2.4 Controlling interactions with other systems

Assurance objective - Manage interactions between the RAS and other systems to ensure they do not result in unsafe behaviour.

Practical guidance – cross-domain

Authors: Muhammad Atif Javed, Faiz Ul Muram, and Sasikumar Punnekkat (Mälardalen University, Sweden)

Dynamic risk management using geofences

Dynamic risk management is essential to ensure safety in production site/factory with mobile elements having enhanced automation and autonomy [1]. We have proposed a framework [2] using virtual boundary around a geographic zone, usually called geofence for dynamic risk management. The framework consists of three steps.

1. Perform hazard analysis (with focus on mobile elements)
2. Define geofences as a mitigation mechanism against identified hazards
3. Validate the adequacy of mitigation mechanisms using simulations (e.g., through 'digital twin')

Geofences

The geofence can be defined by using different shapes, such as circle, rectangle, capsule and freeform (see Figure 1); they can serve as an active countermeasure against operational mishap risks. Typically, the Global Positioning System (GPS) is used for tracking and navigation purposes and its information is used for triggering alerts in circumstances when the device enters or exits the geographical boundary of a point of interest, as shown in Figure 2.

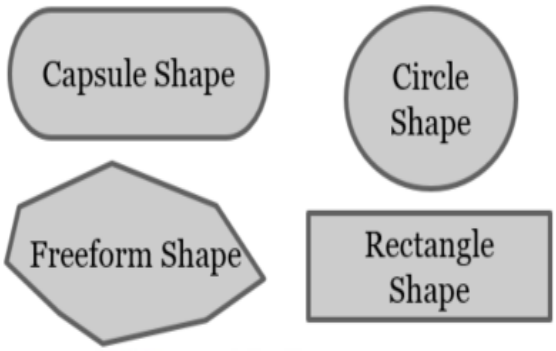

Figure 1 - Different shapes for geofences

Figure 2 - A vehicle is detected in an existing geofenced area [6]

In our demonstrator context, we have categorised geofences into static, dynamic, periodic and conditional geofences. They are defined over a) various zones at the site/factory, b) different machines, c) other actors at the site such as humans, and even d) around specified paths of movements. The geofences-enabled safety is achieved through, central server commands, vehicle level actions, multiple checkpoints and a monitoring system. Vehicle level actions are typically of two categories, viz., those taken by self for normal actions and those taken in response to failure conditions of self or others. There are many challenges and trade-offs which we explored through Volvo CE simulation test-bed ('digital twin') before arriving at reasonable values for the geofences as well as command/action sequences in case of uncertainties [2, 4].

Static geofences

The static (constant or fixed) geofences are defined for areas that may not change over time. For instance, the movement of certain objects (humans, robots, vehicles, etc.) need to be restricted in various fixed locations due to safety reasons. This provide the means to avoid mishap risks; for example, the connection is lost with a server, an incorrect mission or travel path is assigned, then control action is in place, i.e., the movement of autonomous systems is still restricted in static geofenced areas. The obstacle detection sensors, such as Light Detection and Ranging (LIDAR) and cameras can also be used for monitoring and locating objects (such as humans, robots, vehicles, etc.). In circumstances an object appeared in the designated restricted area is classified as prohibited due to safety reasons, then the respective measures can be taken, e.g., the warning can be given via a warning light, alarm or cellphone notification [5].

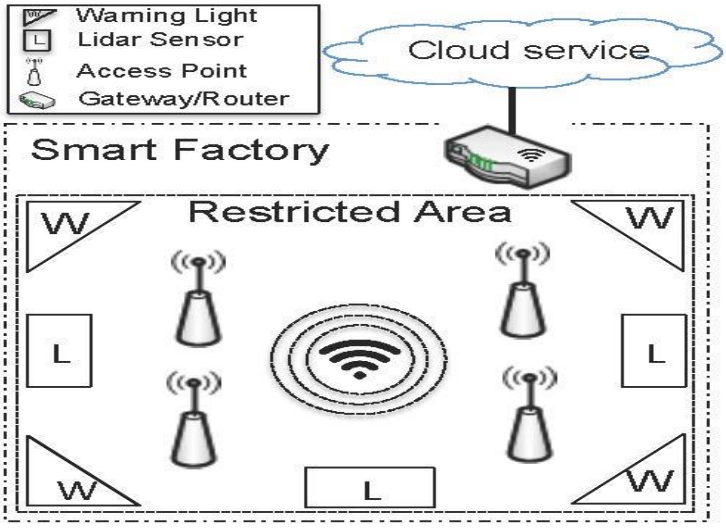

Figure 3 - Smart Factory Use Case (taken from [5])

We have also supported the successful and safe operations in various static areas of quarry site such as loading and unloading points. In these points, the presence of only one autonomous vehicle is allowed, which was ensured through interactions with the server.

Dynamic geofences

The dynamic geofences move over time. They were enforced to reduce mishap risk of emergent and evolving hazards to an acceptable level, for example, the travelling to specific area was blocked and the machines present in area were directed to drive away. The capsule shape was used to widen the boundary for collision avoidance, for instance, a vehicle or robot could potentially become hazardous due to faulty obstacle detection devices, hardware failures and transportation of dangerous materials, etc. The capsule geometry shapes (geofences) around the vehicles or robots provide the means for obstacle avoidance; they can be drawn in different ranges and colours based on their criticality level.

Figure 4 - Capsule geometry shapes (geofences) around the haulers

Periodic geofences

They are only active or inactive for specific time periods. Therefore, they were enforced to stop or control the operation and movement for a certain time-period. An example is site visits. The operation of autonomous vehicles, either in the whole site, or at specific areas/points can be stopped for a specific timeframe. The alternatives were also considered [4]. Another example is termination of operation at the end of the day, so the movement towards areas except parking places is restricted.

Conditional geofencing

The permissions associated with a geofence depends on certain factors like the number of vehicles that can be allowed together, i.e., as a platoon for efficient operation. A condition to be given permission to join a platoon is matching values of current speeds. In case of a higher speed of rear vehicle joining the platoon, depending on the severity risk factor, either its speed needs to be reduced, or the speed of front vehicle may be increased to avoid their collision. These are implemented by changes in the geofence dimensions. In circumstances of a path problem, to create a new path compliant with the conditional geofence, the autonomous vehicle waits for the human-driven vehicle and then follows it to formulate an alternative travel path.

Example of geofencing in the context of an electric quarry site

The electric site research project [7] was used as a use case for applying this approach. More details on the implementation in this context is described in [2]. For designing and configuring the quarry site, we have extended and adapted the Volvo CE simulators. They serve as digital twins of various machines used at the quarry site such as the mobile primary crusher, the excavator, the wheel loader, autonomous haulers, articulated haulers, and the secondary crusher. In the scenarios, the specific spots/zones were marked in the site map, e.g., parking, charging, loading, and dumping. The travel paths were also defined that operating machines use to move between different zones. We have modelled and implemented static, dynamic, time-based and conditional geofences necessary for safe site operations in the Volvo CE simulation test-bed.

Normal flow of operations: In this scenario, three autonomous haulers were used. H1 was present inside loading point which was modelled as a geofence, H2 was located at the entry to the loading zone and H3 was approaching towards the loading zone. The successful and safe loading operation requires the presence of only one hauler H1 in the loading point. There is a need to communicate with the server for entry in geofenced region that is triggered, when the located hauler H2 touches the sensor at entry to the loading zone. Since the hauler H1 was already present in the loading point, the hauler H2 requesting permission to enter was given a command to be in a ‘queue’. After the completion of current loading, an ‘exit’ command was given to the loaded hauler H1, which then start moving. Next, the waiting hauler in queue (H2) was given the permission to enter. The other hauler H3 also arrived in the meanwhile and instructed to be in the queue at next level; H3 moved to the place of H2. The boundary of the loading area is constant/fixed. It should not be violated and the hauler needs to maintain 0 km/h speed while at the loading point. When centre of mass of hauler was not maintained, the risk is not regarded as acceptable; as a control action, the hauler was given a command to exit and approach again. Besides the GPS position, site cameras were also placed to realize precise point positioning. The geofenced regions in quarry site involve many uncertainties and therefore continuously monitored.

Subsystem Failures: The autonomous hauler arrived early in loading zone and did not maintain new speed limit due to brake failures. In this case, besides the steering wheel rotation commands, depending on the severity risk factor, dynamic geofences were enforced. The travelling in nearby area was blocked and the autonomous haulers in travelling path, including in standstill mode, such as loading point are commanded to drive away to reduce the risk to an acceptable level. The capsule geometry shapes were drawn in different ranges and colours based on their criticality level. When an obstacle was detected in yellow range (indicating move with caution at reduced speeds), the slow down or stop measures were taken, the red range was regarded as emergency stopping distance. The

vehicles can maintain assigned speed limit if no deviations are detected. In addition, the autonomous vehicles were not allowed to go for loading when maintenance team was present on site. In case of adverse environmental conditions such as slippery surface, the movement of vehicles can also be avoided in terms of dynamic geofences.

Communication Failures: The loss of communication with the server is a safety risk. Besides that, the messages containing less, or wrong data can also cause mishaps. When the primary crusher was jammed, the human operators can be called on site, during that period a direct loading command is sent to the autonomous hauler instead of the loading from wheel loader. The transformation of an incorrect mission or travel path to an autonomous hauler can be caused by an incorrect command or timing failure that leads to an incomplete mission, machine damage or human injuries. In such cases, the control action was in place, i.e., the movement of autonomous haulers was still restricted in geofenced areas.

Path Problems: When the primary crusher was building a stone piles, the direct loading was disabled. To carry out the loading from a specific stone pile, to create a new path compliant with the conditional geofence, the autonomous hauler waits for the human-driven machine, such as wheel loader to formulate an alternative travel path, and then follows it.

References

- [1] M. A. Javed, F. U. Muram, H. Hansson, S. Punnekkat and H. Thane, “Towards Dynamic Safety Assurance for Industry 4.0”, Journal of Systems Architecture (JSA), 2020.
- [2] M.A. Javed, F.U. Muram, A. Fattouh and S. Punnekkat, “Enforcing geofences for managing automated transportation risks in production sites”, in: 16th European Dependable Computing Conference, EDCC 2020 Companion Proceedings, Munich, Germany, September 7–10, 2020.
- [3] F.U. Muram, M.A. Javed and S. Punnekkat. “System of systems hazard analysis using HAZOP and FTA for advanced quarry production”, in: 4th International Conference on System Reliability and Safety (ICSRS), Rome, Italy, November 20-22, 2019.
- [4] F. U. Muram, M. A. Javed, S. Punnekkat and H. Hansson, “Dynamic Reconfiguration of Safety-Critical Production Systems”, in: 25th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC '20), Perth, Australia.
- [5] O. Jaradat, I. Sljivo, R. Hawkins and I. Habli, “Modular Safety Cases for the Assurance of Industry 4.0”, in: 28th Safety-Critical Systems Symposium, SCSS 2020, York, UK, February 11-13, 2020.
- [6] F. Reclus, K. Drouard, “Geofencing for fleet & freight management”. In: 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST). pp. 353–356 (2009)
- [7] Volvo Construction Equipment, “Emission-free quarry,” [Online] https://www.volvoce.com/global/en/news-and-events/press-releases/2018/testing-begins-at-worlds-first-emission-free-quarry/.