

Communicating & learning in a safety critical environment





Aeronautical information software

Design in a safety critical environment

Gordon B Dennis



Eastern European Aviation and
Business Users Seminar

Agenda

- Introduction – why this is important
- How accidents happen
- Managing risks
- CRM and Ergonomics
- Cognitive learning
- Authoring issues
- Software engineering issues
- Management issues
- Conclusions

Introduction: why this is important

DerefNullPtr.exe

DerefNullPtr.exe has encountered a problem and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, it might be lost.

Please tell Microsoft about this problem.
We have created an error report that you can send to Microsoft. You can also save this report as confidential and anonymous if you prefer.

To see what data this error report contains, click the **Debug** button.

Flight	Action
AC885	Go to gate 28
ME202	Go to gate 5
AC857	Go to gate 21
AA093	Go to gate 7
AA067	Go to gate 18
UA992	Go to Lounge
AH111	Go to Lounge
B1098	Gate open gate 9
AC897	Go to Lounge

have baggage unattended 12

A fatal exception 0E has occurred at 0ACB:00000312 in VEB VM1011:00002012. The current application will be terminated.
Press any key to terminate the current application.
Press CTRL+ALT+DEL to restart your computer. You will

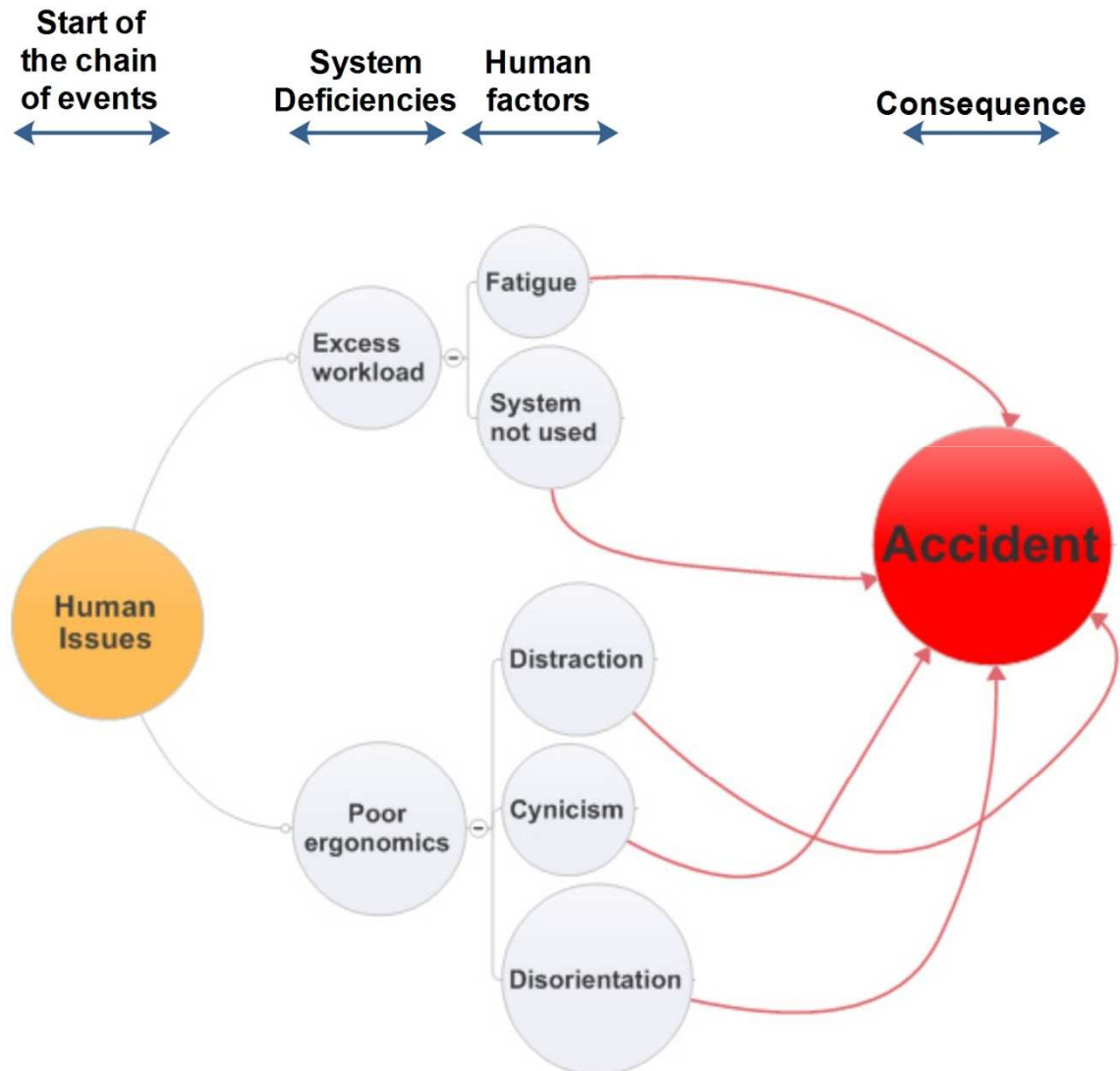
Risks in aviation vs. IT ...

are in a different league !



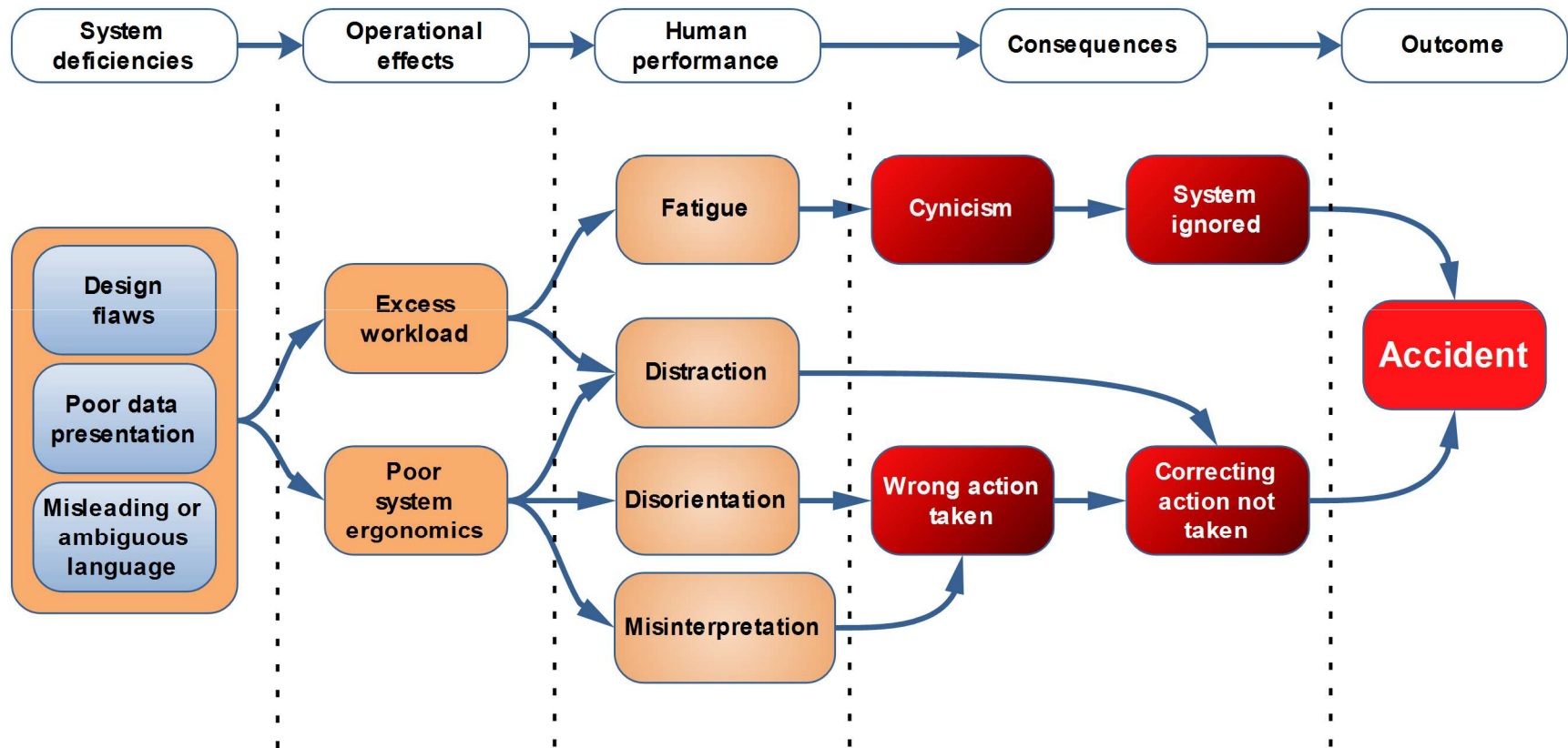


How accidents happen





How accidents happen





Managing risks

Risk classification and required level of confidence

		Probability of occurrence				
		Extremely improbable	Extremely remote	Remote	Reasonably probable	Frequent
		$< 10^{-9}$ per hour	10^{-7} to 10^{-9} per hour	10^{-5} to 10^{-7} per hour	10^{-3} to 10^{-5} per hour	1 to 10^{-3} per hour
ESARR 4 Severity (Required level of confidence)	Accidents	Review (MEDIUM)	Unacceptable (HIGH)	Unacceptable (HIGH)	Unacceptable (HIGH)	Unacceptable (HIGH)
	Serious incidents	Acceptable (LOW)	Review (MEDIUM)	Unacceptable (HIGH)	Unacceptable (HIGH)	Unacceptable (HIGH)
	Major incidents	Acceptable (LOW)	Acceptable (LOW)	Review (MEDIUM)	Unacceptable (HIGH)	Unacceptable (HIGH)
	Significant incidents	Acceptable (LOW)	Acceptable (LOW)	Acceptable (LOW)	Review (MEDIUM)	Unacceptable (HIGH)
	No Effect immediately	Acceptable (LOW)	Acceptable (LOW)	Acceptable (LOW)	Acceptable (LOW)	Review (MEDIUM)

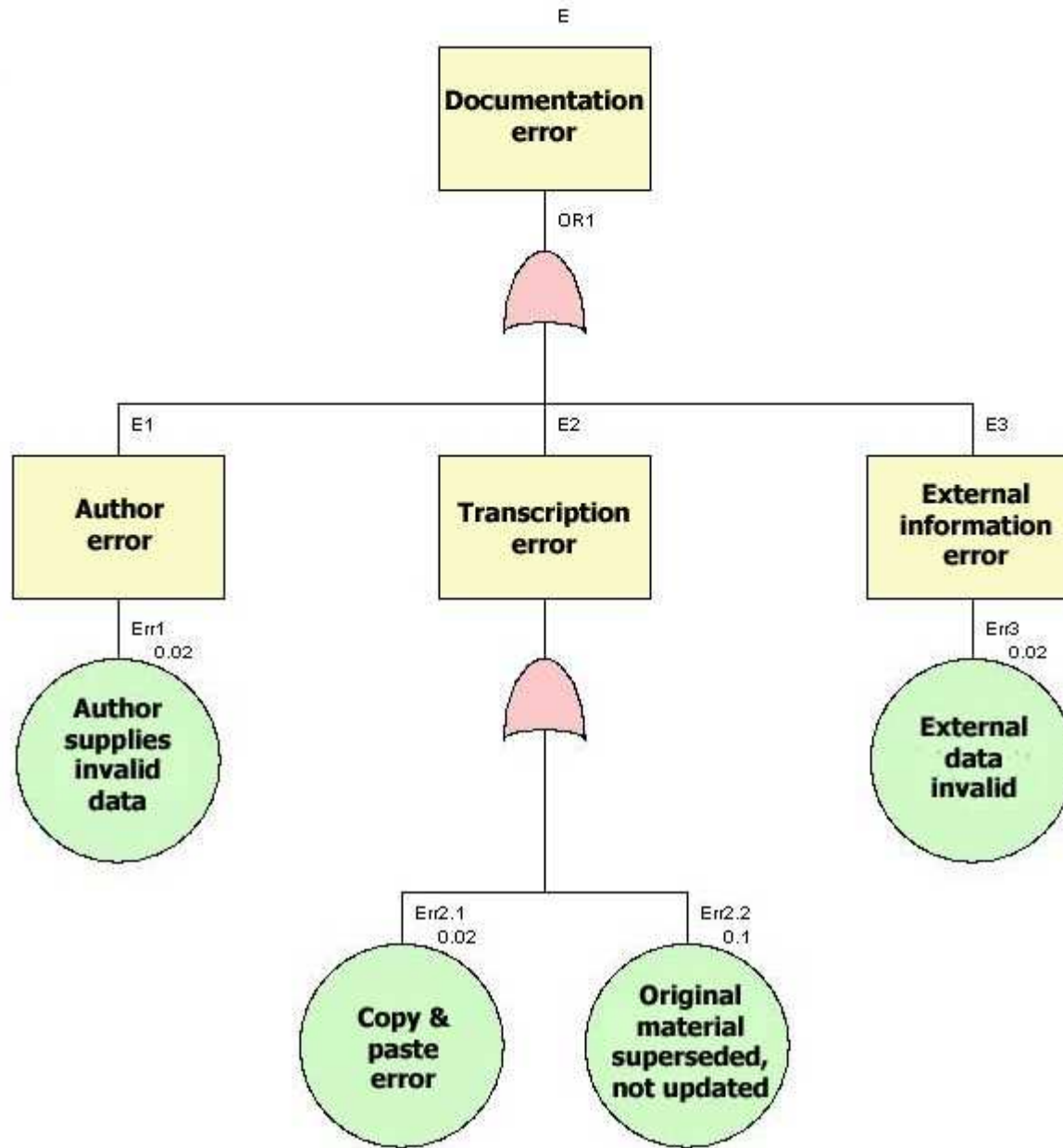
Unacceptable risk

Acceptable risk

Critical risk

Source: CAP 760, Appendix G

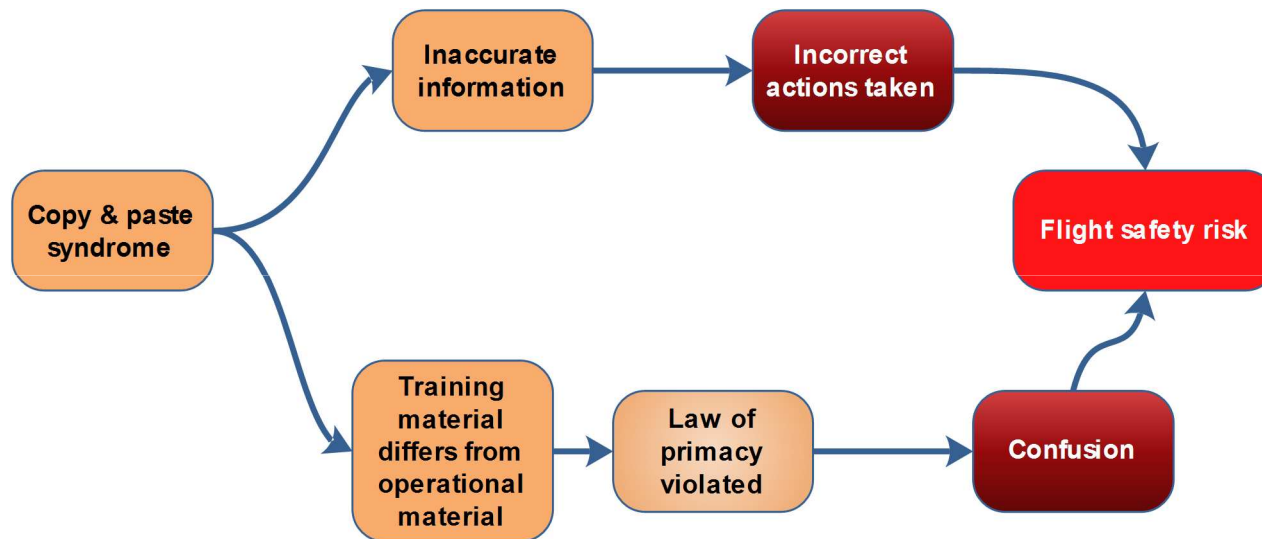
FTA



Authoring issues

- Laws of learning
- Cognitive load & cognitive learning
- Split attention effect
- Use of English - clear & crisp
 - Why say “utilise” rather than “use”?
- Use of Simplified Technical English

Two very good reasons for re-use



Laws of learning

1. Readiness
2. Exercise
3. Effect
4. Primacy
5. Intensity
6. Freedom



Law of primacy

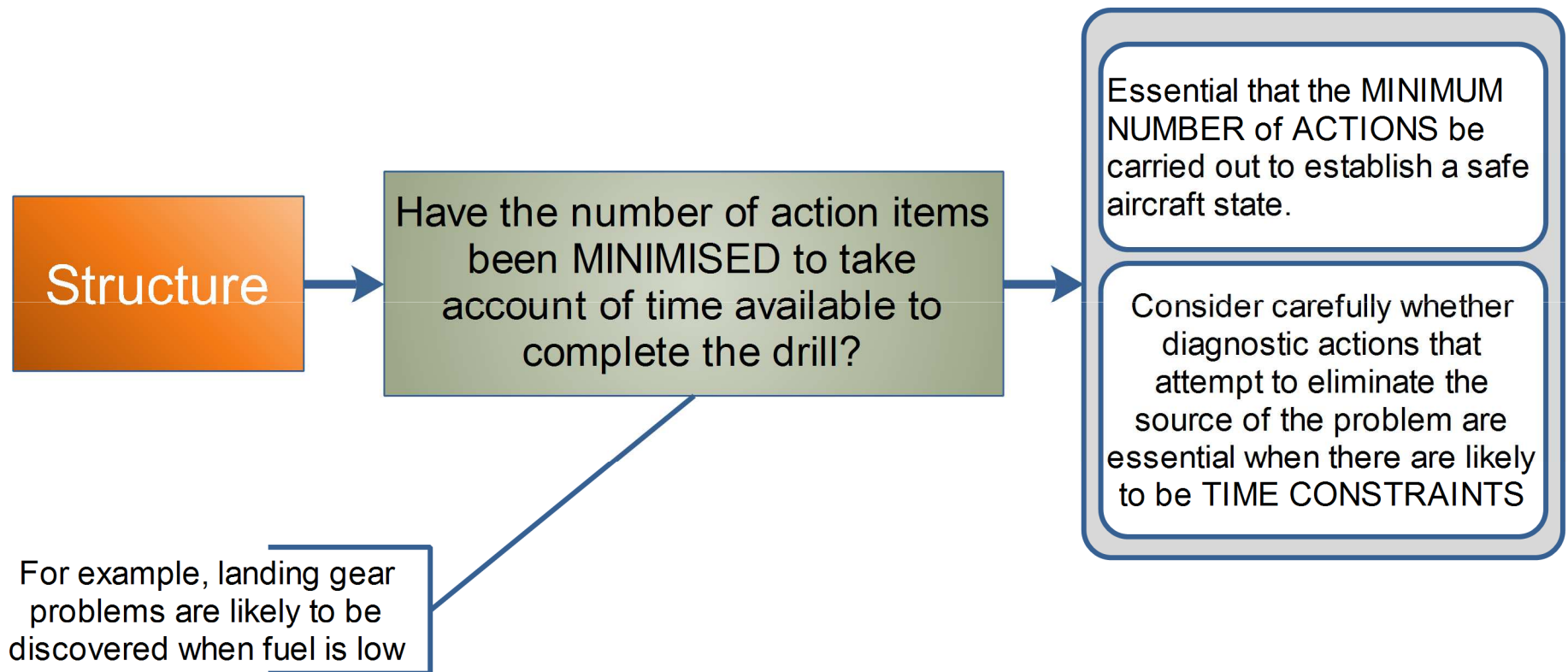
- Things learned first
 - Create strong mental belief
 - Difficult to erase.
- “Unlearning” much harder than learning right first time
- First experience
 - Positive, pleasant
 - Lay foundation



Cognitive load theory

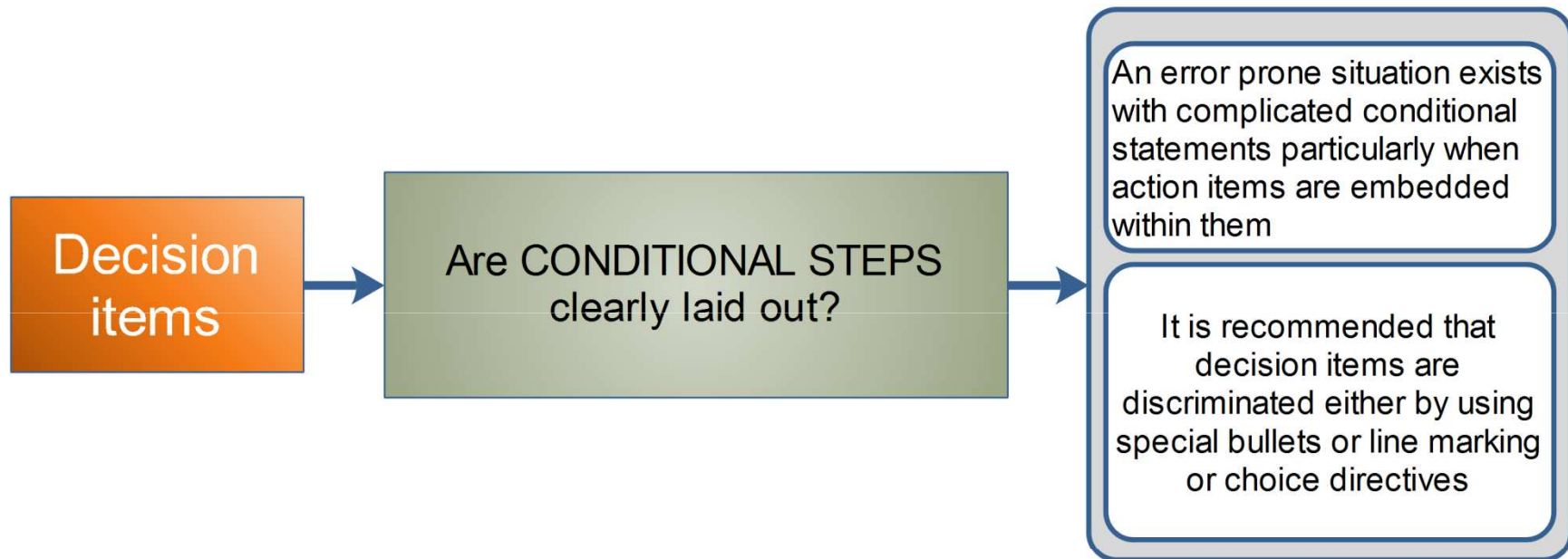
- Format of instructional materials has direct effect on the performance of the learners
 - Structure
 - Texture
 - Presentation
- As we get older, cognitive reasoning becomes more pronounced
- As we get older, learning becomes more difficult

Recommended practice



Source: CAP670

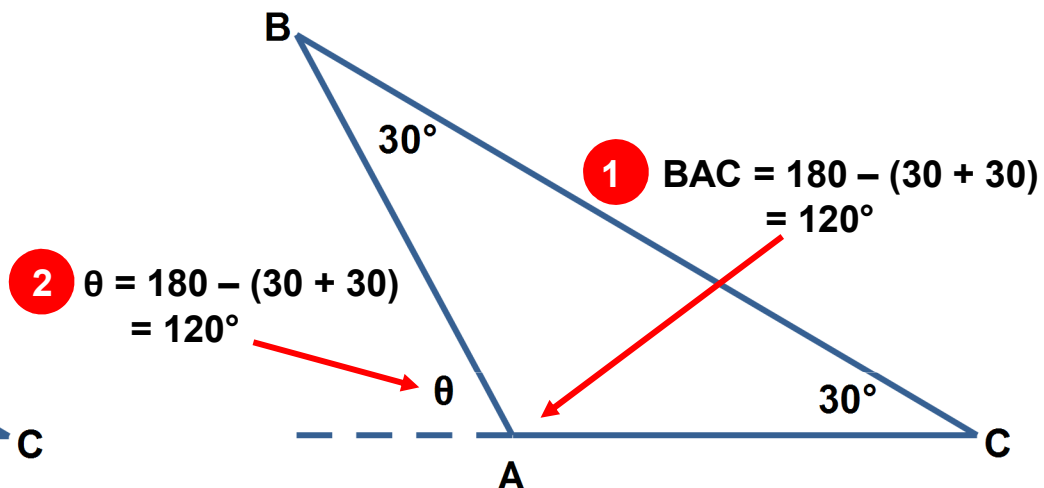
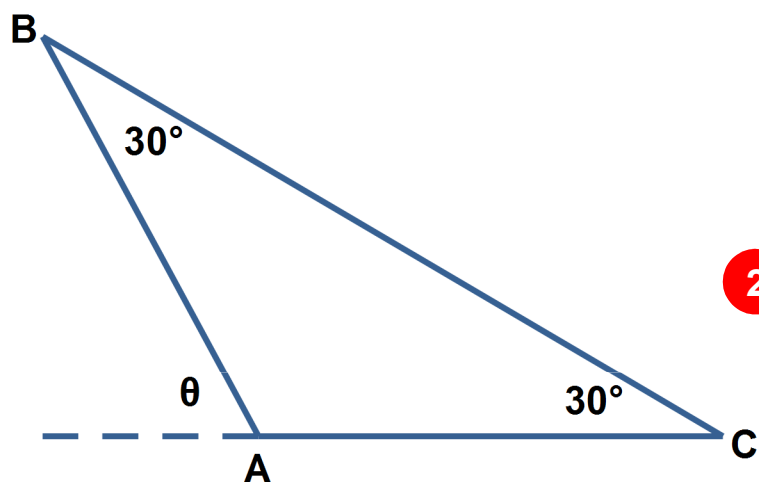
Recommended practice



Source: CAP670

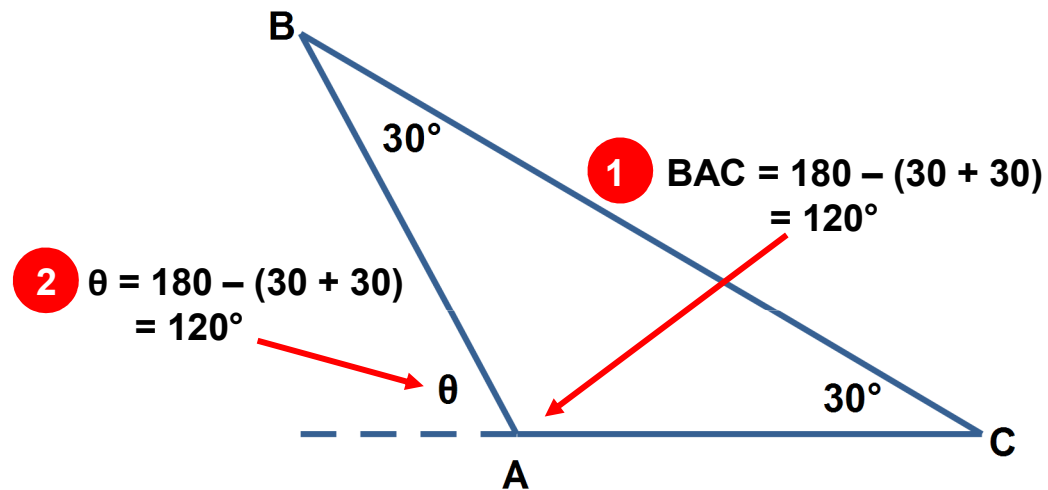


Split attention effect

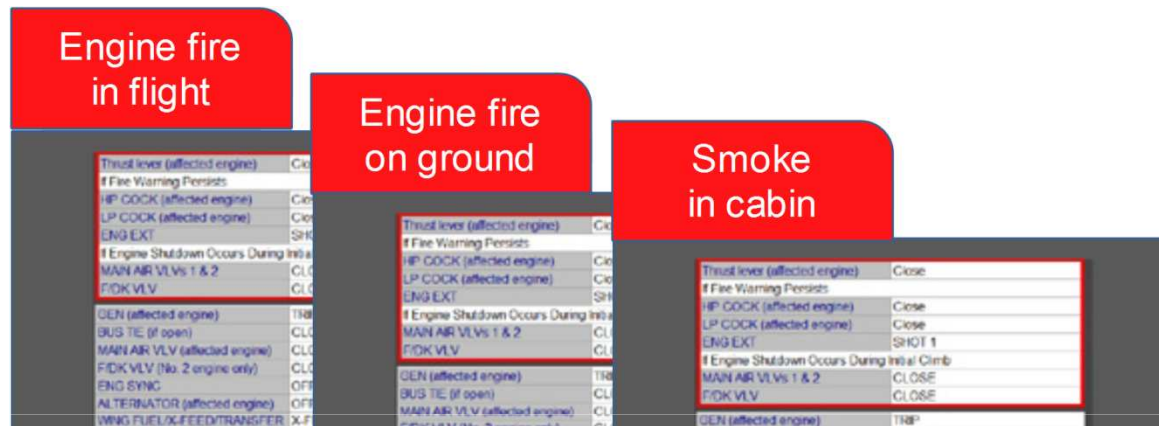


In the figure above, calculate the angle θ
Triangle ABC has total angle = 180°
The angle $BAC = 180 - (30 + 30) = 120^\circ$
Hence, $\theta = 180 - 120 = 60^\circ$

Split attention effect



Topic design practice



A well designed topic :

Is fully described by it's title




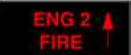
Is a complete procedure:

Has anything related externally linked

CRM and Ergonomics

3.1. Engines

Engine fire in flight

	Fire Bell Sounds and	
or		or
	Fire Bell Sounds and	
Thrust lever (affected engine)	Close	
If Fire Warning Persists		
HP COCK (affected engine)	Close	
LP COCK (affected engine)	Close	
ENG EXT	SHOT 1	
If Engine Shutdown Occurs During Initial Climb		
MAIN AIR VLVs 1 & 2	CLOSE	
F/DK VLV	CLOSE	
GEN (affected engine)	TRIP	
BUS TIE (if open)	CLOSE	
MAIN AIR VLV (affected engine)	CLOSE	
F/DK VLV (No. 2 engine only)	CLOSE	
ENG SYNC	OFF	
ALTERNATOR (affected engine)	OFF	
WING FUEL/X-FEED/TRANSFER lever	X-FEED - Use pumps selectively to balance fuel.	
TCAS	TA only	
If Fire Warning Persists		
ENG EXT	SHOT 2	

CRM and Ergonomics

3.4. Fire or Smoke

Electrical fire or smoke

NOTE: Headsets and hats must be removed before donning oxygen mask.

Crew oxygen	Don masks - 100% EMERG
Mic selector	OXY- MIC
Smoke goggles	Don and vent
Cabin notices	ON

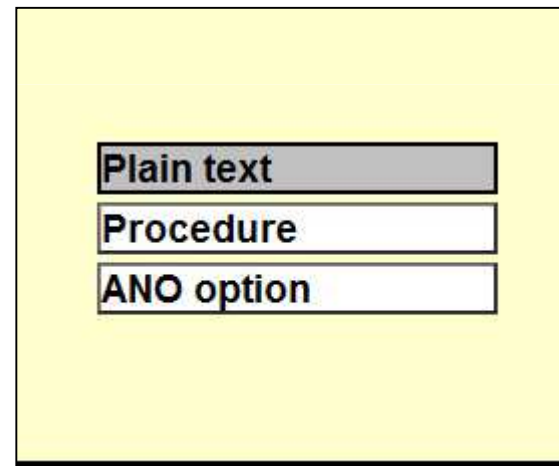
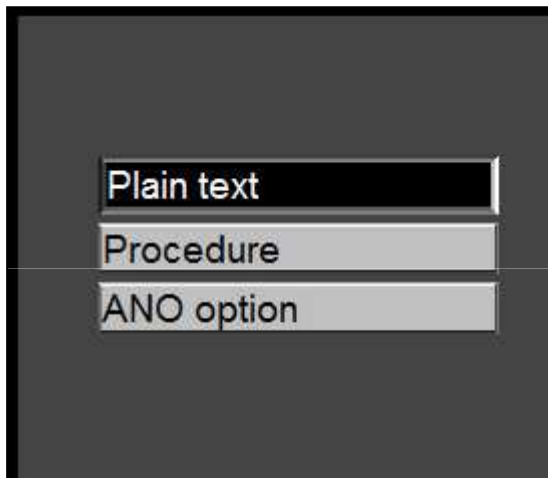
DUMP VALVE	OPEN slowly to assist smoke clearance but maintain cabin pressure.
PANEL LTS (if required)	EMERG
AUTOPILOT & YAW DAMPER	DISENGAGE
BATT	EMERG
GEN 1 & 2	TRIP both
ALTERNATORS 1 & 2	OFF
ENG CMPTR 1 & 2	OFF

SMOKE
DECREASES

SMOKE PERSISTS

CRM and Ergonomics

Night vision



High glare

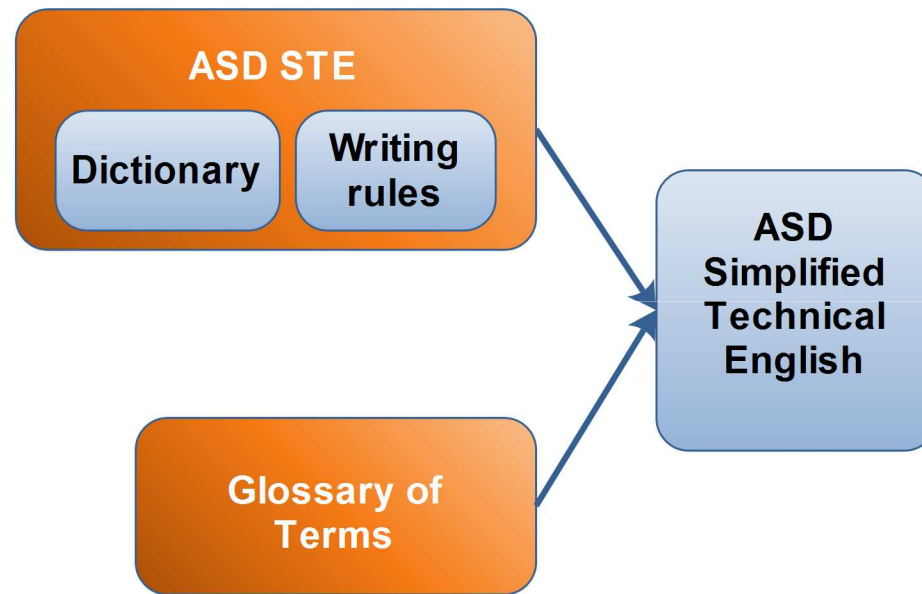
English

1. English is the *lingua-franca* of the industries we work in.
2. Not everyone working in those industries has English as a *first language*.
 - Crisp and clear
 - Formal Simplified Technical English

ASD Simplified Technical English

- What is it?
 - “an international specification for the preparation of maintenance documentation in a controlled language”
- Two parts:
 - Set of writing rules
 - Dictionary sub-set (< 1,000 words)
- ASD-STE100: copyright and a trademark of ASD

STE general principle



Example STE: Rule 1.2

- Use approved words from the dictionary only as the parts of speech given
- Examples:
 - ‘Test’ is approved as a noun, not a verb:
 - Non STE: ‘Test the system for leaks’
 - STE: ‘Do a leak test for the system’
 - ‘Close’ is a verb (and not an adverb):
 - Non STE: ‘Do not go close to the test rig during the test’
 - STE: ‘Do not go near the test rig during the test’

Example STE Rule 1.3:

- Keep to the approved meaning in the dictionary
- Example: ‘Follow’ means ‘to come after’; it does not mean ‘obey’
 - Non STE: ‘Follow the safety instructions’
 - STE: ‘Obey the safety instructions’

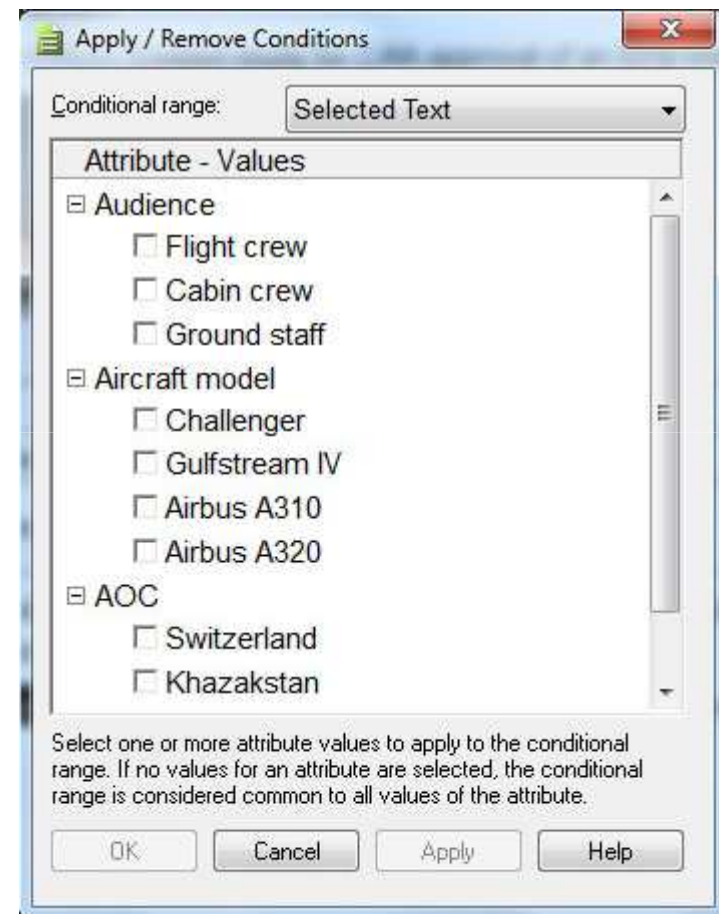
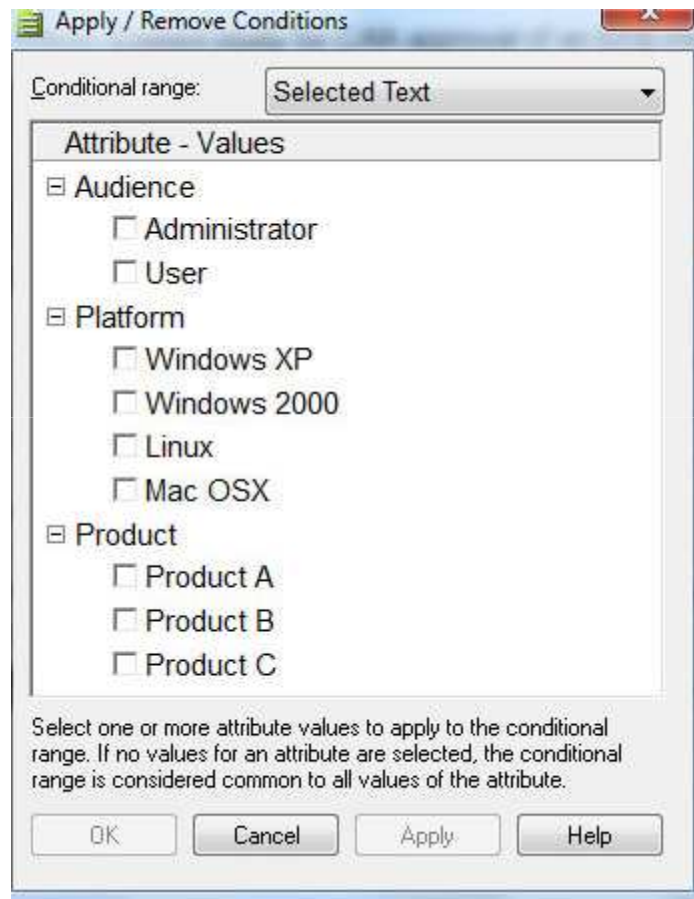
Software engineering issues

- Ditamaps do more
- Specialisation
 - Avoid if you can !
 - Simple is best

Ditamaps do more !

- Separate
 - *Content*: substance of the topic
 - *Context*: links to other topics, navigation
- Relationship tables
 - “Related topic” links
 - Goes beyond typical print sequential order
- Multiple views on same topic
 - By audience; platform etc.

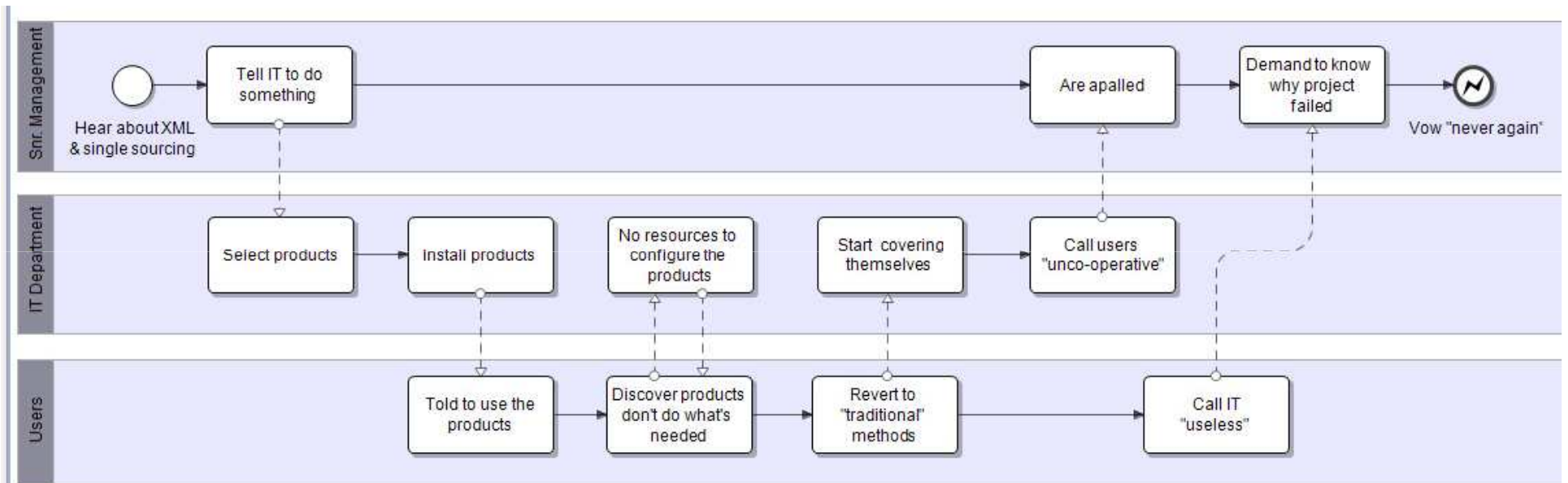
Custom sequential processing



Management issues

- Design the project to work
- Be ready to compromise
- Consider competing standards
- Promote a single vision
- Document what you do

Don't set up to fail ...



Contender standards

DITA

- Does most things but not all
- Easy learning curve
- Inexpensive

S1000D

- Ultimate sophistication and control
- Steep learning curve
- Very expensive

DocBook

- Oriented towards print
- Relatively steep learning curve
- Moderately expensive

Be ready to compromise

- Be prepared to COMPROMISE
- Challenge assertions:
 - “we’ve always done it that way” [*Why* is that?]
 - “we’ve never done that before” [*Why* not?]
 - “our requirements are unique” [*How* so?]
 - “we couldn’t possibly do that” [*What* if you did?]

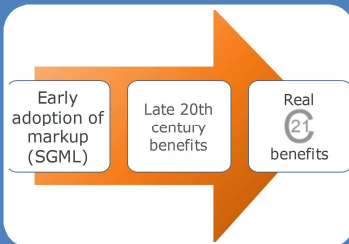
Promote a single vision

- Identify the reasons for
 - Reuse and re-purposing of information
- Clarify the benefits
- Evangelise

Document what you do

- Prince 2 – lessons learned
- If you don't document, in six months nobody will remember:
 - Who decided what
 - Why that was decided
 - Why other alternatives were rejected

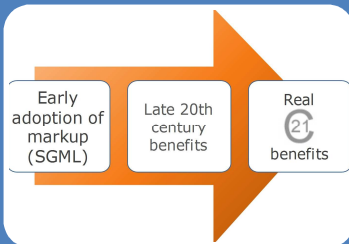
Conclusions



XML allows a structured approach, giving:

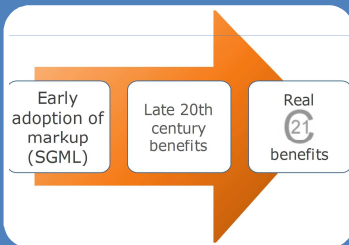
- Cost savings: make once, use many
- Quality enhancements: avoid costly problems
- Do more with the same resources

Conclusions



XML allows a structured approach, giving:

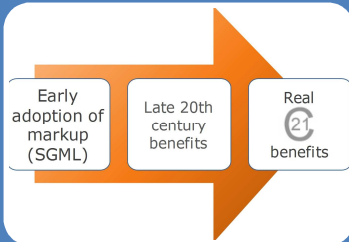
- Cost savings: make once, use many
- Quality enhancements: avoid costly problems
- Do more with the same resources



XML: single sourcing, which reduces risk:

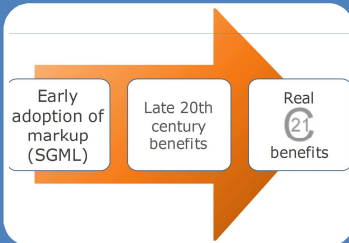
- Avoids the copy & paste disease
- Ensure that the Law of Primacy is obeyed

Conclusions



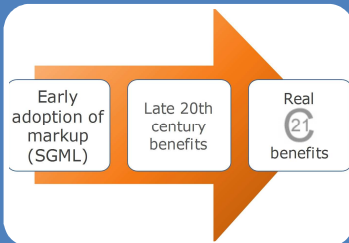
XML allows a structured approach, giving:

- Cost savings: make once, use many
- Quality enhancements: avoid costly problems
- Do more with the same resources



XML: single sourcing, which reduces risk:

- Avoids the copy & paste disease
- Ensure that the Law of Primacy is obeyed



XML is the basis of DITA and S1000d which means:

- We don't have to do everything from scratch
- We are not alone
- We can start with prototypes and scale up

References

Source	Remarks
www.theiet.org/factfiles/health/hsb26a-page.cfm	IET paper on FMEA
www.theiet.org/factfiles/health/hsb26c-page.cfm	IET paper on FTA
www.asd-ste100.org	Official ASD web site for Simplified Technical English
wiki.oasis-open.org/dita/	DITA TC Wiki
www.oasis-open.org/specs/#ditav1.1	DITA 1.1
http://public.s1000d.org/Pages/Home.aspx	S1000d official web site