
# FM24 Homework:
## Formal Analysis of Search-and-Rescue Scenarios

Formal Methods for Concurrent and Real-Time Systems, A.Y. 23/24

**Livia Lestingi**
April 12th, 2024

# 00. Project Goals

**1.** Strengthen your modeling skills:

given an informal description of the system, how can we turn it into a formal model?

# 00. Project Goals

**1.** Strengthen your modeling skills:

given an informal description of the system, how can we turn it into a formal model?

**2.** Exploit formal verification to analyze a system:

the theoretical background is vital, but how can we put it to use?

# 00. Project Goals

**1.** Strengthen your modeling skills:

given an informal description of the system, how can we turn it into a formal model?

**2.** Exploit formal verification to analyze a system:

the theoretical background is vital, but how can we put it to use?

**3.** Practice substantiating your work:

how can you convince your reader/listener that you made the most reasonable and effective choices?

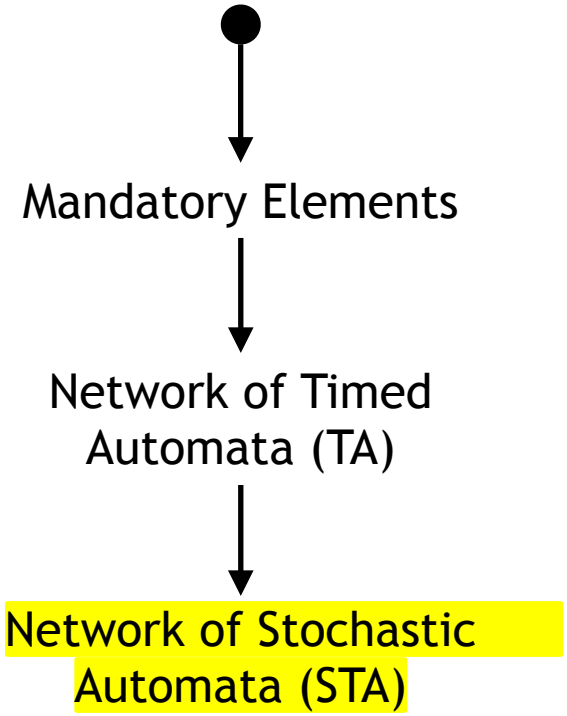
# 00. Project Goals → Deliverables

**1.** Strengthen your modeling skills → Formal Model

**2.** Exploit formal verification to analyze a system → Experimental Results

**3.** Practice substantiating your work → Written Report

# 01. Formal Model



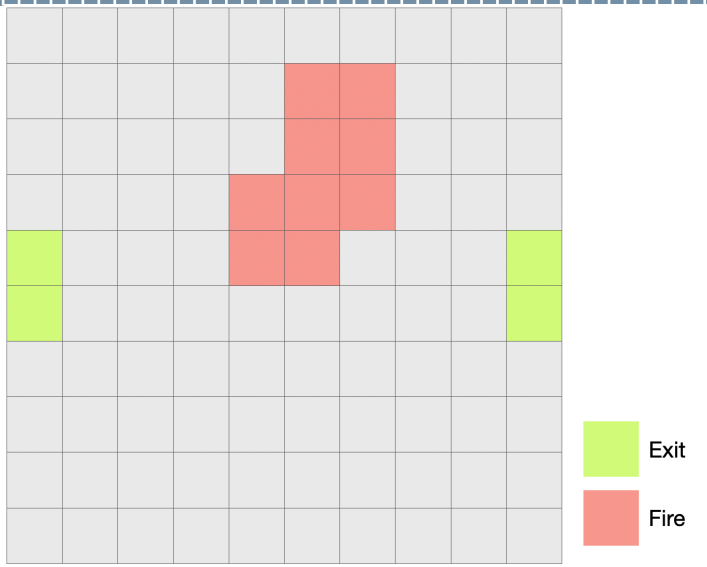

- The main output of the project is the **formal model**.
- Some entities/features (explained in more detail in the upcoming slides) must be **mandatorily** modeled to get a sufficient score.
- The NTA accounts for up to 90% of the total score (i.e., ≤ 27/30). Stochastic features are required to get the full score (i.e., > 27/30).

# 01. Formal Model: Context

- Autonomous agents (e.g., drones) deployed in search-and-rescue scenarios to support rescue services

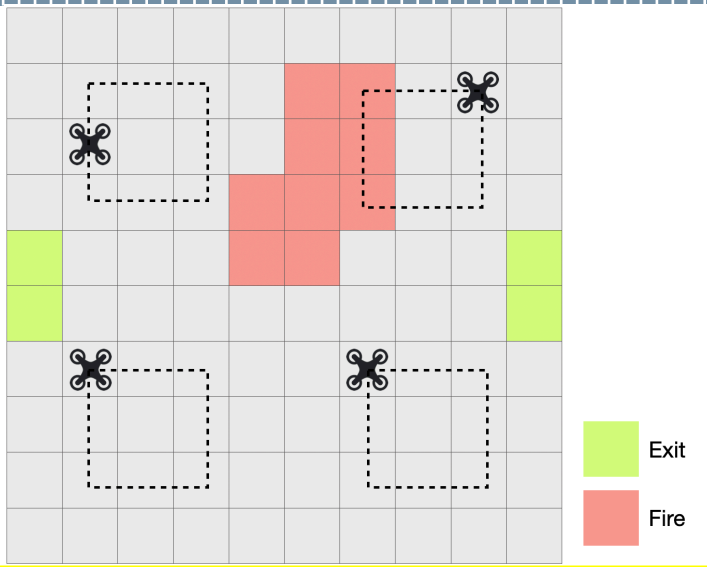
- Drones survey the scene and **decide** whether to instruct civilians to help people in need or contact professionals (i.e., firefighters or medical staff)

# 01. Formal Model: Layout



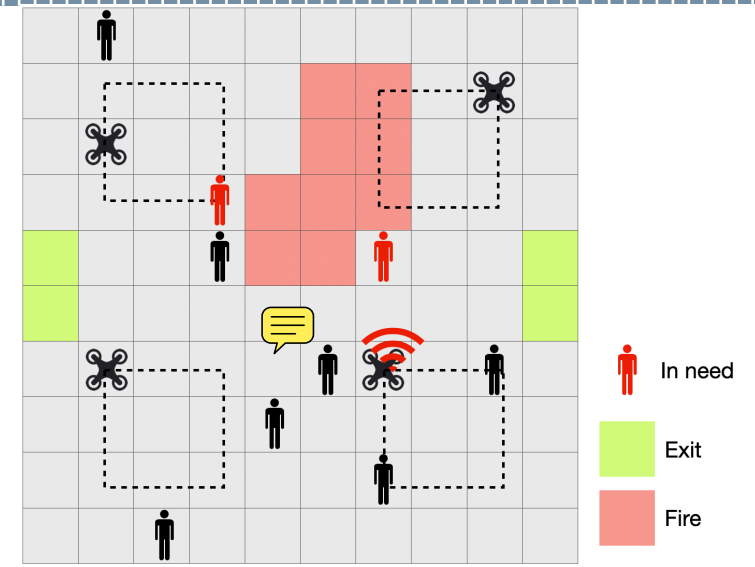

- $m \times n$ grid.
- Emergency exits are placed on the boundary of the layout.
- Fires occupy blocks of adjacent cells
- Agents occupy one cell at a time (drones can hover over cells occupied by a human).
- Agents' positions refresh each time unit (all agents move 1 cell/time unit)

# 01. Formal Model: Drones



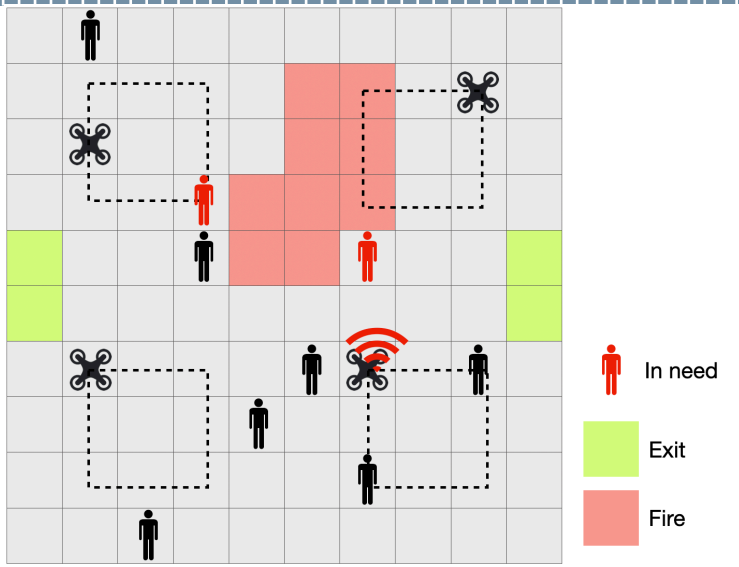

- Drones patrol with a pre-determined movement pattern that you design.
- If dist(drone, survivor) $\leq N_v$ and dist(drone, victim) $\leq N_v$ hold -> a decision must be made
- You design the **decision-making policy** (i.e., how the drone decides whether the civilian should act as a zero-responder or contact a staff member).

# 01. Formal Model: Drones




- Drones patrol with a pre-determined movement pattern that you design.
- If dist(drone, survivor) $\leq N_v$ and dist(drone, victim) $\leq N_v$ hold -> a decision must be made
- You design the **decision-making policy** (i.e., how the drone decides whether the civilian should act as a zero-responder or contact a staff member).

# 01. Formal Model: Drones




- Drones patrol with a pre-determined movement pattern that you design.
- If dist(drone, survivor) $\leq N_v$ and dist(drone, victim) $\leq N_v$ hold -> a decision must be made
- You design the **decision-making policy** (i.e., how the drone decides whether the civilian should act as a zero-responder or contact a staff member).
- **Stochastic version:** When in the proximity of a survivor and a victim, the drone detects it with probability $1 - p_{fail}$.

# 01. Formal Model: First-responders


- If a person needing assistance is within a 1-cell range, the first-responder will assist them for $T_{fr}$ time units.
- Otherwise, the first-responder moves.

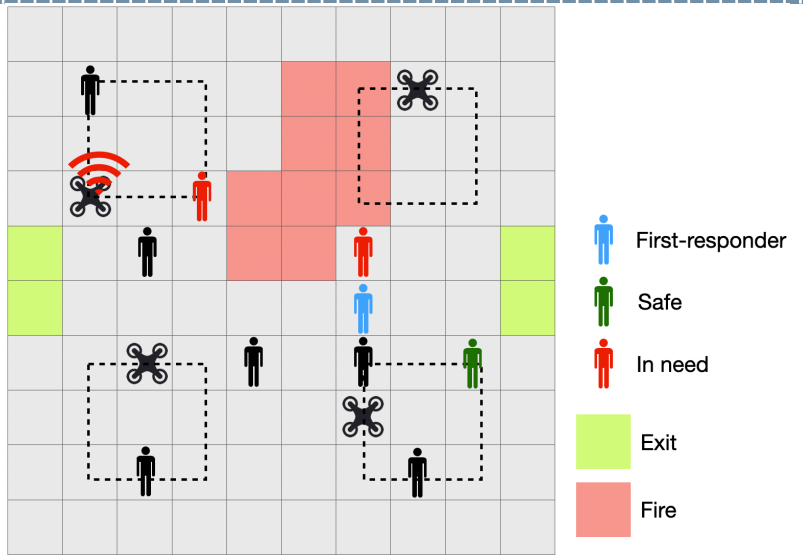
# 01. Formal Model: Civilians


- If an exit is within a 1-cell range, they are considered safe.
- If a tile occupied by a fire is within a 1-cell range, they are considered in need of assistance. They are considered a casualty if not brought to a safe state within $T_v$ time units.
- If the survivor has been instructed to help, they are busy acting as a zero-responder for dist(survivor, victim) + $T_{zr}$ time units.

# 01. Formal Model: Civilians

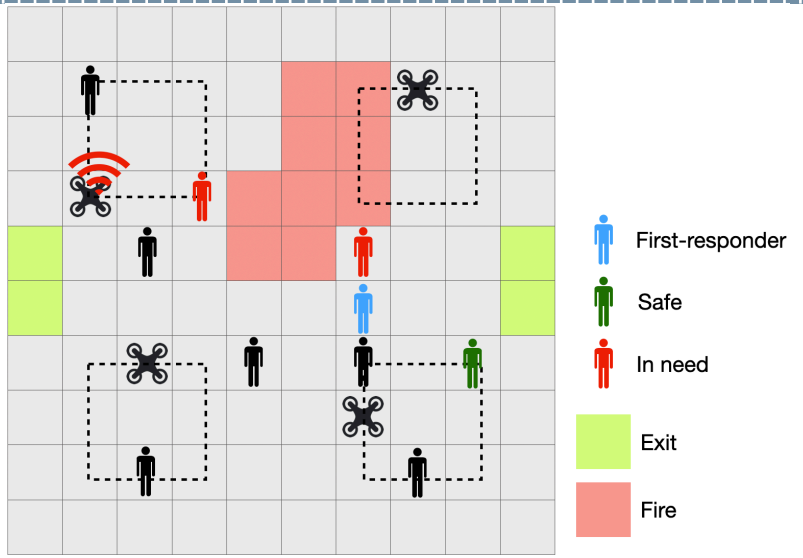

- If the survivor has been instructed to contact the first-responder, they are busy enacting this instruction for dist(survivor, first-responder) + dist(first-responder, victim) + $T_{fr}$ time units
- If none of the above apply, the survivor moves.

# 01. Formal Model: Civilians




- If the survivor has been instructed to contact the first-responder, they are busy enacting this instruction for
  $\text{dist}(\text{survivor}, \text{first-responder}) + \text{dist}(\text{first-responder}, \text{victim}) + T_{fr}$ time units
- If none of the above apply, the survivor moves.

# 01. Formal Model: Civilians




- If the survivor has been instructed to contact the first-responder, they are busy enacting this instruction for
  $\text{dist}(\text{survivor}, \text{first-responder}) + \text{dist}(\text{first-responder}, \text{victim}) + T_{fr}$ time units
- If none of the above apply, the survivor moves.
- **Stochastic version:** When instructed by the drone, they acknowledge the instruction and enact with probability $p_{\text{listen}}$ and ignore it (or miss it) with probability $1 - p_{\text{listen}}$.

# 02. Formal Verification: Properties

- The **mandatory** properties to be verified are:

**P1.** It is **possible** for a percentage $N_{\%}$ of all civilians to reach a safe state within time $T_{scs}$.

**P2.** A percentage $N_{\%}$ of all civilians is **always** guaranteed to reach a safe state within time $T_{scs}$.

# 02. Formal Verification: Properties

- Whether these properties hold or not depends on the **scenario configuration**. Specifically, on the following parameters:

  1. the geometry (i.e., where exits and fires are located);
  2. the number of agents in the scene (i.e., how many drones, civilians, and first-responders are present);
  3. the drones' visibility range $N_v$;
  4. time-related parameters $T_{fr}$, $T_{zr}$, and $T_v$;
  5. the drones' decision-making policy;
  6. the humans' moving policy.

- Present (at least) **three** significant NTA configurations highlighting relevant behavioral aspects of the system.

# 02. Formal Verification: Stochastic Properties

- As for the stochastic version of the model, calculate the **probability** of properties P1-2 holding within a **time bound** (the time bound must also be properly sized).

- The NSTA behavior further depends on the following parameters:
  - the drones' sensor **failure rates**;
  - the civilians' instruction **acknowledgment rates**.

- Present (at least) **three** significant NSTA configurations highlighting relevant behavioral aspects of the system.

# 02. Formal Verification: Tool

- The formal model should be created using the **Uppaal** tool:
  - More info during the student presentation session.

# 02. Formal Verification: Tool

- You can find references in the Getting Started section of the website:
  - Reading the Tutorial (also for the SMC extension) is highly recommended!

- When in doubt, the Documentation is your friend:
  - It contains all the reference for:
    - GUI of the tool
    - System Description
    - Requirement Specification
    - ...everything you need!

# 03. Written Report

- You must **mandatorily** deliver:
  - Uppaal .xml source file for your model:
    **Beware**: I will re-run the queries you describe in your report, so make sure the model is experiment-ready and queries are saved in the verifier section!

# 03. Written Report

- You must **mandatorily** deliver:
  - Uppaal .xml source file for your model:
    **Beware**: I will re-run the queries you describe in your report, so make sure the model is experiment-ready and queries are saved in the verifier section!
  - The project report (possibly a .pdf):
    Max 10 pages: front cover, index page, bibliography, appendices […] do not count.
    No constraints on the template (but you can take this chance to practice with LateX before writing your thesis…).

# 03. Written Report

- Tips for the report:
  - Do not just enumerate variables, locations, clocks […]: what really matters is your **reasoning** and critical thinking.

    For example: "*This feature is modeled as a two-dimensional array of integers.*"…fine, but **why**? There can be more than one valid motivation, but please provide one.

  - I will upload excellent reports from previous years to provide a positive source of inspiration.

# 04. Final Remarks

- Deadline **TBA** (coincides with the exam date in July).

- It is preferable (for you) to carry out the project in teams of 2/3/4 people.

- My job is to support you and provide directions: please drop an email when you need it.

…I cannot solve bugs for you though :) (that's cheating)

- Do not open up with "*Dear prof, we have problems, can we schedule a meeting?*": please describe your issue, and then I will assess if it can be solved via email or if it requires a meeting.

# Questions? :)