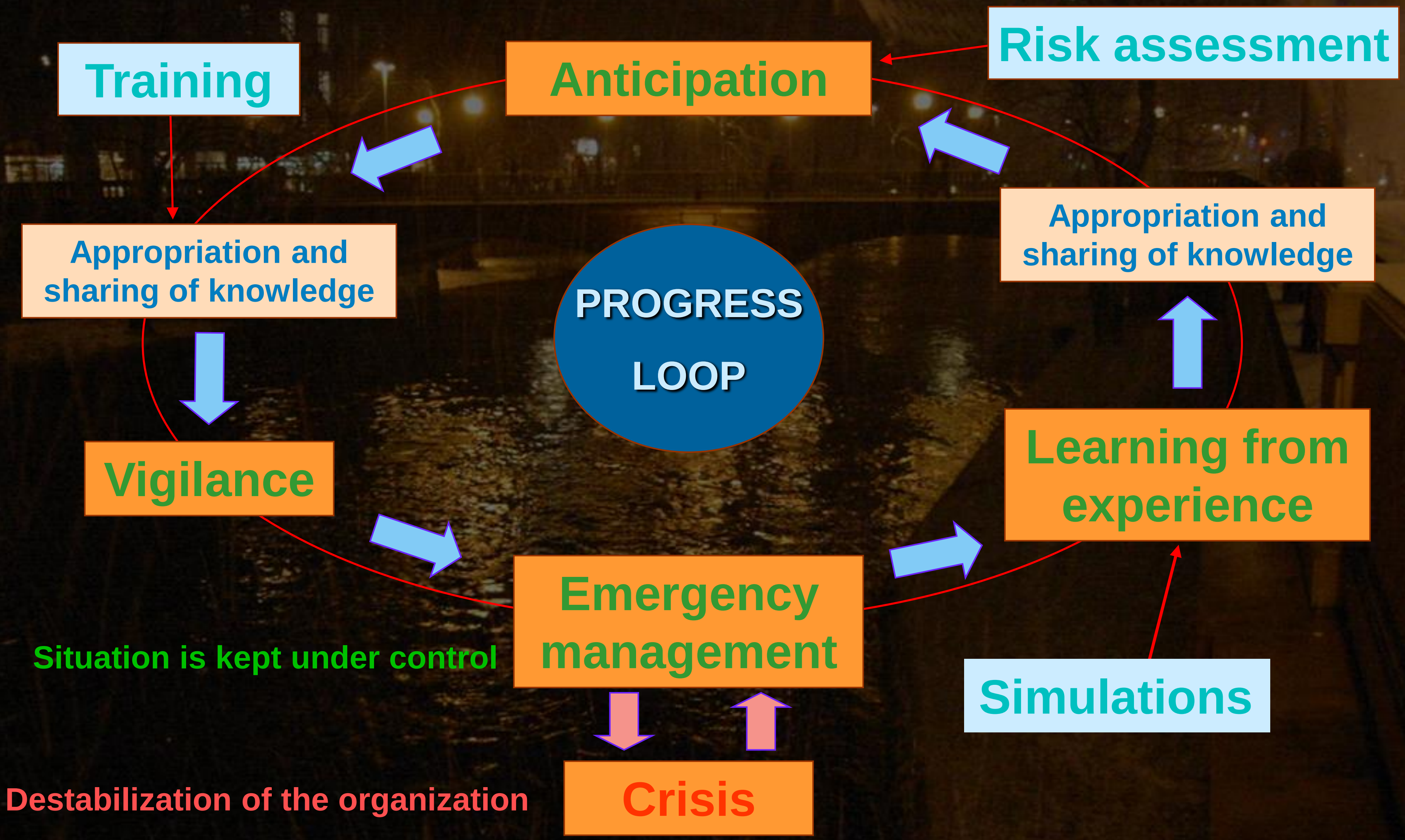
Emergency and crisis management: some trends to improve efficiency

Jean-Luc Wybo

Mines ParisTech / CRC

jean-luc.wybo@mines-paristech.fr

The Risk Management processes



Risk assessment

Anticipation

Training

Appropriation and sharing of knowledge

PROGRESS LOOP

Appropriation and sharing of knowledge

Vigilance

Learning from experience

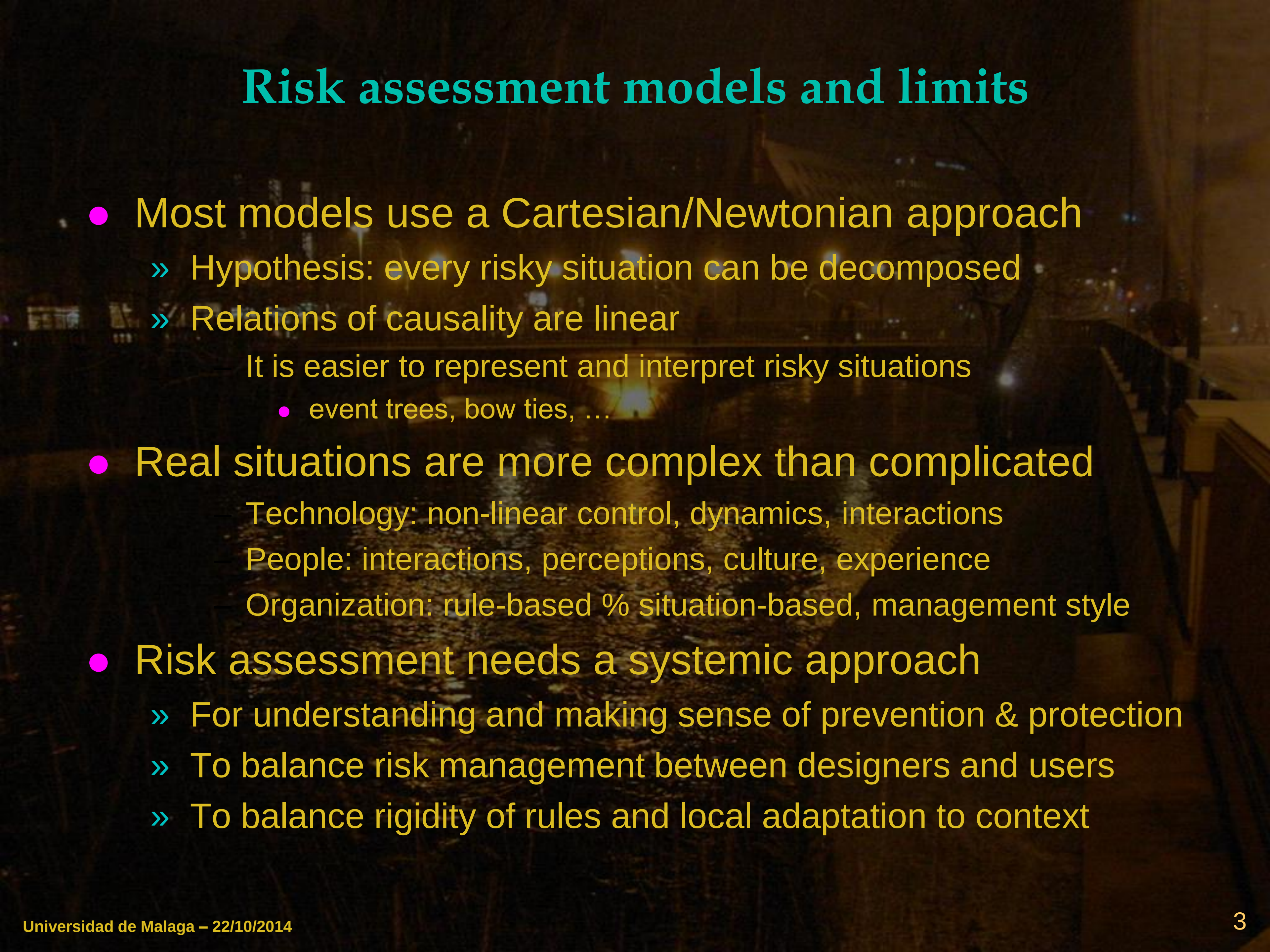
Emergency management

Situation is kept under control

Simulations

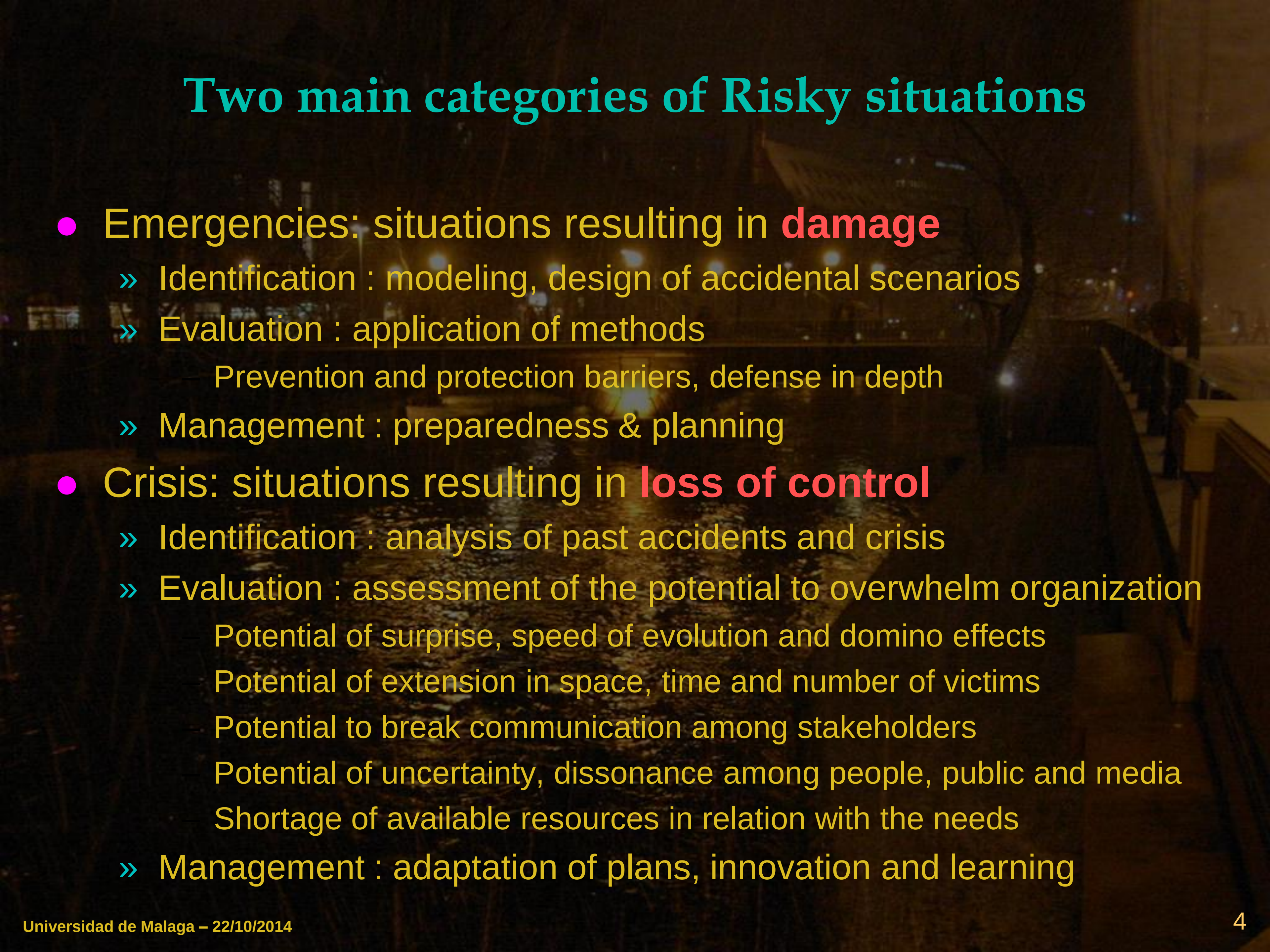
Crisis

Destabilization of the organization



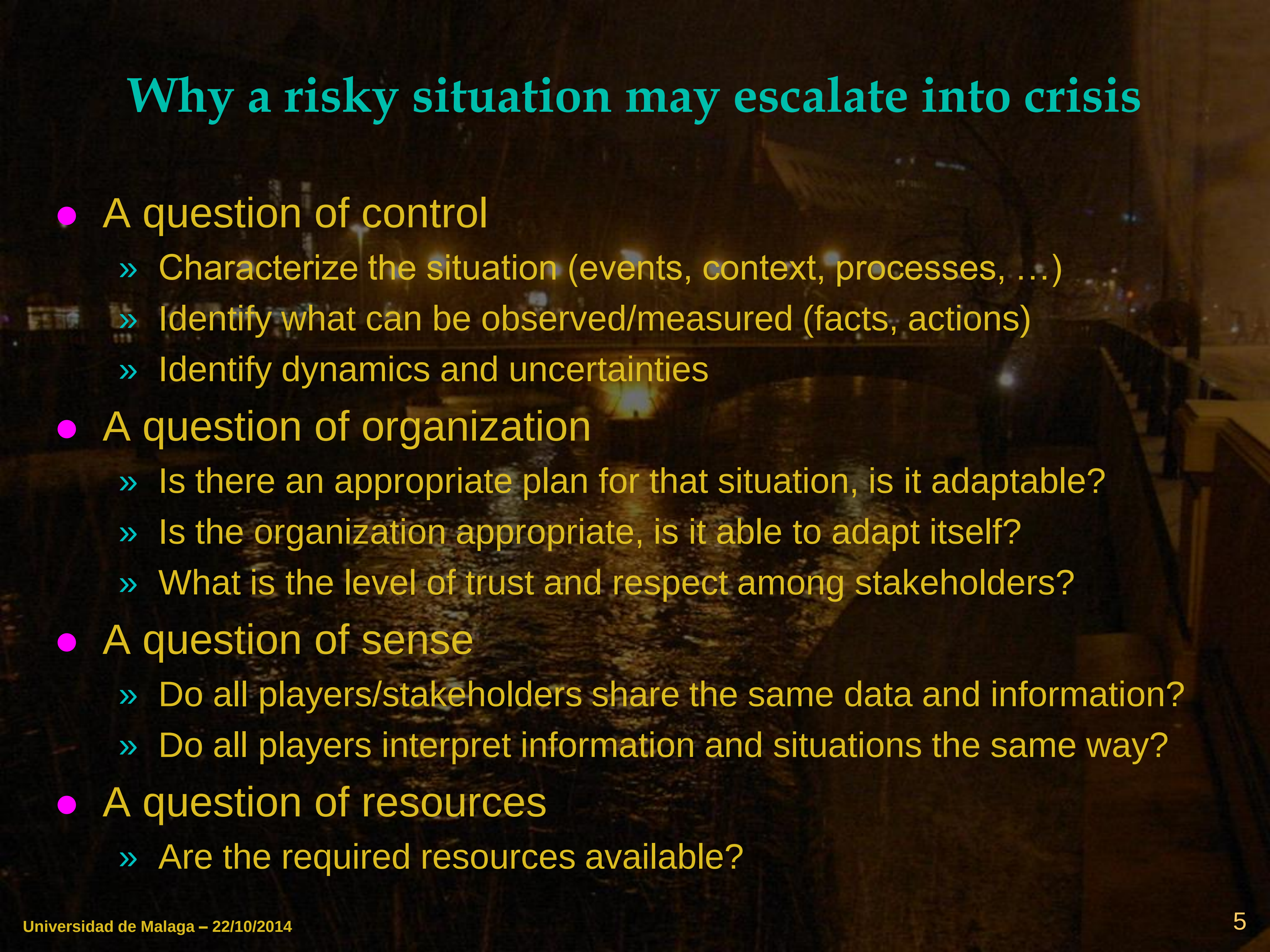
Risk assessment models and limits

- Most models use a Cartesian/Newtonian approach
  - » Hypothesis: every risky situation can be decomposed
  - » Relations of causality are linear
    - It is easier to represent and interpret risky situations
      - event trees, bow ties, …
- Real situations are more complex than complicated
  - Technology: non-linear control, dynamics, interactions
  - People: interactions, perceptions, culture, experience
  - Organization: rule-based % situation-based, management style
- Risk assessment needs a systemic approach
  - » For understanding and making sense of prevention & protection
  - » To balance risk management between designers and users
  - » To balance rigidity of rules and local adaptation to context



Two main categories of Risky situations

- Emergencies: situations resulting in **damage**
  - » Identification : modeling, design of accidental scenarios
  - » Evaluation : application of methods
    - Prevention and protection barriers, defense in depth
  - » Management : preparedness & planning
- Crisis: situations resulting in **loss of control**
  - » Identification : analysis of past accidents and crisis
  - » Evaluation : assessment of the potential to overwhelm organization
    - Potential of surprise, speed of evolution and domino effects
    - Potential of extension in space, time and number of victims
    - Potential to break communication among stakeholders
    - Potential of uncertainty, dissonance among people, public and media
    - Shortage of available resources in relation with the needs
  - » Management : adaptation of plans, innovation and learning



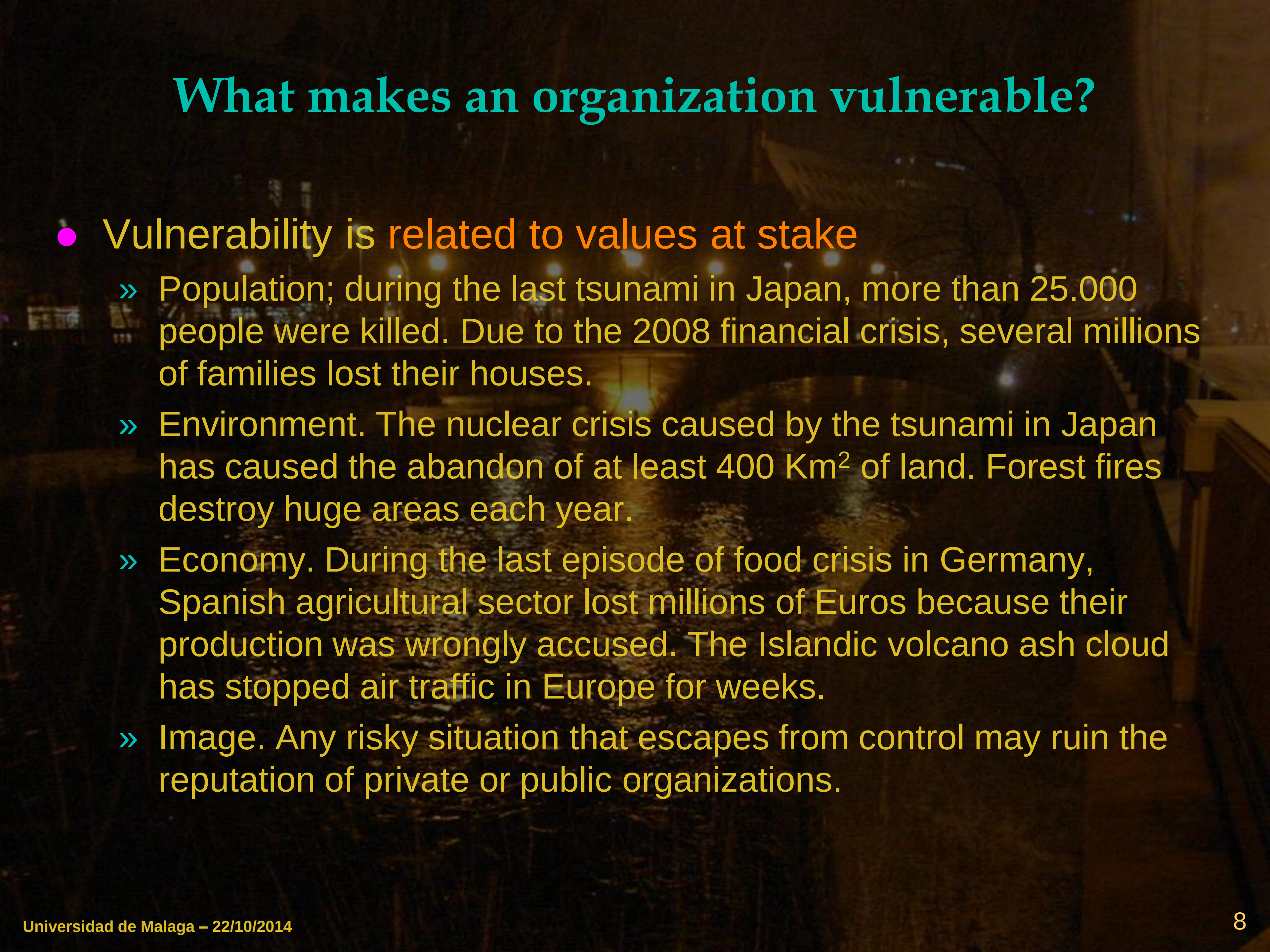
Why a risky situation may escalate into crisis

- A question of control
  - Characterize the situation (events, context, processes, …)
  - Identify what can be observed/measured (facts, actions)
  - Identify dynamics and uncertainties
- A question of organization
  - Is there an appropriate plan for that situation, is it adaptable?
  - Is the organization appropriate, is it able to adapt itself?
  - What is the level of trust and respect among stakeholders?
- A question of sense
  - Do all players/stakeholders share the same data and information?
  - Do all players interpret information and situations the same way?
- A question of resources
  - Are the required resources available?

Assessing vulnerability

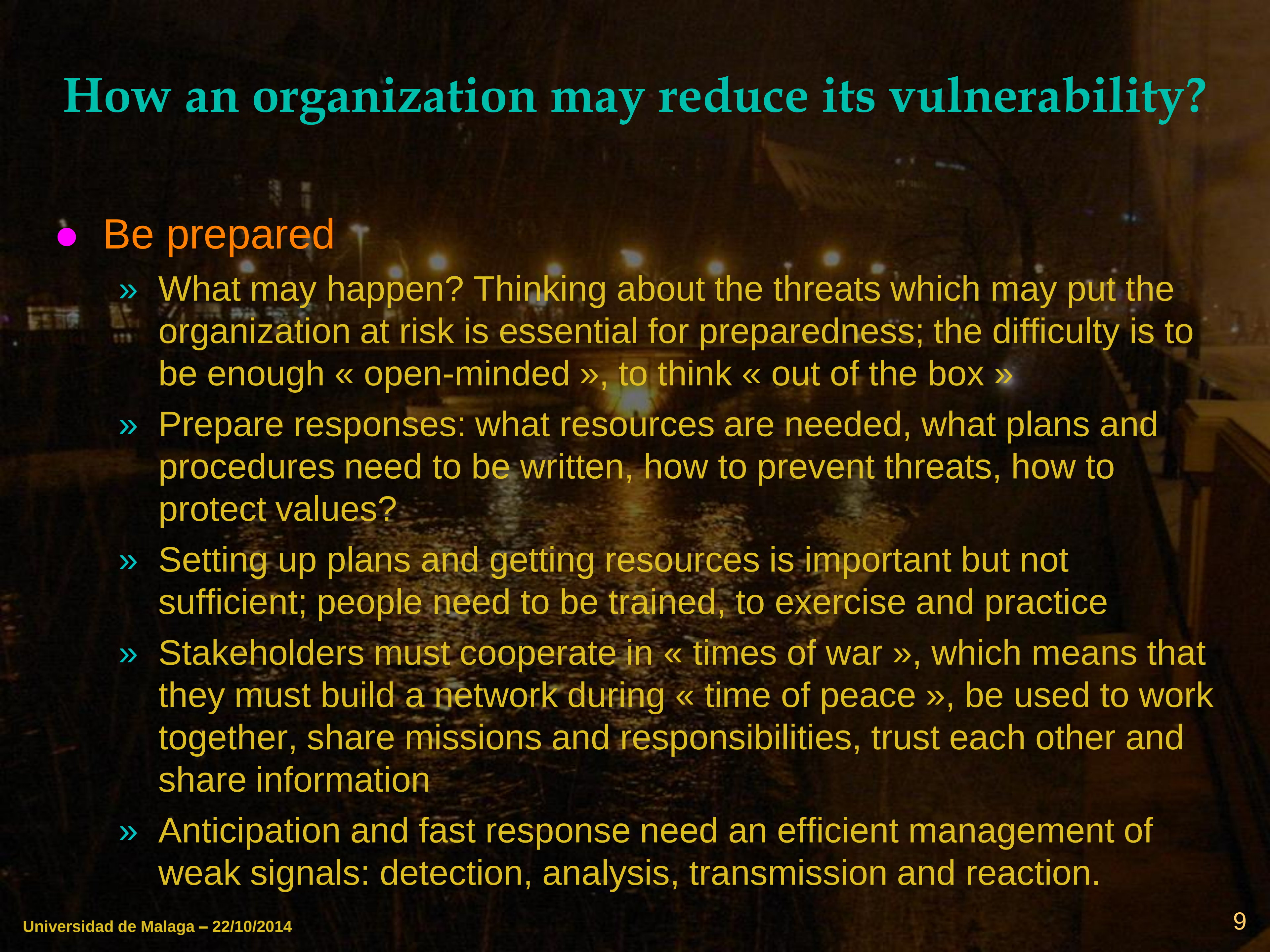
What makes an organization vulnerable?

- Vulnerability is related to threats:
  - » The development of new organizational patterns (“networked companies”, lean management, subcontracting) and worldwide business creates new kinds of threats
  - » Land management and use becomes a source of new threats, by concentrating populations in larger cities and developing housing in risk prone areas
  - » Complexity of technologies makes difficult for managers and authorities to understand situations when something goes wrong
  - » Fast and powerful personal tools for social networking and exchange of images and opinions, associated with the evolution of media coverage may turn any small event into a world crisis.



What makes an organization vulnerable?

- Vulnerability is related to values at stake
  - Population; during the last tsunami in Japan, more than 25.000 people were killed. Due to the 2008 financial crisis, several millions of families lost their houses.
  - Environment. The nuclear crisis caused by the tsunami in Japan has caused the abandon of at least 400 Km^2 of land. Forest fires destroy huge areas each year.
  - Economy. During the last episode of food crisis in Germany, Spanish agricultural sector lost millions of Euros because their production was wrongly accused. The Islandic volcano ash cloud has stopped air traffic in Europe for weeks.
  - Image. Any risky situation that escapes from control may ruin the reputation of private or public organizations.

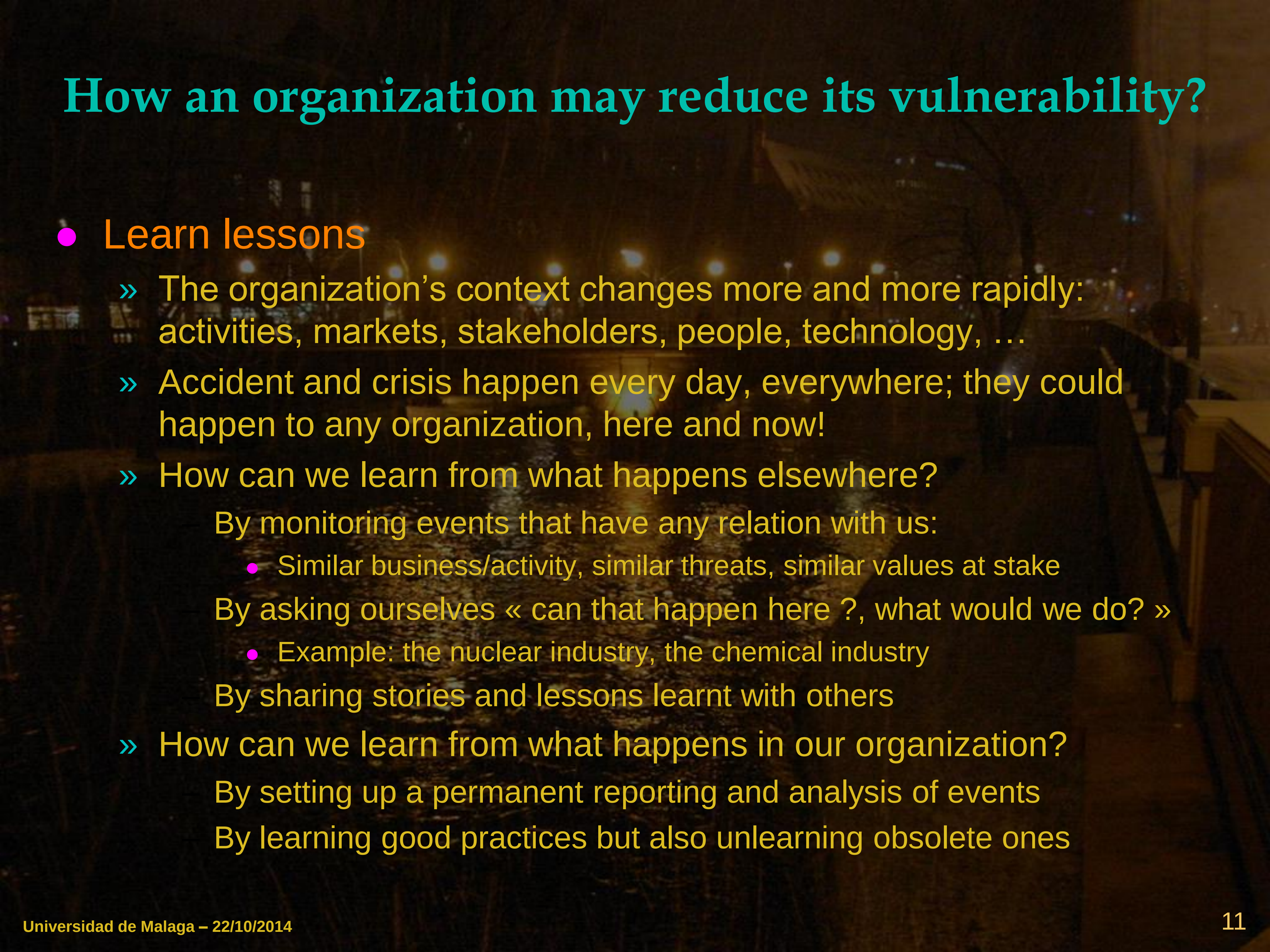


How an organization may reduce its vulnerability?

- Be prepared
  - What may happen? Thinking about the threats which may put the organization at risk is essential for preparedness; the difficulty is to be enough « open-minded », to think « out of the box »
  - Prepare responses: what resources are needed, what plans and procedures need to be written, how to prevent threats, how to protect values?
  - Setting up plans and getting resources is important but not sufficient; people need to be trained, to exercise and practice
  - Stakeholders must cooperate in « times of war », which means that they must build a network during « time of peace », be used to work together, share missions and responsibilities, trust each other and share information
  - Anticipation and fast response need an efficient management of weak signals: detection, analysis, transmission and reaction.

How an organization may reduce its vulnerability?

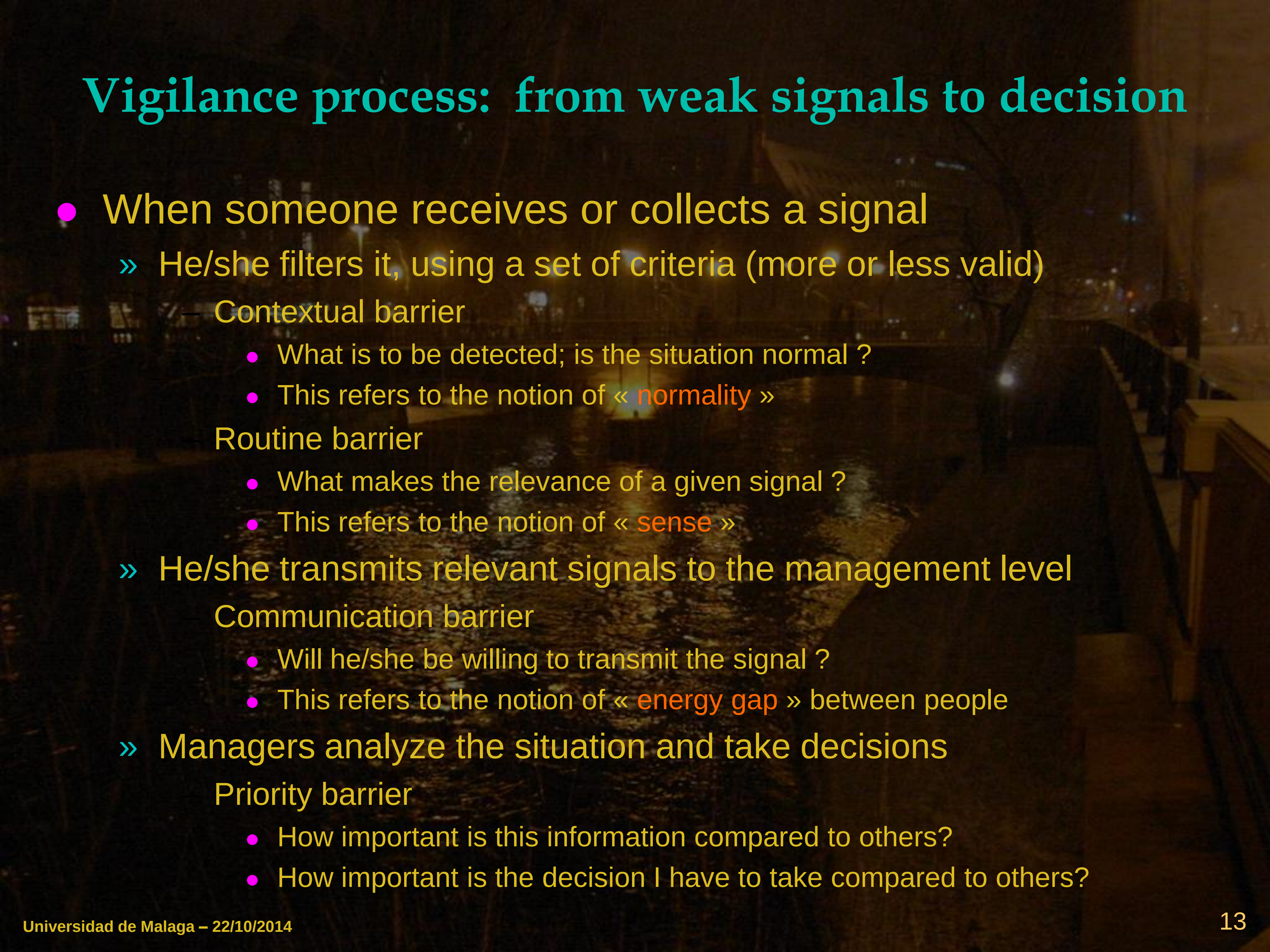
- Be resilient
  - » An organization can be prepared to « known risks », but what about surprises and unforeseen situations?
  - » An organization may have good planning and procedures, but are these plans flexible enough to be fitted to a different situation?
  - » An organization may be prepared to face a crisis on its own, but how to manage unplanned stakeholders (media, volunteers)?
  - » What contributes to the resilience of an organization?
    - Capacities to make sense of situations (« required variety »),
    - A subtle mix of hierarchy and autonomy of departments & staff,
    - Flexible plans and capacities to adapt strategies and tactics,
    - Ability to set up control loops for evaluating progress & difficulties,
    - Efficient sharing and fast diffusion of information,
    - Capacities to manage uncertainty and multiple scenarios, …



How an organization may reduce its vulnerability?

- Learn lessons
  - » The organization’s context changes more and more rapidly: activities, markets, stakeholders, people, technology, …
  - » Accident and crisis happen every day, everywhere; they could happen to any organization, here and now!
  - » How can we learn from what happens elsewhere?
    - By monitoring events that have any relation with us:
      - Similar business/activity, similar threats, similar values at stake
    - By asking ourselves « can that happen here ?, what would we do? »
      - Example: the nuclear industry, the chemical industry
    - By sharing stories and lessons learnt with others
  - » How can we learn from what happens in our organization?
    - By setting up a permanent reporting and analysis of events
    - By learning good practices but also unlearning obsolete ones

Vigilance

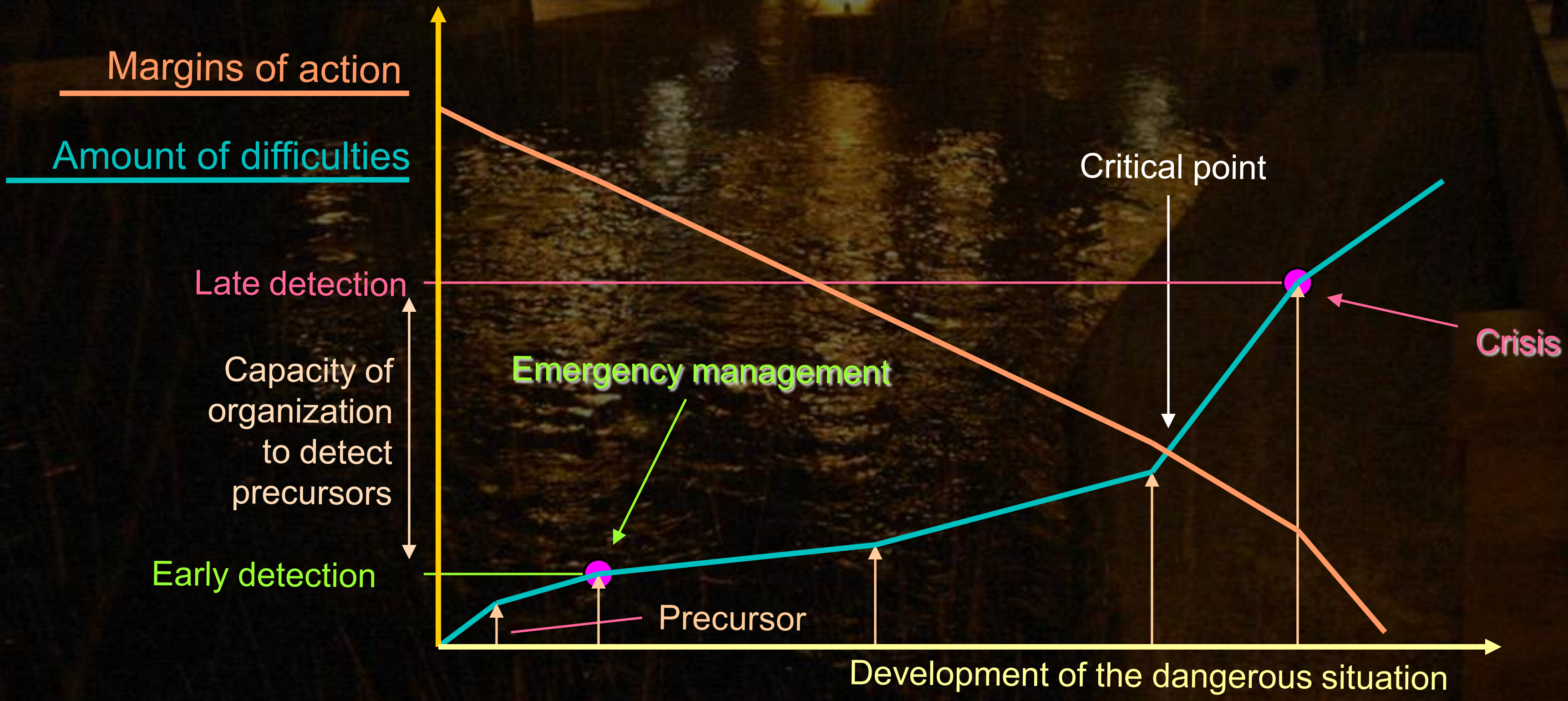


Vigilance process: from weak signals to decision

- When someone receives or collects a signal
  - » He/she filters it, using a set of criteria (more or less valid)
    - – Contextual barrier
      - What is to be detected; is the situation normal ?
      - This refers to the notion of « normality »
    - – Routine barrier
      - What makes the relevance of a given signal ?
      - This refers to the notion of « sense »
  - » He/she transmits relevant signals to the management level
    - – Communication barrier
      - Will he/she be willing to transmit the signal ?
      - This refers to the notion of « energy gap » between people
  - » Managers analyze the situation and take decisions
    - – Priority barrier
      - How important is this information compared to others?
      - How important is the decision I have to take compared to others?

Vigilance and Crisis prevention

- Crisis are quite often the result of a combination of events
- There is generally a « critical point »
  - » Before : margins of actions (plans) are sufficient to cope with
  - » After : organization cannot anymore cope with or is overwhelmed

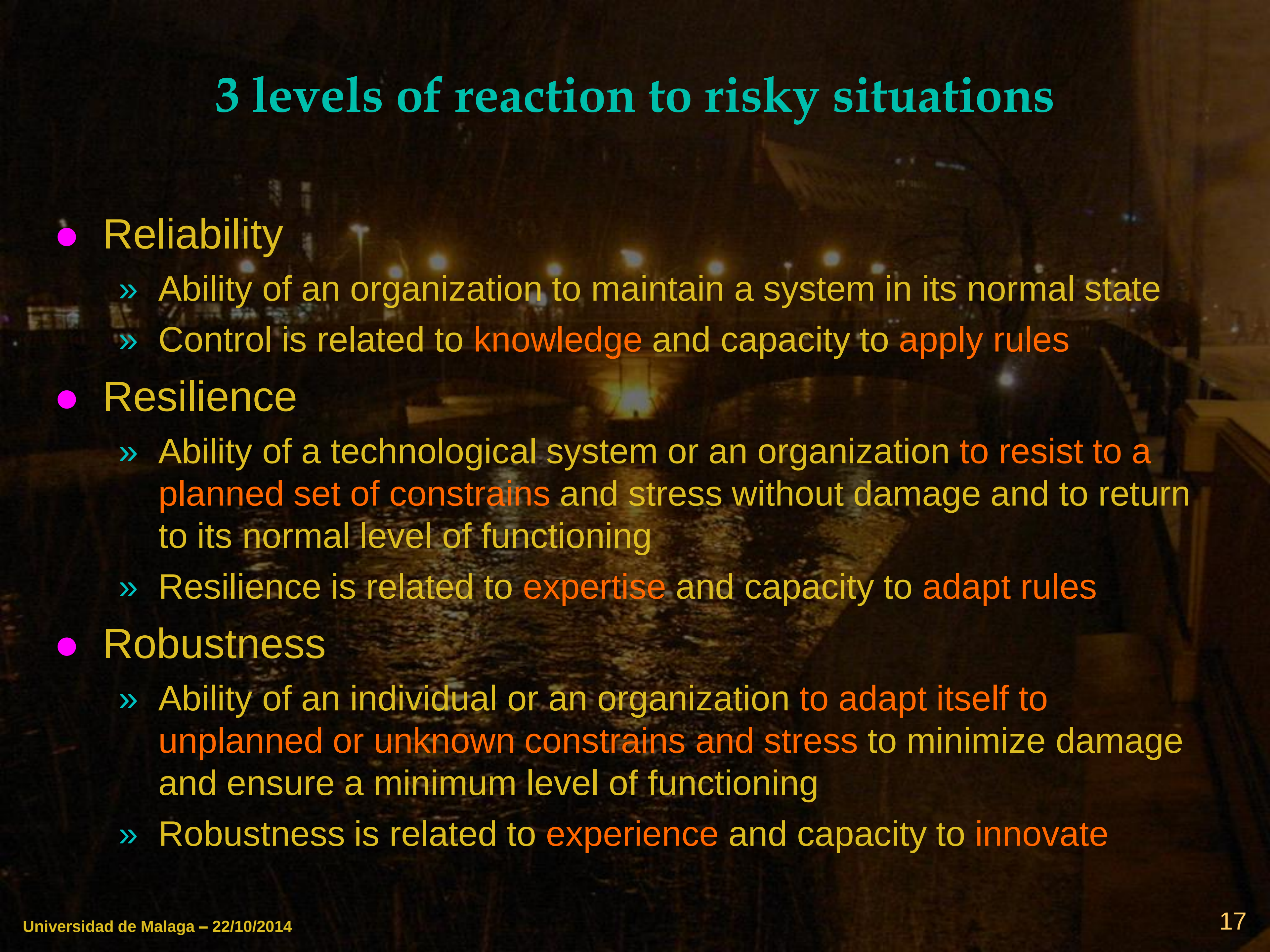


Managing emergencies and crises

Emergency Management Vs. Crisis Management

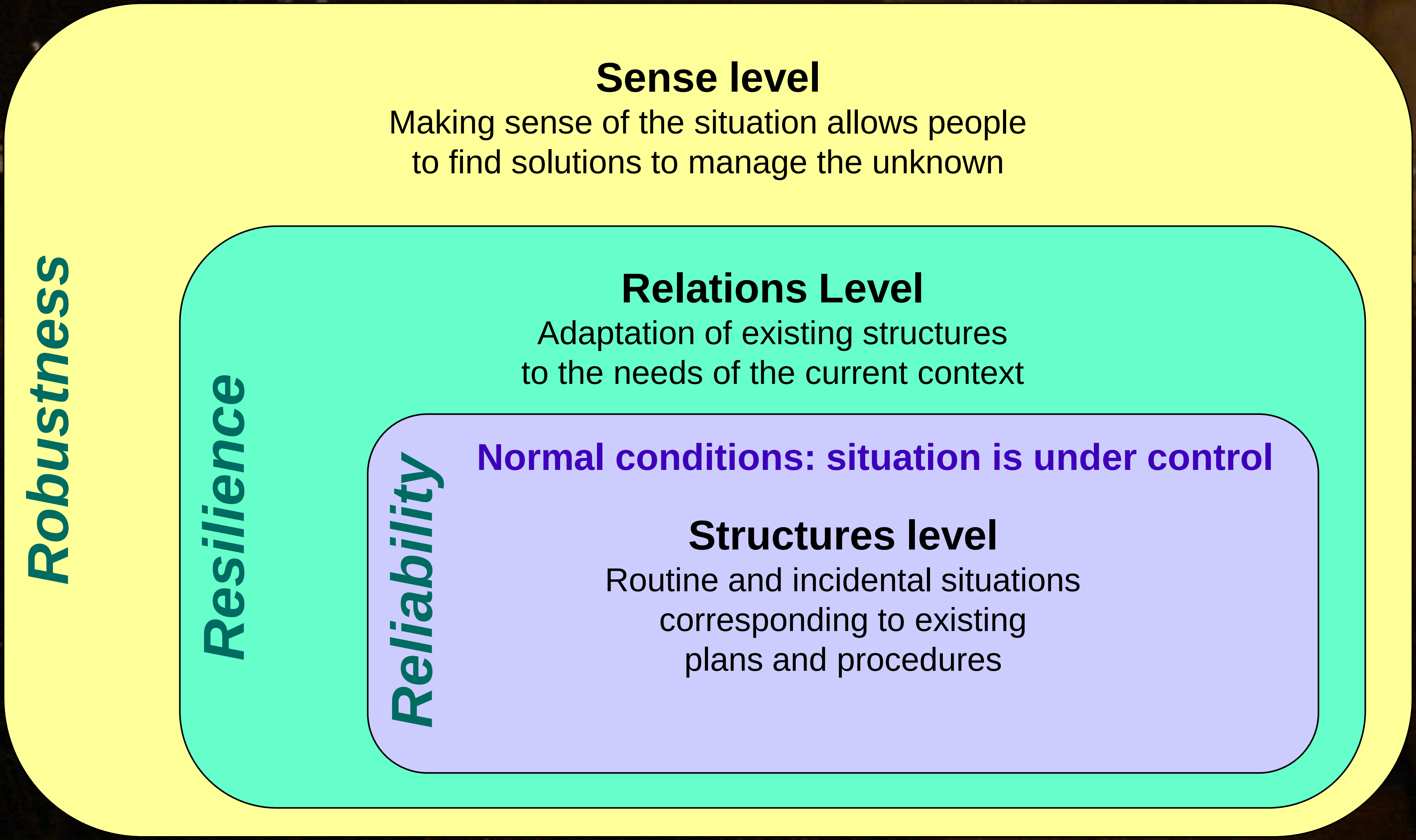
- Emergency management uses plans and procedures
  - » Set up and validated for planned events and situations
  - » Risk management missions and roles are defined and known
- Crisis management cannot be achieved with existing plans
  - » Intervention plans and procedures are no more fitted to the context
  - » Risk “owners” are no more in position to react
  - » **The doctrine** : find an organization that « recovers situation »
    - **Identify an upper level organization**
      - That corresponds to a “known framework”
      - That uses existing plans and procedures to bring back « order »
- **Trends not to enter into crisis**
  - » Develop **anticipation**
  - » Introduce **adaptability** in the design of plans and structures
    - Promote **emergence** of « ad-hoc » organizational patterns
  - » **Learn** from near-misses, accidents and past crisis

3 levels of reaction to risky situations



- Reliability
  - Ability of an organization to maintain a system in its normal state
  - Control is related to knowledge and capacity to apply rules
- Resilience
  - Ability of a technological system or an organization to resist to a planned set of constrains and stress without damage and to return to its normal level of functioning
  - Resilience is related to expertise and capacity to adapt rules
- Robustness
  - Ability of an individual or an organization to adapt itself to unplanned or unknown constrains and stress to minimize damage and ensure a minimum level of functioning
  - Robustness is related to experience and capacity to innovate

Prevention of crisis: a 3-level model
Reliability, resilience and robustness



Robustness

Sense level

Making sense of the situation allows people
to find solutions to manage the unknown

Resilience

Relations Level

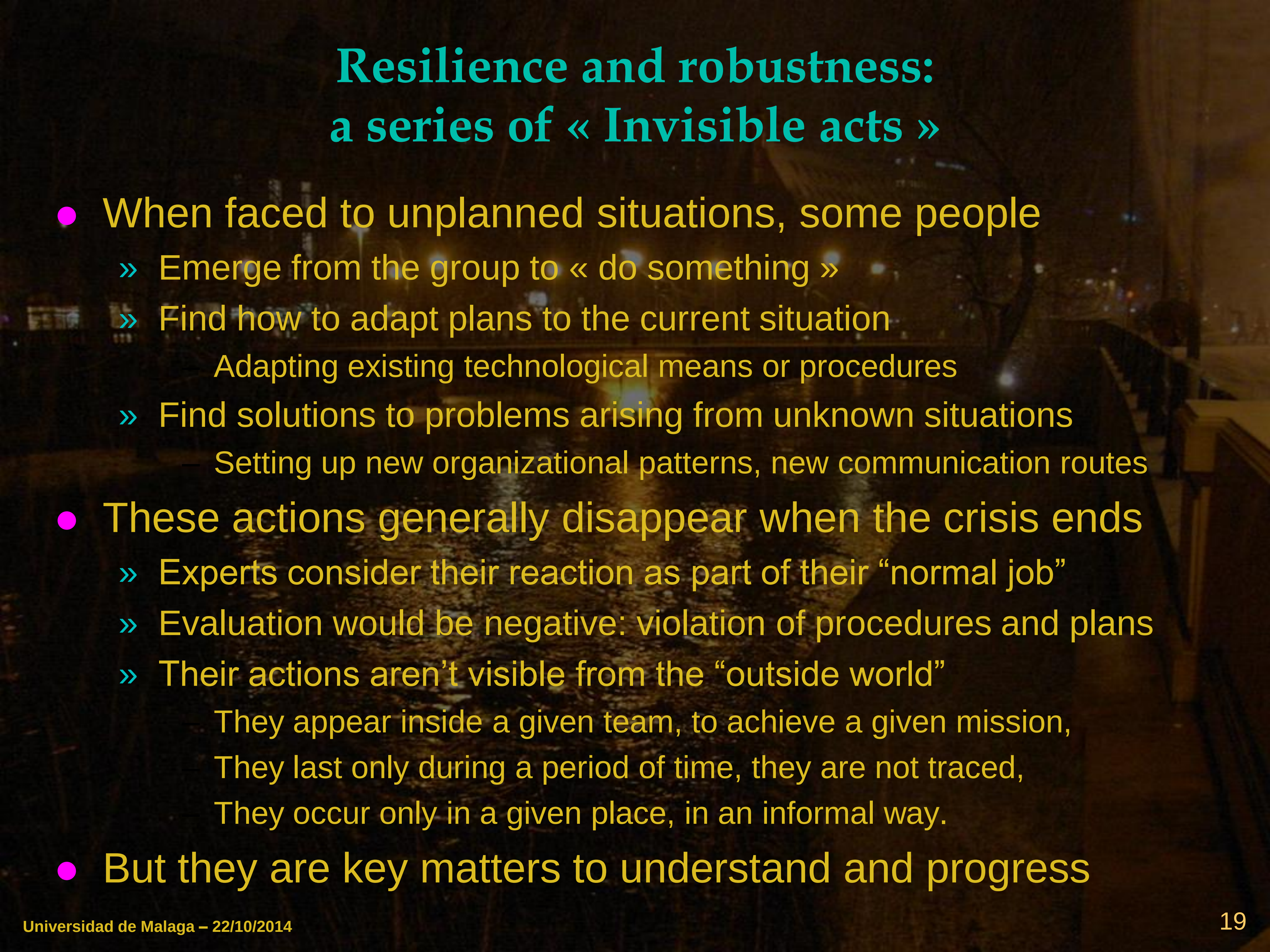
Adaptation of existing structures
to the needs of the current context

Reliability

Normal conditions: situation is under control

Structures level

Routine and incidental situations
corresponding to existing
plans and procedures

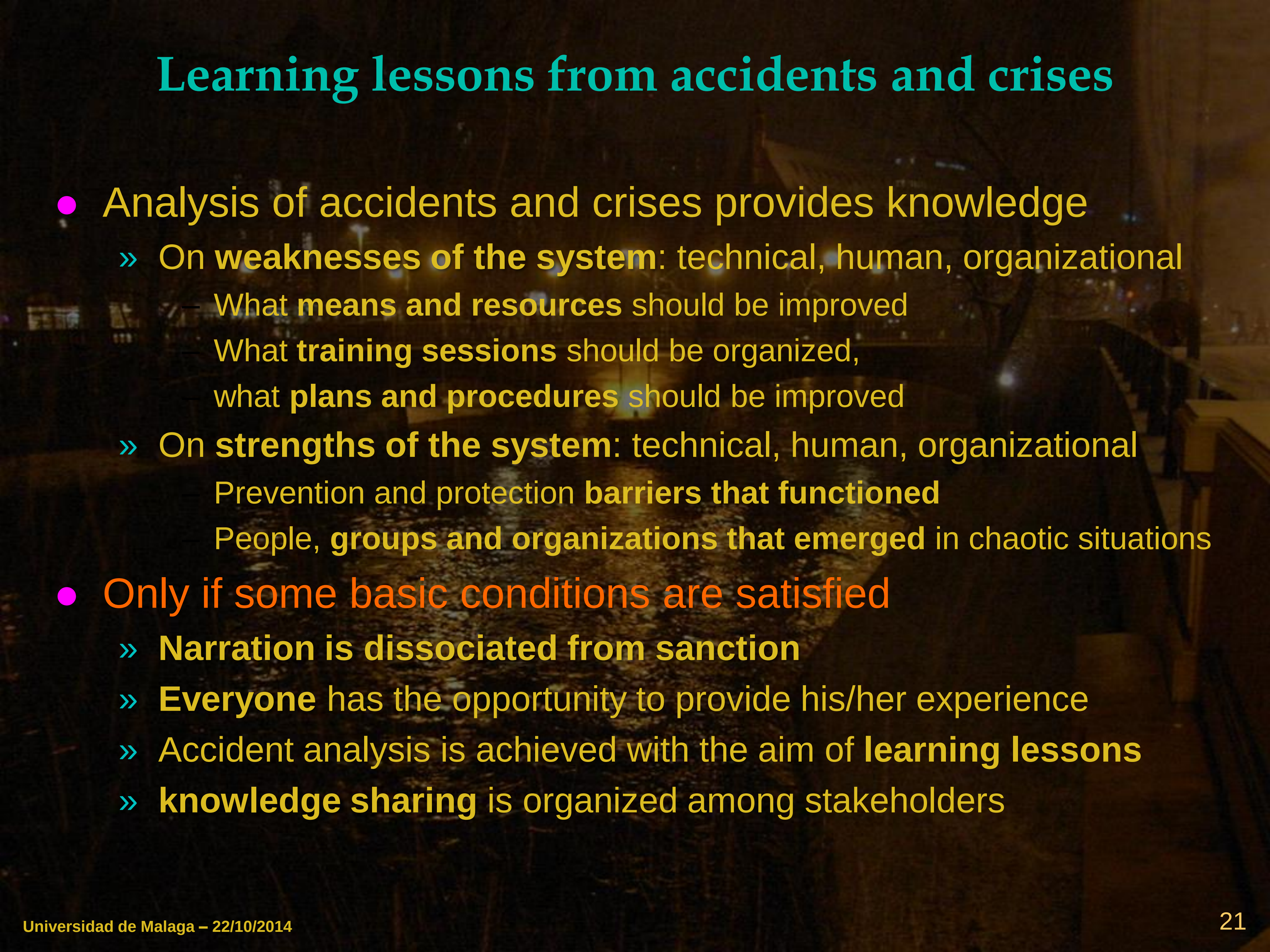


Resilience and robustness: a series of « Invisible acts »

- When faced to unplanned situations, some people
  - » Emerge from the group to « do something »
  - » Find how to adapt plans to the current situation
    - – Adapting existing technological means or procedures
  - » Find solutions to problems arising from unknown situations
    - – Setting up new organizational patterns, new communication routes
- These actions generally disappear when the crisis ends
  - » Experts consider their reaction as part of their “normal job”
  - » Evaluation would be negative: violation of procedures and plans
  - » Their actions aren’t visible from the “outside world”
    - – They appear inside a given team, to achieve a given mission,
    - – They last only during a period of time, they are not traced,
    - – They occur only in a given place, in an informal way.
- But they are key matters to understand and progress

Learning from experience

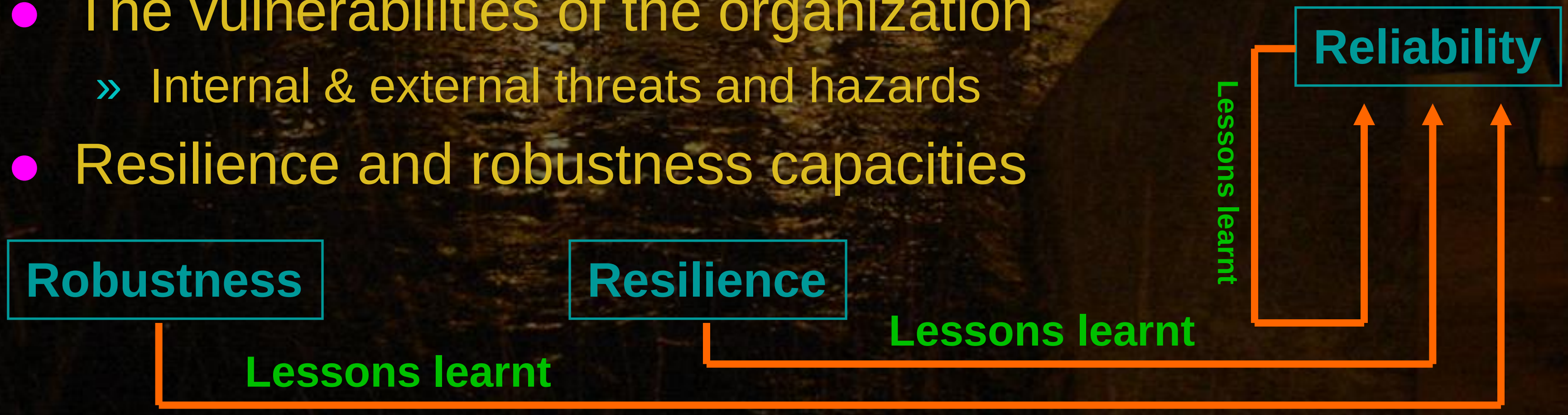
Learning lessons from accidents and crises



- Analysis of accidents and crises provides knowledge
  - » On **weaknesses of the system**: technical, human, organizational
    - What **means and resources** should be improved
    - What **training sessions** should be organized,
    - what **plans and procedures** should be improved
  - » On **strengths of the system**: technical, human, organizational
    - Prevention and protection **barriers that functioned**
    - People, **groups and organizations that emerged** in chaotic situations
- Only if some basic conditions are satisfied
  - » **Narration is dissociated from sanction**
  - » **Everyone** has the opportunity to provide his/her experience
  - » Accident analysis is achieved with the aim of **learning lessons**
  - » **knowledge sharing** is organized among stakeholders

Several kinds of lessons learnt from experience

- Accident scenarios
  - » Causes and consequences
  - » Barriers: prevention and protection (existing or to set up)
- The dynamics of events and decisions
  - » A succession of decision cycles; what else should be done ?
- The « control loops »
  - » They ensure reliability of organizations and processes
- The vulnerabilities of the organization
  - » Internal & external threats and hazards
- Resilience and robustness capacities



Reliability

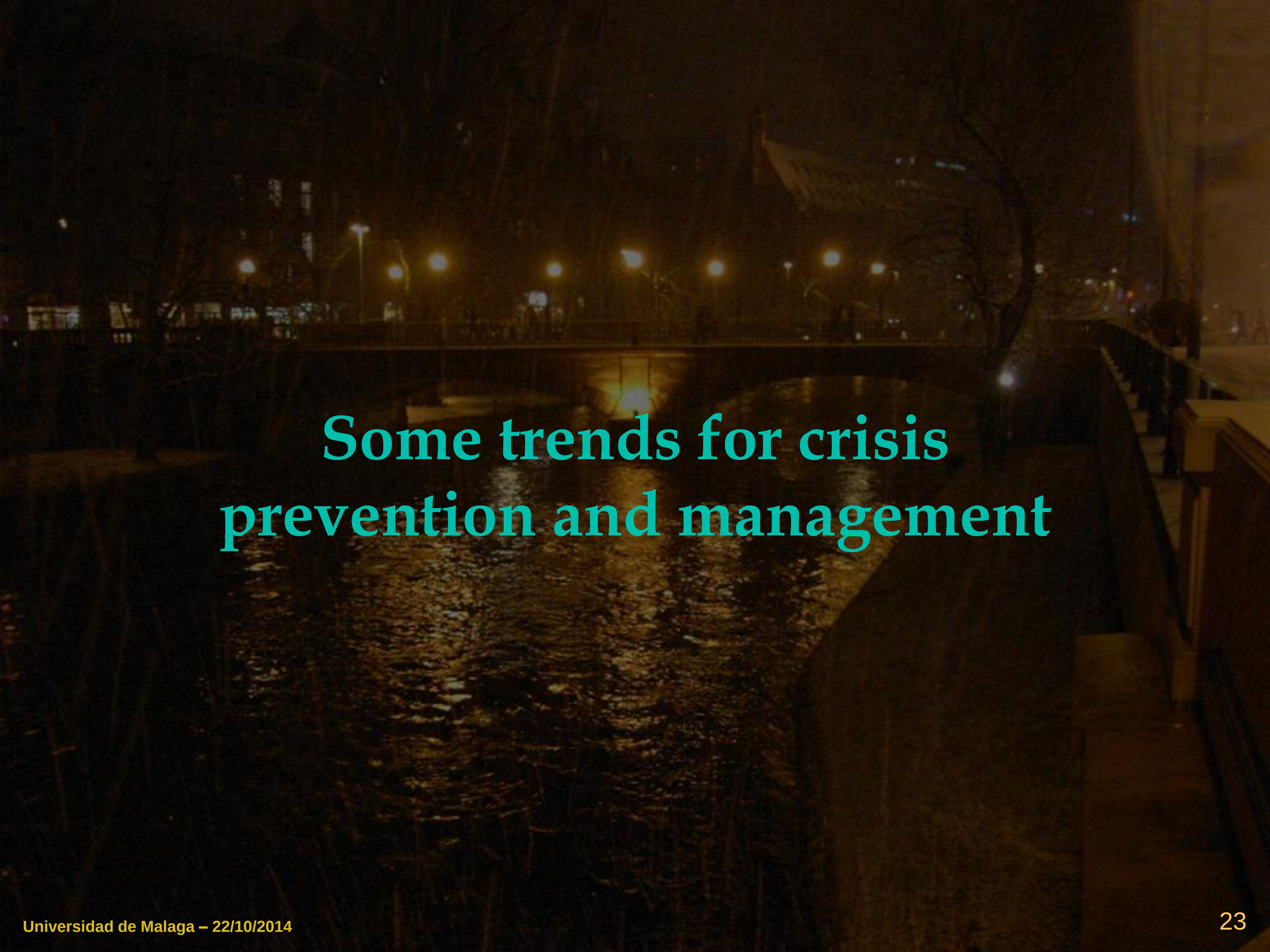
Lessons learnt

Robustness

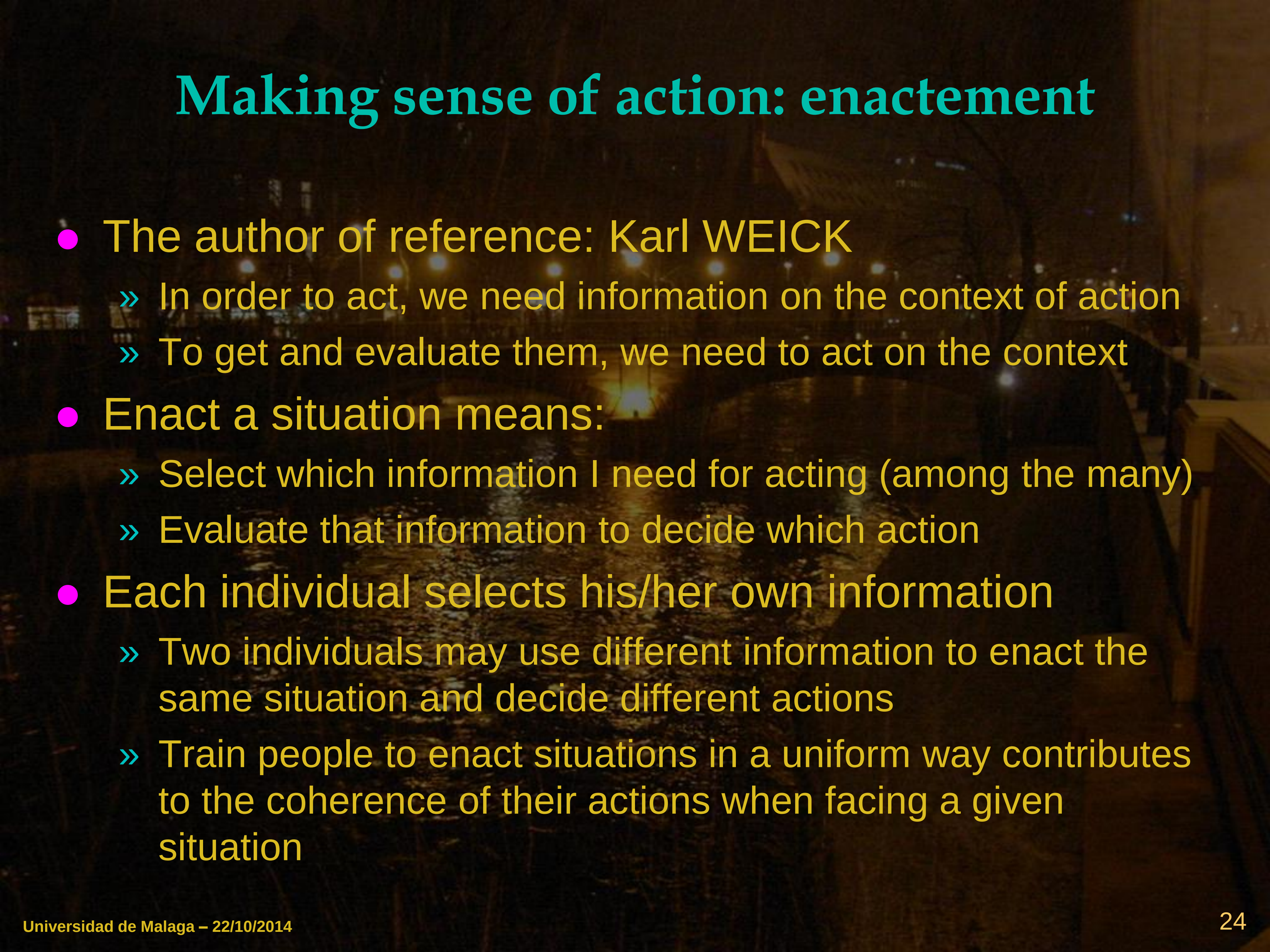
Resilience

Lessons learnt

Lessons learnt

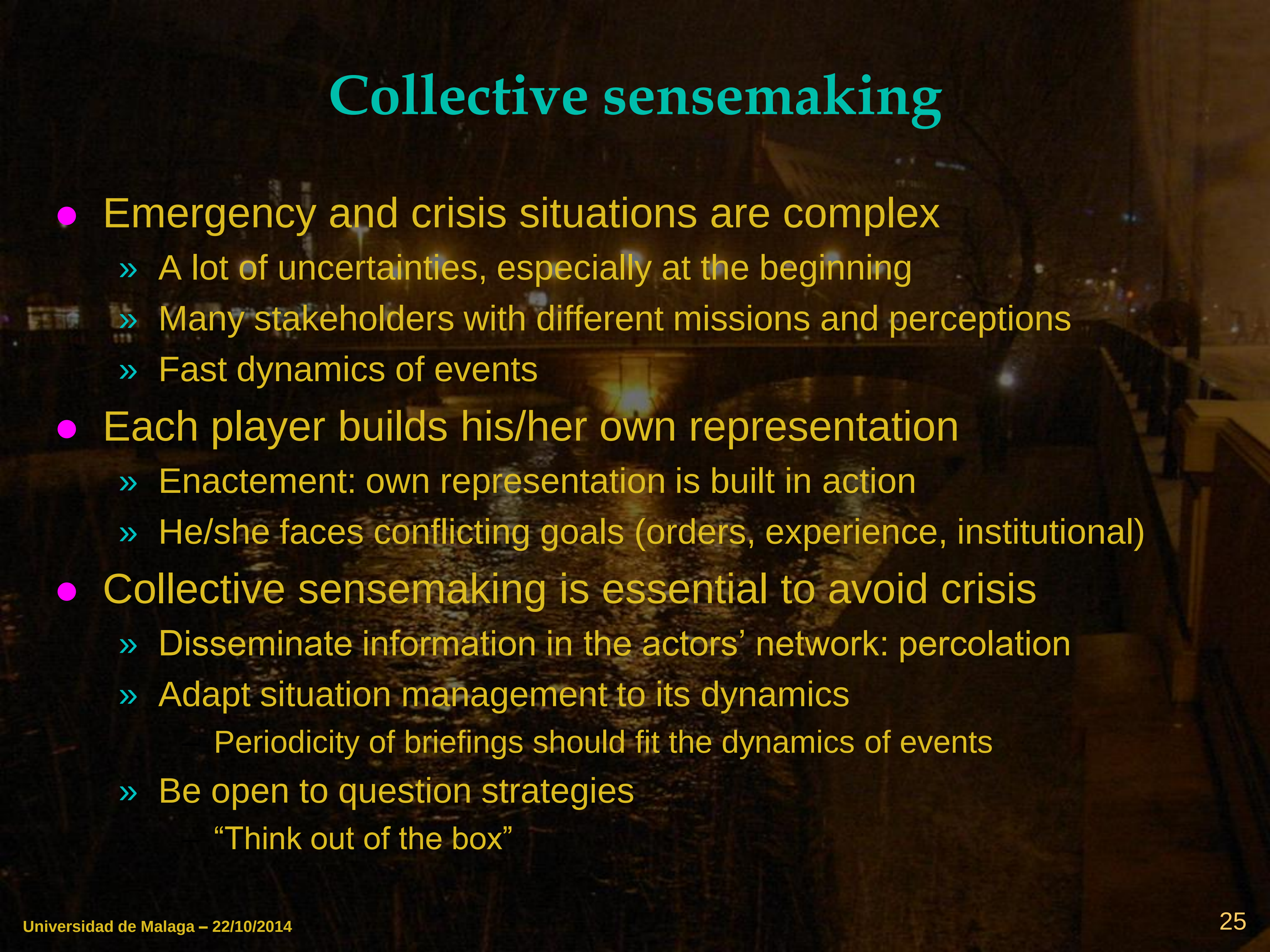


Some trends for crisis prevention and management



Making sense of action: enactement

- The author of reference: Karl WEICK
  - » In order to act, we need information on the context of action
  - » To get and evaluate them, we need to act on the context
- Enact a situation means:
  - » Select which information I need for acting (among the many)
  - » Evaluate that information to decide which action
- Each individual selects his/her own information
  - » Two individuals may use different information to enact the same situation and decide different actions
  - » Train people to enact situations in a uniform way contributes to the coherence of their actions when facing a given situation

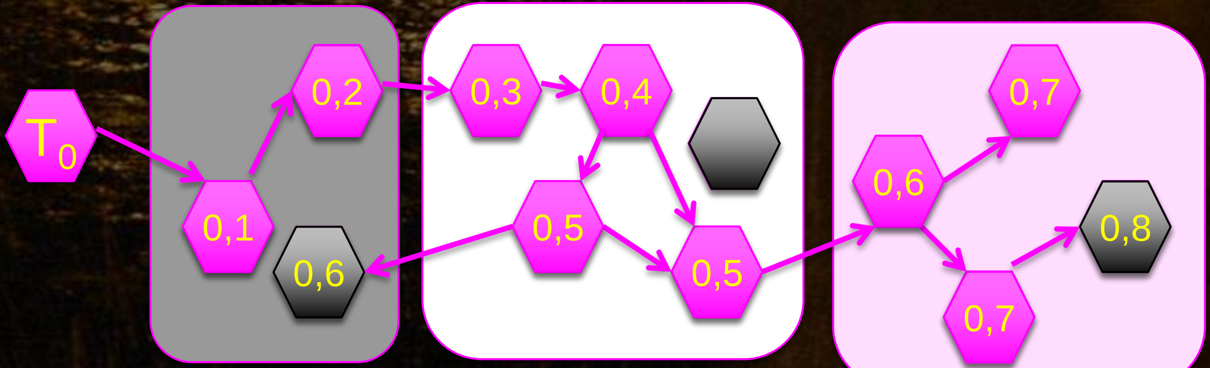


Collective sensemaking

- Emergency and crisis situations are complex
  - A lot of uncertainties, especially at the beginning
  - Many stakeholders with different missions and perceptions
  - Fast dynamics of events
- Each player builds his/her own representation
  - Enactement: own representation is built in action
  - He/she faces conflicting goals (orders, experience, institutional)
- Collective sensemaking is essential to avoid crisis
  - Disseminate information in the actors’ network: percolation
  - Adapt situation management to its dynamics
    - Periodicity of briefings should fit the dynamics of events
  - Be open to question strategies
    - “Think out of the box”

Percolation and crisis management

- Percolation: information flows through a players' network
  - Exists if everyone receives the information and it is still valid
- Percolation depends on 3 parameters:
  - Who receives information?
  - To whom the information is transmitted and after what delay?
  - What is the lifetime of information?
- Percolation and information coherence are ensured if:
  - All network members (stakeholders) get the information
  - They get it before it is outdated



Percolation and crisis management

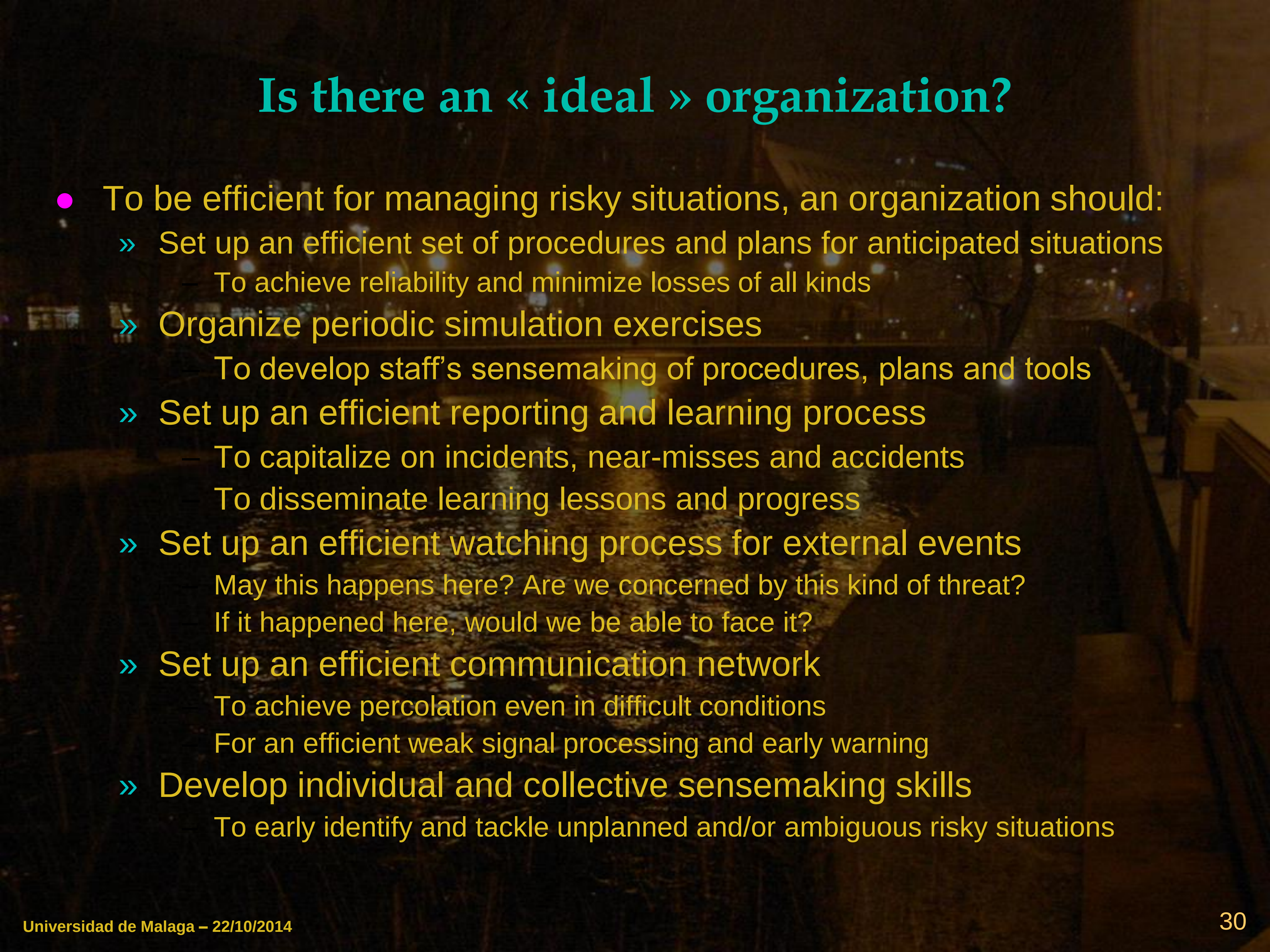
- Temporal coherence of information is a key success factor
  - » By reducing individual differences of perception
  - » By facilitating a shared enactement of situations
- Percolation model helps analyzing coherence
  - » For every kind of information related to the risky situation
    - Check if all stakeholders have access to the information
      - From whom do they get it?
      - How long does it takes to get it?
      - Is it through a reactive or proactive action?
    - Check the transmission delay compared to information lifetime
- Percolation helps defining the communication paths
  - » Players: sensors (human and techniques), transmitters, receivers
  - » Methods and dynamics of exchange

The role of social networks (Tweeter, …)

- Social networks participate in the flow of information
  - People are looking for information in social networks
  - People are willing to share witnesses and feelings
  - They are more and more often the first providers of information
- Analysis of those flows of information is hard (big data)
  - Relevant sources of information are drown in “noise”
  - False information also flows through social networks
- Authorities (public & private) invest in social networks
  - To collect information (through automatic data processing)
  - For an early detection of threats (terrorism, cybercriminality)
  - To provide factual and up to date information to the public
  - To set up interface groups: VOST (virtual operations support teams)

    Trusted volunteers listening to and talking through social networks

Conclusion



Is there an « ideal » organization?

- To be efficient for managing risky situations, an organization should:
  - » Set up an efficient set of procedures and plans for anticipated situations
    - – To achieve reliability and minimize losses of all kinds
  - » Organize periodic simulation exercises
    - – To develop staff's sensemaking of procedures, plans and tools
  - » Set up an efficient reporting and learning process
    - – To capitalize on incidents, near-misses and accidents
    - – To disseminate learning lessons and progress
  - » Set up an efficient watching process for external events
    - – May this happens here? Are we concerned by this kind of threat?
    - – If it happened here, would we be able to face it?
  - » Set up an efficient communication network
    - – To achieve percolation even in difficult conditions
    - – For an efficient weak signal processing and early warning
  - » Develop individual and collective sensemaking skills
    - – To early identify and tackle unplanned and/or ambiguous risky situations

Conclusion

- Crisis prevention is a progress loop
- **Anticipate** situations
  - **emergencies** : identify hazards and vulnerabilities
  - **crisis** : assess the potential of overwhelming
- Organize **vigilance**
  - Listen to what is expected
  - Detect changes and unusual signals
- **Manage unexpected situations**
  - **Planning**, **adaptation and innovation**
- **Learn from** what occurred and what was done
  - Analyze quasi-accidents, accidents, crisis and exercises
  - Validate and share knowledge
  - Use lessons learnt to improve anticipation