

CHAPTER 6 HOMEWORK

Q1. Are customers more likely to feel confident if formal methods are explained to them and then used?

Ans. Formal methods are the techniques based on the mathematical entities for the specification, verification and the development of the software. They provide the support for the development of the complex system. Formal methods require lot of time, knowledge and experience.

I don't think customer will care much about formal or informal methods. The only thing they care about is their project completion without errors. Formal methods are complex to understand. So even if we try to explain about formal methods, they might not be able to understand all the steps. When we intend to explain customers about the benefits of using some different methods, they are always happy to implement that methods, doesn't matter whether they understand or not. We are expert on those things and they fully trust on us. So, , yes if we try to explain about benefits of using formal methods, customers more likely to feel confident to use formal methods.

Q2. Where in the software development process life cycle do formal methods provide the most benefit? (161)

Ans. Formal methods tend to accelerate the development process if they are used properly in the software development life cycle. Formal methods are the keys to all the solution to Software development life cycle process. We need to consider the place in SDLC process where the benefits of using formal methods exceed the financial cost. Formal methods are expensive and require a lot of time and effort. To use formal methods for any project, we should consider using formal methods at the middle-phase of the SDLC process where it is not too late to catch errors if exist in the system. Formal methods should also be used at the end phase of the SDLC process where we should evaluate the overall project.

Q3. Rewrite the train station specification in another formal language like Z or VDM.

Ans.

Specifications

[RECORD]

[TRAIN ID]

[Segment ID]

Output Type ::= NG / YES

TABLE == Train ID \times P Segment ID

System

db : P RECORD

tableList : P TABLE

checking

\exists System

name? : RECORD

Output : Output Type

name? \in db \wedge Output \neq YES \vee name? \notin db \wedge Output \neq NG

Registering

Δ System

t_id? : Train ID

s_ids? : P Segment ID

t : TABLE

$t = (t_id? s_ids?)$

tableList' = tableList \cup {t}

Checking Conflict

\exists System

t? : TABLE

Output : Output Type

\exists a : TABLE. a \in tableList \wedge a \neq t? \wedge second(a) \cap

Output \neq NG

second(t?) $\neq \emptyset$

Q4. Conduct a consistency check for the requirements found in Section 8.2 of the smart home SRS (video entry).

Ans. Section 8.2 of the smart home system:

1. System shall allow for video input into digital library.
2. System shall allow for storage of video metadata such as category, genre, title, rating, and the like.
3. System shall provide interface to users to edit and update video metadata.
4. System shall accept one-button touch support for incorporating VHS tape into digital library.
5. System shall accept one-button touch support for incorporating DVD videos into digital library, where law and technology provide.

Converting the system into Boolean properties:

Let a, b, c, d and e be the Boolean variables and let,

a: "System allow for video input into digital library"

b: "System allow for storage of video meta data"

c: "System provide interface to users to edit and update video metadata"

d: "System accept one-button touch support for incorporating VHS tape into digital library."

e: "System accept one-button touch support for incorporating DVD videos into digital library, where law and technology provide."

From above, we can write the requirement in mathematical formula as:

1. a
2. $a \Rightarrow b$
3. $b \Rightarrow c$
4. $a \Rightarrow d$
5. $a \Rightarrow e$

Truth Table:

A	B	C	D	E	A'	B'	C'	D'	E'	A	$A \Rightarrow B$	$B \Rightarrow C$	$A \Rightarrow D$	$A \Rightarrow E$
T	T	T	T	T	F	F	F	F	F	T	T	T	T	T
T	T	T	T	F	F	F	F	F	T	F	T	T	T	F
T	T	T	F	F	F	F	F	T	T	F	T	T	F	F
T	T	F	F	F	F	F	T	T	T	F	T	F	F	F
T	F	F	F	F	F	T	T	T	T	F	F	T	F	F
F	F	F	F	F	T	T	T	T	T	T	T	T	T	T
T	T	T	F	T	F	F	F	T	F	F	T	T	F	T
T	T	F	T	T	F	F	T	F	F	F	T	F	T	T
T	F	T	T	T	F	T	F	F	F	F	F	F	T	T
F	T	T	T	T	T	F	F	F	F	T	F	T	F	F

If we looked the two rows, we can see “T” for all the combination of Boolean values which prove that the set of requirements are consistent

Q5. Conduct a consistency check for the requirements found in Section 8.3 of the smart home SRS (video playback).

Ans. Section 8.3 of the smart home system:

1. System shall allow for recorded video playback at any television in the house.
2. System shall allow for other video media to be available for playback in any room with a television.
3. System shall allow all common features of a VCR or DVD player, such as fast forward, rewind, chapter skip, and so on.
4. System shall allow user to skip commercials where commercials are detected.
5. System shall prevent user from playing back identical media on multiple televisions at the same time.
6. System shall allow user to remove the recording from storage when they are done watching.
7. System shall allow user to remove other video media from the storage.

Converting the system into Boolean properties:

Let a, b, c, d and e be the Boolean variables and let,

a: “System allow for recorded video playback at any television in the house.”

b: “System allow for other video media to be available for playback in any room with a television.”

c: “System allow all common features of a VCR or DVD player, such as fast forward, rewind, chapter skip, and so on.”

d: “System allow user to skip commercials where commercials are detected”.

e: “System prevent user from playing back identical media on multiple televisions at the same time.”

f: “System allow user to remove the recording from storage when they are done watching.”

g: “System allow user to remove other video media from the storage.”

From above, we can write the requirement in mathematical formula as,

1. A
2. $a \Rightarrow b$
3. $b \Rightarrow c$
4. $c \Rightarrow d$
5. $d \Rightarrow e$
6. $c \Rightarrow f$
7. $c \Rightarrow g$

Truth Table:

a	b	c	d	e	f	g	a'	b'	c'	d'	e'	f'	g'	a	a=>b	b=>c	c=>d	d=>e	c=>f	c=>g
T	T	T	T	T	T	T	F	F	F	F	F	F	F	T	T	T	T	T	T	T
T	T	T	T	T	T	F	F	F	F	F	F	F	T	T	T	T	T	T	T	F
T	T	T	T	T	F	F	F	F	F	F	F	T	T	T	T	T	T	T	F	F
T	T	T	T	F	F	F	F	F	F	F	T	T	T	F	T	T	T	F	F	F
T	T	T	F	F	F	F	F	F	F	T	T	T	T	F	T	T	F	T	F	F
T	T	F	F	F	F	F	F	F	T	T	T	T	T	F	T	F	T	T	T	T
T	F	F	F	F	F	F	F	T	T	T	T	T	T	F	F	T	T	T	T	T
F	F	F	F	F	F	F	T	T	T	T	T	T	T	F	T	T	T	T	T	T
T	T	T	T	T	F	T	F	F	F	F	F	T	F	F	T	T	T	T	F	T
T	T	T	T	F	T	T	F	F	F	F	T	F	F	F	T	T	T	F	T	T
T	T	T	F	T	T	T	F	F	F	T	F	F	F	F	T	T	F	F	T	T
T	T	F	T	T	T	T	F	F	T	F	F	F	F	F	T	F	F	T	F	F
T	F	T	T	T	T	T	F	T	F	F	F	F	F	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	T	T
T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F	F	F	F	F	T
T	T	T	T	F	F	T	F	F	F	F	T	T	F	T	T	T	T	F	F	T
T	T	T	F	F	F	T	F	F	F	T	T	T	F	T	T	T	F	T	F	T
T	T	F	F	F	F	T	F	F	T	T	T	T	F	T	T	F	T	T	T	F
T	F	F	F	F	F	T	F	T	T	T	T	T	F	T	F	T	T	T	T	F
F	F	F	F	F	F	T	T	T	T	T	T	T	F	F	T	T	T	T	T	F
T	T	T	F	F	T	T	F	F	F	T	T	F	F	T	T	T	F	T	T	T
T	T	F	F	F	T	T	F	F	T	T	T	F	F	T	T	F	T	T	F	F
T	F	F	F	F	T	T	F	T	T	T	T	F	F	T	F	T	T	T	F	F
F	F	F	F	F	T	T	T	T	T	T	T	F	F	F	T	T	T	T	F	F
T	T	F	F	T	T	T	F	F	T	T	F	F	F	T	T	F	T	F	F	F
T	F	F	F	T	T	T	F	T	T	T	F	F	F	T	F	T	T	F	F	F
F	F	F	F	T	T	T	T	T	T	T	F	F	F	F	T	T	T	F	F	F
T	T	F	F	T	T	F	F	F	T	T	F	F	T	T	T	F	T	F	F	T
T	F	F	F	T	T	F	F	T	T	T	F	F	T	T	F	T	T	F	F	T
F	F	F	T	T	T	T	T	T	T	F	F	F	F	T	T	T	F	F	F	F

If we looked at the first row, we can see “T” for all the combination of Boolean values which prove that the set of requirements are consistent.

Q6. Consider the following set of requirements for insulin pump system:

3.1 If the morphine dose button is pressed then morphine dose is administered.

3.2 If the morphine dose is administered then the dose indicator light is off.

3.3 If the morphine dose button is pressed and the dose indicator light is on then the morphine dose is administered.

3.4 If the morphine dose is administered then the dose indicator light is on.

Determine using truth table if these requirements are consistent or not.

Ans. Let p, q, and r be the Boolean variables and let,

p-morphine dose button is pressed
q-morphine dose is administered
r-morphine dose indicator light is on

From above, we can write the requirement in mathematical formula as,

3.1: $p \Rightarrow q$

3.2: $q \Rightarrow \sim r$

3.3: $(p \wedge r) \Rightarrow q$

3.4: $q \Rightarrow r$

P	Q	R	$\sim R$	$P \wedge R$	$P \Rightarrow Q$	$Q \Rightarrow \sim R$	$(P \wedge R) \Rightarrow Q$	$Q \Rightarrow R$
T	T	T	F	T	T	F	T	T
T	T	F	T	F	T	T	T	T
T	F	T	F	T	F	T	T	T
T	F	F	T	F	F	T	T	T
F	T	T	F	F	T	F	T	T
F	T	F	T	F	T	T	T	F
F	F	T	F	F	T	T	F	T
F	F	F	T	F	T	T	F	T

From the above truth table, if we look at all the requirements, no single row has value equivalent to truth for all requirements. Thus, they are not consistent.

Q7. Which requirements (group) in the requirements in the SRS of Appendix A would benefit from formalization?

Ans. The requirements groups in the SRS of Appendix A that would benefit from formalization are as follows:

S.No.	Requirements Group	Models
1	3.1	VDM
2	4.1	Z
3	5.1	Z
4	5.2	CSP
5	6.1	B
6	6.2	VDM
7	6.4	B
8	6.5	CSP
9	7.2	VDM
10	7.3	VDM
11	7.4	State Charts
12	8.1	B
13	8.2	State Charts

14	8.3	State Charts
15	8.4	B
16	9.6	VDM
17	9.12	Z

All the requirements group mentioned will benefit from the formalization techniques.

Q8. For the formalization in section 3.2.1 and section 3.2.5 in the SRS of Appendix B discuss the problem that exist. Use whatever assumptions you need, rewrite theses formalizations using Z, B or VDM or other formal method choose.

Ans. The problems in the requirements of the SRS of Appendix B are as follows:

3.2.1.5 -> Because in the requirement it is mentioned that an alternate pump should come into play when the original pump shuts off, but it is not mentioned as to how many number of alternate pumps are there and which ones should be used.

3.2.1.6 & 3.2.1.7 -> An alarm must be set off, but which alarm in which motor is to set off should also be mentioned. Is there a same alarm for high water level and methane or do they have different alarms.

3.2.1.11 & 3.2.10 -> Similar issue, does not specifies which alarms to set off and how to handle if the alarms are set off.

Overall it provides ambiguous details and incorrect assumptions could be made if the requirements are not mentioned clearly.

3.2.5.1 -> Which state shall be instated is not mentioned and that state should also be clearly mentioned in the requirements where the ventilation of the fan system is being done.

It is very important to have these methods formalized as they belong to high risk areas.