



UNIVERSITY
of York

MATT OSBORNE

UNDERSTANDING & ASSESSING SOFTWARE SAFETY PRACTICE

CONTENTS

- ▶ Purpose & Scope
- ▶ Framework (& Process)
- ▶ Introduction to FRAM
- ▶ Modified FRAM for this Research
- ▶ Practical Session (Evaluation)
- ▶ Questions



PURPOSE & SCOPE

- ▶ VERY brief introduction to Research
- ▶ Introduction to the Framework
- ▶ Tutorial:
 - ▶ FRAM & Modified FRAM
 - ▶ (Process not part of the 'Tutorial')
- ▶ Evaluation of Framework and Process



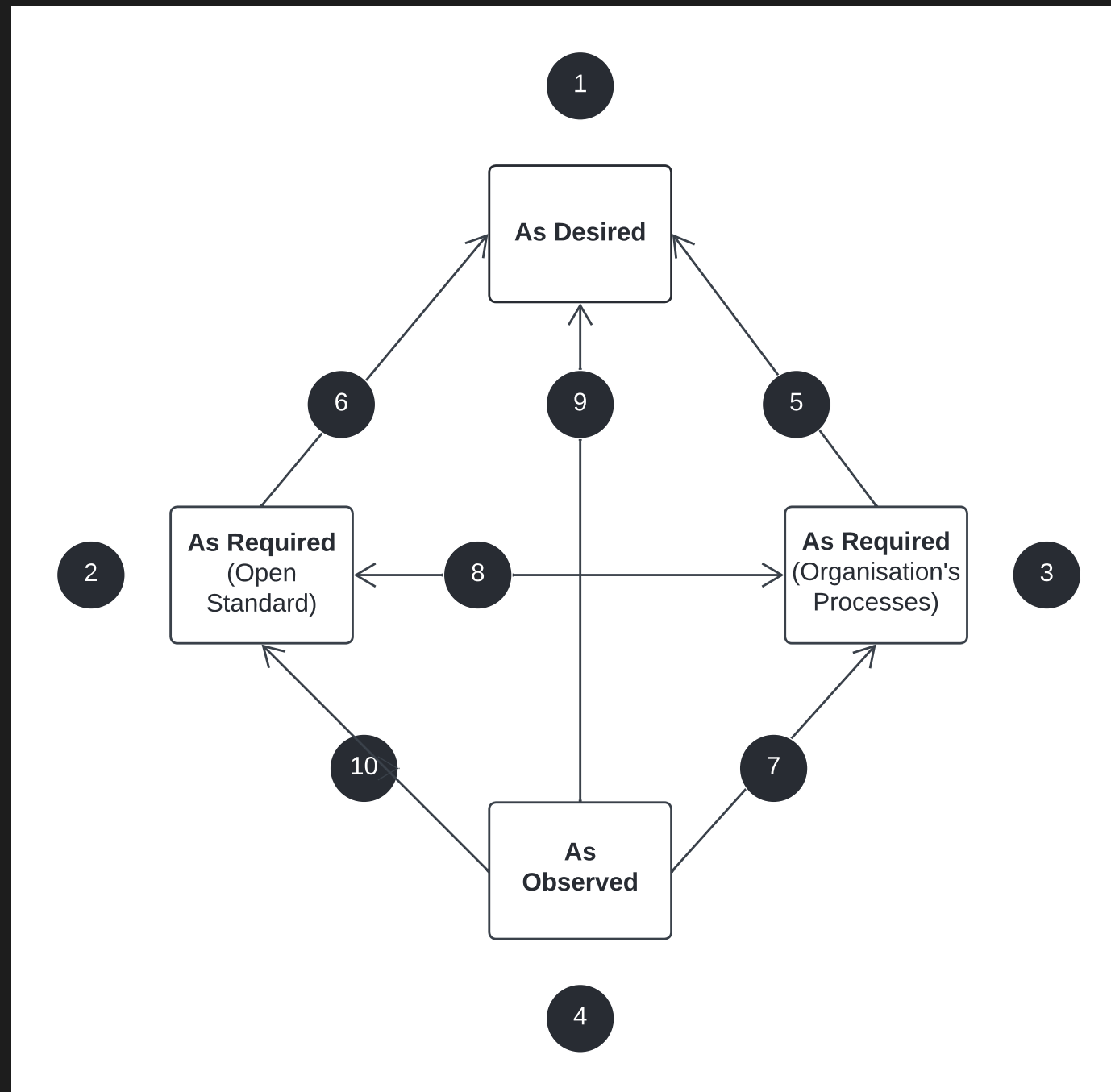
RESEARCH

▶ 4 Research Questions:

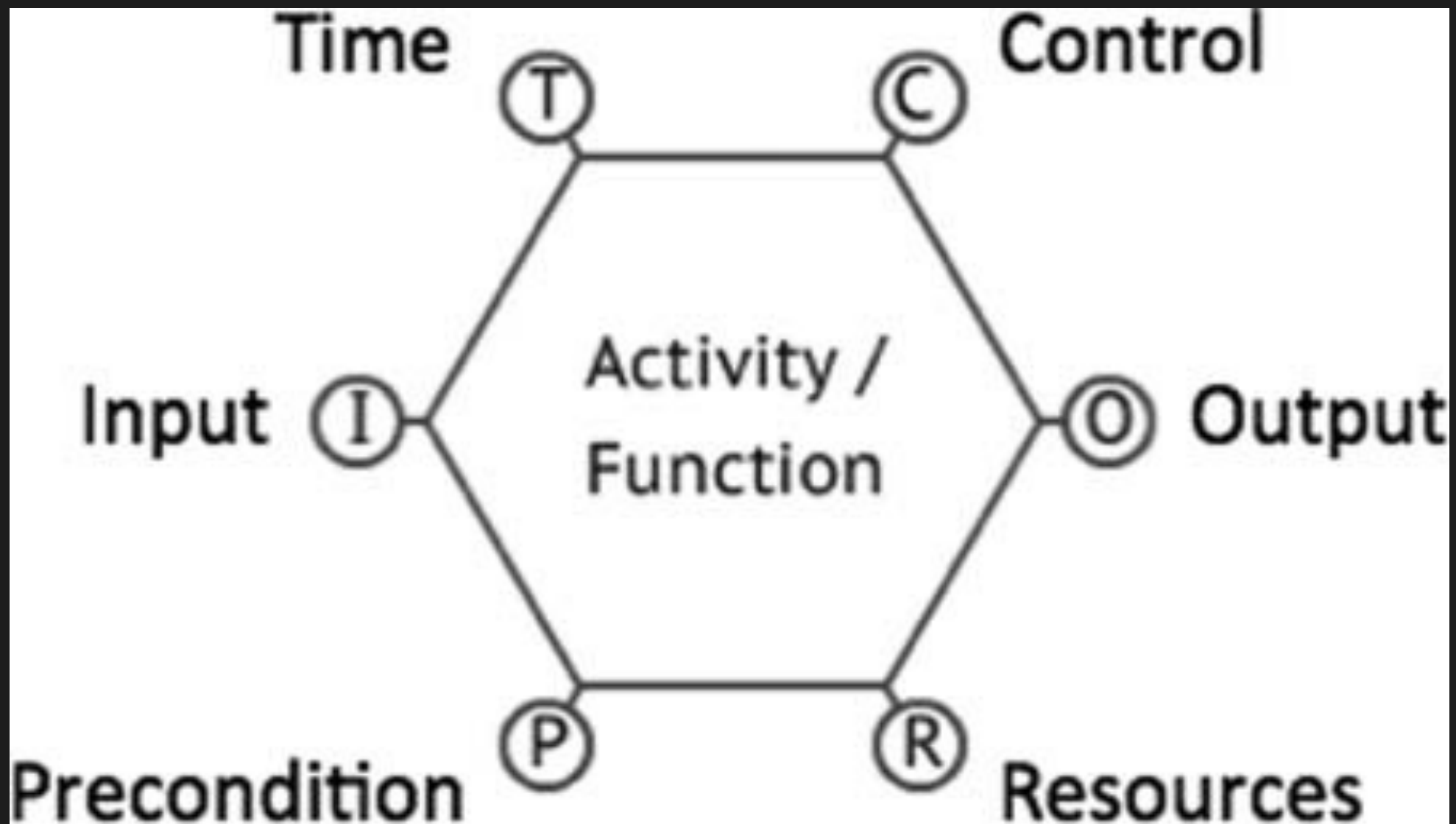
- ▶ 1. How can a project understand its software safety engineering practice?
- ▶ 2. How can a project assess its software safety engineering practice?
- ▶ 3. How can a project identify true impediments (i.e. appropriately-distal) to achieving best practice for its software safety practice?
- ▶ 4. How can a project derive effective mitigations for the identified impediments to software safety engineering best practice?



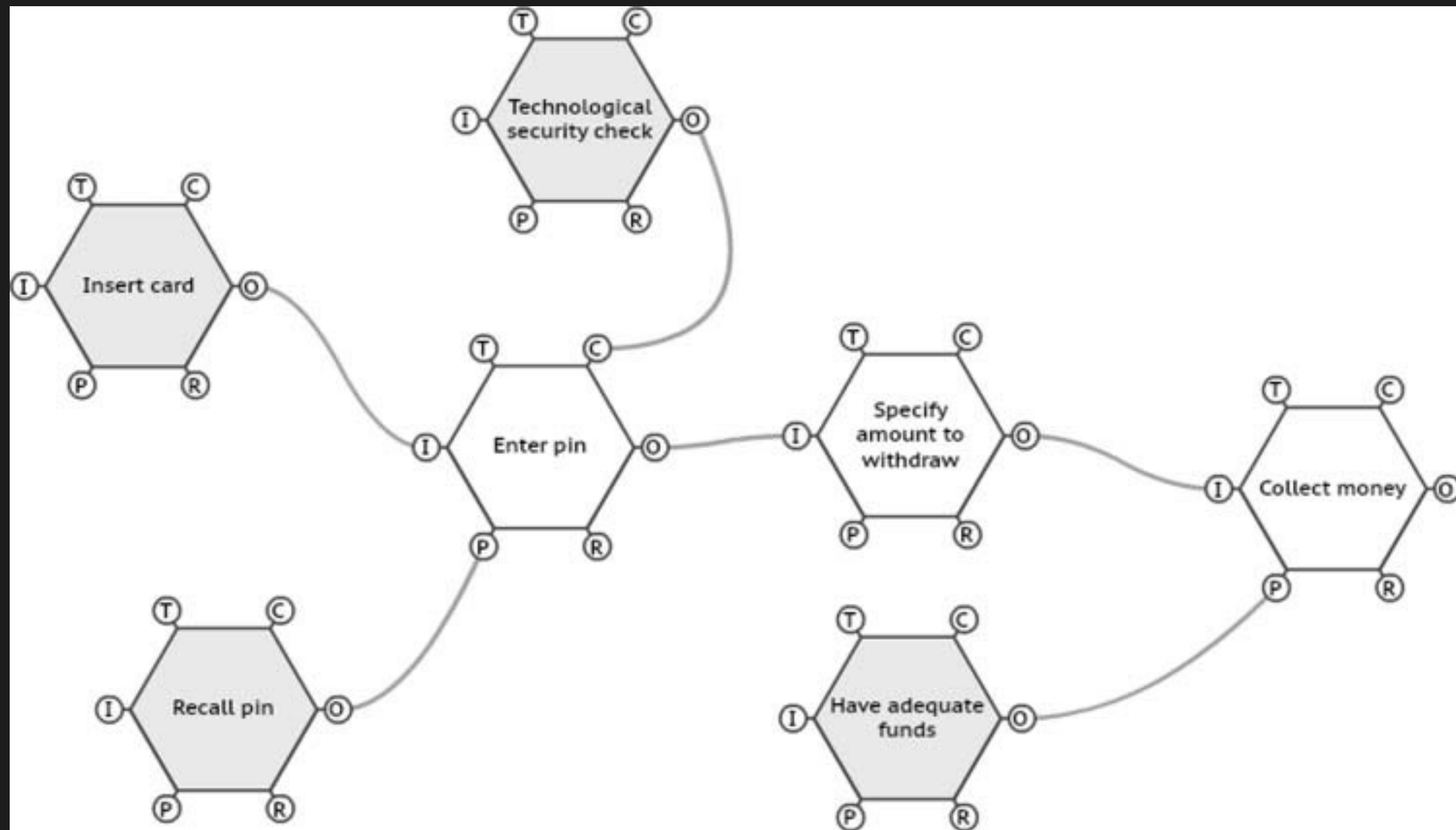
FRAMEWORK



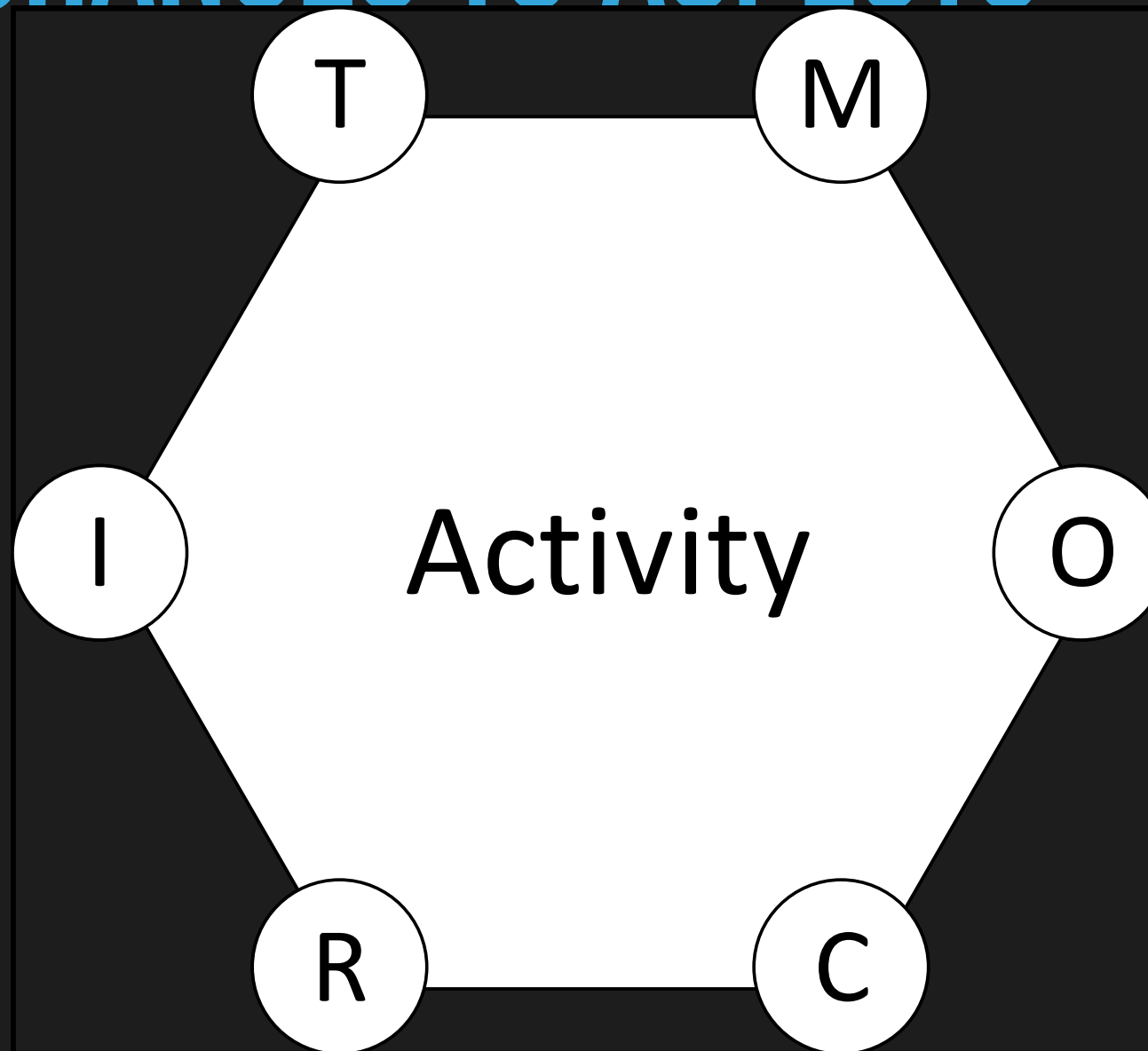
INTRODUCTION TO FRAM – ORIGINAL FRAM



INTRODUCTION TO FRAM – ORIGINAL FRAM EXAMPLE



FRAM^{SP} – CHANGES TO ASPECTS



FRAM^{SP} – ASPECTS OF ACTIVITIES

Aspect	Description
Input	That which is used or transformed by the activity to produce the Output, or that which activated an activity (always stated as a noun or noun-phrase)
Output	Describes the result of what the activity does. The description of the output should be a noun or noun-phrase. Something that is defined as an Output from one activity must also be defined as either an Input, Method, Resource, Control, or Time of another activity or activities
Method	A technique/method that can be employed to carry out the activity. The description of the Method should be a noun or noun-phrase

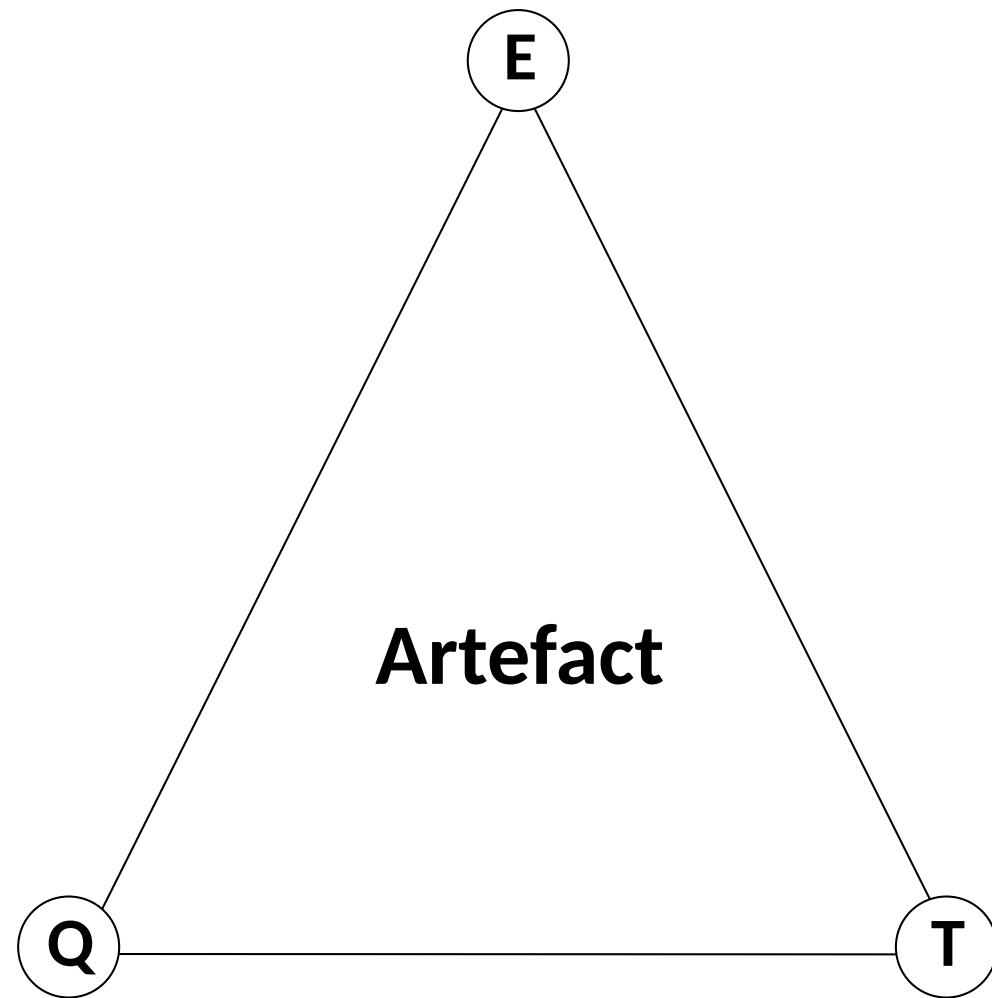


FRAM^{SP} – ASPECTS OF ACTIVITIES CONT'D

Aspect	Description
Resource	Something that is needed or consumed whilst an activity is carried out. The description of the Resource should be a noun or noun-phrase.
Control	That which supervises or regulates an activity so that it produces the desired Output (i.e. a plan, a process, a document etc.). A Control may also be a quality stipulation. The description of a Control should be a noun or noun-phrase
Time	Temporal relations that represent the various ways in which time can affect how an activity is carried out. It may relate to an activity alone (i.e. elapsed time/clock time); or relate to a sequence of actions. It can also represent the point at/by which an activity must occur. The description of Time should be a noun or noun-phrase



FRAM^{SP} – INTRODUCING ARTEFACTS



E: Existence

Q: Quality Criteria

T: Time



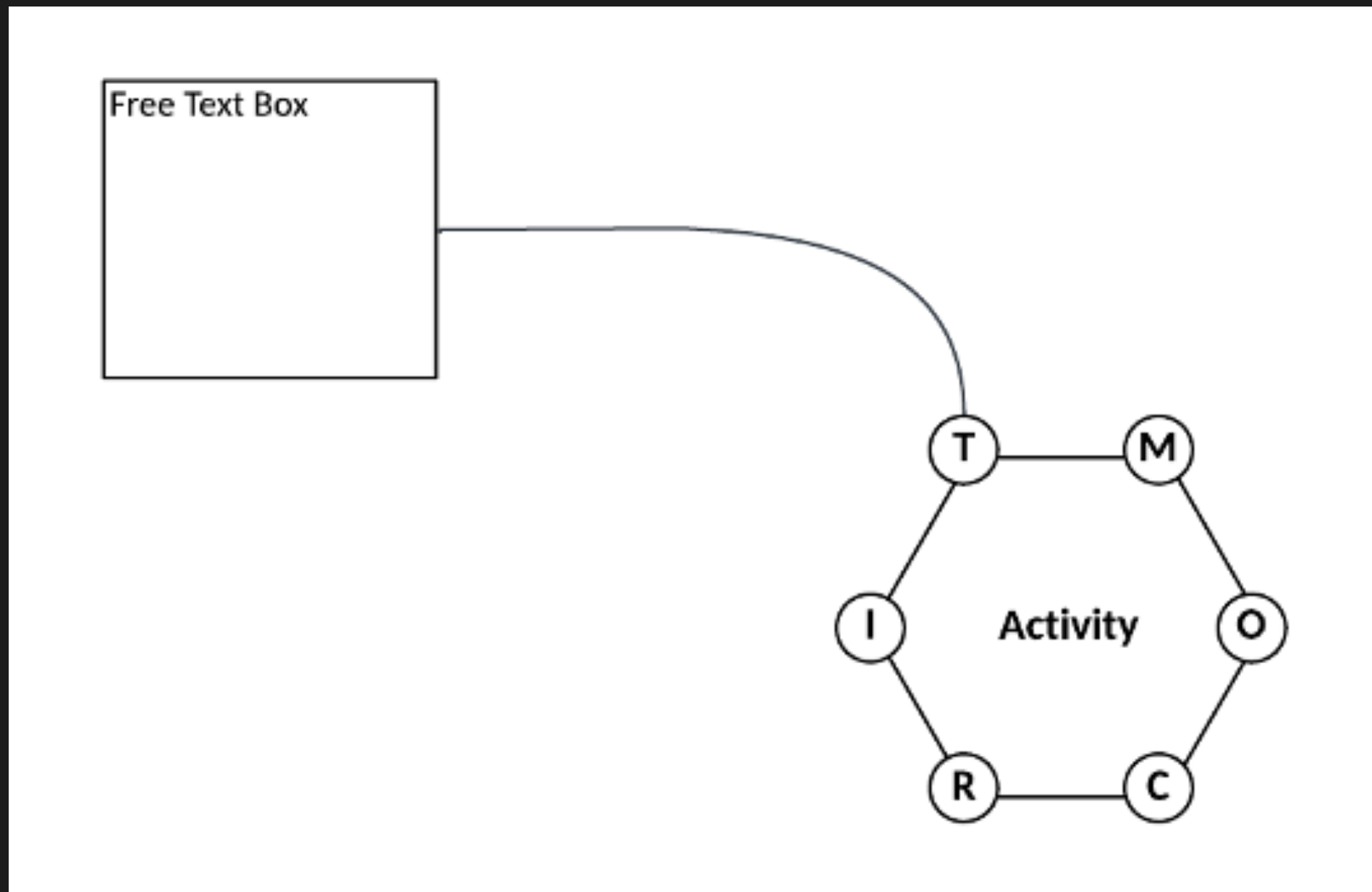
UNIVERSITY
of York

FRAM^{SP} – ASPECTS OF ARTEFACTS

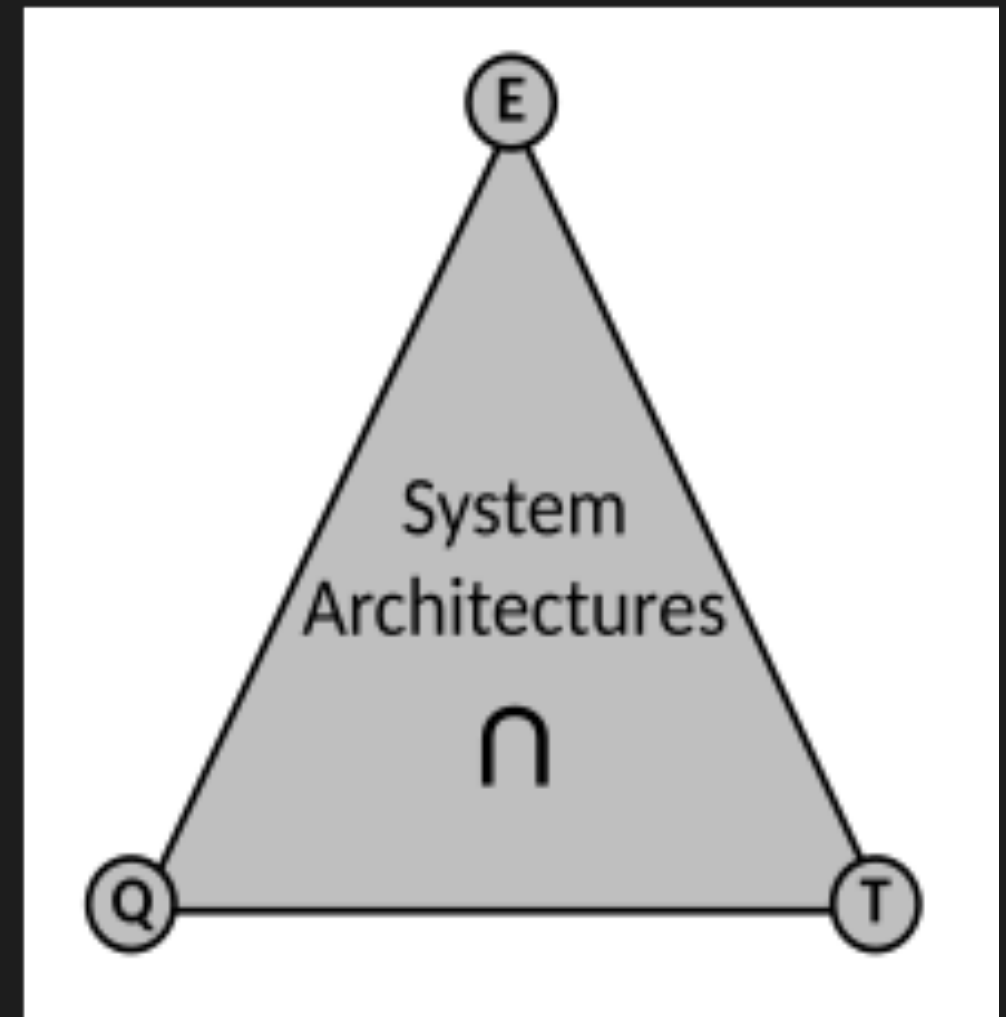
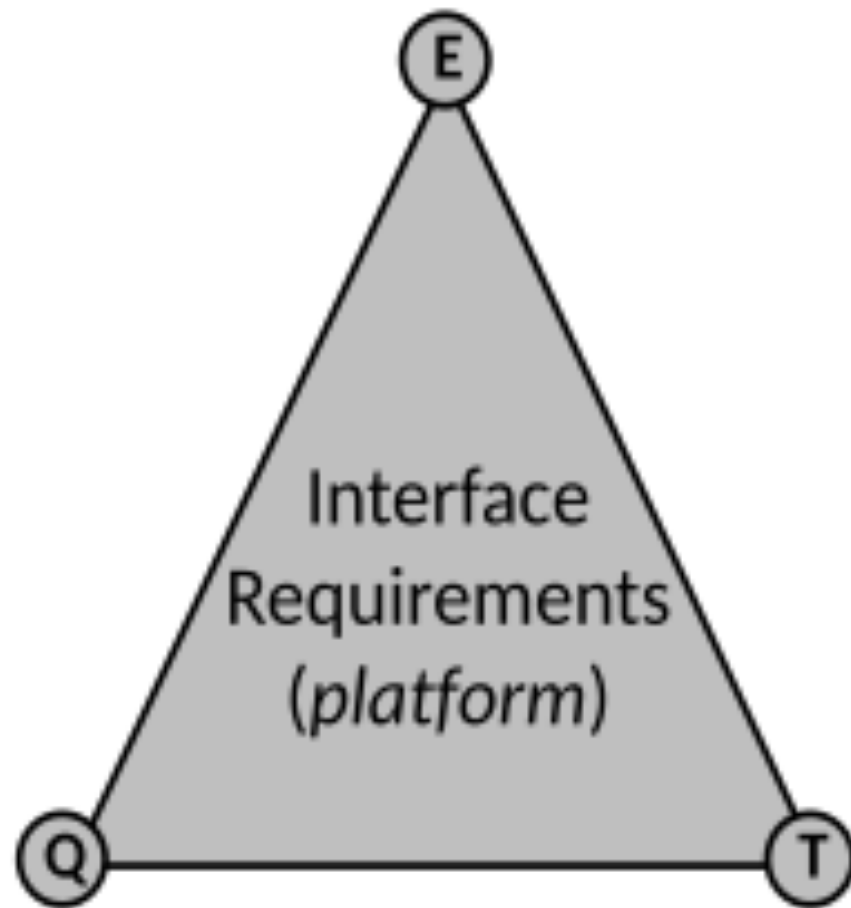
Aspect	Description
Time	Expressed as the point by which the artefact should be created by or supplied to an activity (i.e. a calendar date, or phase in the programme)
Quality Criteria	The Quality attributes required of an artefact, such as the skills and experience required of the person charged with carrying out an activity; or the format and contents required of a report
Existence	Does the artefact (yet) exist? This attribute is used to consider whether the artefact needs to be produced ahead of the supported activity (and therefore whether another activity should be modelled to create it, or a dependency places on a department other than Safety): or whether a person exists within the organisation who has the requisite skills and/or independence (as but two examples)



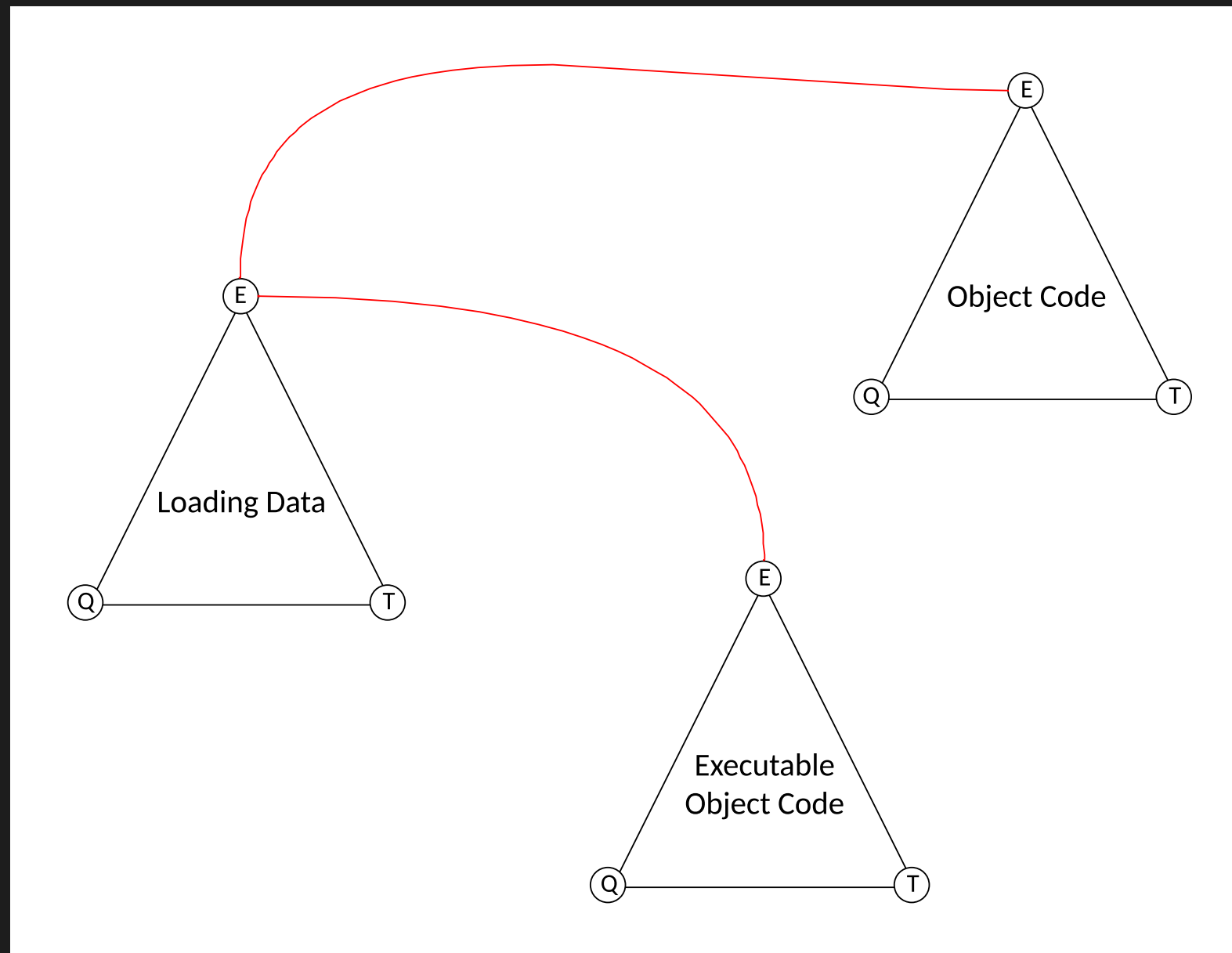
FRAM^{SP} – ASPECTS (GENERAL)



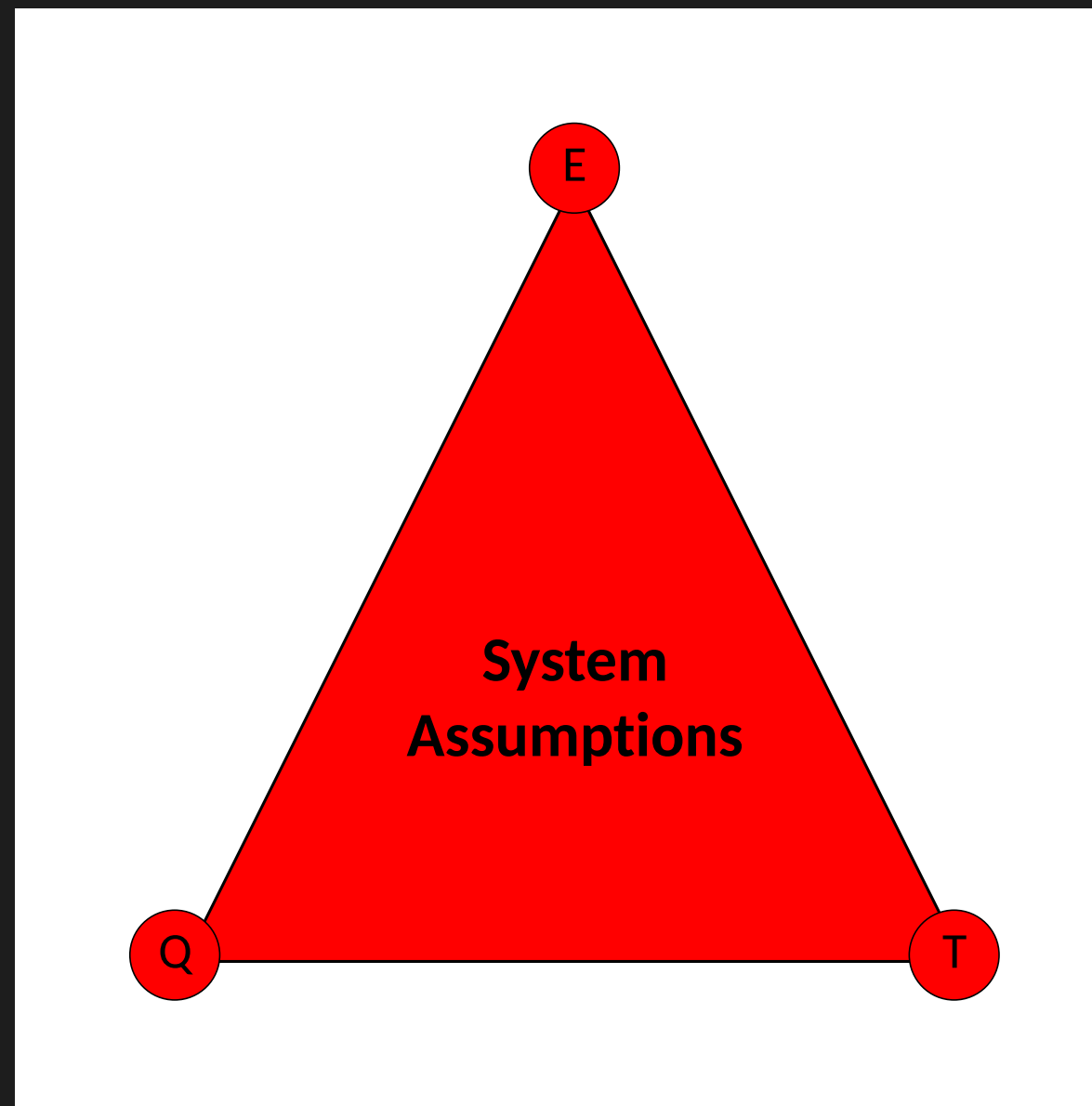
FRAM^{SP} – LAYERS OF ABSTRACTION



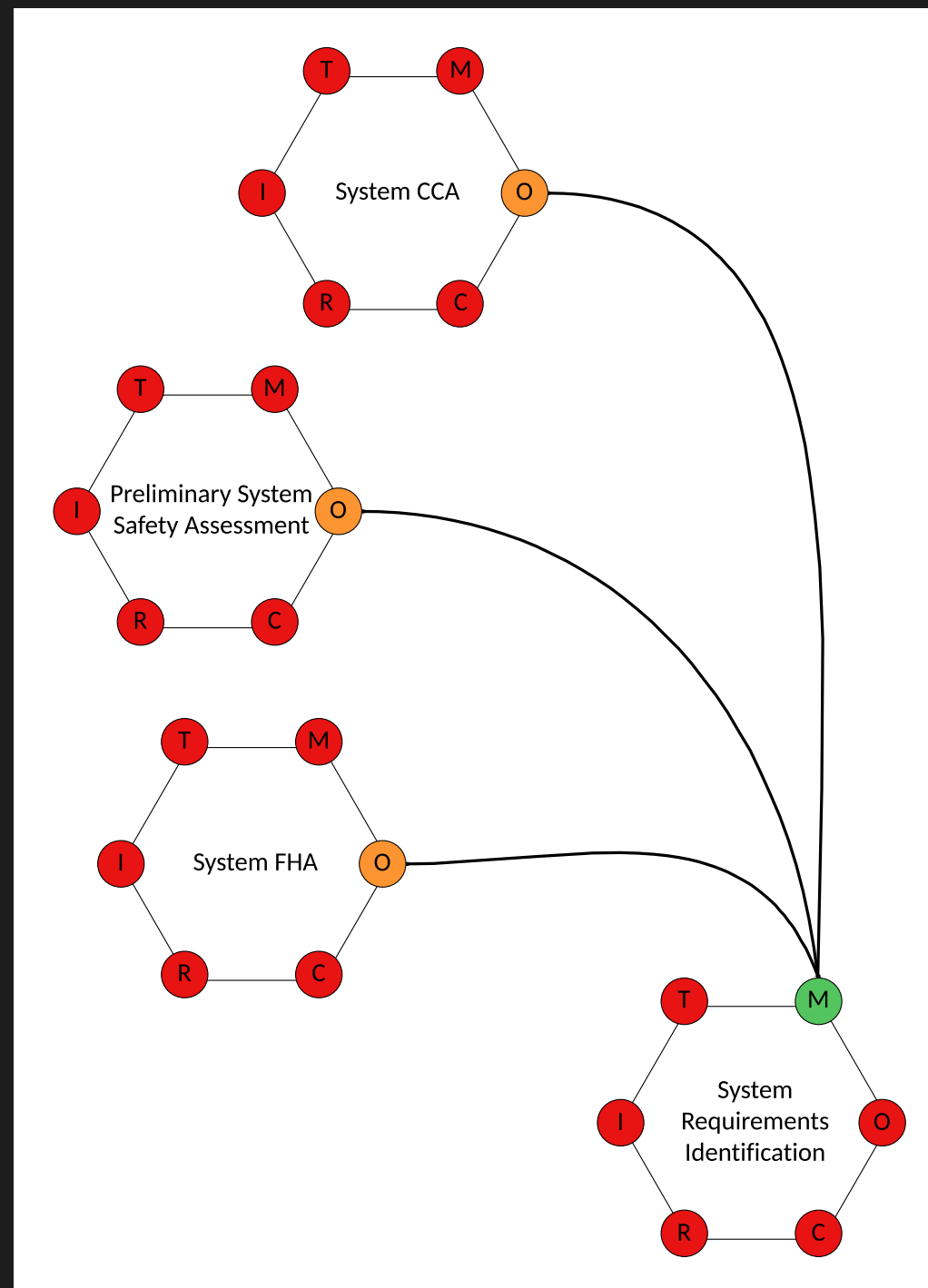
FRAM^{SP} – ARTEFACTS LINKED BY ARTEFACTS





FRAM^{SP} – INFERRED OR ASSUMED ELEMENTS



FRAM^{SP} – OPTIONALITY



FRAM^{SP} – OPTIONALITY

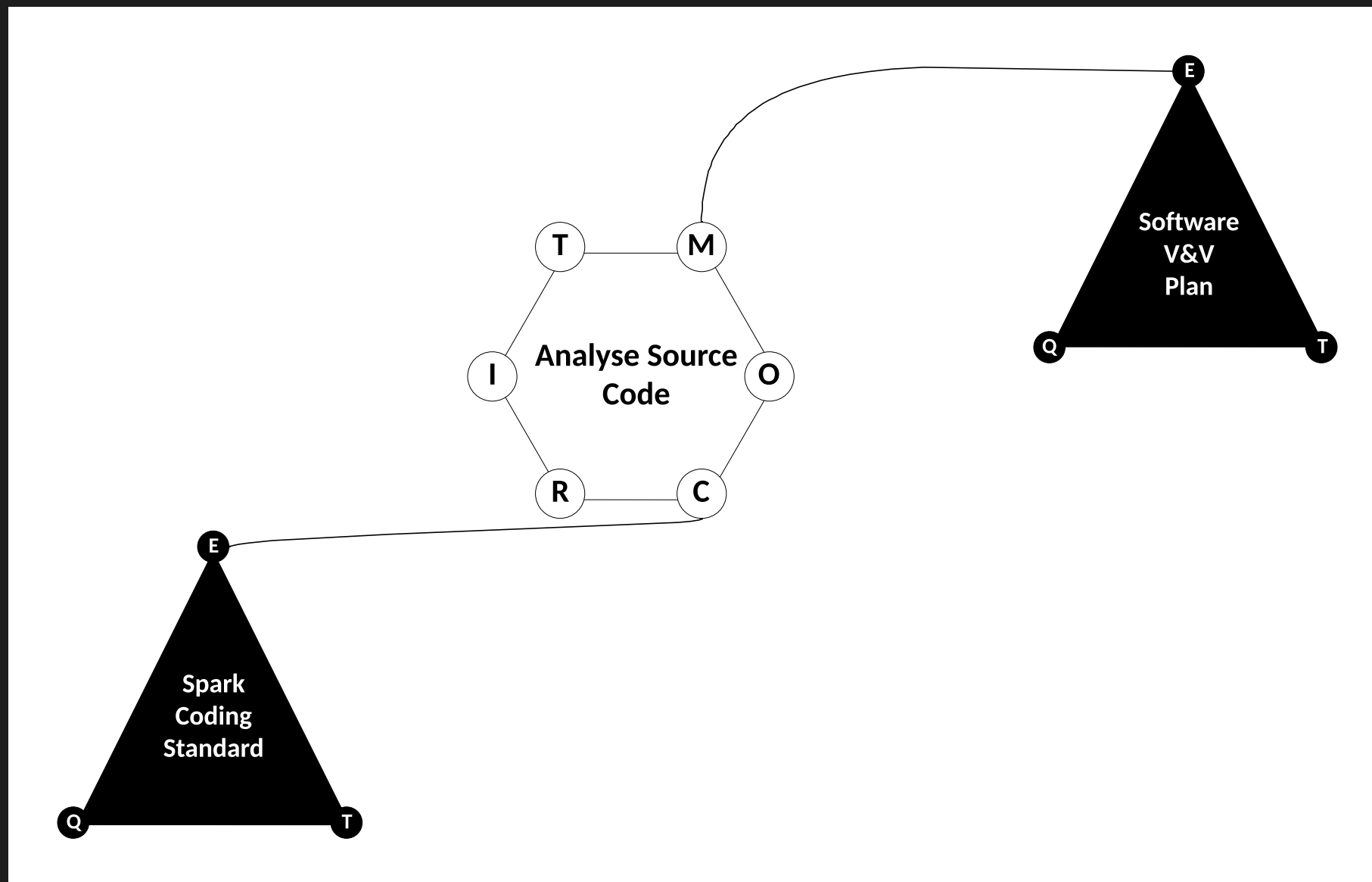
	A solid ball is the symbol for many (meaning zero or more). The label next to the ball indicates the cardinality of the relationship.
	A hollow ball indicates 'optional' (meaning zero or one).



The Diamond – representing a GSN ‘option’ that denotes possible alternatives in satisfying a relationship.



FRAM^{SP} – REFERENCED ARTEFACTS



PROCESS – PRACTICAL



END OF FIRST SESSION – THANK YOU

- ▶ Next Steps:
 - ▶ Analysis of output from Session One
 - ▶ Analysis of Questionnaires
 - ▶ Session Two date and time confirmation



ANY QUESTIONS?