Software Engineering COMP1035

Lecture 17

Risk Management

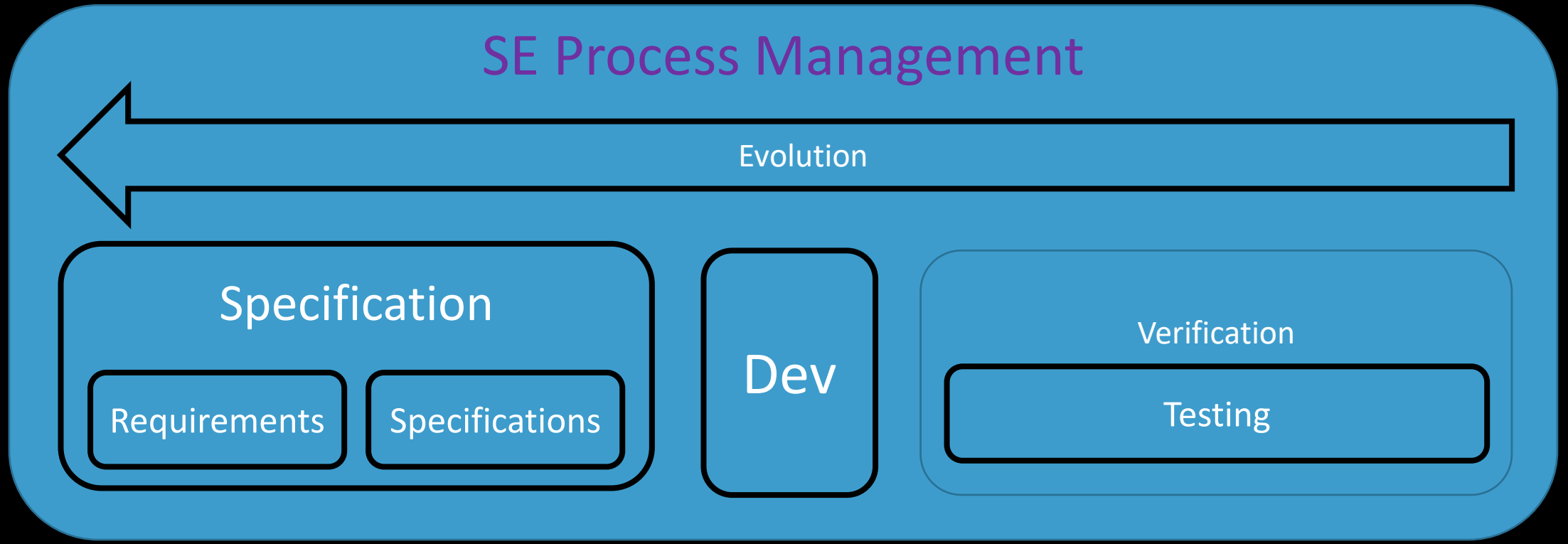
Outline

- Risk
- Risk monitoring
- Risk analysis
- Risk management

Where We Are In the Process

University of Nottingham
UK | CHINA | MALAYSIA

Keeping Track of SE Module



Process/Project Management

- Deliver good quality product
- Use good reliable methods
- **Reducing as much risk as possible**
- Plan / budget / manage a project based on these

Risks, Opportunities, and Problems

- A **risk** is the probability of unwanted consequences of an event and decision
- An **opportunity** is the probability of exceeding expectations. A risk is the probability of failing to meet expectations
- A **risk** is **not** a problem. A risk is a potential problem over which we have some choices.
- Causes of Risks:
  - Uncertainty in time
  - Uncertainty in control
  - Uncertainty in information
- There is no software project without risks…

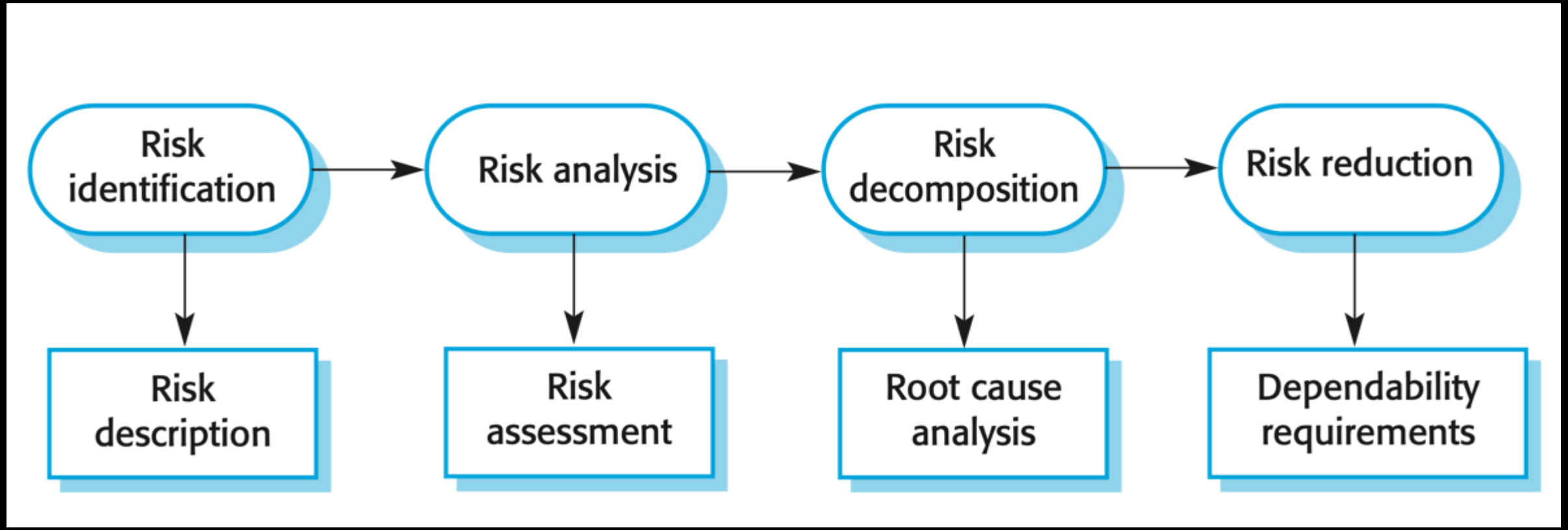
Risk Requirements for Software

- Requirements & Specs were all about '**should**' and '**shall**'
- What about '**should not**'?
  - we have to actively think about this
- What should definitely not happen with software?
  - people access other people's personal info
  - software doesn't break during critical processes
  - services go down for periods of time

Shall-not Requirements

- Functional Requirements
  - what **should not** happen
  - what should happen for **non-correct** usage or errors
- Non-functional Requirements
  - define the **reliability** and **availability** of software

Risks » Requirements



Risk Identification

- **Interviewing/Brainstorming**
  - Interview or brainstorm with project personnel, customers, and vendors. Open-ended questions can help identify potential areas of risk such as:
    - What new or improved technologies does this project implement?
    - What interfaces issues still need to be defined?
    - What requirements exist that we aren’t sure how to implement?
    - What concerns do we have about our ability to meet the required quality and performance levels?
- **Voluntary Reporting**
  - Any individual who identifies a risk is encouraged and rewarded for bringing that risk to management’s attention.
- **Decomposition**
  - Every TBD ("To Be Done/Determined") is a potential risk
  - Decomposition in the form of work breakdown structures during project planning can also help identify areas of uncertainty that may need to be recorded as risks

Risk Identification

- **Critical Path Analysis**
  - Any possibility of schedule slippage on the critical path must be considered a risk because it directly impacts our ability to meet schedule
- **Assumption Analysis**
  - Process and product assumptions must be analyzed, for example:
    - We might assume the hardware would be available by the system test date
    - Or assume three additional experienced C++ programmers will be hired by the time coding starts
- **Risk Taxonomies**
  - Lists of problems that have occurred on other projects and can be used as checklists to help ensure all potential risks have been considered

Risk Analysis: Insulin Delivery System

Identified hazard	Hazard probability	Accident severity	Estimated risk	Acceptability
1.Insulin overdose computation	Medium	High	High	Intolerable
2. Insulin underdose computation	Medium	Low	Low	Acceptable
3. Failure of hardware monitoring system	Medium	Medium	Low	ALARP
4. Power failure	High	Low	Low	Acceptable
5. Machine incorrectly fitted	High	High	High	Intolerable
6. Machine breaks in patient	Low	High	Medium	ALARP
7. Machine causes infection	Medium	Medium	Medium	ALARP
8. Electrical interference	Low	High	Medium	ALARP
9. Allergic reaction	Low	Low	Low	Acceptable

[Product] Risk Decomposition

- There might be several ways that a risk can occur
- Sometimes best solution to solve a problem
  - is not the ‘best for that problem’
  - but the **best** for **all related problems**
- If you collect shall-not specifications
  - you make it part of your collective design decisions

[Product] Risk Reduction

1. **Hazard Avoidance** - so it cannot occur
2. **Hazard Detection & Removal** - so systems recover nicely
3. **Damage Limitation** - so the impact is limited

- These are design issues
  - and might affect the design in the first place

Non-functional Risks

Failure type	Description
Loss of service	The system is unavailable and cannot deliver its services to users. You may separate this into loss of critical services and loss of non-critical services, where the consequences of a failure in non-critical services are less than the consequences of critical service failure.
Incorrect service delivery	The system does not deliver a service correctly to users. Again, this may be specified in terms of minor and major errors or errors in the delivery of critical and non-critical services.
System/data corruption	The failure of the system causes damage to the system itself or its data. This will usually but not necessarily be in conjunction with other types of failures.

- Unlike risks and hazards, reliability can be measured!
  - downtime - or uptime (availability)
  - rate of failures
  - recovery time

Availability Measures

Availability	Explanation
0.9	The system is available for 90% of the time. This means that, in a 24-hour period (1,440 minutes), the system will be unavailable for 144 minutes.
0.99	In a 24-hour period, the system is unavailable for 14.4 minutes.
0.999	The system is unavailable for 84 seconds in a 24-hour period.
0.9999	The system is unavailable for 8.4 seconds in a 24-hour period. Roughly, one minute per week.</TB>

Security Concerns

- Your test plan (for release or acceptance tests) might be driven by these
- What are the **most valuable components** in the project
  - credit card data?
  - customer patient data?
  - proprietary algorithms?
- Identify possible routes to this information
- Especially relevant for APIs, which purposefully give access

Risk Analysis at 3 Project Stages

1. **Preliminary Risk Analysis**
   - to help identify critical requirements
2. **Lifecycle Risk Analysis**
   - when system implementation decisions are made
3. **Operational Risk Analysis**
   - when the user interaction design decisions are made

Ongoing SE Project Failures

- The global cost of IT failure was estimated at + 6 trillion dollars in 2009
  Source: Roger Sessions, The IT Complexity Crisis: Danger and Opportunity
- Only 32% of software projects were “successfully completed” (i.e., on time, on cost, and with expected functionality) in 2009
  Source: Standish CHAOS 2009 Update
- Only 16% of software projects were successfully completed in the UK in 2009
  Source: British Computer Society

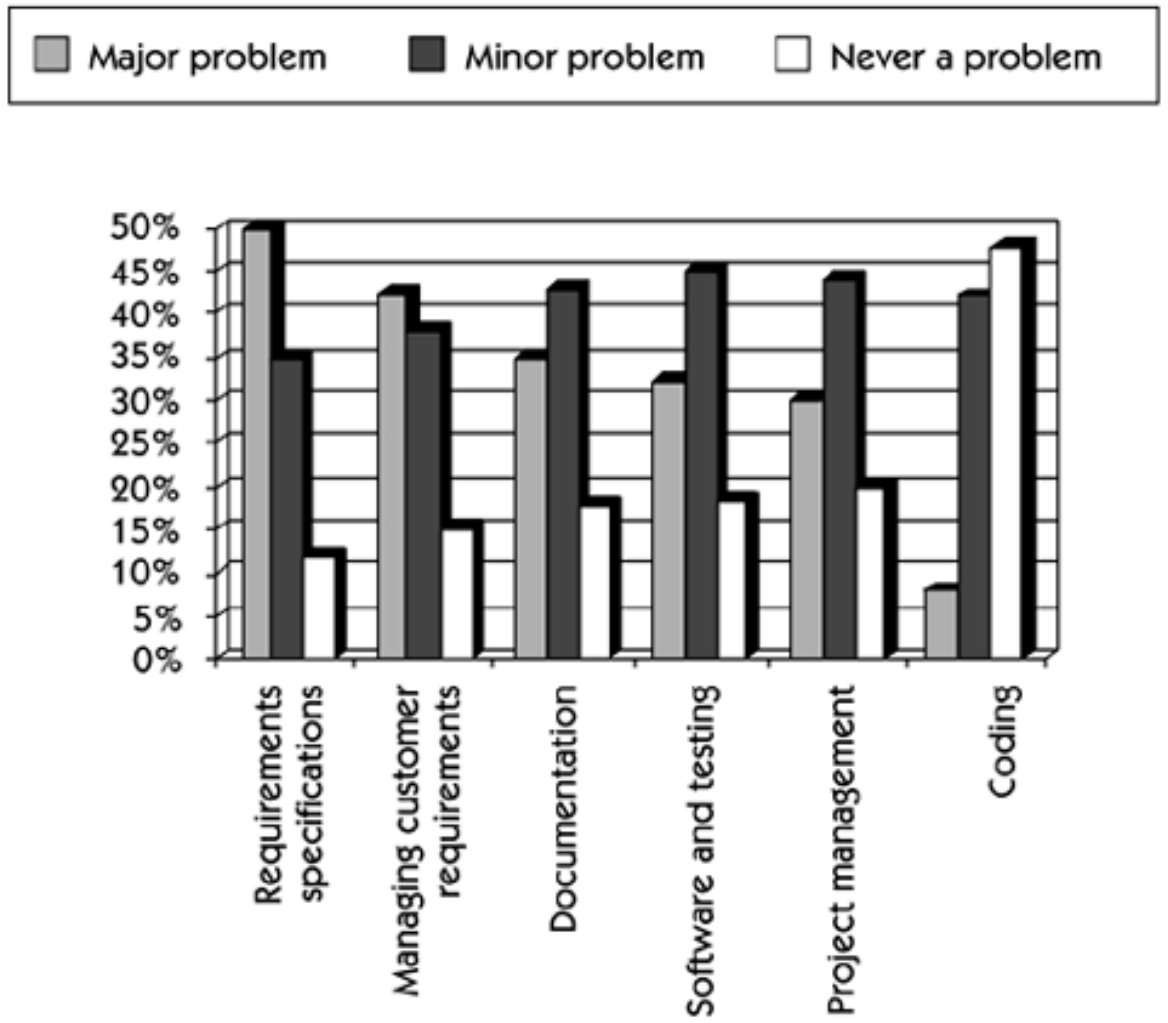
Ongoing SE Project Failures

- "A failing industry … ."
  - **If building engineers built buildings with the same care as software engineers build systems, the first woodpecker to come along would be the end of civilization as we know it**

    Source: Paul Dorsey, Top 10 Reasons Why Systems Projects Fail

What causes failure?

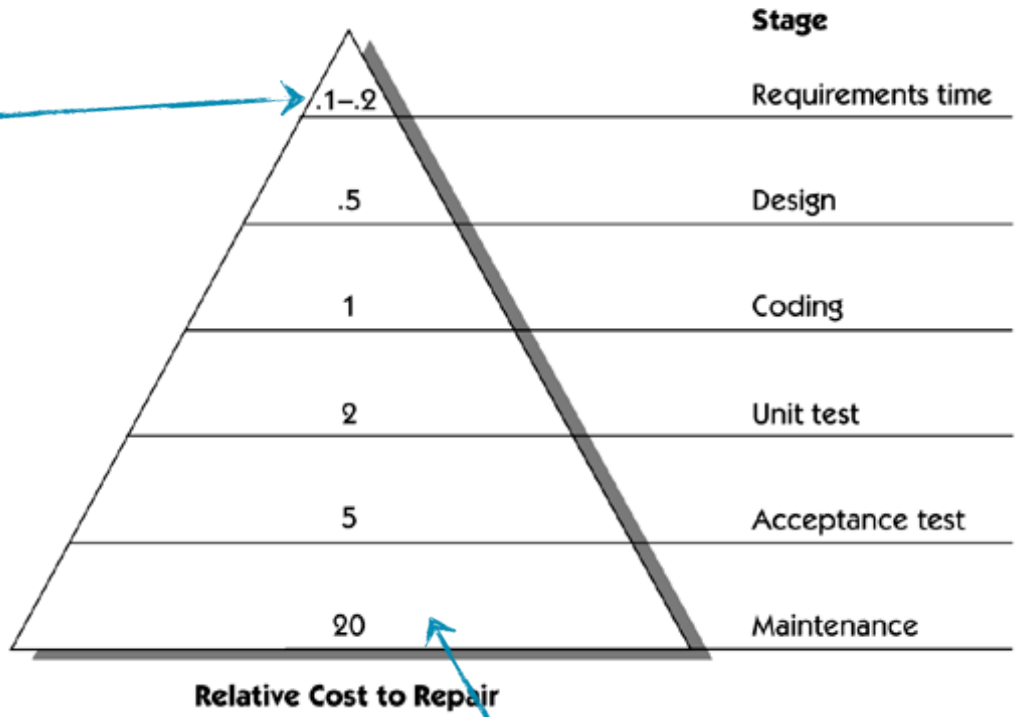
Figure 1-1. Largest software development problems by category. (Data derived from ESPITI [1995].)



What causes failure?

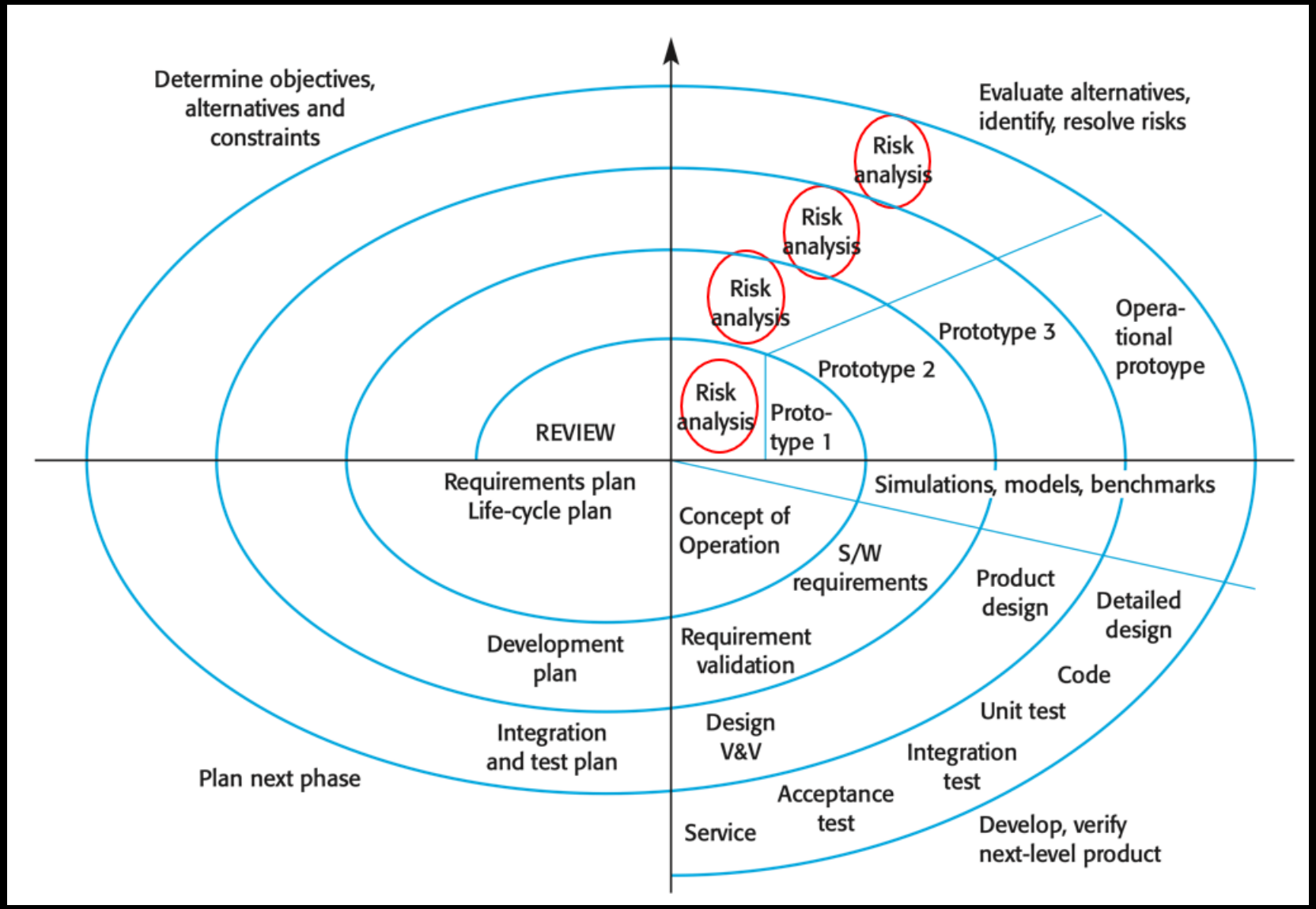
We want to fix problems here (obviously)

Figure 1-2. Relative cost to repair a defect at different lifecycle phases. (Data derived from Davis [1993].)



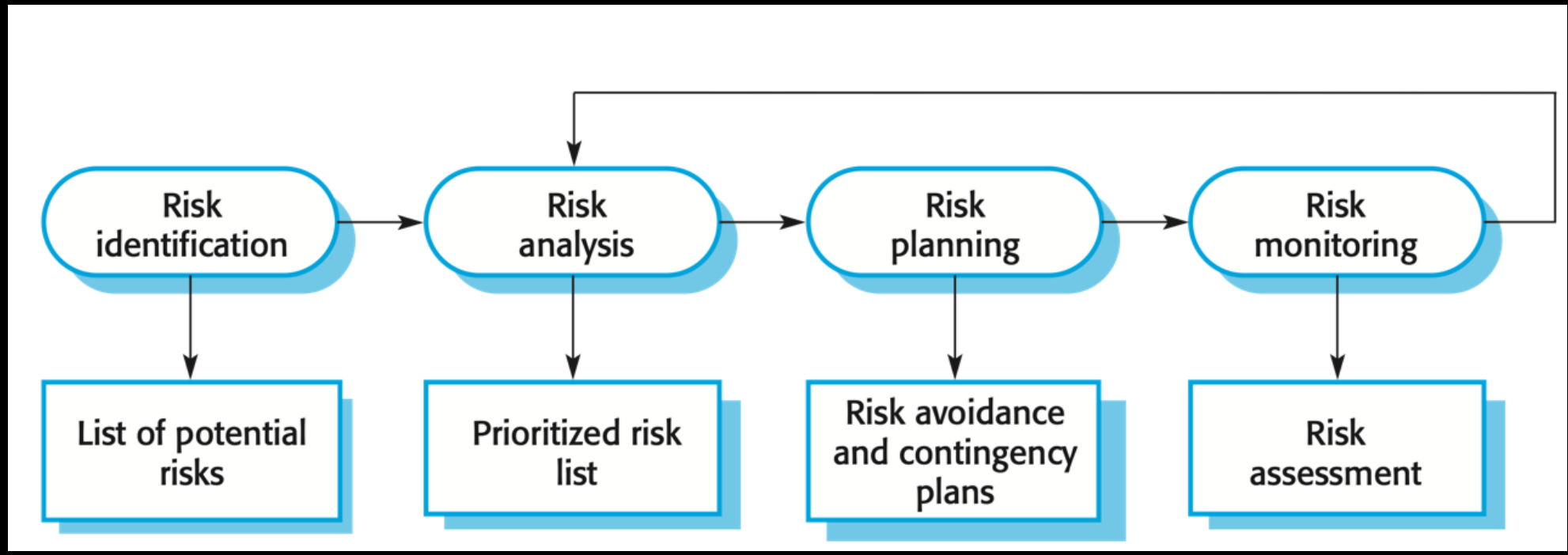
Basically, you want to avoid changes after release

Iterative Models - Boehm's Spiral



[Project] Risk Analysis

- Risk Management is one of the most important jobs for a project manager
  - considering and preparing for possible problems in the future
  - for the project going smoothly (not software going wrong)
- All risks should be listed, and a strategy considered



Project Risk: Management Concerns

- Deliver the software to the customer **on schedule**
- Keep overall costs **within** budget
- Deliver software that **meets** the customer's **expectations**
- Maintain a **happy** and **well-functioning** dev **team**

Recognizing and Controlling Risk

- Establish a Risk Review Board (RRB) led by the project manager.
- Representatives from each of the functional and support areas.
- Risks are documented and include a short description of the **risk type** (cost, schedule, technical); **severity** (low, moderate, high); **risk management plan**, etc

[Project] Risk Types

Risk type	Possible risks
Technology	The database used in the system cannot process as many transactions per second as expected. (1) Reusable software components contain defects that mean they cannot be reused as planned. (2)
People	It is impossible to recruit staff with the skills required. (3) Key staff are ill and unavailable at critical times. (4) Required training for staff is not available. (5)
Organizational	The organization is restructured so that different management are responsible for the project. (6) Organizational financial problems force reductions in the project budget. (7)
Tools	The code generated by software code generation tools is inefficient. (8) Software tools cannot work together in an integrated way. (9)
Requirements	Changes to requirements that require major design rework are proposed. (10) Customers fail to understand the impact of requirements changes. (11)
Estimation	The time required to develop the software is underestimated. (12) The rate of defect repair is underestimated. (13) The size of the software is underestimated. (14)

[Project] Risk Examples

Risk	Affects	Description
Staff turnover	Project	Experienced staff will leave the project before it is finished.
Management change	Project	There will be a change of organizational management with different priorities.
Hardware unavailability	Project	Hardware that is essential for the project will not be delivered on schedule.
Requirements change	Project and product	There will be a larger number of changes to the requirements than anticipated.
Specification delays	Project and product	Specifications of essential interfaces are not available on schedule.
Size underestimate	Project and product	The size of the system has been underestimated.
CASE tool underperformance	Product	CASE tools, which support the project, do not perform as anticipated.
Technology change	Business	The underlying technology on which the system is built is superseded by new technology.
Product competition	Business	A competitive product is marketed before the system is completed.

[Project] Risk Prioritisation

- **Probability** of it
  - very low (<10%)
  - low (10-25%)
  - moderate (25-50%)
  - high (50-75%)
  - very high (>75%)
- The **effect** of it!
  - catastrophic (project fail)
  - serious (expense/delays)
  - tolerable (in contingency)
  - insignificant (don't care)
- Both are important

Risk	Probability	Effects
Organizational financial problems force reductions in the project budget (7).	Low	Catastrophic
It is impossible to recruit staff with the skills required for the project (3).	High	Catastrophic
Key staff are ill at critical times in the project (4).	Moderate	Serious
Faults in reusable software components have to be repaired before these components are reused. (2).	Moderate	Serious
Changes to requirements that require major design rework are proposed (10).	Moderate	Serious
The organization is restructured so that different management are responsible for the project (6).	High	Serious
The database used in the system cannot process as many transactions per second as expected (1).	Moderate	Serious
The time required to develop the software is underestimated (12).	High	Serious
Software tools cannot be integrated (9).	High	Tolerable
Customers fail to understand the impact of requirements changes (11).	Moderate	Tolerable
Required training for staff is not available (5).	Moderate	Tolerable
The rate of defect repair is underestimated (13).	Moderate	Tolerable
The size of the software is underestimated (14).	High	Tolerable
Code generated by code generation tools is inefficient (8).	Moderate	Insignificant

[Project] Risk Planning

- You should choose a strategy for handling the risks
- **Avoidance strategies** - actions taken to reduce the risk happening
- **Minimization strategies** - reducing the impact if it happens
- **Contingency plans** - what you will do/change if it happens
- Avoidance is always the best strategy, if possible.
  - it's often worth taking pre-emptive actions to avoid risks

[Project] Risk Strategies

Risk	Strategy
Organizational financial problems	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of the business and presenting reasons why cuts to the project budget would not be cost-effective.
Recruitment problems	Alert customer to potential difficulties and the possibility of delays; investigate buying-in components.
Staff illness	Reorganize team so that there is more overlap of work and people therefore understand each other's jobs.
Defective components	Replace potentially defective components with bought-in components of known reliability.
Requirements changes	Derive traceability information to assess requirements change impact; maximize information hiding in the design.
Organizational restructuring	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of the business.
Database performance	Investigate the possibility of buying a higher-performance database.
Underestimated development time	Investigate buying-in components; investigate use of a program generator.

Minimisation

Avoidance

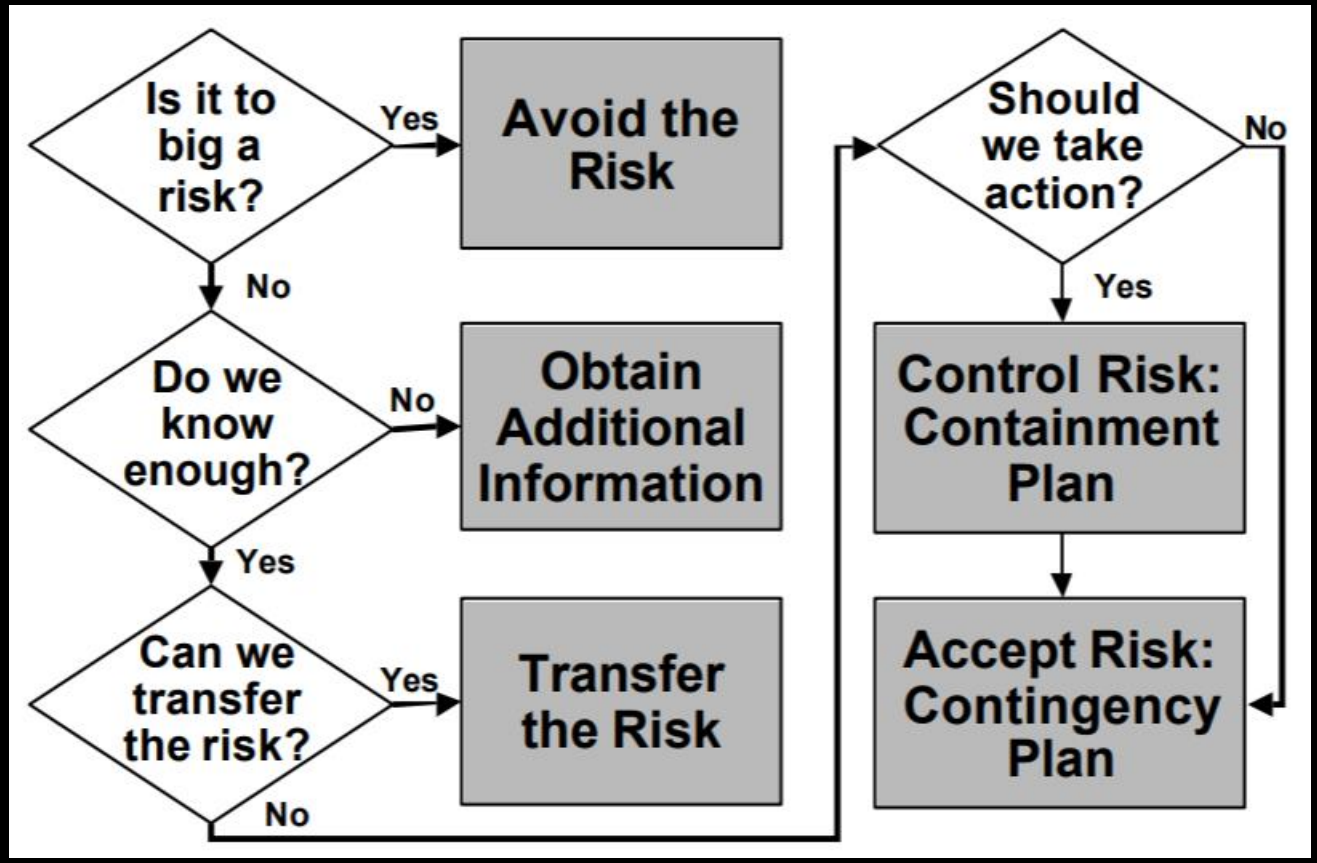
Contingency

[Project] Risk Monitoring

Risk type	Potential indicators
Technology	Late delivery of hardware or support software; many reported technology problems.
People	Poor staff morale; poor relationships amongst team members; high staff turnover.
Organizational	Organizational gossip; lack of action by senior management.
Tools	Reluctance by team members to use tools; complaints about CASE tools; demands for higher-powered workstations.
Requirements	Many requirements change requests; customer complaints.
Estimation	Failure to meet agreed schedule; failure to clear reported defects.

- Obviously, you want to check to see if any appear to be happening

Risk Management Plan



Risk Management Plan

- **Is it too big a risk?**
  - If the risk is too big for us to be willing to accept, we can avoid the risk by changing our project strategies and tactics to choose a less risky alternate or we may decide not to do the project at all
- Things to remember about avoiding risks:
  - Avoiding risks may also mean avoiding opportunities
  - Not all risks can be avoided
  - **Avoiding a risk in one part of the project may create risks in other parts of the project**

Risk Management Plan

Risk	Avoid the Risk
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications	Develop all software in-house. Switch to a subcontractor with a proven reliability track record even though they are more expensive.
The interface with the new control device is not defined and as a result its driver may take more time to implement than scheduled	Negotiate with the customer to move the implementation of this control device into a future software release. Replace the selected control device with an older device that has a well-defined interface.

Risk Management Plan

- **Do we know enough?**
  - If we don't know enough, we can plan to "buy" additional information through mechanisms such as prototyping, modeling, simulation, or conducting additional research.

Risk	Obtain Additional Information
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications	Perform a capability assessment of the subcontractor. Ask for references from past customers and check on the reliability of previous products.
The interface with the new control device is not defined and as a result its driver may take more time to implement than scheduled	Establish a communications link with device provider to obtain early design specifications for the device. Research interface specifications for other similar control devices by the same provider

Risk Management Plan

- **Can we transfer the risk?**
  - If it is not our risk or if it is economically feasible to pay someone else to assume all or part of the risk, we can plan to transfer the risk to another organization.

Risk	Transfer the Risk
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications	Transfer the risk to the subcontractor by building penalties into the contract for delivered software that does not have the required reliability.
The interface with the new control device is not defined and as a result its driver may take more time to implement than scheduled	Transfer the risk to the customer by building additional charges to the customer and/or late delivery alternatives into the contract if the customer does not supply the specification by its due date.

Risk Management Plan

- **Should action be taken now?**
  - If we decide to attack the risk directly, we typically start with creating a list of possible risk reduction actions that can be taken for the risk.
- Two major types of risk reduction actions should be considered:
  - Actions that **reduce** the **likelihood** that the risk will occur
  - Actions that **reduce** the **impact** of the risk should it occur

Risk Management Plan

Risk	Control the Risk / Containment Plan
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications	Assign a project engineer to participate in the requirements & design inspection and to conduct alpha testing at the subcontractor's site. Require defect data reports from the subcontractor on a weekly basis during integration and system test.
The interface with the new control device is not defined and as a result its driver may take more time to implement than scheduled	Assign a senior software engineer who has experience with similar control devices to the design task. Move the design task later in the schedule and increase its effort estimate.

Risk Management Plan

- **Contingency plans**:
  - If immediate risk reduction actions are not taken or if those actions reduce but do not eliminate the risk, it may be appropriate to develop risk contingency plans.

Risk	Contingency Plans
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications	Assign an engineer to work with the subcontractor on defect resolution and implement our regression test plan for maintenance releases from the subcontractor.
The interface with the new control device is not defined and as a result its driver may take more time to implement than scheduled	Hold Critical Design Review (CDR) with a TBD and hold a second CDR for just the subsystem that uses the device.

Risk Management Common Practices

- **Create a list of potential risks on your project**
  - List down a couple of risks right from the top of your head, categorize them according to type
- **Analyze the probability of each risk**
  - One recommended way of ordering risks according to their potential impact
- **Create an action plan for each risk you define**
  - Use the list of risks you've prepared and make sure you have a strategy listed down if any of the risks turn into a burning problem

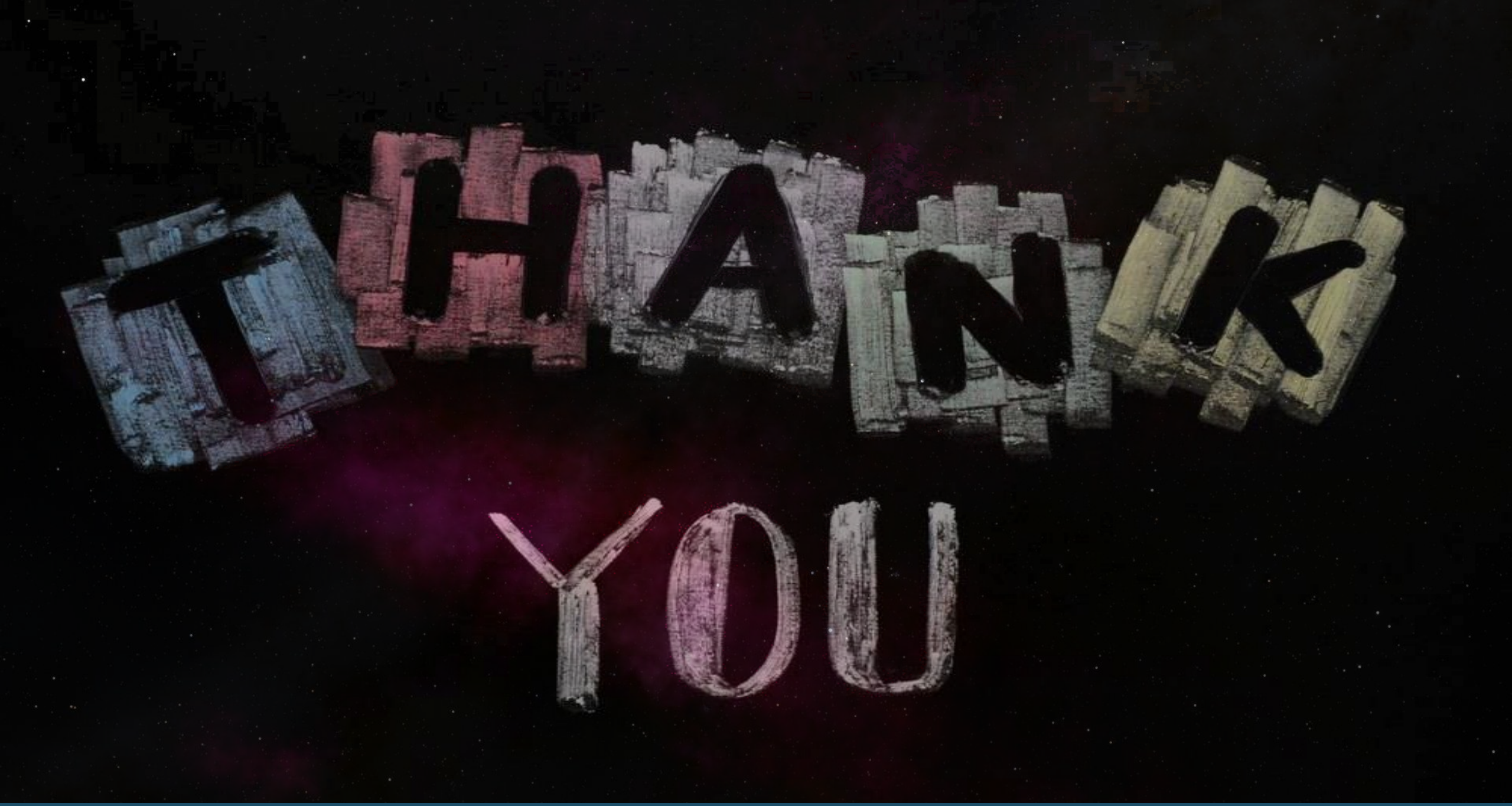
Risk Management Common Practices

- **Develop a risk monitoring system**
  - Go through the list of risks regularly and make sure their impact on the project and their probability of happening are up-to-date
- **Create a knowledge base of crises that have taken place in the past**
  - Create a knowledge base where you and your team can add tips and step-by-step strategies on handling obstacles
- **Promote openness among team members and with your contractors**
  - Put honest communication at the forefront

University of Nottingham
UK | CHINA | MALAYSIA

Summary

- **Software Risks** » reqs, specs, designs
  - so do a functional risk analysis early as possible
  - create some clear ‘shall-nots’
- Most project planning is about managing Project Risk
  - avoiding, or handling
  - so do a project risk analysis at the start
- Don’t forget - Risk Monitoring - its not over after the **planning**


THANK
YOU