Applying STAMP to safety standards of mowing robots

Mitka Eleftheria

Electrical and Computer Engineering
Democritus University of Thrace
University Campus, Xanthi
67100 Greece
em3933@ee.duth.gr

Abstract: The use of mowing robots in anthropic environment is increasing, leading to the call for specific safety standards. This is a challenging endeavour, however, because the user must usually be placed in the robot's workspace and the residents must frequently interact with the robot. Although specific safety standards for mowing robots do not yet exist, there are several mowing device standards and well-established principles of risk analysis and safety design that can and should be applied. This paper presents an overview of safety constraints for mowing robots, starting with a discussion of high-level system safety requirements, followed by methods for risk assessment (or hazard analysis) and a presentation of STAMP (Systems-Theoretic Accident Modelling and Processes) as a safety strategy.

1 Introduction

Mowing robot is a mechatronic system used in a domestic environment. Robotic mower is constructed to cut grass in gardens at any day and time without human intervention. It is usually small, compact, noiseless and light enough to be transported manually. This home-used appliance could be adjusted to cut in different locations. Throughout its task, the apparatus cut the grass surrounded by a perimeter cable. Its scope is to cut wide locations, preferably at daytime according to the battery charging cycle. When it bangs with an obstacle such as branches, small stones, wall or fence, it bounces and goes along a different direction. The lawn-mower executes an asymmetrical movement pattern that is not recurred depending on its sensing of growth of grass.

Since particular safety guidelines for mowing robots do not exist, the authors suggest that their safety-guided design should be based on standards that developed in areas of agriculture and garden equipment. In addition, the methodologies for safety for agricultural equipment [AA09], the standard for safety of household and similar electrical appliances [EN94] providing safety requirements for domestic environment may be useful in establishing standards for these robots. Every manufacturer should follow the basic instructions summarized in the basic safety standards such as safety of machinery [EN91], safety distances and danger zones [EN92], emergency stop requirements [EN92], safety of household and similar electrical appliances [BS97], Safety Specifications for Commercial Turf Care Equipment [AO04] and safe features

according to Safety Specifications for Turf Care Equipment – Power Lawn Mowers, Lawn and Garden Tractors [AO03]. Establishing standards for controlling hazards in anthropic environment involves the entire control system and modelling the socio-technical diagram that will enforce the primary constraints in design level. Ineffective control is a consequence of lack of standards or from standards that are not enhanced adequately. The author below apply STAMP in order to build a robust base with safety requirements regarding mowing robots.

2 Applying STAMP to standards

2.1 Identify the accidents

The first step in any safety analysis is to define which types of accidents needs to be considered. Indeed, the manufacturer that develops this kind of robotic system has to take account of the accidents occurred. The accident model that derives from this definition does not indicate a particular causal factor [Le09]. In other words, in a systems-theoretic view of safety, accidents could be recognized, by categorizing the set of safety requirements that were ignored and answering why the control efforts were inaccurate in enforcing them. In addition, an accident definition in the design of a mowing robot is:

A1. Explosion of the device caused by storing the device in an improper place against manufacturer's specifications.
A2. The mower is moving near an operating rotisserie or barbecue where vapor may reach a flame or a spark causing an explosion of the device.
A3. The user is changing the operating program leading to a harmful injury.
A4. An abnormal high speed movement is not blocked by the stop button damaging property or robot's equipment.
A5. The perimeter wire is cut leading to breakdown of the robot.
A6. The mower chassis has burnt signs or signs of corrosion causing skin/eyes damage.
A7. The drive motors are damaged due to severe overloading of the wheel motors and overheating.
A8. A pet or children could be pinned under the robot if the alarm of the robot doesn't warn about restart or scheduled programming operation.
A9. The mower is mowing outside the yard and not across the perimeter wire hitting someone.
A10. A resident is mowing via manual control over an obstacle and the object is thrown at speeds greater than 200 mph and 50 feet or more, causing death or injuries ranging from blindness to severe bruising.
A11. The collision detection system of the device is not functioning leading to trapping points.
A12. The equipment of the lawn mower starts vibrating abnormally.
A13. Water and other liquids are sprayed directed to the robot with a garden or a liquid spray hose causing internal electronic damage of electrical connections.
A14. Inability of the device to follow the tasking path due to incorrectly placed perimeter wire/ too much slope/ overheated power supply unit/ incorrect wheel transmission/ bumper pressed during warm up/ bumper pressed for more than 2 sec during manual mowing/ bumper pressed while departing from the charging station.
A15. A resident could be injured by contact with the blades.
A16. A child may fall off and be seriously injured if he rides on an operating robot.
A17. A resident that uses the robot via remote control hits a person or a pet by pulling the mower backwards without looking.
A18. Severe injury could occur if hair, fingers or clothing of resident are caught in the exposed mechanism of the robot due to indented opening of the cover.

2.2 Assign a level of severity

With aim to arrange the severity of the above accidents, the precedence of the levels of severity is considered necessary. Severity is described as the seriousness of the hazard. The overall safety policy for arranging a level of severity for an accident is that all

accidents leading to death or injury must be restricted from the design level [Le95].

Level 1
A1-1: The collision detection system of the device is not functioning.
A1-2: A resident is mowing over an obstacle.
A1-3: The mower is mowing outside the yard hitting someone.
A1-4: The user is changing the operating program leading to a harmful injury.
A1-5: Vapor may reach a flame or a spark causing an explosion of the device.
A1-6: Explosion of the device caused by storing the device in an improper place.
A1-7: Rotating blades catches part of resident's body.
A1-8: Coming in contact with any exposed mechanism part of the robot.
A1-9: A child rides on an operating robot.
A1-10: A resident is pulling the mower backward without paying attention.
Level 2:
A2-1: A pet or children could be pinned under the robot.
A2-2: The mower chassis has burnt signs or signs of corrosion.
Level 3:
A3-1: An abnormal high speed movement is not blocked by the stop button.
A3-2: Inability of the device to follow the tasking path.
A3-3: Water and other liquids causing damage of electrical connections.
A3-4: The mowing equipment starts vibrating abnormally.
A3-5: The drive motors are damaged due to severe overloading of the wheel motors.
A3-6: The robot ceases its operation due to cut of the perimeter wire.

2.3 Identify the High-Level System Hazards

On top of the measures taken by the manufacturer to avoid the risk of hazards that robots in general might cause to the user, the product should also be evaluated against the following list of possible dangers [MGKM12]:

- Mechanical Hazard (Crushing, Shearing, Cutting or severing, Entanglement, Impact, High pressure fluid injection, Shape, Acceleration/deceleration, inadequate mechanical strengths, Mass and velocity, Potential elements or elastic elements).
- Electrical Hazard (Contacts of persons with live parts, Breakdown, Leakage current, Electrostatic phenomena, Thermal radiation)
- Hazard generated by vibration (White-finger disease, Neurological, osteo-articular disorders)
- Hazard generated by radiation (electromagnetic fields, infra-red light, visible light and ultra-violet, light Laser radiation, X and γ rays, α and β rays, electron or ion beams, neutrons, ionizing or non-ionizing radiation)
- Thermal Hazard (Burns and scalds)
- Hazards generated by neglecting ergonomic principles in machine (physiological and psycho-physiological effects, human errors)
- Slipping, tripping and falling hazards.
- Hazard generated by materials and substances (ingestion, inhalation of fluids, gases, mists, fumes, fibers, dusts or aerosols (harmful, toxic, corrosive, teratogenic, carcinogenic, mutagenic, irritant or sensitizing effect, biological hazards))
- Environmental Hazards (temperature, wind, snow, lightning, vapor, explosive or flammable atmospheres) [ISO10].

For practical reasons, a restricted set of high level system hazards need to be identified considering safety as an emergent property and not a component property, as a freedom of accidents or losses and combining potentially hazardous conditions with accidents identified at first step [Le09]. Beginning with an extensive set of system hazards, usually result in a confused hazard analysis even in the case of the most simple systems. The preliminary hazards might be defined as [MGKM12]:

H1: Environmental hazards [A1, A2]
H2: Electrical hazards [A5, A8]
H3: Mechanical hazards [A4, A7, A10, A12, A14, A15]
H4: Falling and tripping hazards to residents [A9, A11, A16, A17]
H5: Hazards generated by materials and substances [A6]
H6: Hazards generated by neglecting ergonomic principles in machine [A3, A13, A18]

2.4 Identifying Safety design constraints and safety requirements for the hazards

After the hazard and system identification, the next important step is to define the system-level safety requirements and design constraints that are essential to protect from incidents (Table 1). Hazard identification is considered as a top-down procedure that must take into account the harmonization of the system, eliminating or controlling a hazard that is considered possible to allow a loss to take place [Le09]. According to

STAMP, the constraints may differ in the design level [Le12].

Table I. Design constraints and safety requirements such as user instructions, user information and observations for some of the mowing robot's hazards identified above

HAZARD	SAFETY DESIGN CONSTRAINTS
Explosion of the device due to improper storing leading to environmental hazard.	a. Remove the power plug from the charging station in case of storing the robot. b. The mower shall be equipped with a manual controller so that the user can simply move it from the grass back to a storage place when not in use. User shall not store the robotic equipment in an overheated and enclosed space, such as a garage or shed, where vapour may reach a flame or a spark or a source of extreme heat or on a hill. c. Do not leave containers with grass cuttings in the storage or charging area of the device. d. The appliance should be stored in a sheltered and dry place with good ventilation and lightning conditions. e. To reduce the fire hazard, keep the robot, charging station and storage area free of grass, leaves, or excessive grease.
The mower explodes due to flame or spark leading to environmental hazard.	a. Always keep the mower away from water, heat sources (stoves, radiators, open flames, water heater etc.), and hazardous chemicals to avoid electrocution, overheating or chemical burn hazard. b. Human–robot environment (chemical, thermal conditions). If gasses, liquids or combustible substances are contained inside the robot, the designer should ensure that any increase of temperature will not cause burn injury.
The user is changing the operating program leading to a harmful injury leading to hazard caused by neglecting ergonomic principles in machine.	a. Settings that could be stored in ROM might include: manual user options, user preferences (sound, wire position, language, learn edge, blades replaced, anti-theft), charging options (weekly program, entry points, auto depart), safety tests, information (total time, run time), temperature, software version, charging voltage, charging temperature, entry points (set, default), child guard, lock settings, alarm function (disable, enable), rain sensor (restart, disabled, pause), auto setup (enable, disable), sound, date and distance format, time (set real time clock), signal type, lock keyboard, scan width, zones setup, first time calibration and ground clearance, follow loop, garden shape (open, normal, complex). b. Robot with operating units shall use only ROM to prevent from changing the operating program. c. Faulty programming may result in anti-theft alarm don't stop beeping or not operating, incorrect set of clock, incorrect work time, not enough work hours, not completely mowed the secondary area, the remote control don't work.
An abnormal high speed movement is not blocked by the stop button leading to mechanical hazard.	a. The software of the robot should bear a self-checking program that manages suspicious movements. Unless such a program exists, the user shall not be able to reach a control to stop a disoriented robot in proper time (as in industrial robots). Suspicious movements are mowing out of the mowing area due to a disconnection of the wire, work less that being programmed, doesn't cross over the wire, doesn't complete the edge, doesn't following the plot, doesn't working at the time scheduled, doesn't position correctly in the charging station, doesn't mow properly around the flowerbeds. b. Frequent stops and restarts require additional battery energy. c. User should try to control continuously the robot when operating it via remote control.
The perimeter wire is cut leading to breakdown of the robot leading to electrical hazard.	a. In the user's guide, the user of mower is informed that he should periodically inspect blades for foreign material or debris, calibration for interference, loop signal from the wire for interference from metallic objects (perimeter fence, reinforcement bar), the shield of wires for damaging, the battery for leading of corrosive liquid, the covering hood for opening, to clean base-station with a damp cloth, to confirm good contacts between station wires and contacts and that power supply is plugged at main power receptacle and that the coiled cord is properly placed in the holder, to check the reliable connection of the power cable with the wire connector.
The mower chassis has burnt signs or signs of corrosion leading to hazard generated by materials and substances.	a. Frequently clean the charging station and the robotic contacts using only a damp cloth. b. Use only a damp, soft sponge or cloth and a dry brush to wipe the outer surfaces after scraping. c. User shall not use harsh or abrasive cleaning solutions. d. If the chassis remains dirty, a soap or washing-up liquid might be necessary. e. User shall not wash the inherent components so as not damage electric and electronic elements since mower is non-waterproof.
The drive motors are damaged due to severe overloading of the wheel motors and overheating.	a. User shall not cut grass on slippery conditions where the traction is reduced and it may block the discharge or dry/scorched lawn. b. User shall inspect the drive wheel and remove grass residuals or other object. c. If the motor overheats, then there are two ways of unblock. If the parameters fall within the first range, the robot will execute manoeuvres to unblock the blade. If the over-current is below the allowable limit, the robot will stop and signal an error. Motors have operated with over-current for too long or some objects are accumulated or clogged around the blades.
A pet or children could be pinned under the robot if the alarm of the robot doesn't warn about restart or scheduled programming operation leading to electrical hazard.	a. Before turning on the mower, user should make sure that small children, pets or obstructions are far away of the yard where the robot is operating. b. If a dog hits a mower or put its paws, nose, or mouth-parts under the edge of the chassis, the possibility of injury increases. c. The restart procedure for lawn mower should require returning it manually to charging position, entering a restart password, checking the functionality and reliability of sensors by the robot software itself, releasing stored energy and troubleshooting any software bug caused by the emergency stop, diagnostics software detects the cause of any malfunction that lead to the stop. d. Improper restart might happen after an incorrect restart position, after wrong reminder counter of blades after the replacement, a temporary power loss, a prolonged activity. e. The robot may restart its operation elsewhere especially near obstacles (fallen branches, forgotten objects) due to severe load on wheel drive motors, due to unknown fault, due temporary power loss, after a long period of inactivity or after the replacement of the blades. f. Residents should be informed by the user for the user-programmed automatic weekly scheduled day and time. g. Control access of small children before mow in reverse, up and down via manual control. User should ensure that children younger than 6 are indoors, at least 100 feet away from the mowing field the robot are

		programmed to mow at all times and under the watchful care of a responsible individual.
The mower is mowing outside the yard leading to falling and tripping hazards	a. b.	User shall not use an extension cord to increase this distance from power receptacle. This event may be due to the perimeter wire being routed in the wrong direction around an obstacle, which blocks the signal. User shall pay extra attention if the area around the mowing field is populated or congested. Always look for traffic when mowing near roadways, walks or gravel drives.
A resident is mowing via manual control over an obstacle and the object is thrown at speeds greater than 200 mph and 50 feet leading to mechanical hazard.	a. b. c. d. e.	The area where the robot will execute must be well defined and operational flaws detected must be mitigated. Such operational contingencies include: inability to determine location in the lawn; inoperative sensors; not accessible charging/ base/ docking station; charging station not charging due to not active charging process; sensor failure; high temperature of an actuator or a wheel/ electrical blade/ drive motor; low battery due to inability to detect the charging station or wrong search settings or cutting long and dense grass, and so on. A wheel over the edge or an edge caving in could cause unexpected rollover. Obstacles that could lead to a collision, such as trees or bushes higher than 15 cm, do not have to be delimited by the perimeter cable. Mower will bang and bounce when it collides with this type of obstacle creating an island around them. User shall not operate the robot for trimming hedges, for mowing vegetation other than grass, for leaf or debris collection, or on grounds other than mowing field, for pulling or carrying loads. User should not mow over gravel, stones or hard, immovable objects like pipes, rocks or sidewalk edges or objects like blind corners, shrubs, trees with holes or flower around it that might obscure vision.
The collision detection system of the device is not functioning leading to trapping points.	a. b. c.	A subsystem that accomplishes the whole range management of collision detection through a virtual force field. This system allocates a force vector to obstacles across the mowing field. This force is controlled by the system using the signals obtained from sensory devices. Obstacles such as trees, flower beds, fountains or bushes higher than 15 cm shall not have to be delimited by the perimeter wire. Mower will bang and bounce when it collides with this type of obstacle creating an island around them. The perimeter wire shall not be laid around an object that robot can be allowed to collide with, like a fence or a dense hedge.
The equipment of lawn mower starts vibrating abnormally leading to mechanical hazard.	a. b. c. d.	In case of abnormal vibrations, user should stop the robot, remove the power plug and visually check for any damage of the blade or mowing chassis and search directly for the cause. The cause might be unstable blade disc or worn out blades. Vibration is usually a sign of malfunction. Remove the power plug from mower, in case that it begins trembling irregularly. User shall check the blades and screws and replace them if they are damaged. The malfunction that leads to continuous vibration has to be repaired by service experts.
Liquids are sprayed directed to the robot leading to hazard caused by neglecting ergonomic principles in machine.	a. b. c.	User or residents shall not spray water towards the robot, the charging station or the panel of the station. Never use the charger or charge the device in grasses with dampness or when wet contact is expected. User must not, under all circumstances, remove, bend, and cut, fit, weld electrical or electronic parts inside the chassis of the robot.
Inability of the device to follow the tasking path leading to mechanical hazard.	a. b. c. d.	User and residents should be aware of the automatic departure, the mowing path, the scheduled work time on an automatic weekly program for the season and the case of sudden overturn on slopes in order to detect when the device does not follow the operating path. Mowing robots might be used from physically and visually impaired persons and this affects the control design. Navigation control on mowers requires a cable to delimit the area to be trimmed. The manufacturer should inform the buyer of mower that he/she should keep all guards, shields, switches, safety devices such as front and rear bumpers, thermistors (overheat protection), manual controller buttons and lift sensors in place and properly connected. Inspect to verify that these protective devices are appropriately installed and operating correctly. User ought to be advised not to remove the protective guards that need to be used with the mower.
Exposed mechanism leading to hazard caused by neglecting ergonomic principles in machine.	a. b.	The mowing covering hood shall not collect grass residuals after mowing damp or wet lawn. It shall be inspected and maintained regularly for foreign material using a damp cloth or another similar tool [MM12]. The mechanism of the mowing robot shall be protected with plastic cover to prevent from bumping or changing it [MM12].
Pulling the mower backwards without looking leading to falling and tripping hazards.	a. b. c.	Online tutorials and help menus shall contain the appropriate instructions, so that users shall have direct access to information on how to operate the robot. 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. Mowing robot shall be equipped with an emergency stop switch on the manual controller that ceases the rotation of blades and wheels within seconds [MM12].
A child rides on an operating robot leading to falling and tripping hazards.	a. b. c.	Warning signs shall be established to protect residents who may consider that they can ceaselessly be reckless with the operating robot. Specific responsibilities concerning safety shall be assigned to an adult user. 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. Use a frequency that is not within the range of noise frequencies, in case of an audio signal [MM12].
Contact with the sharp rotating blades leading to mechanical hazard.	a. b. c.	Manual should advice the user to present dramatic description on the hazardous behaviors of mistreating the robot and warn correctly concerning the appropriate safety features. The replacement of not well-maintained or worn out blades shall not require routine or extraordinary maintenance more than once a year. User's manual indicates that every maintenance, service, replacement or inspection of worn or damaged parts should be carried out by service experts [MM12].

Conclusion

Since specific safety standards for mowing robots are not available, the author here proposed that they should be carried out based on the fundamental user / designer requirements in the domain of robotics safety. Moreover, the author proposed the implementation of STAMP on establishing standards that links system requirements with accidents, in order to ensure safety on such an emerging technology and to spread the presence of such robots in every-day life. A system is considered safe when firstly meets the basic standards of safety, which are defined from the national directives and regulations, and secondly all the safety requirements that had been pointed out by the authors, are fulfilled. These requirements could serve as a base on building standards in order to increase commercialization and acceptance of these robots by the customers.

References

[AA09] ANSI/ASAE S318: Safety for Agricultural Equipment, 2009.

[AO03] ANSI/OPEI B71.1: Safety Specifications for Turf Care Equipment – Power Lawn Mowers, Lawn and Garden Tractors, 2003.

[AO04] ANSI/OPEI B71.4: Commercial Turf Care Equipment - Safety Specifications, 2004.

[BS97] BS 3456: Part 2 Safety of household and similar electrical appliances - Section 2.42 Battery-operated lawnmowers, 1997.

[EN94] EN 60335: Part 1 - Safety of household and similar electrical appliances, 1994.

[EN91] EN 292: Parts 1 and 2 Safety of Machinery - Basic concepts, general principles for design, 1991.

[EN92] EN 294: Safety of Machinery - Safety distances to prevent danger zones being reached by the upper limbs, 1992.

[EN92] EN 418: Safety of Machinery - Emergency stop equipment, functional aspects – Principles for design, 1992.

[Le12] Leveson, N.: Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2012.

[Le95] Leveson, N.: Safeware, System Safety and Computers, Addison-Wesley, 1995.

[Le09] Leveson, N.: Applying systems thinking to analyze and learn from events, Safety Science, Vol. 49, pp. 55–64, 2009.

[MGKM12] Mitka, E.; Gasteratos A.; Kyriakoulis N.; Mouroutsos G.S.: Safety certification requirements for domestic robots, Safety Science, 2012.

[MM12]Mouroutsos G.S., Mitka, E.: Safety-guided design concerning standardization's requirements of mowing robots, In proc. of International Conference APMS 2012: Advances In Production Management Systems, Rhodes, Greece, 2012.

[ISO10] ISO 12100: Safety of machinery —general principles for design, risk assessment and risk reduction, 2010.