanding **systems** and analyzing the **interactions** between **components**.

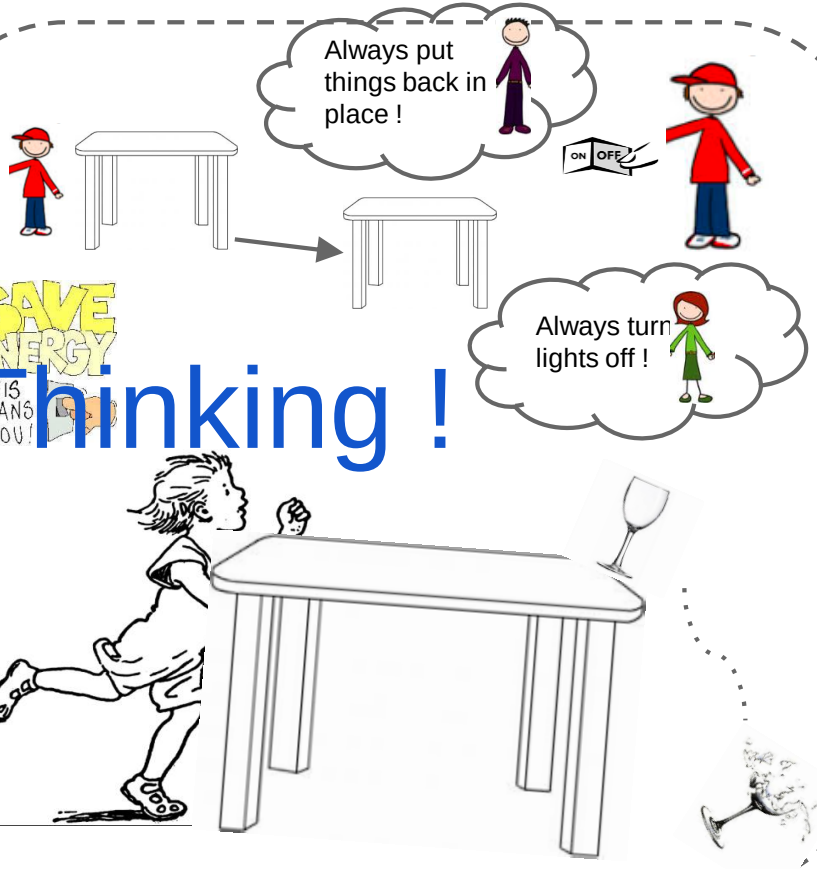
Goal

- The **main goal** of our **work** is to **help analysts** to both **understand** and **use** STPA
  - To get the **most** of its **benefits** !

Blaming culture !



Systems Thinking !



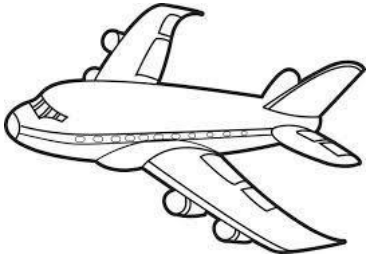
Accidents

- **Accident** is defined as an **unacceptable loss**.
  - It is a **result** of a **system's hazardous state** in **combination** with a **worst-case set of environmental conditions**.

Sociotechnical system

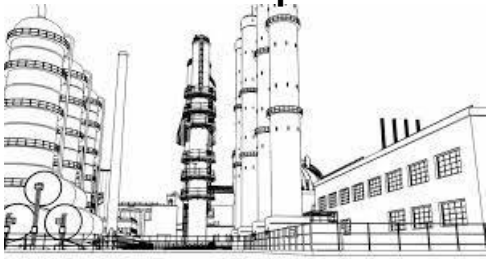
- Every **sociotechnical system** has the s**ame structure**:

Aircraft



Nuclear power plant

Chemical plant



Our system

- **Human** controllers
- **Automated** controllers
- Controlled **process**.

A daily life example

- Although some **published works** do **illustrate** the use of **STPA** in some detail, the reader suffers from the obstacles of understanding the **particularities** of the **domain**.

- In order to make this work understandable to a **broad audience**, we employ STPA in the context of a **daily-life example**

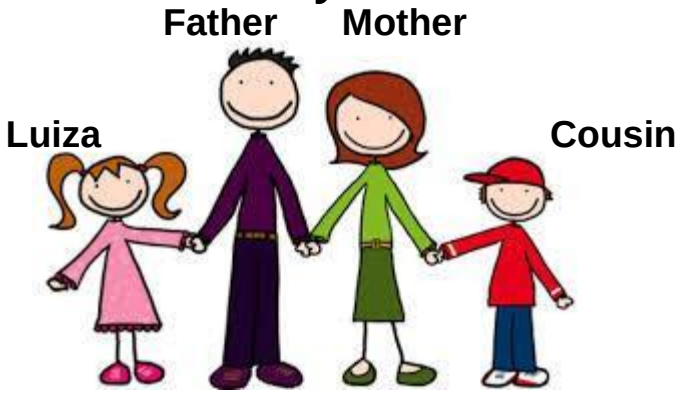
Example

- We present a **daily life example** of the use of **STPA**

- In this **system**, the **family members** are the **human controllers** and the **daily life activities** are viewed as the **controlled process**.

Example

- This example is about a typical **family**, composed of a **father**, a **mother** and one **daughter**, named **Luiza**.
  - We also included a visitor, a **Luiza's cousin**.
  - The **family members** and the **cousin** are **controllers** in a system we call "**Home**"



Our system

- As **humans** we all live in **society** and our lives are affected by **district**, **city**, **state**, **national** and **global connections**, which give us **infinite possibilities** to define the **system**.

- Therefore, to start our study, we need to define the **boundaries** of our **system**.
  - We decided to study the **family life** inside their **home, assuming** the **boundaries** are **drawn** at the **physical limits** of their **house**.

Our system

- We chose to name the system as “**home**”, instead of “**house**”.
  - The reason is that one common **difficulty** some people have, while **modeling** the **system**, is to **differentiate** the **physical structure** from the **control structure.**

House?

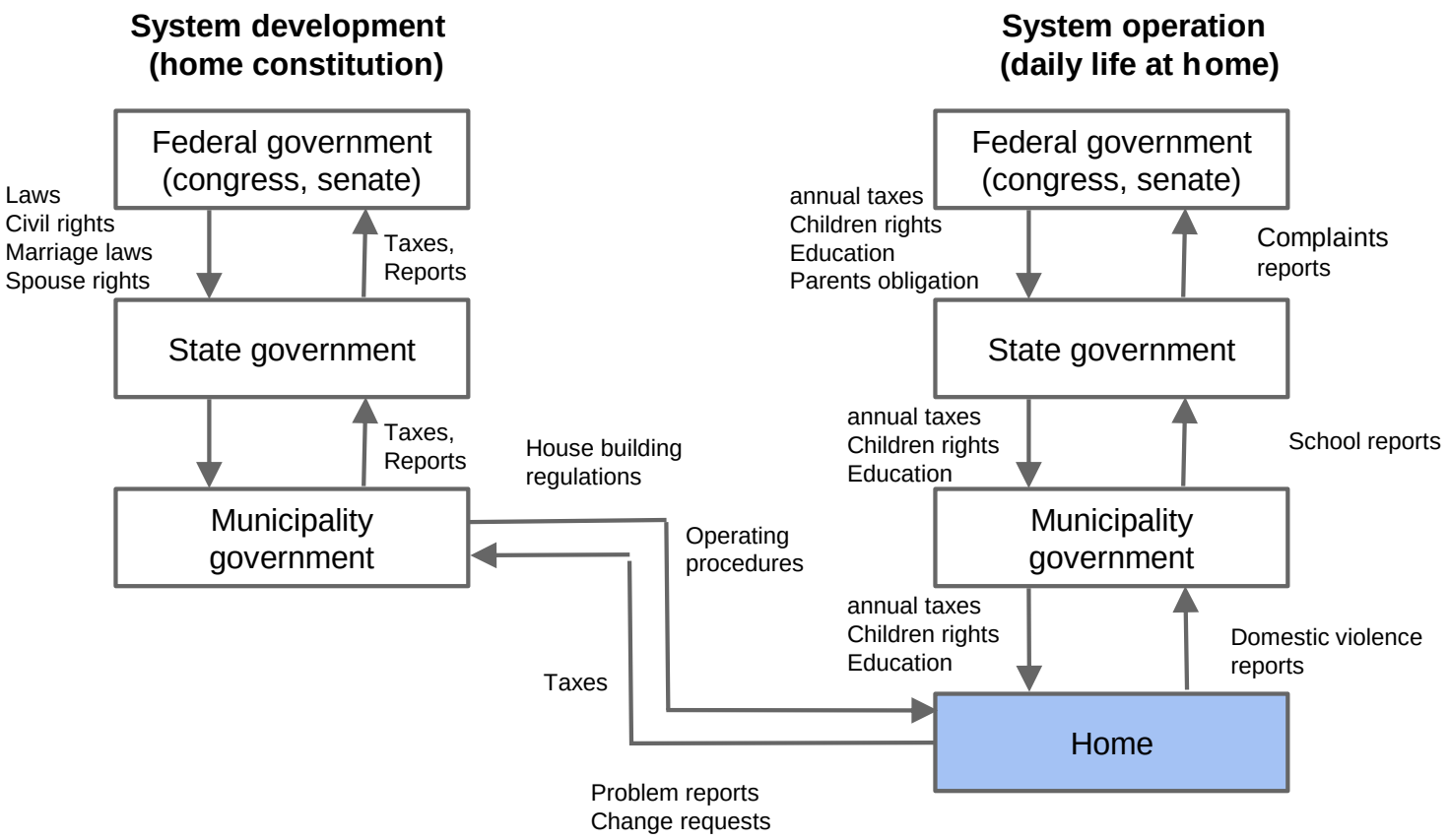
Home?

System elements

- **Human Controllers**:
  - The **family members**
    - father, mother, daughter and a cousin

- **Controlled Process**:
  - The **daily life activities** related to:
    - education, personal health, finances, nutrition, etc.

High-level safety control structure



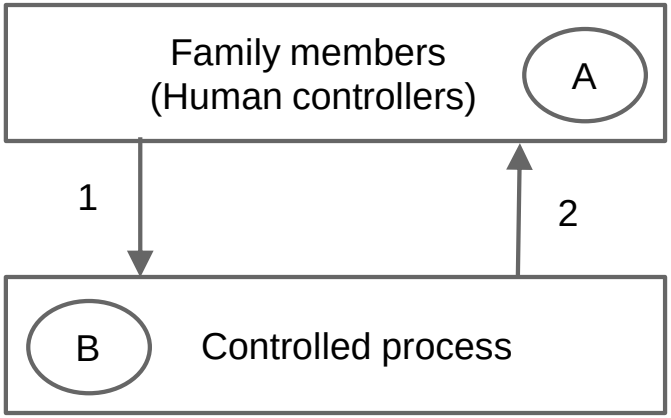
The home system

A. Human Controllers

- Father
- Mother
- Daughter
- Cousin

B. Controlled proces

- Cleanness of floor
- Furniture location or arrangement
- Food quality
- Health of family members
- Condition of home objects such as glasses, dishes, et (broken, clean, ...)



Control structure for a typical home

System goals

- **System** is an **entity** that has **goals** that are defined according to **stakeholders**.

- In **our example**, the following **goals** are defined:
  - **G1**: Luiza's successful education
  - **G2**: Family members living healthy and unharmed
  - **G3**: Family economically sound

Accidents

- In our example, we defined **5 accidents** as listed below:
  - **A1:** Luiza fails to achieve success at school
  - **A2:** Family bankruptcy
  - **A3:** Member of the family gets sick
  - **A4:** Member of the family gets injured
  - **A5**: Damage to equipment

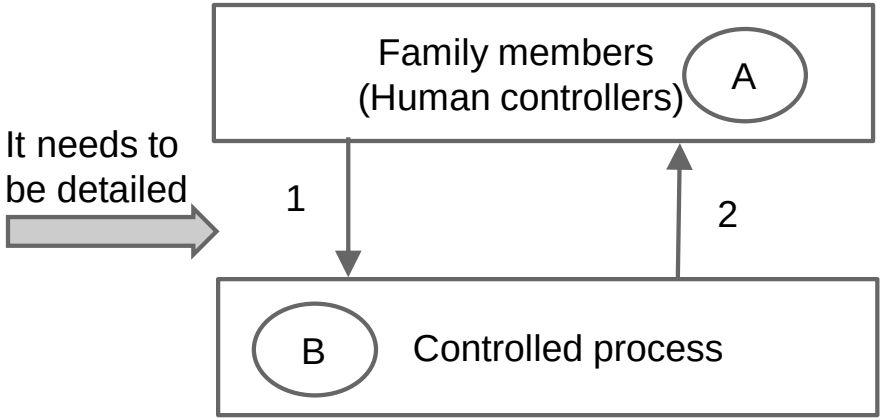
Hazards in the system home

A1: Luiza fails to achieve success at school
A2: Family bankruptcy
A3: Member of the family gets sick
A4: Member of the family gets injured
A5: Damage to equipment

- **H1** - Messy house **[A1] [A3] [A4]**
  - **H1.1** - Objects and furniture misplaced **[A4]**
  - **H1.2** - Family member acting recklessly **[A1] [A2] [A3] [A4][A5]**
- **H2** – Children not doing well at school **[A1]**
- **H3** – Family owing more than earns **[A2]**
- **H4** – Unhealthy living condition **[A3]**

Detailed control structure

- We need to build a more **detailed control structure** for the **system, identifying:**
  - **Responsibilities**, **mental maps**, **control actions** and **algorithms** for each controller
  - The **level of hierarchy** for the **controllers**



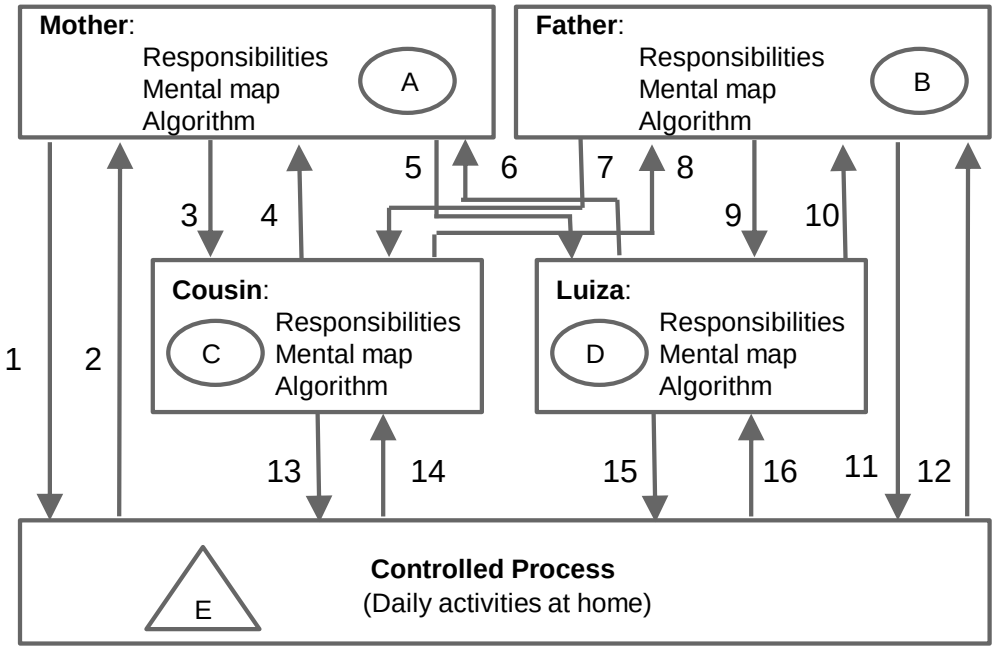
Detailed control structure

A. Mother (Controller)
Responsibilities:

- make sure children get proper nutrition and healthy habits; the house is well kept;
- keep a healthy mental environment;
- food preparation;

B. Father (Controller)
Responsibilities:

- provide financial support for school; food;
- keep a healthy mental environment;
- entertainment activities; house cleaning;
- nutrition; family member's health;

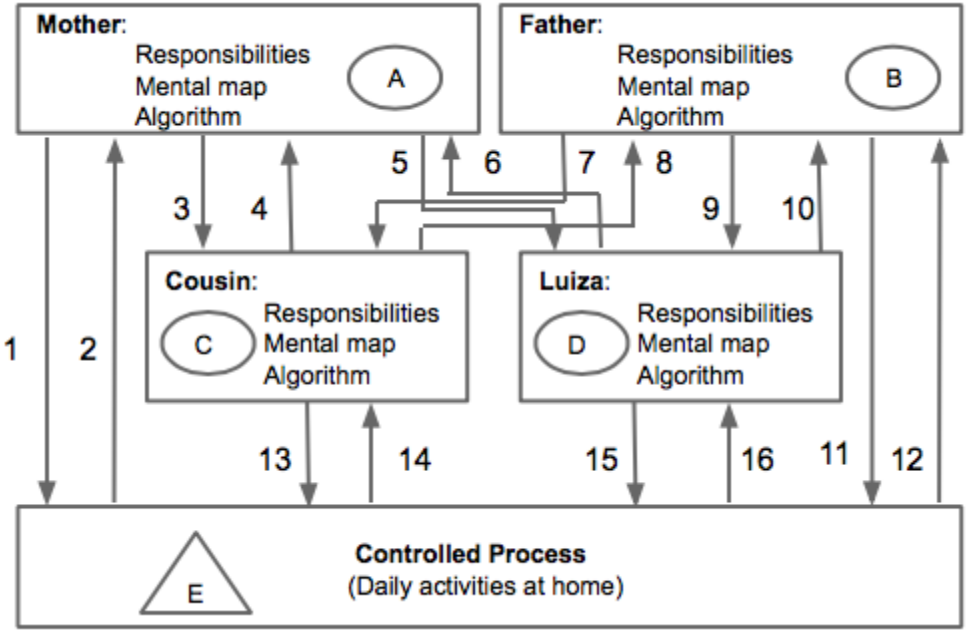


Detailed control structure

C. Cousin (Controller)

Responsibilities:

- following home rules.
- put back everything he uses
- cooperate with other members of family
- fulfill his appointments
- turn of the lights when there are no people in room

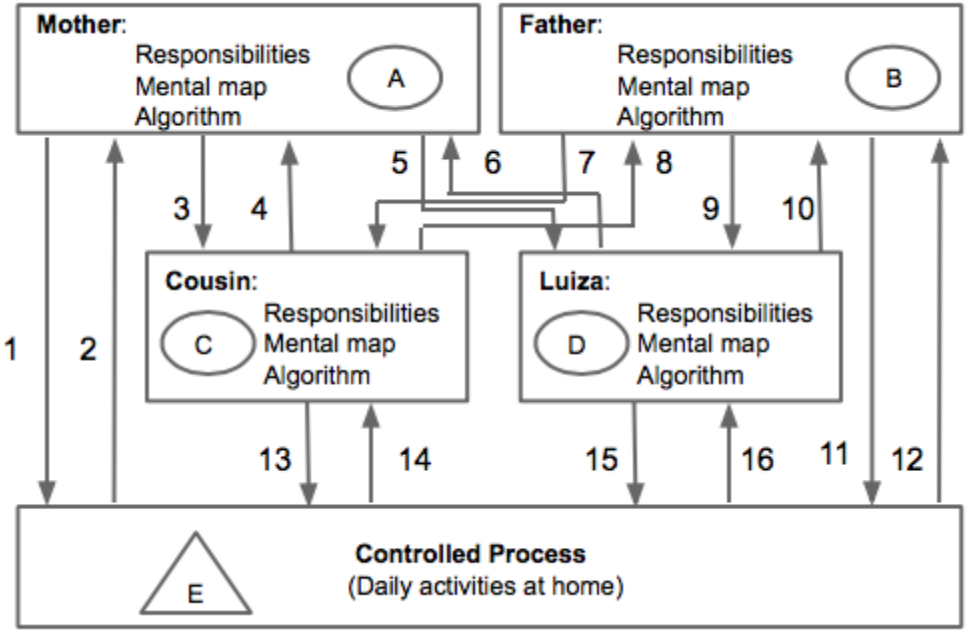


Detailed control structure

D. Luiza (Controller)

Responsibilities:

- keep the house always clean ensuring that no objects get broken during cleaning
- keep her room in order
- do homework
- follow home rules
- eat correctly



Detailed control structure

1. Control actions (Mother => Home):

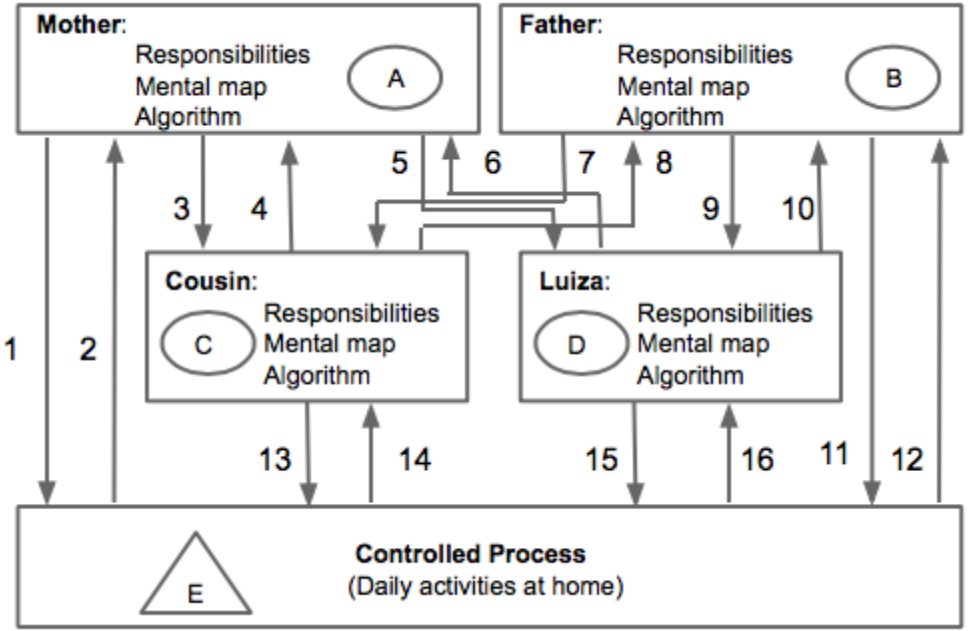
- furniture arrangement
- help chose balanced meals

2. Feedback (Home => Mother):

- furniture position
- cold floor
- dirty glass is not in kitchen sink

3. Control actions (Mother => Cousin):

- reward
- instruct



Detailed control structure

10. Feedback (Luiza => Father):

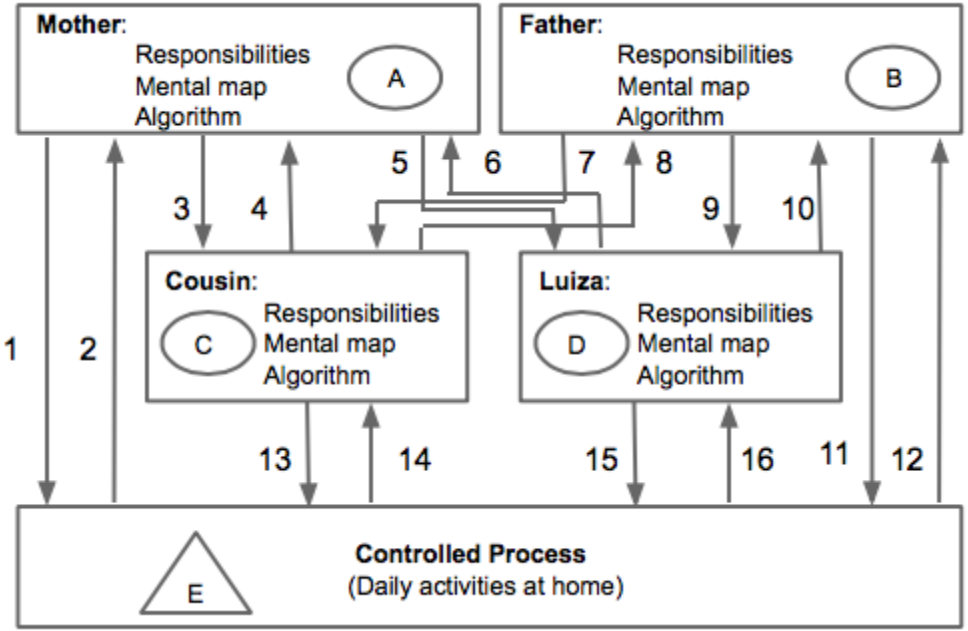
- school reports
- health complaints
- conversations with cousin

11. Control actions (Father => Home):

- furniture arrangements
- Help chose balanced meals

12. Feedback (Home => Father):

- furniture position
- utensils position
- Luiza is wearing slippers
- Luiza's health
- floor temperature (Cold floor)



Prioritization

List of goals	List of accidents	List of system hazards
G1: Luiza's successful education **G2**: Family members living healthy and unharmed **G3**: Family economically sound	**A1:** Luiza fails to achieve success at school **A2:** Family bankruptcy **A3:** Member of the family gets sick **A4:**Member of the family gets injured **A5**: Damage to equipment	**H1:** Messy house **[A1] [A3] [A4]** ○ **H1.1:** Objects and furniture misplaced **[A4]** ○ **H1.2:** Family member acting recklessly **[A3] [A4] [A5]** **H2**: Children not doing well at school **[A1]** **H3**: Family owing more than earns **[A2]** **H4**: Unhealthy living condition **[A3]**

Prioritization

List of goals	List of accidents	List of system hazards
G1: Luiza's successful education **G2: Family members living healthy and unharmed** **G3**: Family economically sound	**A1:** Luiza fails to achieve success at school **A2:** Family bankruptcy **A3:** Member of the family gets sick **A4:**Member of the family gets injured **A5: Damage to equipment**	**H1: Messy house [A1] [A3] [A4]** ○ **H1.1: Objects and furniture misplaced [A4]** ○ **H1.2: Family member acting recklessly [A3] [A4] [A5]** **H2**: Children not doing well at school **[A1]** **H3**: Family owing more than earns **[A2]** **H4**: Unhealthy living condition **[A3]**

Unsafe control actions

Table 1. Unsafe control actions for the Luiza's home example (Luiza).

Luiza control action	Not providing causes hazard	Providing causes hazard	Too wrc haz	
Take the dirty glass to the kitchen sink (walking)	Hazardous **[H1.1] [H4]** Food will deteriorate and cause contamination	Hazardous **when** conditions are not favorable **[H1.1] [H1.2]**	NA	
Speed up when heading to the kitchen sink	Hazardous **when** cold floor and Luiza is barefoot **[H4]**	Hazardous **when** conditions are not favorable (e.g. bump a table or other furniture and breaking something) **[H1.1] [H1.2]**	NA	
Put on slippers	Hazardous **when** cold floor **[H4]**	Not hazardous	**[Too late]** Hazardous **when** Luiza wears the slippers after taking the dirty glass to the kitchen sink and cold floor **[H1.2] [H4]**	**[Too soon]** Hazardous **when** Luiza takes the slippers off in the middle way to the kitchen sink and cold floor **[H1.2] [H4]**

H1: Messy house **[A1] [A3] [A4]**
- **H1.1:** Objects and furniture misplaced **[A4]**
- **H1.2:** Person behaving absently **[A3] [A4] [A5]**

H2: Children not doing well at school **[A1]**

H3: Family owing more than earns **[A2]**

H4: Unhealthy living condition **[A3]**

H5: Family member acting recklessly.

Unsafe control actions

Table 2. Unsafe control actions for the Luiza's home example (Cousin).

Cousin control actions	Not providing causes hazard	Providing causes hazard	Too wron haza	
Put table back in place	Hazardous **when** the table is not in its original place **[H1.1]**	Hazardous **when** he moved the table into a not usual place **[H1.1] [H5]**	NA	
Turn off the kitchen light	Hazardous **when** there is nobody is at the kitchen **[H1] [H3]**	Hazardous **when** furniture is out of place **[H1.2]**	**[Too early]** hazardous **when** there are still people in kitchen **[H1.2]**	NA

H1: Messy house **[A1] [A3] [A4]**
- **H1.1:** Objects and furniture misplaced **[A4]**
- **H1.2:** Person behaving absently **[A3] [A4] [A5]**

H2: Children not doing well at school **[A1]**

H3: Family owing more than earns **[A2]**

H4: Unhealthy living condition **[A3]**

H5: Family member acting recklessly.

Safety constraints

Table 3. Unsafe control actions from Table 1 (Luiza) and their correspondent safety constraints

Unsafe control action (Luiza)	Safety constraint
Take the dirty glass to the kitchen sink	Not provided => [H1.1] [H4]. **Luiza must always things on their right place** Provided => [H1.1] [H1.2]. **She must always avoid or mitigate bad environmental conditions**
Speed up when heading to the kitchen sink	Not provided => [H4]. **She must always speed up to mitigate environmental conditions.** Provided => [H1.1] [H1.2]. **Luiza must always be aware of furniture position**
Put on slippers	Not provided => [H4]. **Luiza must always wear slippers when floor is too cold** Provided too late => [H1.2] [H1.4]. **Luiza must always wear the slippers before taking the dirty glass to the kitchen sink and the floor is cold** Stopped too soon => [H1.2] [H4]. **Luiza must keep the slippers on during all the way to the kitchen sink**

Safety constraints

Table 4. Unsafe control actions from Table 2 (Cousin) and their correspondent safety constraints

Unsafe control action (Cousin)	Safety constraint
Put table back in place	Not provided [H1.1] [H5] => **The cousin must always take the table back to original place**. Provided => [H1.1]. **The cousin must be informed of the right position of the house furniture.**
Turn off the kitchen light	Not provided => [H1][H3]. **The cousin must always turn the lights off when nobody at the kitchen.** Provided => [H1.2]. **The furniture must always be visible when out of place.** Provided too early => [H1.2]. **The cousin must not turn off the lights when there are still people in the kitchen**

Step 2

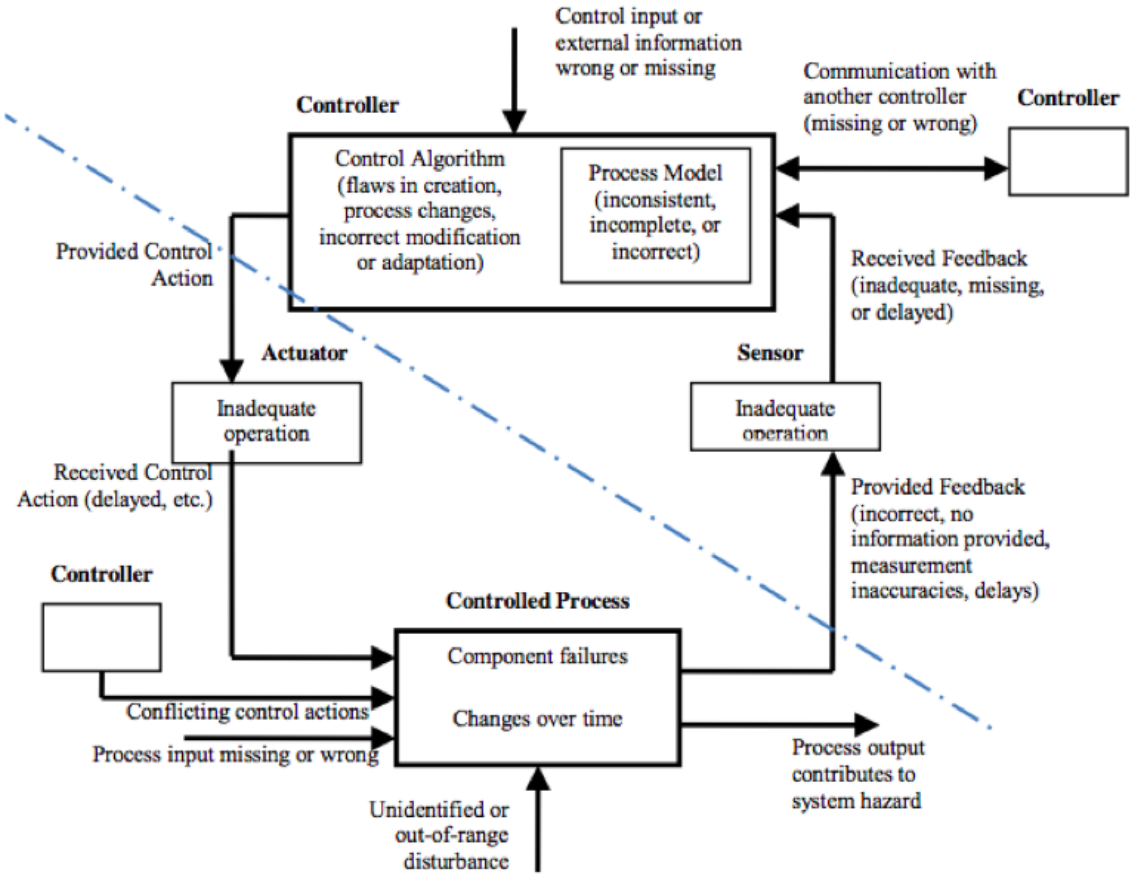


Figure 4. Generic control loop for one controller [1] [9].

Step 2: Causal Factors

Table 5. Unsafe control action scenarios and associated causal factors for Luiza

UCA : Speed up when heading to kitchen sink (Daughter)

Scenario	Associated causal factors
[Communication flaw] Luiza is unaware of the cousin changing the furniture position	Luiza is not informed about the change of the table position. Cousin moves the table to a position he thinks is the correct one.
[Lack of or incorrect feedback] The lights are turned off	The cousin turns off the kitchen lights because nobody is inside.

Step 2: Causal Factors

Table 6. Unsafe control action scenarios and associated causal factors for the cousin.

UCA : Put table back in place (Cousin)

Scenario	Associated causal factors
[Inconsistency between mental map of the cousin and state of the system] In his mental map he thinks the table should be in a position different from the right position. **[Lack of or incorrect feedback]** Other family members have a different mental map from the cousin Other family members are not informed about the change.	Accordingly to his responsibility he should put the table back to its original position. He is not informed about what should be the exact position of the table Luiza's Parents thinks her cousin knows what should be the exact position of the table

Discussions: common problems

- Some **common problem**s that also **exist** in **other systems** could be **found** in **our example** as well
  - For example, **multiple controllers**, **common variables**, **priority of access** to **equipment**, etc.

Discussions: culture of blame

- We could see that, although we are analyzing **simple daily life activities**, how **difficult** it is to get **rid of** the **culture of blame**.

- For example, it could easily be **concluded** that:
  - **Luiza** should have **checked furniture position**
  - **Luiza** should have been careful **not to run**
  - **Luiza** should have been **cautious** and **always put slippers** on when **walking** on **cold floor**

Discussions: safety culture

- Another **lesson learned** from this example is that, although the **control structure is fixed**, we should keep in mind that the **human relations** are **dynamic**.

- This reminds us of the **safety culture**, which can lead to serious **violations** of **safety constraint**s, making the **system** to **migrate** to **hazardous states**.
  - This could be an interesting subject for a **follow on work**.

Thank you !