Software Project Management 4th Edition

Chapter 7

Risk management

Risk management

This lecture will touch upon:

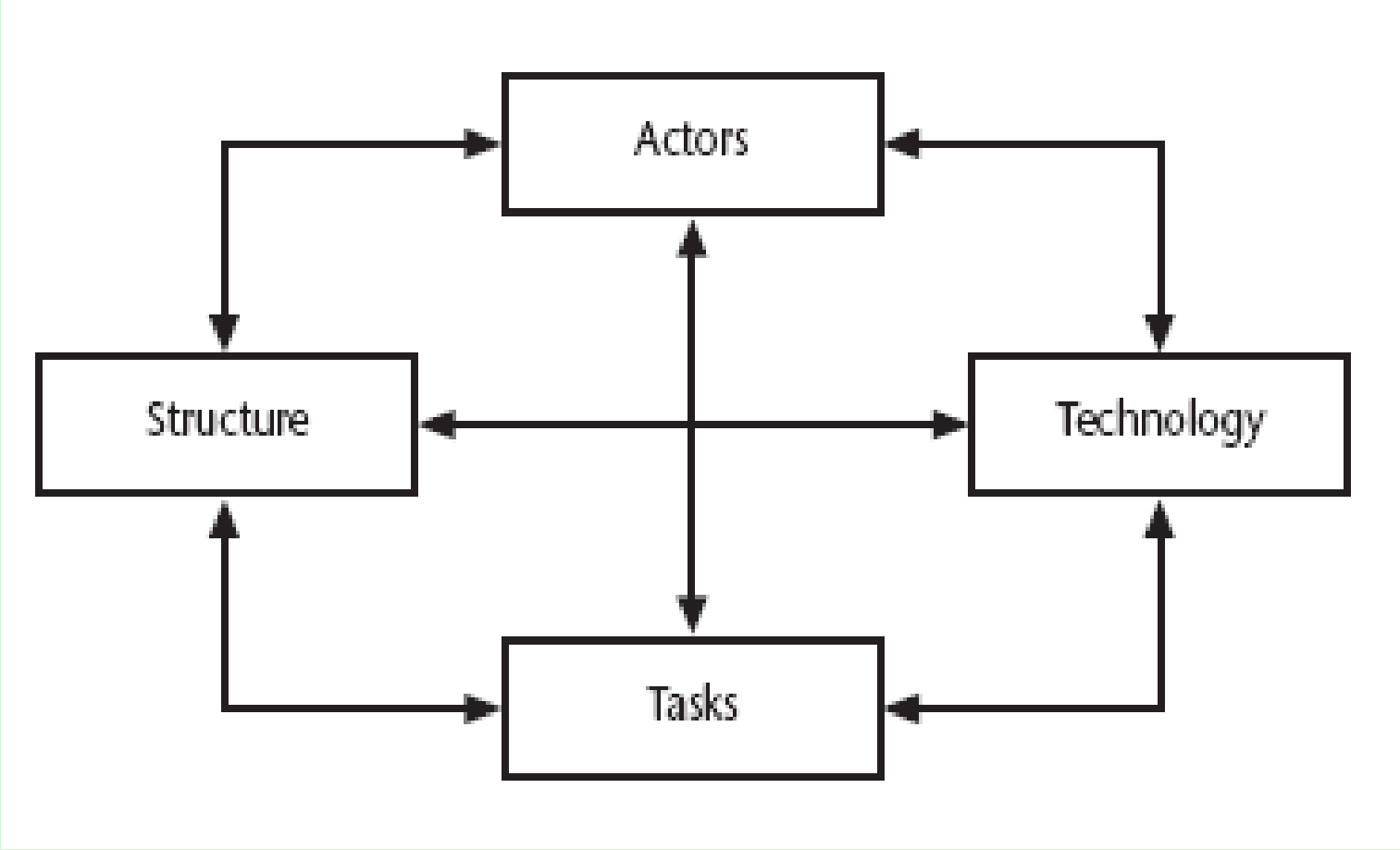
- Definition of 'risk' and 'risk management'
- Some ways of categorizing risk
- Risk management
  - Risk identification – what are the risks to a project?
  - Risk analysis – which ones are really serious?
  - Risk planning – what shall we do?
  - Risk monitoring – has the planning worked?
- We will also look at PERT risk and critical chains

Some definitions of risk

'the chance of exposure to the adverse consequences of future events' PRINCE2

- Project plans have to be based on *assumptions*
- *Risk* is the possibility that an assumption is wrong
- When the risk happens it becomes a *problem* or an *issue*

Categories of risk



ISPL situational factors: the target domain

class	*description*
information system	the characteristics of the information system - these are independent of the technologies that might be used
computer system	the characteristics of the part of the information system that have been computerized

ISPL situational factors: project domain

Project	• the types of task to be undertaken
Structure	• the communication systems, management structures, work flows etc
Actors	• the people involved in the project
Technology	• the methods, techniques and tools to be used

A framework for dealing with risk

The planning for risk includes these steps:

- Risk identification – what risks might there be?
- Risk analysis and prioritization – which are the most serious risks?
- Risk planning – what are we going to do about them?

Risk monitoring – what is the current state of the risk?

Risk identification

Approaches to identifying risks include:

- Use of checklists – usually based on the experience of past projects
- Brainstorming – getting knowledgeable stakeholders together to pool concerns
- Causal mapping – identifying possible chains of cause and effect

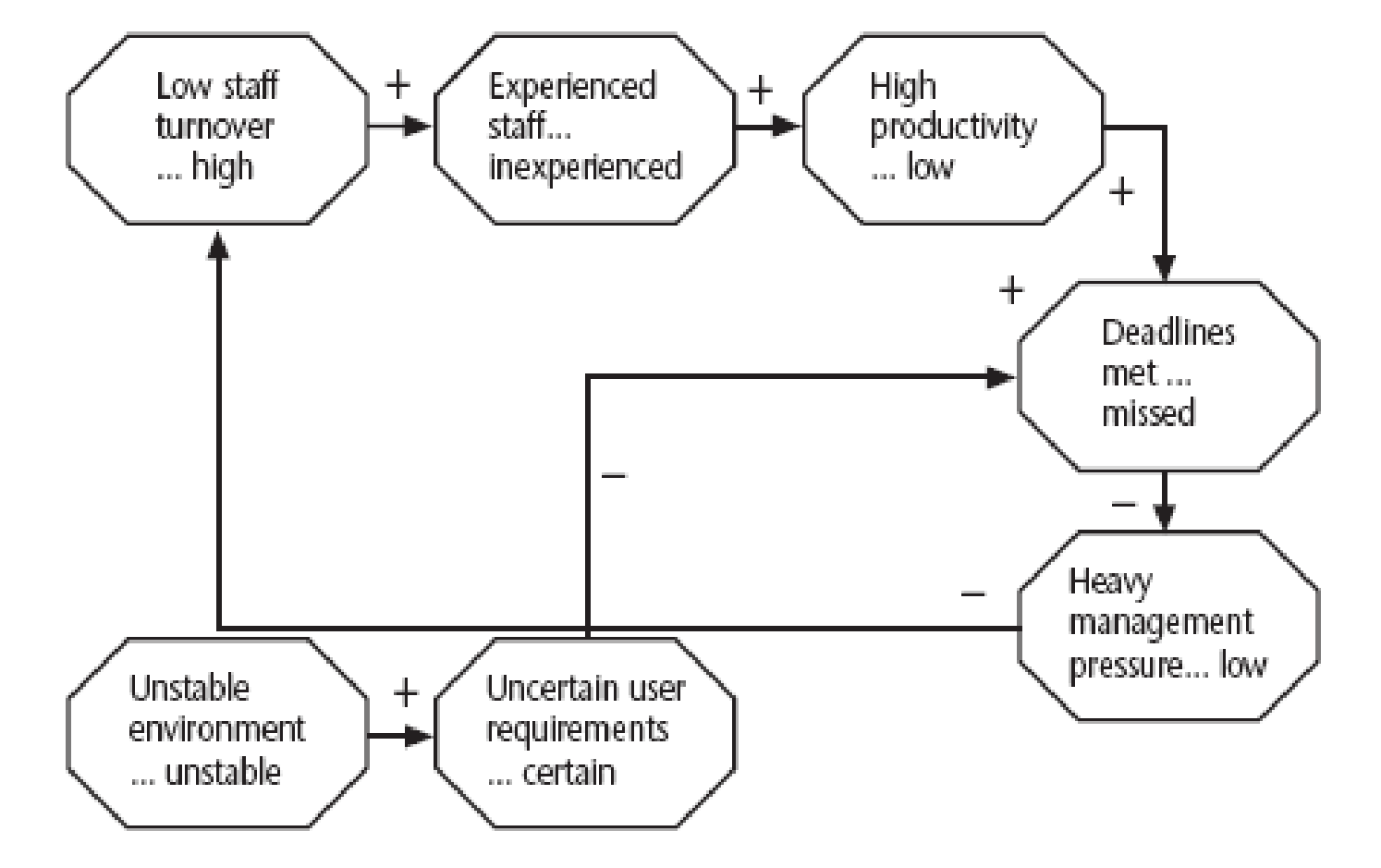
Boehm's top 10 development risks

Risk	*Risk reduction techniques*
Personnel shortfalls	Staffing with top talent; job matching; teambuilding; training and career development; early scheduling of key personnel
Unrealistic time and cost estimates	Multiple estimation techniques; design to cost; incremental development; recording and analysis of past projects; standardization of methods
Developing the wrong software functions	Improved software evaluation; formal specification methods; user surveys; prototyping; early user manuals
Developing the wrong user interface	Prototyping; task analysis; user involvement

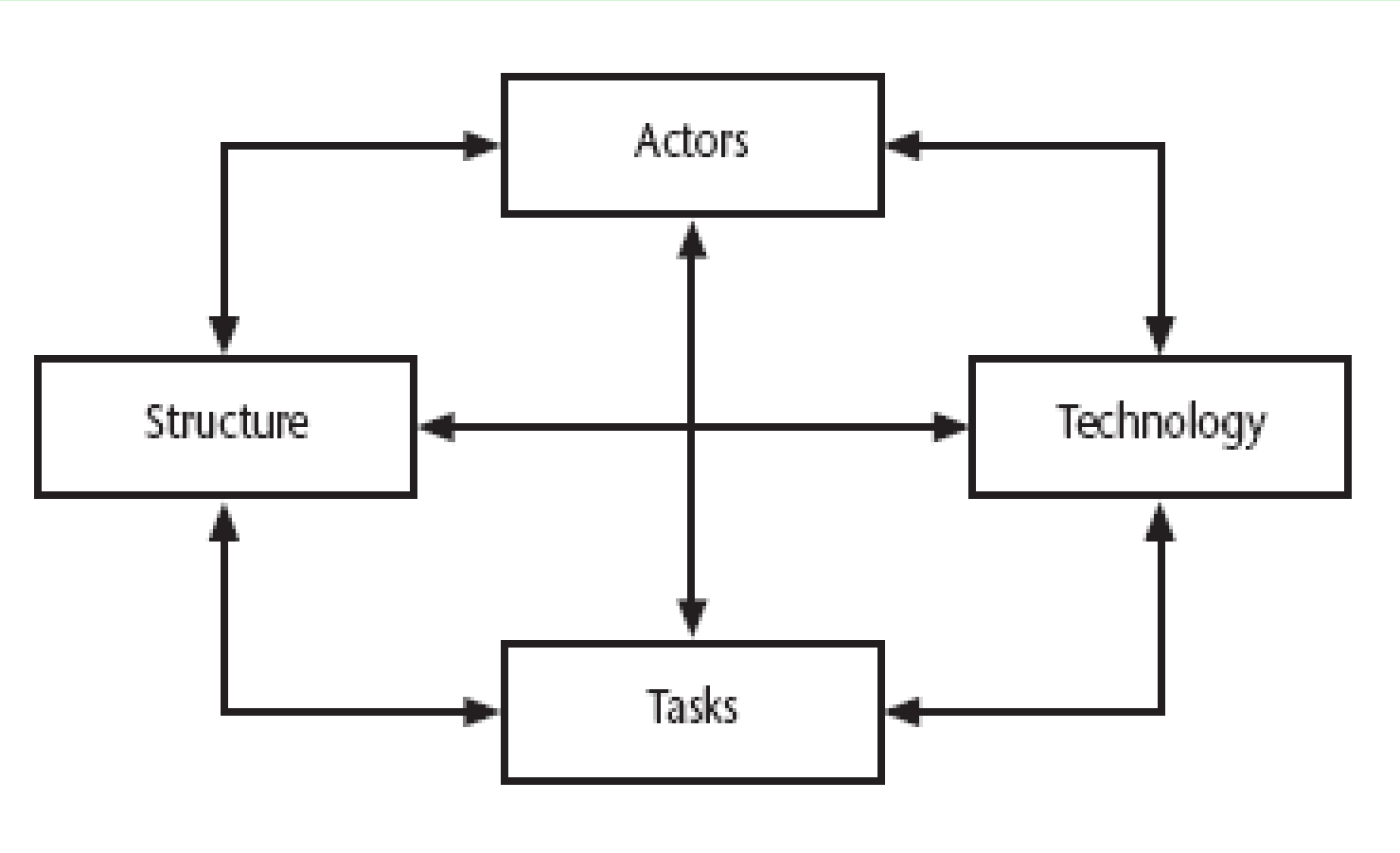
Boehm's top ten risk - continued

Gold plating	Requirements scrubbing, prototyping, design to cost
Late changes to requirements	Change control, incremental development
Shortfalls in externally supplied components	Benchmarking, inspections, formal specifications, contractual agreements, quality controls
Shortfalls in externally performed tasks	Quality assurance procedures, competitive design etc
Real time performance problems	Simulation, prototyping, tuning
Development technically too difficult	Technical analysis, cost-benefit analysis, prototyping , training

Causal mapping



Causal mapping - interventions



Background Risk Assessment

- Risk projection (or estimation) attempts to rate each risk in two ways
  - The probability that the risk is real
  - The consequence of the problems associated with the risk, should it occur
- The project planner, managers, and technical staff perform four risk projection steps (see next slide)
- The intent of these steps is to consider risks in a manner that leads to prioritization
- By prioritizing risks, the software team can allocate limited resources where they will have the most impact

Risk Projection/Estimation Steps

1) Establish a scale that reflects the perceived likelihood of a risk (e.g., 1-low, 10-high)
2) Delineate the consequences of the risk
3) Estimate the impact of the risk on the project and product
4) Note the overall accuracy of the risk projection so that there will be no misunderstandings

Assessing Risk Impact

- Three factors affect the consequences that are likely if a risk does occur
  - **Its nature** – This indicates the problems that are likely if the risk occurs
  - **Its scope** – This combines the severity of the risk (how serious was it) with its overall distribution (how much was affected)
  - **Its timing** – This considers when and for how long the impact will be felt
- The overall risk exposure formula is RE = P x C
  - P = the probability of occurrence for a risk
  - C = the cost to the project should the risk actually occur
- Example
  - P = 80% probability that 18 of 60 software components will have to be developed
  - C = Total cost of developing 18 components is $25,000
  - RE = .80 x $25,000 = $20,000

Risk prioritization

Risk exposure (RE)

= (potential damage) x (probability of occurrence)

Ideally

Potential damage: a money value e.g. a flood would cause £0.5 millions of damage

Probability 0.00 (absolutely no chance) to 1.00 (absolutely certain) e.g. 0.01 (one in hundred chance)

RE = £0.5m x 0.01 = £5,000

Crudely analogous to the amount needed for an insurance premium

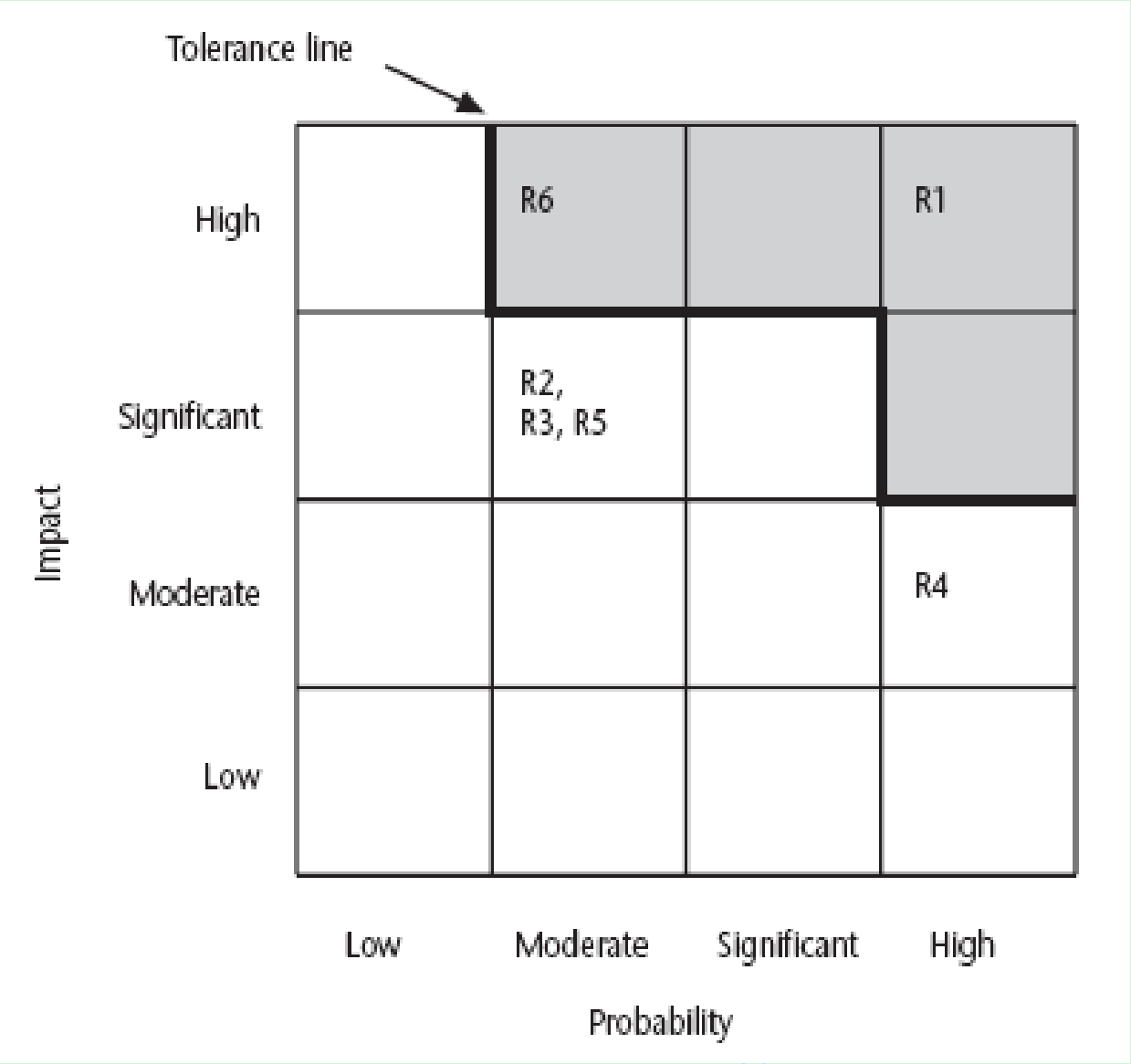
Risk probability: qualitative descriptors

Probability level	*Range*
High	Greater than 50% chance of happening
Significant	30-50% chance of happening
Moderate	10-29% chance of happening
Low	Less than 10% chance of happening

Qualitative descriptors of impact on cost and associated range values

Impact level	*Range*
High	Greater than 30% above budgeted expenditure
Significant	20 to 29% above budgeted expenditure
Moderate	10 to 19% above budgeted expenditure
Low	Within 10% of budgeted expenditure.

Probability impact matrix



Risk planning

Risks can be dealt with by:

- Risk acceptance
- Risk avoidance
- Risk reduction
- Risk transfer
- Risk mitigation/contingency measures

Risk acceptance

- The risk is acknowledged, but no action is taken unless the risk occurs
- Appropriate when it is not possible or cost-effective to address a specific risk in any other way

Risk Avoidance

- *Risk avoidance* evades a risk, eliminates the cause of the risk event, or changes the project plan to protect the project objectives from the risk event
- Risk avoidance eradicates the risk by removing the risk or its cause
- Risk avoidance is most suitable in the early stages of a project, through improved communications, additional resources, or more-clearly defined scope

Risk transfer

- *Risk transfer* moves the risk and the consequences of that risk to a third party
- Responsibility for the management of that risk now rests with another party
- Risk transfer comes in many forms but is most effective for financial risks
  - *Example:* Insurance is one form of risk transfer

Risk Reduction and Mitigation

- Risk Reduction attempts to reduce the likelihood of the risk occurring.
- Risk Mitigation is action taken to ensure the impact of the risk is lessened when it occurs.
- For ex, taking regular backups of data storage would reduce the impact of data corruption but not its likelihood.
- Mitigation is closely associated with contingency planning which is discussed presently.

Fairley's four commercial off-the shelf(COTS) Software Acquisition risks

- Integration –Difficulties in integrating the data formats and communication protocols of different appln.
- Upgrading – When the supplier upgrades the package, the package might no longer meet the user's requirements.
- No Source code –If you want to enhance the system, you might not be able to do so as you do not have access to the source code.
- Supplier failures or buyouts – The supplier of the application might go out of business or be bought out by a rival supplier.

Risk contingency plans

- *Contingency planning* involves planning alternatives to deal with the risks should they occur
- Contingency plans do not seek to reduce the probability or impact of risks—the strategy accepts that the risk may occur and plans ways to respond to the risk
- A contingency plan is executed when the risk event occurs
- Contingency plans must be in place well before the time the risk may occur
- Contingency (fallback) plans are developed for risks:
  - With very high impact or:
  - With response strategies that may themselves be risky
- Contingency plans usually entail a significant alternative path through part of the project
- *Example:* disaster recovery plan

Deciding on the risk actions

- The countermeasures that are considered , they must be cost effective.
- On that occasions where a risk exposure value can be calculated as a financial value using

Value of damage X Probability of occurrence

The cost effectiveness of a risk reduction action can be assessed by calculating the risk reduction leverage (RRL)

Risk reduction leverage

Risk reduction leverage =

$(RE_{before} - RE_{after}) / (\text{cost of risk reduction})$

RE_{before} is risk exposure before risk reduction e.g. 1% chance of a fire causing £200k damage

RE_{after} is risk exposure after risk reduction e.g. fire alarm costing £500 reduces probability of fire damage to 0.5%

RRL = (1% of £200k)-(0.5% of £200k)/£500 = 2

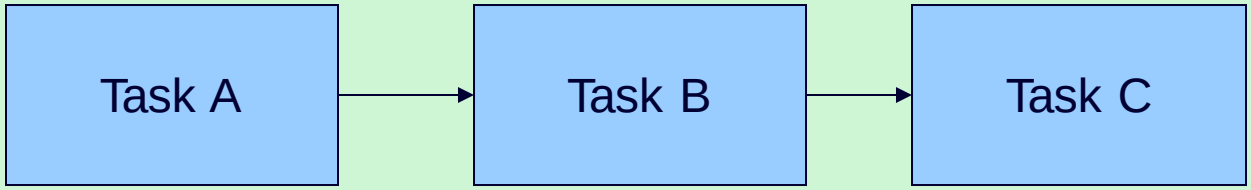
RRL > 1.00 therefore worth doing

Using PERT to evaluate the effects of uncertainty

Three estimates are produced for each activity

- *Most likely time (m)*
- *Optimistic time (a)*
- *Pessimistic (b)*
- 'expected time' $t_e = (a + 4m + b) / 6$
- 'activity standard deviation' $S = (b-a)/6$

A chain of activities



Task	a	m	b	t_e	s
A	10	12	16	?	?
B	8	10	14	?	?
C	20	24	38	?	?

A chain of activities

- What would be the expected duration of the chain A + B + C?
- Answer: 12.66 + 10.33 + 25.66 i.e. 48.65
- What would be the standard deviation for A + B+ C?
- Answer: square root of (1^2 + 1^2 + 3^2) i.e. 3.32

Assessing the likelihood of meeting a target

- Say the target for completing A+B+C was 52 days (T)
- Calculate the z value thus

  $z = (T - t_e)/s$
- In this example $z = (52-48.33)/3.32$ i.e. 1.01
- Look up in table of z values – see next overhead

Labelling Convention

PERT Example

Consider a small project that involves the following activities.

	Preceding	Completion Times (days)		
Activity	Activity	Optimistic	Most Likely	Pessimistic
a	-	5	6	7
b	-	4	5	18
c	a	4	15	20
d	b,c	3	4	5
e	a	5	16	18

PERT Example (cont'd)

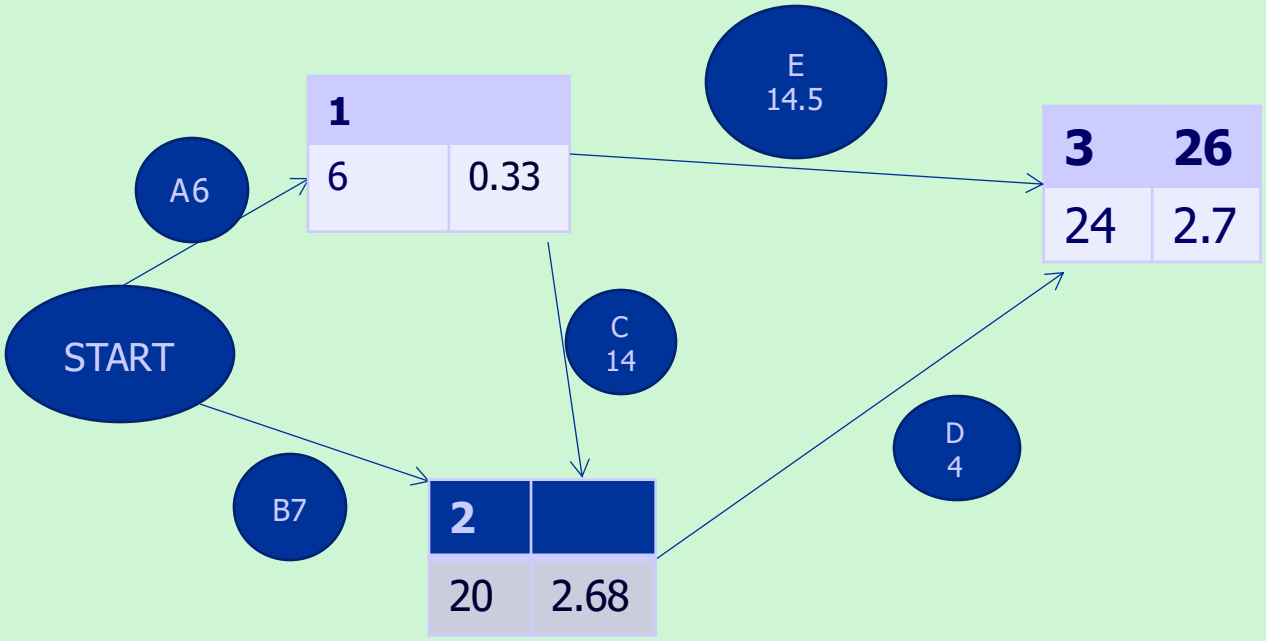
- (a) Determine the expected value and the variance of the completion time for each activity.
- (b) Use the expected times from (a) to find the critical path.
- (c) Assuming that the normal distribution applies, determine the probability that the target days are 18 and 26 days to complete.
- (d) How much time must be allowed to achieve a 90% probability of timely completion?

Exercise Solution

Activity	Te	Std Dev
a	6	2/6 =0.33
b	7	14/6= 2.33
c	14	16/6=2.66
d	4	2/6=0.33
e	14.5	13/6=2.16

Exercise Solution

(a)



Exercise Solution (cont'd)

Two separate z computations are required. First at 26 we have

$$z_{26} = (26-24) / 2.708 = 0.739$$

Then by looking up the normal graph with $z_{26}=0.739$, we have one result that is

Probability of not meeting the target is 30%

Exercise Solution (cont'd)

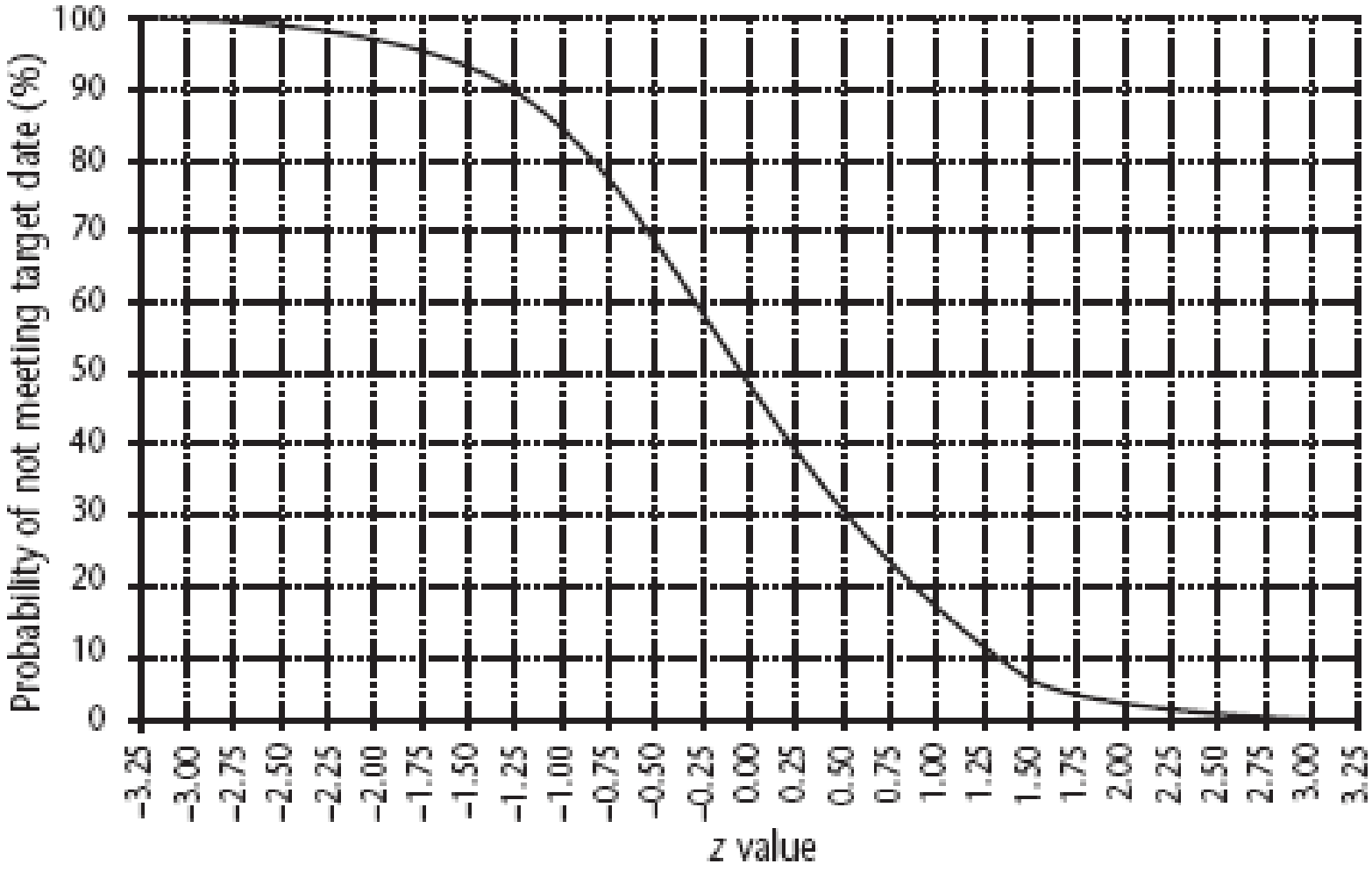
Secondly, at 18 we have

$$z_{18} = (18-24) / 2.708 = -2.216$$

Then by looking up the normal graph with $z_{18}=-2.216$, we have one result that is

Probability of not meeting the target is 98%

Graph of z values



Exercise Solution (cont'd)

(d) For 90% probability, we must pick a z value corresponding to 90% of the area under the normal curve, 50% left of mean and 40% right of mean, so z = 1.282.

Then solving for t we have

$$t = 24 + 1.282 * 2.708 = 27.47 \text{ days.}$$

Critical chain approach

One problem with estimates of task duration:

- Estimators add a safety zone to estimate to take account of possible difficulties
- Developers work to the estimate + safety zone, so time is lost
- No advantage is taken of opportunities where tasks can finish early – and provide a buffer for later activities

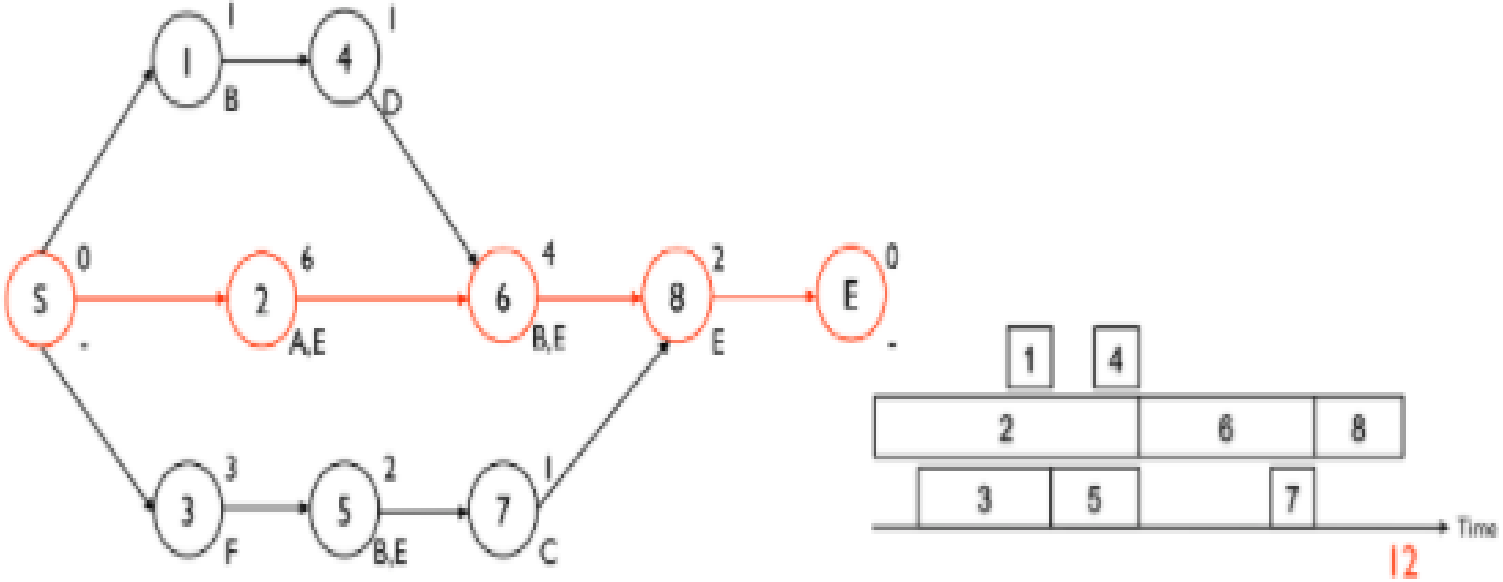
Critical chain approach

One answer to this:

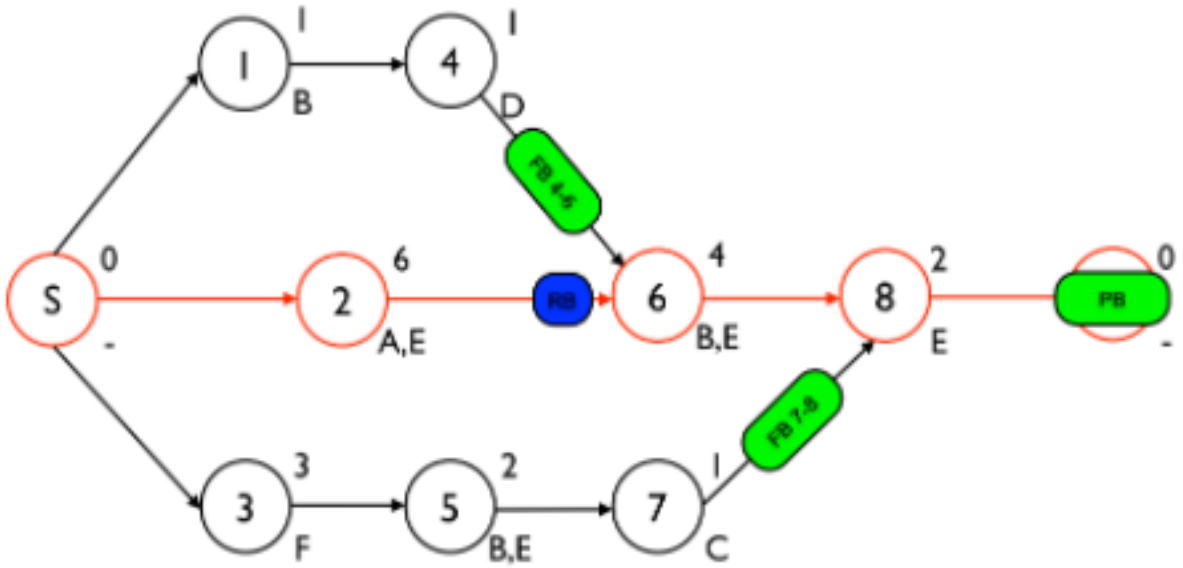
- Base targets on midpoints (i.e. t_e)
- Accumulate 50% of the safety zones (between t_e and b) into a buffer at the end of the project
- Work backwards and start all activities at their latest start dates
- During project execution use relay race model

- To cope with activity over runs, a project buffer is inserted at the end of the project before the target completion date.
- *A project buffer protects the project deadline against violations in the critical chain.*
- The buffer is the equivalent of 50% of the length of the comfort zone that has been removed from the critical chain.
- The critical chain is the longest chain of activities in the project, taking account of both the task and resource dependencies.

- This is different from the critical path as the latter only takes account of task dependencies
- Buffers are also inserted into the project schedule where a subsidiary chain of activities feeds into the critical chain.
- *A feeding buffer protects the critical chain against violations in the feeding chain.*
- These feeding buffers could be set at 50% of the length of the comfort zone from the subsidiary or feeding chain.
- Comfort zone – difference between the pessimistic and the most likely durations.



?Figure 1. An example project network and a resource feasible latest start schedule



?Figure 2. The project network of figure 1 with feeding, resource and project buffers