Apply STAMP to Safety Standards of home-surveillance Robots

Mitka Eleftheria, Spyridon G. Mouroutsos
Democritus University of Thrace,
Electrical and Computer Engineering,
School of Engineering, Greece
Contact details:
em3933@ee.duth.gr
sgmour@ee.duth.gr

Presentation for:
MIT STAMP Workshop

Standards…

- Useful tool in determining how adequate safety potential behaviour can be achieved by a system, especially with respect to its interaction with other systems.
- Define the design and development activities and offer enough confidence that these guidelines are actually contented in any specific level of the system.

Safety Standards

- Describe a compromise as to what constitutes best practice in achieving safety in systems, and what comprises best practice in the design level used for the production.
- Since specific safety standards for home-surveillance robots are not available, we propose that their safety standards should be carried out on the base of STAMP that is discussed here.

Robotic System

- Comprising robot, end-effector, any equipment, devices, or sensors required for the robot to perform its task, and any communication interface that is operating and monitoring the robot, equipment, or sensors, as far as these peripheral devices are supervised by the robot control system.

Domestic Robot

- Mechatronic system for residential home use.
- The term “domestic” indicates the use domain which is the domestic environment.
- Completes a wide variety of tasks such as vacuum cleaning, fetch and carry tasks, lawn mowing, window cleaning etc.

Home-surveillance robots

- They gather information and report back, offering home intervention and security services, protecting user's property from sudden dangerous situations and particularly against crime.
- They ward off remote or local defenders from entering a property.
- Audio/ video sense, low mobility, audio output, ultrasound, microwaves, and lasers or inform police station through telephone or wireless 802.11 network used as primary communication mode.

Home-surveillance Robot - Illustration

Sociotechnical System

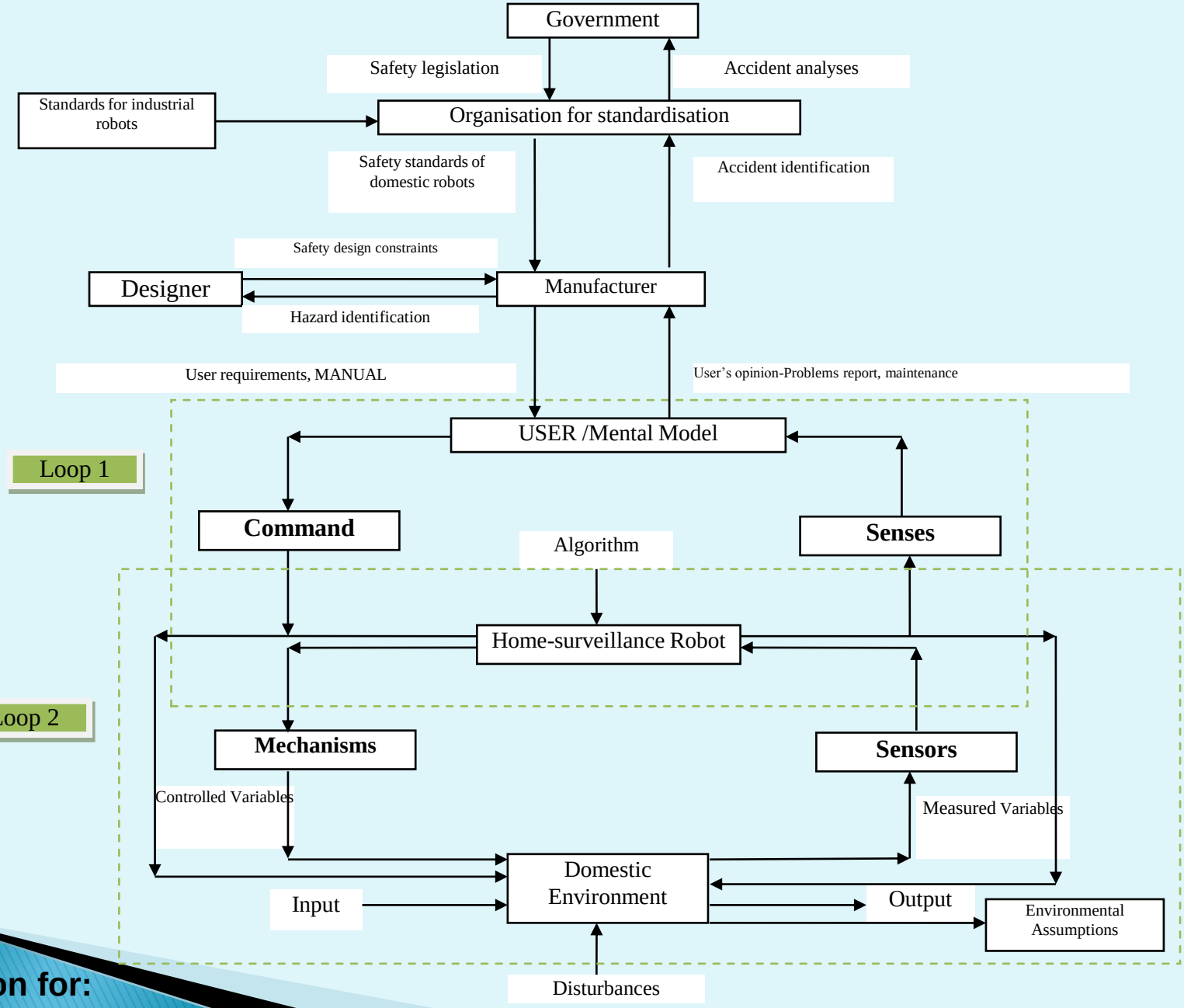
- They are far beyond a group of technological artifacts.
- Home-surveillance robots could be considered as socio-technical systems since they are capable of taking over chores in the house which is inhabited by groups of people and human-robot interactions constitute basic functions of any of these robotic systems.
- Their safety standards should be carried out on the base of STAMP.

STAMP–(1)

- **Safety**: an emergent property and not an element property that derives from the interaction among the components and shall be controlled at system level not at level of interrelated components.
- **Accidents** are complex processes involving the entire socio-technical system.
- **Hazard identification** is a top-down procedure that eliminating or controlling a hazard that is possible to lead to an unacceptable loss.

STAMP–(2)

- Covers the whole range of **management** of a system.
- It goes far beyond covering only the hardware and the related process models of safer systems.
- It includes designing and production stage, management of a socio-technical system such as the **coexistence human – robot** at home, the relation between manufacturer, user and government that results from **safety standards** with respective **safety requirements**, interface from industrial to domestic safety, effect of the use of safety standards on accident analysis.
- All the above **non-technical features** of this system could not be disregarded.



Presentation for:

MIT STAMP Workshop

Indentify the accidents – (1)

- **A1.** An intruder interrupts the robot's network which is infrastructure 802.11 wireless, leaking private information through MAC addresses. Eavesdrop on private information is intercepts even if the network is protected by WEP, WPA, or WPA2 encryption. An intruder could hijack valid username and password by eavesdropping on ad hoc mode or on 802.11 wireless mode of robot.
- **A2.** A remote attacker interrupts packets aloof over the Internet stealing opprobrious photos.
- **A3.** A wireless attacker is aggressively cracking the robot's home network controlling the robot so as to fall from stairs or jumping out of a window.
- **A4.** A defender may control the audio capabilities to upset a child.

Indentify the accidents – (2)

- **A5.** The constantly on nature of a home surveillance robot indicates greater capabilities for an intruder to control the robot in order to spy on a house.
- **A6.** A defender could impose the deficiencies of the robot to cause property damage in the domestic environment.
- **A7.** Watch a child in private locations through robot's mobile video camera in case the robot is in remote access mode.
- **A8.** Direct sunlight or infrared signals towards robot's sensors cause interference.
- **A9.** The released electrolyte of an intended open of the power pack may cause damages to skin or eyes.

Assign a level of severity

- Level 1:
- A1-1: An intruder interrupts the robot's network with infrastructure 802.11 wireless, leaking private information through MAC addresses.
- A1-2: A wireless attacker is aggressively cracking the robot's home network controlling the robot so as to fall from stairs or jumping out of a window.
- A1-3: A defender may control the audio capabilities to upset a child.
- A1-4: The constantly on nature of a home surveillance robot indicates greater capabilities for an intruder to control the robot in order to spy on a house.
- Level 2:
- A2-1: A defender could impose the deficiencies of the robot to cause property damage in the domestic environment.
- A2-2: Direct sunlight or infrared signals towards robot's sensors cause interference.
- Level 3:
- A3-1: A remote attacker interrupts packets aloof over the Internet stealing opprobrious photos.
- A3-2: Watch a child in private locations.
- A3-3: Released corrosive electrolyte affects human skin and eyes.

Identify safety requirements for the hazards -1

Breakdown of the robot
Electrical Hazard

Safety characteristics shall continue to be active, so that the robot will halt when necessary to protect people. Otherwise a person might be crushed between the robot and another object, person or the wall or robot being controlled to commit suicide.

Dynamic brakes for the case of network cracking shall be provided. When software shuts down robots may follow arbitrary trajectories and breakdown.

A built-in electronic hardware control system and/or safety operational software shall be selected to force the robot to shut itself down in an emergency, so that to prevent harmful accidents of robotic system.

Identify safety requirements for the hazards -2

Environmental hazard generated by lightning or radiation

→ Warning signals if any environmental condition is violated.

→ Sensors shall remain functioning, so that the robot will pause when necessary to protect people.

Identify safety requirements for the hazards -3

Contact with poisonous or noxious substances of the robot's body surface
Hazard generated by materials and substances

Power pack or sealed batteries shall continue to be active in order to protect residents under all emergency circumstances.

User shall be warned by the manufacturer that regarding surveillance robot functioning on batteries, there exist electrical hazards such as fire, electrical surge or chemical hazard in case that battery is misused and explosion hazard, if the power pack is improperly handled.

Identify safety requirements for the hazards –4 (1)

Hazards generated by neglecting ergonomic principles in machine taking advantage of privacy vulnerabilities

Secure Sockets Layer (SSL) virtual private networks (VPN) facilitate safe remote access to the robot's network.

The SSL Portal VPNs should be used from the robot since it provides a single SSL connection to a Web page to safely gain access to multiple network resources. The robot uses the SSL VPN gateway via its Web browser, log on itself to the gateway using an authentication procedure required by the gateway, and is then accessible to a Web site that acts as the gate to the other resources.

The SSL Tunnel VPNs should be used from the robot since it provides a normal Web browser to safely access multiple network resources, including protocols that are not web-based, through a tunnel that is using SSL. SSL tunnel VPNs require that the Web browser can handle active content, which offers functionality that is not accessible to SSL portal VPNs.

Identify safety requirements for the hazards –4 (2)

Hazards generated by neglecting ergonomic principles in machine taking advantage of privacy vulnerabilities

IPsec offers peer authentication and integrity including two security protocols, Authentication Header and Encapsulating Security Payload (ESP), Internet Key Exchange protocol and IP Payload Compression Protocol.

An intruder that is spying network packets does not know which residents are talking, how often contacts are taking place, or how much packets is being delivered. Moreover, the amount of data being swapped could be counted.

IPsec encrypts information using a cryptographic algorithm and a confidential value recognized by the persons who are communicating. The network information can only be decrypted by someone who has the confidential key.

Identify safety requirements for the hazards -5

Hazards generated by neglecting ergonomic principles in machine causing psychological effects

The robot shall be equipped with a specific audio or visual signal, easily recognizable by everyone, to let people know whether it is on or off.

Monitor the privacy policy of the user by sustaining the particular sensing capabilities of the robot, mainly when it is incorporated with privacy sensitive sensors, such as web cameras or stereo microphones.

Identify safety requirements for the hazards –6

Mechanical hazard cause property damage

Recognize the requirements to defend privacy vulnerabilities of network performance and identify how those deficiencies can best be accomplished.

Take decisions in four parameters: architectural policy, authentication models, cryptography method and packet filters.

An authentication method ought to be chosen depending on potential maintenance and privacy policy requirements. Packet filters should implement the necessary measures to control traffic and do not block traffic for interoperability factors.

Recognize any possible threats such as numerous parameters, including authentication, implementation compatibility, management, performance, the privacy of the development, and element interoperability.

Final thoughts about STAMP

- A helpful method in the attempt to analyse the entire socio-technical system
- Systems thinking provides a structured way to estimate the system and recognise weak points.
- Leading safety requirements regarding standardization of home-surveillance robots could be proposed based on STAMP.

Related Works

- Mouroutsos G.S., Mitka E., "*A Guide to safety standards of toy-robots*", In Proc. of IEEE/RSJ Int. Conference On Intelligent Robots and Systems (IROS 2012): SAFETY IN HUMAN-ROBOT COEXISTENCE & INTERACTION, 7-12 Okt. 2012, Vilamoura, Portugal.
- Mouroutsos G.S., Mitka E., "*Applying System Safety Engineering to Safety Standards of Domestic Robots*", 8th HSSS National and International Conference, Systems approach to Strategic Manage-ment, 5-7 July 2012, Thessaloniki, Greece.
- Mouroutsos G.S., Mitka E., "*Safety-guided design concerning standardization's requirements of mowing robots*", APMS 2012 - Advances in Production Management Systems International Conference, 26-28 Sept. 2012, Rhodes Island, Greece.
- Eleftheria Mitka, Antonios Gasteratos, Nikolaos Kyriakoulis and Spyridon G. Mouroutsos "*Safety certification requirements for domestic robots*", Safety Science, (Elsevier), 50 (9), p.1888-1897, Nov 2012.{doi:10.1016/j.ssci.2012.05.009}

Thank you!

Mitka Eleftheria
PhD Candidate
Department of Electrical & Computer Engineering
School of Engineering, Democritus University of Thrace,
University Campus, Kimmeria, Xanthi, 671 00 Greece
em3933@ee.duth.gr