Chapter 22

Formal Proof of Explanation

Proving correct a complex object like the WB-Graph we have developed based on the specifications of Chapter 16 requires the use of a strict proof scheme. Without a systematic approach it is difficult to maintain the overview over the proof. We decided to use a hierarchical proof scheme, allowing the systematic decomposition into substeps, which can be proved separately. This allows the development of proof templates (section A) we will use for the proof of the graph.

22.1 The Hierarchical Proof-scheme

The principle we use to decompose the proof into substeps is *inverse natural deduction*. We try to find proof-steps, which we can assume to be correct for the current step. So we can complete the current step under this assumption and prove the correctness of these proof-steps later on.
To find these steps is straight forward in our case. Since we wish to prove the correctness of a WB-graph, the structure of the proof is directly given by the structure of the graph. All we need to do is to prove the completeness and correctness for the internal nodes of the graph (see figure 22.1).

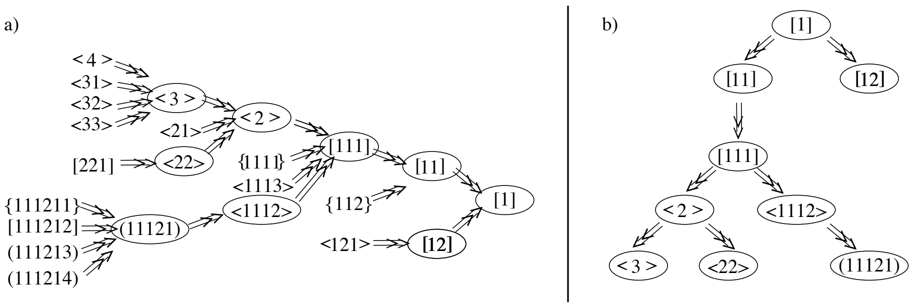

Figure 22.1: (a) Structure of the intuitive WB-Graph and (b) resulting Proof Structure

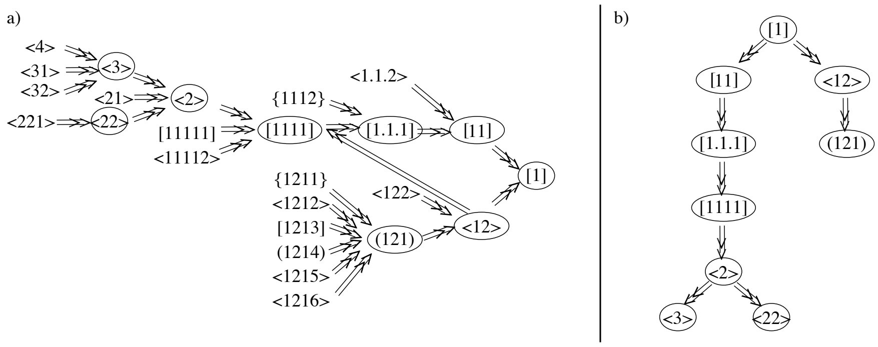

Figure 22.2: (a) Structure of the proved WB-Graph and (b) resulting Proof Structure

During the proof, we determined inaccuracies in the intuitive WB-Graph presented in Figure 17.4. It was necessary to implement several changes and eventually we got the graph shown in figure22.5.

Similar to the hierarchical specifications we presented in chapter 16, we split the proof into several modules. Each module contains one of the proof-steps illustrated in figure 22.2 (b). The proof-steps are formulated as theorems. We formulate the main theorem –"*WB-Graph is causally sufficient*"– in a top-level module and include the subproofs as shown in figure 22.3.

22.2 Sufficient Causal Explanation Proof

In the following sections we will present the modules – and their proofs – used to state the top-level theorem in figure 22.3. Furthermore, we will formulate the assumptions we made during the proof in module *Proof-Obligations* (section 22.2.10). In the final section of this chapter we will present the textual and pictorial form of the causally sufficient explained WB-Graph.

22.2.1 Proof of [1]

For a better readability we write down the used WB-graph nodes before we present the proof steps. There is no formal need to do so!

[1] /* AC lands at Brussels RWY 25 */
[11] /* CRW opts to continue landing */
⟨12⟩ /* AC near Brussels Airport */

module *[1]_is_explained_causally_sufficient*

VARIABLES
extends *Landing_Specs*
extends *PARDIA−Axioms*
extends *PARDIA−Norms*
CONSTANTS $CRW, AC, BRU, APPR$

$$Hypotheses \triangleq \wedge [11] \; \wedge \langle 12 \rangle$$

$$Procedures \triangleq \wedge Landing\_Specs.Spec \; \wedge PARDIA{-}Axioms.Spec \; \wedge PARDIA{-}Norms.Spec$$

THEOREM $(Hypotheses \wedge Procedures) \Box\!\!\Rightarrow \Diamond[1]$

PROOF:

⟨1⟩1. $[11] \Leftrightarrow \wedge Decide(CRW, \Box(AC)in\_landing\_phase) \wedge \Box\neg distress\_decl(CRW) \wedge \Box\neg urgency\_decl(CRW) \wedge \Box(AC)in\_landing\_phase$

PROOF:
Interpretation: we take "opts to continue" to mean "decides to continue and acts successfully to continue" which we formulate as a state pedicate.

⟨1⟩2. $\langle 12 \rangle \Leftrightarrow (AC)near(BRU)$

PROOF:
We interpret ⟨12⟩ as a state predicate.

⟨1⟩3. $(Hypotheses \wedge Procedures) \Box\!\!\Rightarrow \Diamond[1]$

PROOF:
⟨2⟩1. *Hypotheses*
PROOF:
⟨3⟩1. [11]
PROOF:
[11] under the interpretation of ⟨1⟩1 is true from the sources.
⟨3⟩2. ⟨12⟩
PROOF:
⟨12⟩ under the interpretation of ⟨1⟩2 is true from the sources.
⟨3⟩3. Q.E.D.
Follows by ($\wedge - intro$) from ⟨3⟩1, and ⟨3⟩2.
⟨2⟩2. *Procedures*

PROOF:
We assume that *Landing_Specs.Spec*, *PARDIA-Axioms.Spec* and *PARDIA-Norms.Spec* hold.

⟨2⟩3. $(Hypotheses \land \Box Procedures) \succ \Diamond[1]$

PROOF:

⟨3⟩1. $\vdash_{TLA} (Hypotheses \land \Box Procedures) \Rightarrow \Diamond[1]$

PROOF:

$$\langle 4\rangle 1.\ \begin{pmatrix} \land & Decide(CRW, \Box(AC) in\_landing\_phase) \\ \land & (AC) near(BRU) \\ \land & \Box Landing\_Specs.Spec \\ \land & \Box PARDIA{-}Norms.Spec \\ \land & \Box PARDIA{-}Axioms.Spec \end{pmatrix} \Rightarrow (AC)\_lands\_at(BRU)$$

PROOF:

$$\langle 5\rangle 1.\ \begin{pmatrix} \land & Decide(CRW, \Box(AC)\_in\_landing\_phase) \\ \land & \Box PARDIA{-}Norms.Spec \\ \land & \Box PARDIA{-}Axioms.Spec \end{pmatrix} \leadsto \Box(AC)\_in\_landing\_phase$$

PROOF:

$$\langle 6\rangle 1.\ \begin{pmatrix} \land & Decide(CRW, \Box(AC)\_in\_landing\_phase) \\ \land & \Box PARDIA{-}Norms.Spec \end{pmatrix} \leadsto$$
$$\leadsto Intend(CRW, \Box(AC)\_in\_landing\_phase)$$

PROOF:
This is *PARDIA-Norms.N3*.

$$\langle 6\rangle 2.\ \begin{pmatrix} \land & Indend(CRW, \Box(AC)\_in\_landing\_phase) \\ \land & \Box PARDIA{-}Norms.Spec \end{pmatrix} \leadsto$$
$$\leadsto Act(CRW, \Box(AC)\_in\_landing\_phase)$$

PROOF:
This is *PARDIA-Norms.N4*.

$$\langle 6\rangle 3.\ \begin{pmatrix} \land & Act(CRW, \Box(AC)\_in\_landing\_phase) \\ \land & \Box PARDIA{-}Axioms.Spec \end{pmatrix} \Rightarrow \Box(AC)\_in\_landing\_phase$$

PROOF:
Since $\Box(AC)\_in\_landing\_phase$ is a state predicate, this follows from Axiom *PARDIA-Axioms.A10*.

⟨6⟩4. Q.E.D.

PROOF:
Follows by temporal logic from ⟨6⟩1, ⟨6⟩2 and ⟨6⟩3.

$$\langle 5\rangle 2.\ \begin{pmatrix} \land & \Box(AC)\_in\_landing\_phase \\ \land & (AC) near(BRU) \end{pmatrix} \Rightarrow (AC)\_lands\_at(BRU)$$

PROOF:
This is an Axiom (*Landing_Specs.LandingRule*)!

⟨5⟩3. Q.E.D.
Follows by propositional logic from ⟨5⟩1 and ⟨5⟩2.

⟨4⟩2. Q.E.D.
Follows by definition of strict implication (inference rule 14.21). □

⟨2⟩4. $\Diamond[1]$

PROOF:
This is a fact explicitly given in the sources.

⟨2⟩5. Q.E.D.
Directly follows by Inference Rule 15.7 from ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 and ⟨2⟩4. □

22.2.2 Proof of [11]

Nodes used in the following module:

[11] /* CRW opts to continue landing */
[111] /* CRW realizes they are landing at the wrong airport */
⟨112⟩ /* CRW has safety reasons for continuing landing */
⟨113⟩ /* Standard Operating Procedures */

module *[11]_is_explained_causally_sufficient*

DECLARATIONS
extends *PARDIA−Axioms*
extends *PARDIA−Norms*
instance *Landing_Specs*
instance *Landing_Norms*
instance *Phases*
CONSTANTS CRW, AC, TFC

$$Hypotheses \triangleq \wedge [111] \quad \wedge \langle 112 \rangle$$

$$Procedures \triangleq \langle 113 \rangle$$

$$\text{THEOREM} \begin{pmatrix} \wedge & Hypotheses \\ \wedge & \Box Procedures \\ \wedge & \Box Phases.Decision \\ \wedge & [11] \end{pmatrix} \Box\!\!\Rightarrow [11]$$

PROOF:

$$\langle 1\rangle 1.\ \langle 111\rangle \Leftrightarrow \wedge\ Reason(CRW, APT \neq destAPT) \quad \wedge\ (AC)near(APT)$$

PROOF:
We interpret ⟨111⟩ as the corresponding reasoning by the crew.

$$\langle 1\rangle 2.\ \langle 112\rangle \Leftrightarrow \begin{pmatrix} \wedge & Reason(CRW, (\Diamond\neg(AC)in\_landing\_phase \Rightarrow endanger(CRW, TFC))) \\ \wedge & \Box\neg distress\_decl(CRW) \\ \wedge & \Box\neg urgency\_decl(CRW) \\ \wedge & \Box(AC)in\_landing\_phase \end{pmatrix}$$

PROOF:
We interpret ⟨112⟩ as a state predicate. We interpret the phrase '*reasons for continuing landing*' as indicating not only that they had reasons, but also successfully continued, without declaring urgency or emergency.

$$\langle 1\rangle 3.\ \langle 113\rangle \Leftrightarrow \wedge\ PARDIA\_Norms.Spec \quad \wedge\ PARDIA\_Axioms.Spec \quad \wedge\ Landing\_Specs.Spec \quad \wedge\ Landing\_Norms.LNSpec$$

PROOF:
We consider the SOPs for this case to be described sufficiently by our specifications *PARDIA_Norms.Spec*, *PARDIA_Axioms.Spec* and *landing_specs.Spec*.

$$\langle 1\rangle 4.\ [11] \Leftrightarrow \begin{array}{l} \wedge\ Decide(CRW, \Box(AC)in\_landing\_phase) \\ \wedge\ \Box\neg distress\_decl(CRW) \\ \wedge\ \Box\neg urgency\_decl(CRW) \\ \wedge\ \Box(AC)in\_landing\_phase \end{array}$$

PROOF:
Interpretation: we take "opts to continue" to mean "decides to continue and acts successfully to continue"

$$\langle 1\rangle 5.\ \left(\begin{array}{ll} \wedge & Hypotheses \\ \wedge & \Box Procedures \\ \wedge & \Box Phases.Decision \\ \wedge & [11] \end{array}\right) \Box\!\!\Rightarrow [11]$$

$\langle 2\rangle 1.$ *Hypotheses*
PROOF:
$\langle 3\rangle 1.$ [111]
PROOF:
Under the interpretation of $\langle 1\rangle 1$ we consider the truth of [111] to be stated in the sources.
$\langle 3\rangle 2.$ $\langle 112\rangle$
PROOF:
Under the interpretation of $\langle 1\rangle 2$ we consider the truth of $\langle 112\rangle$ to be stated in the sources.
$\langle 3\rangle 3.$ Q.E.D.
PROOF:
Follows immediately by /intro
$\langle 2\rangle 2.$ $(Hypotheses \wedge \Box Procedures) \succ \bot$
PROOF:
$\langle 3\rangle 1.$ $\vdash_{TLA} (Hypotheses \wedge \Box Procedures) \Rightarrow \bot$
PROOF:

$$\langle 4\rangle 1.\ \vdash_{TLA} \left(\begin{array}{ll} \wedge & Landing\_Specs.Spec \\ \wedge & Landing\_Norms.Normal\_Progress \\ \wedge & Landing\_Norms.Landing\_Procedures \\ \wedge & \Box(AC)in\_landing\_phase \\ \wedge & \Box\neg distress\_decl(CRW) \\ \wedge & \Box\neg urgency\_decl(CRW) \end{array}\right) \Rightarrow \bot$$

PROOF:

$$\langle 5\rangle 1.\ \vdash_{TLA} \left(\begin{array}{ll} \wedge & Landing\_Specs.Spec \\ \wedge & Landing\_Norms.Landing\_Procedures \\ \wedge & \Box(AC)in\_landing\_phase \end{array}\right) \Rightarrow \Diamond(AC)lands\_at(APT)$$

PROOF:

$\langle 6\rangle 1.\ \vdash_{TLA} \left(\begin{array}{ll} \wedge & (AC)near(APT) \\ \wedge & \wedge\ (AC)near(APT) \qquad \Rightarrow \Diamond(AC)lands\_at(APT) \\ & \wedge\ \Box(AC)in\_landing\_phase \\ \wedge & \Box(AC)in\_landing\_phase \end{array} \right) \Rightarrow$
$\Diamond(AC)lands\_at(APT)$

PROOF:

Follows immediately by propositional logic

$\langle 6\rangle 2.$ Q.E.D.

PROOF:

Follows immediately by propositional logic from $\langle 6\rangle 1$ upon observing that $(AC)near(APT)$ is a conjunct of $\langle 111\rangle$.

$\langle 5\rangle 2.\ \vdash_{TLA} \left(\begin{array}{ll} \wedge & Landing\_Norms.Normal\_Progress \\ \wedge & APT \neq destAPT \\ \wedge & \Box\neg distress\_decl(CRW) \\ \wedge & \Box\neg urgency\_decl(CRW) \end{array} \right) \Rightarrow \neg\Diamond(AC)lands\_at(APT)$

PROOF:

Immediate by propositional logic using the definition of $Landing\_Norms.Normal\_Progress$.

$\langle 5\rangle 3.$ Q.E.D.

Follows immediately by propositional logic from $\langle 5\rangle 1$ and $\langle 5\rangle 2$

$\langle 4\rangle 2.$ Q.E.D.

Follows immediately by propositional logic by inspection of the constituent clauses

$\langle 3\rangle 2.$ Q.E.D.

Follows by Inference Rule 14.21. □

$\langle 2\rangle 3.$ $Hypotheses \succ (AC)in\_landing\_phase$

The consequent is a conjunct of $\langle 112\rangle$.

$\langle 2\rangle 4.$ 11

This is stated in the sources.

$\langle 2\rangle 5.$ Q.E.D.

Follows immediately from $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$ and $\langle 2\rangle 4$ by EL-Rule 19.10. □

22.2.3 Proof of [111]

Nodes used in the following module:

[111] /* Crew (CRW) realizes they are landing at the wrong airport */
[1111] /* CRW gets visual contact to Brussels airport */
{1112} /* CRW notices that Brussels' airport layout is different from Frankfurt's */

module *[111]_is_explained_causally_sufficient*

THEOREM $([1111] \wedge \{1112\}) \;\Box\!\!\Rightarrow [111]$

PROOF:

$\langle 1\rangle 1.$ $\langle 111\rangle \Leftrightarrow \wedge\ Reason(CRW, APT \neq destAPT)$
$\wedge\ (AC)near(APT)$

PROOF:
We interpret $\langle 111\rangle$ as the corresponding reasoning by the crew.

$\langle 1\rangle 2.$ $([1111] \wedge \{1112\}) \;\Box\!\!\Rightarrow [111]$

$\langle 2\rangle 1.$ $[1111] \Rightarrow\!\!\succ [111]$

PROOF:

$\langle 3\rangle 1.$ $[1111] \wedge [111]$

PROOF:

$\langle 4\rangle 1.$ [1111]
PROOF: This is a fact explicitly given in the sources.

$\langle 4\rangle 2.$ [111]
PROOF: This is a fact explicitly given in the sources.

$\langle 4\rangle 3.$ Q.E.D.
($\wedge$-introduction) from $\langle 4\rangle 1$ and $\langle 4\rangle 2$. □

$\langle 3\rangle 2.$ $\neg[1111] \;\Box\!\!\rightarrow \neg[111]$

PROOF:
The CRW did not realize their wrong position earlier although sufficient hints were available. *Given that* instruments providing the information necessary to determine the position without visual contact were ignored, the only other way to obtain this information is visual contact. The theorem follows by *modus tollens*.

$\langle 3\rangle 3.$ Q.E.D.
Directly follows by Inference Rule 14.20 from $\langle 3\rangle 1$ and $\langle 3\rangle 2$. □

$\langle 2\rangle 2.$ $\{1112\} \Rightarrow\!\!\succ [111]$

PROOF:

$\langle 3\rangle 1.$ $\{1112\} \wedge [111]$

PROOF:

$\langle 4\rangle 1.$ {1112}
PROOF: This is a fact explicitly given in the sources.

$\langle 4\rangle 2.$ [111]
PROOF: This is a fact explicitly given in the sources.

$\langle 4\rangle 3.$ Q.E.D.
($\wedge$-introduction) from $\langle 4\rangle 1$ and $\langle 4\rangle 2$. □

$\langle 3\rangle 2.$ $\neg\{1112\} \;\Box\!\!\rightarrow \neg[111]$

PROOF:
Apart from technical means which were earlier ignored or at least misinterpreted by the CRW the only way to differentiate between airports is to compare their layouts.

Given that the evidence of the instruments was ignored, if they hadn't recognized the layout they saw was different from the expected (flight documents contain 2D maps of the destination airport) they wouldn't have recognized their mistake at that time.

⟨3⟩3. Q.E.D.

Directly follows by Inference Rule 14.20 from ⟨3⟩1 and ⟨3⟩2. □

⟨2⟩3. $\neg[111] \Box\!\!\rightarrow \neg([1111] \wedge \{1112\})$

Given that no use of evidence from instrumentation was made, if neither [1111] nor {1112} then no evident was available that could call their attention to the wrong airport.

⟨2⟩4. Q.E.D.

Follows by definition of " $\Box\!\!\Rightarrow$ " and from steps ⟨2⟩1,⟨2⟩2 and ⟨2⟩3. □

22.2.4 Proof of [1111]

Nodes used in the following module:

[1111] /* CRW gets visual contact to Brussels airport */
[11111] /* AC breaks out under clouds */
⟨11112⟩ /* CRW procedures */
⟨12⟩ /* AC near Brussels Airport */
⟨2⟩ /* AC in BATC area */

module *[1111]_is_explained_causally_sufficient*

VARIABLES
extends *Landing_Specs*
extends *Naturals*
extends *RealTime*
$RTT \triangleq$ **instance** *RealTimeTheorems*
with $lower\_bound \leftarrow TDZE$,
$upper\_bound \leftarrow current\_alt$,
$f \leftarrow alt$
CONSTANTS $AC, ATC, CRW, APT, TFC, APPR$
VARIABLES alt

$Hypotheses \triangleq \land [11111]$
$\land \langle 12 \rangle$
$\land \langle 2 \rangle$
$Procedures \triangleq \langle 11112 \rangle$

ASSUMPTIONS
$ASSUMPTION1 \triangleq DH \in (TDZE, alt]$

THEOREM $(Hypotheses \land Procedures) \Box\!\!\Rightarrow \Diamond[1111]$

PROOF:

⟨1⟩1. $[11111] \Leftrightarrow below\_clouds(AC)$
PROOF:
We interpret [11111] as a state predicate.
⟨1⟩2. $\langle 12 \rangle \Leftrightarrow (AC)near(APT)$
PROOF:
We interpret ⟨12⟩ as a state predicate.
⟨1⟩3. $\langle 2 \rangle \Leftrightarrow (AC)in\_area(atc)$
PROOF:
We interpret ⟨2⟩ as a state predicate.
⟨1⟩4. $\langle 11112 \rangle \Leftrightarrow \land ILS\_approach(AC, APT)$
$\land \Box\neg CRW\_breakoff(CRW)$
PROOF:
As described below, a part of the procedures (i.e. $ILS\_approach(AC, APT)$ and $\Box\neg CRW\_breakoff(CRW)$) are sufficient for our needs.

$\langle 1\rangle 5.$ $(Hypotheses \wedge Procedures) \;\Box\!\!\Rightarrow \Diamond[1111]$
$\langle 2\rangle 1.$ *Hypotheses*
PROOF:
$\langle 3\rangle 1.$ [11111]
PROOF:
[11111] under the interpretation of $\langle 1\rangle 1$ is true from the sources.
$\langle 3\rangle 2.$ $\langle 12\rangle$
PROOF:
$\langle 12\rangle$ under the interpretation of $\langle 1\rangle 2$ is true from the sources.
$\langle 3\rangle 3.$ $\langle 2\rangle$
PROOF:
$\langle 2\rangle$ under the interpretation of $\langle 1\rangle 3$ is true from the sources.
$\langle 3\rangle 4.$ Q.E.D.
$\wedge$-intro from $\langle 3\rangle 1$, $\langle 3\rangle 2$ and $\langle 3\rangle 3$.
$\langle 2\rangle 2.$ *Procedures*
PROOF:
$\langle 3\rangle 1.$ $\langle 11112\rangle$
PROOF:
$\langle 11112\rangle$ under the interpretation of $\langle 1\rangle 4$ is true from the sources.
$\langle 2\rangle 3.$ $(Hypotheses \wedge \Box Procedures) \succ \Diamond[1111]$
PROOF:
$\langle 3\rangle 1.$ $\vdash_{TLA} (Hypotheses \wedge \Box Procedures) \Rightarrow \Diamond[1111]$
PROOF:
We intend to reformulate this expression in logic. Formulation of the goal

$\langle 4\rangle 1.$ $[1111] \Leftrightarrow \Diamond visual\_contact(CRW, APT)$
PROOF:
Interpretation: [1111] corresponds to a state predicate.

as well as use of the logical equivalents defined above results in:

$$\langle 4\rangle 2. \quad \begin{pmatrix} \wedge & below\_clouds(AC) \\ \wedge & (AC)near(BRU\_APT) \\ \wedge & (AC)in\_area(atc) \\ \wedge & \Box \begin{pmatrix} \wedge & ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix} \end{pmatrix} \Rightarrow \Diamond visual\_contact(CRW, APT)$$

PROOF:

$\langle 5\rangle 1.$ $\Diamond\Box visual\_contact(CRW, APT) \Rightarrow \Diamond visual\_contact(CRW, APT)$
PROOF:
Derivable from TLA-Rules. □

$$\langle 5\rangle 2. \quad \begin{pmatrix} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \\ \wedge & \Diamond\Box \begin{pmatrix} \wedge & ILS\_approach(AC, APT) \\ \wedge & below\_DH \end{pmatrix} \end{pmatrix} \Rightarrow \Diamond\Box visual\_contact(CRW, APT)$$

PROOF:

$$\langle 6\rangle 1. \quad \begin{pmatrix} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix} \Rightarrow \Diamond\Box visibility\_acceptable(CRW)$$

PROOF:

$\langle 7\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \\ \wedge & \Diamond below\_DH \end{array}\right) \Rightarrow \Diamond\Box visibility\_acceptable(CRW)$

PROOF:

$\langle 8\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \\ \wedge & below\_DH \end{array}\right) \Rightarrow \Box visibility\_acceptable(CRW)$

PROOF:

Follows by Propositional Logic from $ILS - APPR\_Rule$.

$\langle 8\rangle 2.\ \left(\left(\begin{array}{ll} \wedge & \Box A \\ \wedge & B \end{array}\right) \Rightarrow C\right) \Rightarrow \left(\left(\begin{array}{ll} \wedge & \Box A \\ \wedge & \Diamond B \end{array}\right) \Rightarrow \Diamond C\right)$

PROOF:

$\langle 9\rangle 1.\ \left(\left(\begin{array}{ll} \wedge & \Box A \\ \wedge & \Diamond B \end{array}\right)\right) \Rightarrow \Diamond \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & B \end{array}\right)$

PROOF:

$\langle 10\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & \neg\Diamond \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & B \end{array}\right) \end{array}\right) \Rightarrow \neg\Diamond B$

PROOF:

$\langle 11\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & \Box \left(\begin{array}{ll} \vee & \neg\Box A \\ \vee & \neg B \end{array}\right) \end{array}\right) \Rightarrow \Box\neg B$

PROOF:

$\langle 12\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box\Box A \\ \wedge & \Box \left(\begin{array}{ll} \vee & \neg\Box A \\ \vee & \neg B \end{array}\right) \end{array}\right) \Rightarrow \Box\neg B$

PROOF:

$\langle 13\rangle 1.\ \Box \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & \left(\begin{array}{ll} \vee & \neg\Box A \\ \vee & \neg B \end{array}\right) \end{array}\right) \Rightarrow \Box\neg B$

PROOF:

$\langle 14\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & \left(\begin{array}{ll} \vee & \neg\Box A \\ \vee & \neg B \end{array}\right) \end{array}\right) \Rightarrow \neg B$

PROOF:

This is always a logical Truth !

$\langle 14\rangle 2.$ Q.E.D.

PROOF:

Follows by STL4 from $\langle 14\rangle 1$. □

$\langle 13\rangle 2.$ Q.E.D.

Follows by STL5 from $\langle 13\rangle 1$. □

$\langle 12\rangle 2.$ Q.E.D.

Follows by STL3 from $\langle 12\rangle 1$. □

$\langle 11\rangle 2.$ Q.E.D.

Follows by Propositional Logic from $\langle 11\rangle 1$. □

$\langle 10\rangle 2.$ Q.E.D.

PROOF:

Follows by Propositional Logic from $\langle 10\rangle 1$. □

$\langle 9\rangle 2.\ \Diamond \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & B \end{array}\right) \Rightarrow \Diamond C$

PROOF:

$\langle 10\rangle 1.\ \left(\begin{array}{ll} \wedge & \Box A \\ \wedge & B \end{array}\right) \Rightarrow C$

PROOF:

With:
$A \triangleq \wedge\ ILS\_approach(AC, APT)$
$\quad\ \wedge \neg CRW\_breakoff(CRW)$
$B \triangleq below\_DH$
$C \triangleq \Box visibility\_acceptable(CRW)$ and Propositional Logic this is $ILS - APPR\_rule$.

⟨10⟩2. Q.E.D.
PROOF:
Follows from ⟨10⟩1 by STL4 (◇-Form). □

⟨9⟩3. Q.E.D.
PROOF:
Follows by Propositional Logic from ⟨9⟩1 and ⟨9⟩2. □

⟨8⟩3. Q.E.D.
Derivable from ⟨8⟩1 by ⟨8⟩2 with:
$A \triangleq \wedge\ ILS\_approach(AC, APT)$
$\quad\ \wedge \neg CRW\_breakoff(CRW)$
$B \triangleq below\_DH$
$C \triangleq \Box visibility\_acceptable(CRW)$. □

⟨7⟩2. $\begin{pmatrix} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix} \Rightarrow \Diamond below\_DH$

PROOF:

⟨8⟩1. $\begin{pmatrix} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix}$
$\Rightarrow \forall x \in [TDZE, current\_alt] : \Diamond alt = x$

PROOF:

⟨9⟩1. $\begin{pmatrix} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix} \Rightarrow \Diamond landing$

PROOF:
This is an Axiom ($ILS - LandingRule$)!

⟨9⟩2. $\begin{pmatrix} \wedge & \Box ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix} \Rightarrow \begin{pmatrix} alt\ is\ a\ \text{'}monotone\ decreasing \\ continuous\ function\ of\ RealTime\text{'} \end{pmatrix}$

PROOF:
This is an Axiom ($ILS - AltProperty$)!

⟨9⟩3. $\begin{pmatrix} alt\ is\ a\ \text{'}monotone\ decreasing \\ continuous\ function\ of\ RealTime\text{'} \end{pmatrix} \Rightarrow \frac{\delta\ alt}{\delta t} < 0\ in\ [TDZE, current\_alt]$

PROOF:
This is the definition of a 'decreasing continuous function'.

⟨9⟩4. $\begin{pmatrix} \wedge & \frac{\delta\ alt}{\delta t} < 0\ in\ [TDZE, current\_alt] \\ \wedge & alt = current\_alt \\ \wedge & \Diamond(alt = TZDE) \end{pmatrix}$
$\Rightarrow \forall x \in [TDZE, current\_alt] : \Diamond alt = x$

PROOF:
This is RTT.MeanValueTheorem.

⟨9⟩5. Q.E.D.
PROOF:
Follows by Propositional Logic from ⟨9⟩1, ⟨9⟩2, ⟨9⟩3 and ⟨9⟩4. □

⟨8⟩2. $\begin{pmatrix} \wedge & \forall x \in [TDZE, current\_alt] : \Diamond alt = x \\ \wedge & ASSUMPTION1 \end{pmatrix} \Rightarrow \Diamond below\_DH$

PROOF:

Follows immediatly from Calculus and definition of $below\_DH$.

⟨8⟩3. $\Diamond\Box below\_DH \Rightarrow \Diamond below\_DH$

PROOF:

Derivable by TLA-Rules.

⟨8⟩4. Q.E.D.

PROOF:

Follows from ⟨8⟩1, ⟨8⟩2 and ⟨8⟩3 by Propositional Logic. □

⟨7⟩3. Q.E.D.

PROOF:

Follows from ⟨7⟩1 and ⟨7⟩2 by Propositional Logic. □

⟨6⟩2. $$\left(\begin{array}{ll} \wedge & \Diamond\Box visibility\_acceptable(CRW) \\ \wedge & \Diamond\Box \left(\begin{array}{ll} \wedge & ILS\_approach(AC, APT) \\ \wedge & below\_DH \end{array}\right) \end{array}\right) \Rightarrow \Diamond\Box visual\_contact(CRW, APT)$$

PROOF:

⟨7⟩1. $$\Diamond\Box \left(\begin{array}{ll} \wedge & visibility\_acceptable(CRW) \\ \wedge & \left(\begin{array}{ll} \wedge & ILS\_approach(AC, APT) \\ \wedge & below\_DH \end{array}\right) \end{array}\right) \Rightarrow \Diamond\Box visual\_contact(CRW, APT)$$

PROOF:

⟨8⟩1. $$\Box \left(\begin{array}{ll} \wedge & visibility\_acceptable(CRW) \\ \wedge & \left(\begin{array}{ll} \wedge & ILS\_approach(AC, APT) \\ \wedge & below\_DH \end{array}\right) \end{array}\right) \Rightarrow \Box visual\_contact(CRW, APT)$$

PROOF:

⟨9⟩1. $$\left(\begin{array}{ll} \wedge & visibility\_acceptable(CRW) \\ \wedge & \left(\begin{array}{ll} \wedge & ILS\_approach(AC, APT) \\ \wedge & below\_DH \end{array}\right) \end{array}\right) \Rightarrow visual\_contact(CRW, APT)$$

PROOF:

⟨10⟩1. $$\left(\begin{array}{ll} \wedge & visibility\_acceptable(CRW) \\ \wedge & \vee \wedge ILS\_approach(AC, APT) \\ & \quad \wedge below\_DH \\ & \vee \wedge NPA\_approach(AC, APT) \\ & \quad \wedge at\_MDA \end{array}\right) \Rightarrow visual\_contact(CRW, APT)$$

PROOF:

This is an Axiom ($Landing\_Criterion$).

⟨10⟩2. $ILS\_approach(AC, APT) \Leftrightarrow \neg NPA\_approach(AC, APT))$

PROOF:

This is an Axiom ($Unique\_Approach - Type\_Rule$).

⟨10⟩3. Q.E.D.

Follows from ⟨10⟩1 and ⟨10⟩2 by Propositional Logic. □

⟨9⟩2. Q.E.D.

Follows immediately from STL4. □

⟨8⟩2. Q.E.D.

Follows immediately from STL4 (◇-Form). □

⟨7⟩2. Q.E.D.

Follows immediately from STL6. □

⟨6⟩3. Q.E.D.

Follows by Propositional Logic from ⟨6⟩1 and ⟨6⟩2. □

⟨5⟩3. Q.E.D.

Follows by Propositional Logic (transitivity of implication) from ⟨5⟩1 and ⟨5⟩2. □

⟨4⟩3. Q.E.D.
Follows from steps ⟨4⟩1 and ⟨4⟩2. □
⟨3⟩2. Q.E.D.
Follows by definition of strict implication (inference rule 14.21). □
⟨2⟩4. $\Diamond[1111]$
PROOF:
This is a fact explicitly given in the sources.
⟨2⟩5. $\neg\Diamond[1111] \Box\!\!\rightarrow \neg(\mathit{Hypotheses} \wedge \Box \mathit{Procedures})$
PROOF:

⟨3⟩1. $$\Box\neg visual\_contact(CRW, APT) \Box\!\!\rightarrow \begin{pmatrix} \vee & \neg below\_clouds(AC) \\ \vee & \neg(AC) near(APT) \\ \vee & \neg(AC) in\_area(atc) \\ \vee & \neg\Box \begin{pmatrix} \wedge & ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix} \end{pmatrix}$$

PROOF:
We argue that in the nearest possible world,
$$\neg\Box \begin{pmatrix} \wedge & ILS\_approach(AC, APT) \\ \wedge & \Box\neg CRW\_breakoff(CRW) \end{pmatrix}$$
is the least possible alternative. Under this assumption, $\neg below\_clouds(AC)$, $\neg(AC) near(APT)$ or $\neg(AC) in\_area(atc)$ would all lead to $\neg visual\_contact(CRW, APT)$.
⟨3⟩2. Q.E.D.
Follows by Propositional Logic, STL2 and STL3 as well as use of definitions from ⟨2⟩1 and ⟨2⟩2.
⟨2⟩6. Q.E.D.
Directly follows by Inference Rule 15.7 from ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4 and ⟨2⟩5. □

22.2.5 Proof of Node 12

Nodes used in the following module:

⟨12⟩ /* AC near Brussels Airport */
(121) /* CRW did not realize that they were on wrong course, UNTIL:[111] */
⟨122⟩ /* AC cleared to BATC according to ATC procedures */

module *⟨12⟩_is_explained_causally_sufficient*

THEOREM ((121) ∧ ⟨122⟩) □⇒ ⟨12⟩

PROOF:

⟨1⟩1. ((121) ∧ ⟨122⟩) □⇒ ⟨12⟩
⟨2⟩1. (121) ⇛ ⟨12⟩
PROOF:
⟨3⟩1. (121) ∧ ⟨12⟩
PROOF:
⟨4⟩1. (121)
PROOF: This is assumed in the sources and can be derived from the CRW's behavior.
⟨4⟩2. ⟨12⟩
PROOF: This is a fact explicitly given in the sources.
⟨4⟩3. Q.E.D.
(∧-introduction) from ⟨4⟩1 and ⟨4⟩2. □
⟨3⟩2. ¬(121) □→ ¬⟨12⟩
PROOF:
The flight destination was Frankfurt. If they had realized they were on the wrong course, they would likely have taken actions to return to the course they were supposed to be on unless other more pressing considerations intervened. This is exactly what the counterfactual says.
⟨3⟩3. Q.E.D.
Directly follows by Inference Rule 14.20 from ⟨3⟩1 and ⟨3⟩2. □
⟨2⟩2. ⟨122⟩ ⇛ ⟨12⟩
PROOF:
⟨3⟩1. ⟨122⟩ ∧ ⟨12⟩
PROOF:
⟨4⟩1. ⟨122⟩
PROOF: We assume this from facts given in the sources.
⟨4⟩2. ⟨12⟩
PROOF: This is a fact explicitly given in the sources.
⟨4⟩3. Q.E.D.
(∧-introduction) from ⟨4⟩1 and ⟨4⟩2. □
⟨3⟩2. ¬⟨122⟩ □→ ¬⟨12⟩
PROOF:
We consider, that in the nearest possible world the SOPs are followed. In this particular case we assume that an AC only enters a specific area when it has obtained an ATC clearance before. Therefore without a clearance to BATC area the AC will not be able to get into Brussels Airport area.
⟨3⟩3. Q.E.D.
Directly follows by Inference Rule 14.20 from ⟨3⟩1 and ⟨3⟩2. □

$\langle 2 \rangle 3.$ $\neg\langle 12 \rangle \ \Box\!\!\rightarrow \neg(\langle 121 \rangle \wedge \langle 122 \rangle)$
In the nearest possible world they had not been near Brussels airport, since their destination was Frankfurt. Because their flightpath in that case had led from LATC area to MATC area they weren't supposed to be cleared to BATC.
Since they are assumed to follow the SOPs in the nearest possible world, they would have realized hints about a possible wrong course.

$\langle 2 \rangle 4.$ Q.E.D.
Follows by definition of "$\Box\!\!\Rightarrow$" and from steps $\langle 2 \rangle 1$ and $\langle 2 \rangle 3$. □

22.2.6 Proof of (121)

Nodes used in the following module:

(121) /* CRW did not realize that they were on wrong course, UNTIL:[111] */
{1211} /* CRW addresses BATC controller as "Frankfurt" several times */
⟨1212⟩ /* ILS has different frequency for Frankfurt. */
[1213] /* CRW asks for the Bruno VOR's frequency. */
(1214) /* Brussels did not question the addressing error although it happened more than once */
⟨1215⟩ /* Situation remains safe during landing */
⟨1216⟩ /* Current approach plates are used */

module *(121)_is_explained_causally_sufficient*

VARIABLES
extends *PARDIA−Axioms*
extends *PARDIA−Norms*
extends *Landing_Specs*
CONSTANTS $CRW, AC, ATC, BATC, BRU, FRA, this\_approach, freq$

$$Hypotheses \triangleq \land \{1211\} \land \langle 1212\rangle \land [1213] \land (1214) \land \langle 1215\rangle \land \langle 1216\rangle$$

$$Procedures \triangleq \land PARDIA{-}Axioms.Spec \land Landing\_Specs.Spec$$

THEOREM $(Hypotheses \land Procedures) \Box\!\!\Rightarrow \Diamond(121)$

PROOF:

⟨1⟩1. $\{1211\} \Leftrightarrow Perceive(BATC, addressing\_error(CRW, BATC))$
PROOF:
We claim, that the addressing error has not only been made but must also have been perceived, since this information wouldn't be in the sources otherwise.
⟨1⟩2. $\langle 1212\rangle \Leftrightarrow$
$$Attend(CRW, data\_inconsist(appr\_plate[this\_approach][LOC[freq]], appr\_plate[FRA][LOC[freq]]))$$
PROOF:
Since mentioned in the sources, the CRW must at least have paid attention to the fact of inconsistent data.
⟨1⟩3. $[1213] \Leftrightarrow Attend(CRW, BrunoVor[freq] \notin Navaids[appr\_plate[this\_approach]])$
PROOF:
From the fact, they asked for the Bruno VOR frequency, we can derive, that they at least attended that this information was not presented in the approach plate they used.
⟨1⟩4. $(1214) \Leftrightarrow \neg question(BATC, CRW, addressing\_error(CRW, BATC))$
PROOF:

We interpret (1214) as a state predicate.
⟨1⟩5. ⟨1215⟩ $\Leftrightarrow \wedge \Diamond(AC) lands\_at(BRU)$
$\wedge \Box\neg distress\_decl(CRW)$
$\wedge \Box\neg urgency\_decl(CRW)$
$\wedge \Box\neg endanger\_decl(CRW, TFC)$
PROOF:
Since we do not find contrary information in the sources, we may adopt ⟨1215⟩ as hypothesis.
⟨1⟩6. ⟨1216⟩ $\Leftrightarrow \wedge current(appr\_plate[this\_approach])$
$\wedge current(appr\_plate[FRA])$
PROOF:
Since we do not find contrary information in the sources, we may adopt ⟨1216⟩ as hypothesis.
⟨1⟩7. (121) $\Leftrightarrow \wedge O(Attend(CRW, APT \neq destAPT))$
$\wedge \neg Attend(CRW, APT \neq destAPT)$
PROOF:
(121) is a non-event and therefore we cannot simply express it as a state. According to the principle of contrastive explanation we need to state that some action awaited to be done was not executed.
⟨1⟩8. $(Hypotheses \wedge Procedures) \Box\!\!\Rightarrow \Diamond(121)$
⟨2⟩1. *Hypotheses*
PROOF:
⟨3⟩1. {1211}
PROOF:
{1211} under the interpretation of ⟨1⟩1 is true from the sources.
⟨3⟩2. ⟨1212⟩
PROOF:
⟨1212⟩ under the interpretation of ⟨1⟩2 is true from the sources.
⟨3⟩3. [1213]
PROOF:
[1213] under the interpretation of ⟨1⟩3 is true from the sources.
⟨3⟩4. (1214)
PROOF:
(1214) under the interpretation of ⟨1⟩4 is true from the sources.
⟨3⟩5. ⟨1215⟩
PROOF:
⟨1215⟩ under the interpretation of ⟨1⟩5 is true from the sources.
⟨3⟩6. ⟨1216⟩
PROOF:
⟨1216⟩ under the interpretation of ⟨1⟩6 is true from the sources.
⟨3⟩7. Q.E.D.
Follows by $(\wedge - intro)$ from ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5 and ⟨3⟩6. □
⟨2⟩2. *Procedures*
PROOF:
⟨3⟩1. $\wedge$ *PARDIA−Axioms.Spec*
$\wedge$ *Landing_Specs.Spec*
PROOF:
We assume that the procedures are implemented as specified in *PARDIA-Axioms.Spec* and *Landing_Specs.Spec.*
⟨2⟩3. $(Hypotheses \wedge \Box Procedures) \succ \Diamond(121)$
PROOF:
⟨3⟩1. $\vdash_{TLA} (Hypotheses \wedge \Box Procedures) \Rightarrow \Diamond(121)$
PROOF:

⟨4⟩1. (121) ⇒ ◇(121)

PROOF:

Follows by ◇-intro.

$$\langle 4\rangle 2.\ \begin{pmatrix} \wedge & \mathit{Perceive}(BATC, \mathit{addressing\_error}(CRW, BATC)) \\ \wedge & \mathit{Attend}(CRW, \mathit{data\_inconsist}(\mathit{appr\_plate}[\mathit{this\_approach}][LOC[\mathit{freq}]]), \\ & \qquad \mathit{appr\_plate}[FRA][LOC[\mathit{freq}]])) \\ \wedge & \mathit{Attend}(CRW, \mathit{BrunoVor}[\mathit{freq}] \notin \mathit{Navaids}[\mathit{appr\_plate}[\mathit{this\_approach}]]) \\ \wedge & \neg \mathit{question}(BATC, CRW, \mathit{addressing\_error}(CRW, BATC)) \\ \wedge & \mathit{current}(\mathit{appr\_plate}[\mathit{this\_approach}]) \\ \wedge & \mathit{current}(\mathit{appr\_plate}[FRA]) \\ \wedge & \Diamond(AC)\mathit{lands\_at}(BRU) \\ \wedge & \Box\neg \mathit{distress\_decl}(CRW) \\ \wedge & \Box\neg \mathit{urgency\_decl}(CRW) \\ \wedge & \Box\neg \mathit{endanger\_decl}(CRW, TFC) \\ \wedge & \Box \mathit{PARDIA{-}Axioms.Spec} \\ \wedge & \Box \mathit{Landing\_Specs.Spec} \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} \wedge & O(\mathit{Attend}(CRW, APT \neq \mathit{destAPT})) \\ \wedge & \neg \mathit{Attend}(CRW, APT \neq \mathit{destAPT}) \end{pmatrix}$$

PROOF:

$$\langle 5\rangle 1.\ \begin{pmatrix} \wedge & \Diamond(AC)\mathit{lands\_at}(BRU) \\ \wedge & \mathit{current}(\mathit{appr\_plate}[\mathit{this\_approach}]) \\ \wedge & \mathit{current}(\mathit{appr\_plate}[FRA]) \\ \wedge & \Box\neg \mathit{distress\_decl}(CRW) \\ \wedge & \Box\neg \mathit{urgency\_decl}(CRW) \\ \wedge & \Box\neg \mathit{endanger\_decl}(CRW, TFC) \\ \wedge & \Box \mathit{PARDIA{-}Axioms.Spec} \\ \wedge & \Box \mathit{Landing\_Specs.Spec} \end{pmatrix}$$

$$\Rightarrow \neg \mathit{Attend}(CRW, APT \neq \mathit{destAPT})$$

PROOF:

$$\langle 6\rangle 1.\ \begin{pmatrix} \wedge & \Box \mathit{Attend}(CRW, APT \neq \mathit{destAPT}) \\ \wedge & \Box\neg \mathit{distress\_decl}(CRW) \\ \wedge & \Box\neg \mathit{urgency\_decl}(CRW) \\ \wedge & \Box\neg \mathit{endanger\_decl}(CRW, TFC) \\ \wedge & \Box \mathit{PARDIA{-}Axioms.Spec} \\ \wedge & \Box \mathit{Landing\_Specs.Spec} \end{pmatrix} \Box\!\!\rightarrow \neg\Diamond(AC)\mathit{lands\_at}(APT)$$

PROOF:

$$\langle 7\rangle 1.\ \begin{pmatrix} \wedge & \Box \mathit{Attend}(CRW, APT \neq \mathit{destAPT}) \\ \wedge & \Box \mathit{PARDIA{-}Axioms.Spec} \end{pmatrix}$$

$$\Rightarrow APT \neq \mathit{destAPT}$$

PROOF:

This is an axiom (*PARDIA-Axioms.A12*)!

$$\langle 7\rangle 2.\ \begin{pmatrix} \wedge & APT \neq \mathit{destAPT} \\ \wedge & \Box\neg \mathit{distress\_decl}(CRW) \\ \wedge & \Box\neg \mathit{urgency\_decl}(CRW) \\ \wedge & \Box\neg \mathit{endanger\_decl}(CRW, TFC) \\ \wedge & \Box \mathit{Landing\_Specs.Spec} \end{pmatrix} \Rightarrow \neg\Diamond(AC)\mathit{lands\_at}(APT)$$

PROOF:

This is a rule (*Landing_Norms.Normal-Progress*).

⟨7⟩3. Q.E.D.

PARDIA-Axioms and *NormalProgress* hold in the nearest possible world, in which A holds. ⟨6⟩1 therefore follows by (∧-intro) from ⟨7⟩1 and ⟨7⟩2. □

⟨6⟩2. Q.E.D.

With: $A \triangleq Attend(CRW, APT \neq destAPT)$
$B \triangleq \Diamond(AC) lands\_at(APT)$

we can also derive $\neg B$ by a derived inference rule: $\dfrac{A \quad A \Box\!\!\rightarrow \neg B}{\neg B}$

But we know that B occurred.
Therefore by modus tollens we can derive $\neg A$. □

$$\langle 5\rangle 2. \begin{pmatrix} \wedge & Attend(CRW, data\_inconsist(appr\_plate[this\_approach][LOC[freq]]), \\ & \qquad appr\_plate[FRA][LOC[freq]])) \\ \wedge & current(appr\_plate[this\_approach]) \\ \wedge & current(appr\_plate[FRA]) \\ \wedge & \Box PARDIA\!-\!Axioms.Spec \\ \wedge & \Box Landing\_Specs.Spec \end{pmatrix} \Rightarrow O(Attend(CRW, apt \neq destAPT))$$

PROOF:

$\langle 6\rangle 1.$ $O(Procs)$

PROOF:

This is an EL-Axiom (cf. Axiom 10).

$$\langle 6\rangle 2. \begin{pmatrix} \wedge & Attend(CRW, data\_inconsist(appr\_plate[this\_approach][LOC[freq]]), \\ & \qquad appr\_plate[FRA][LOC[freq]])) \\ \wedge & current(appr\_plate[this\_approach]) \\ \wedge & current(appr\_plate[FRA]) \\ \wedge & \Box PARDIA\!-\!Axioms.Spec \\ \wedge & \Box Landing\_Specs.Spec \end{pmatrix} \Rightarrow Attend(CRW, APT \neq destAPT)$$

PROOF:

$$\langle 7\rangle 1. \begin{pmatrix} \wedge & Attend(CRW, data\_inconsist(appr\_plate[this\_approach][LOC[freq]], \\ & \qquad appr\_plate[FRA][LOC[freq]])) \\ \wedge & \Box PARDIA\!-\!Axioms.Spec \end{pmatrix} \Rightarrow data\_inconsist(appr\_plate[this\_approach][LOC[freq]], appr\_plate[FRA][LOC[freq]]))$$

PROOF:

This is an Axiom (*PARDIA-Axioms.A12*).

$$\langle 7\rangle 2. \begin{pmatrix} \wedge & data\_inconsist(appr\_plate[this\_approach][LOC[freq]], \\ & appr\_plate[FRA][LOC[freq]]) \\ \wedge & current(appr\_plate[this\_approach]) \\ \wedge & current(appr\_plate[FRA]) \\ \wedge & \Box Landing\_Specs.Spec \end{pmatrix} \Rightarrow (APT \neq destAPT)$$

PROOF:

This is a rule (*Landing_Norms.UniqueApproachPlates*).

$\langle 7\rangle 3.$ Q.E.D.

Follows by ($\wedge$-intro) from $\langle 7\rangle 1$ and $\langle 7\rangle 2$. □

$\langle 6\rangle 3.$ Q.E.D.

Follows from EL (SDL Rule K_O): $O(A \Rightarrow B) \Rightarrow (O(A) \Rightarrow O(B))$ □

$\langle 5\rangle 3.$ Q.E.D.

Follows by ($\wedge$-intro) from $\langle 5\rangle 1$ and $\langle 5\rangle 2$. □

$\langle 4\rangle 3.$ Q.E.D.

Insertion of interpretations from $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 1\rangle 5$, $\langle 1\rangle 6$, $\langle 2\rangle 2$ and $\langle 1\rangle 7$ into $\langle 3\rangle 1$. □

$\langle 3\rangle 2.$ Q.E.D.

Follows by definition of strict implication (Inference Rule 14.21). □

$\langle 2 \rangle 4.$ $\diamond(121)$
PROOF:
This is a fact explicitly given in the sources.
$\langle 2 \rangle 5.$ Q.E.D.
Directly follows by Inference Rule 15.7 from $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$ and $\langle 2 \rangle 4$. $\square$

22.2.7 Proof of Node 2

Nodes used in the following module:

⟨2⟩ /* AC in BATC area */
⟨3⟩ /* AC in LATC area */
⟨21⟩ /* LATC procedures */
⟨22⟩ /* LATC uses false flight data for NW052 */

module *⟨2⟩_is_explained_causally_sufficient*

VARIABLES
extends *SOP_Specs*
CONSTANTS $AC, BATC, LATC$

$$Hypotheses \triangleq \wedge \langle 22\rangle \quad \wedge \langle 3\rangle$$
$$Procedures \triangleq \langle 21\rangle$$

THEOREM $(Hypotheses \wedge Procedures) \;\Box\!\!\Rightarrow \Diamond\langle 2\rangle$

PROOF:

$$\langle 1\rangle 1.\ \langle 22\rangle \Leftrightarrow \begin{pmatrix} \wedge & fdata(ac)[destAPT] = \text{`}BRU\text{`} \\ \wedge & nextATC(AC) = BATC \\ \wedge & responsibleATC(\text{`}BRU\text{`}) = BATC \\ \wedge & destAPT(AC) = \text{`}FRA\text{`} \end{pmatrix}$$

PROOF:
We interpret "false flightdata" as deviation of the used data - determined (det) from the ATCs FDC - from the original data. All we use from the flighdata is the information on the AC's destination airport. This piece of information usually suffices to calculate a flight route containing the start and landing ATCCs as well as all intermediate ATCCs. We do not specify this process at this point and define this information as a part of the conjunct describing ⟨22⟩ instead.

$\langle 1\rangle 2.\ \langle 3\rangle \Leftrightarrow (AC)in\_area(LATC)$
PROOF:
We interpret ⟨3⟩ as a state predicate.

$\langle 1\rangle 3.\ \langle 21\rangle \Rightarrow SOP\_Specs.ATC\text{−}Responsibility\text{−}Rule$
PROOF:
In the sources the *Procedures* are assumed to be implemented correctly. We claim *SOP_Specs.ATC−Responsibilit*
is sufficient to explain the ATC procedures significant for this case.

$\langle 1\rangle 4.\ (Hypotheses \wedge Procedures) \;\Box\!\!\Rightarrow \Diamond\langle 2\rangle$
⟨2⟩1. *Hypotheses*
PROOF:
⟨3⟩1. ⟨22⟩
PROOF:
⟨22⟩ under the interpretation of ⟨1⟩1 is true from the sources.

⟨3⟩2. ⟨3⟩
PROOF:
⟨3⟩ under the interpretation of ⟨1⟩2 is true from the sources.
⟨3⟩3. Q.E.D.
∧-intro from ⟨3⟩1 and ⟨3⟩2. □

⟨2⟩2. *Procedures*
PROOF:
⟨3⟩1. ⟨21⟩
PROOF:
⟨21⟩ under the interpretation of ⟨1⟩3 is true from the sources.
⟨3⟩2. Q.E.D.
Follows immediately from ⟨3⟩1. □

⟨2⟩3. $(\mathit{Hypotheses} \wedge \Box \mathit{Procedures}) \succ \Diamond \langle 2 \rangle$
PROOF:
⟨3⟩1. $\vdash_{TLA} (\mathit{Hypotheses} \wedge \Box \mathit{Procedures}) \Rightarrow \Diamond \langle 2 \rangle$
PROOF:
We argue in the forward sense of natural deduction.
We reformulate this expression in logic. Formulation of the goal as well as use of the logical equivalents defined above results in:

$$\langle 4 \rangle 1. \quad \begin{pmatrix} \wedge & \mathit{fdata}(ac)[\mathit{destAPT}] = \text{‘}\mathit{BRU}\text{‘} \\ \wedge & \mathit{nextATC}(AC) = \mathit{BATC} \\ \wedge & \mathit{responsibleATC}(\text{‘}\mathit{BRU}\text{‘}) = \mathit{BATC} \\ \wedge & \mathit{destAPT}(AC) = \text{‘}\mathit{FRA}\text{‘} \\ \wedge & (AC)\mathit{in\_area}(\mathit{LATC}) \\ \wedge & \Box \mathit{ATC{-}Responsibility{-}Rule} \end{pmatrix} \Rightarrow \Diamond (AC)\mathit{in\_area}(\mathit{BATC})$$

PROOF:

$$\langle 5 \rangle 1. \quad \begin{pmatrix} \wedge & \mathit{fdata}(ac)[\mathit{destAPT}] = \text{‘}\mathit{BRU}\text{‘} \\ \wedge & \mathit{nextATC}(AC) = \mathit{BATC} \\ \wedge & \mathit{responsibleATC}(\text{‘}\mathit{BRU}\text{‘}) = \mathit{BATC} \\ \wedge & \mathit{destAPT}(AC) = \text{‘}\mathit{FRA}\text{‘} \\ \wedge & (AC)\mathit{in\_area}(\mathit{LATC}) \\ \wedge & \Box \mathit{SOP\_Specs.ATC{-}Responsibility{-}Rule} \end{pmatrix} \Rightarrow \Diamond \mathit{Handoff}(\mathit{LATC}, \mathit{BATC}, AC)$$

PROOF:

$$\langle 6 \rangle 1. \quad \begin{pmatrix} \wedge & (AC)\mathit{in\_area}(\mathit{LATC}) \\ \wedge & \Box \mathit{ATC{-}Responsibility{-}Rule} \end{pmatrix} \Rightarrow \mathit{EnRouteProcessing}(\mathit{LATC}, AC)$$

PROOF:
Follows by STL2 and Propositional Logic from
SOP_Specs.ATC-Responsibility-Rule.

$$\langle 6 \rangle 2. \quad \begin{pmatrix} \wedge & \mathit{EnRouteProcessing}(\mathit{LATC}, AC) \\ \wedge & (AC)\mathit{in\_area}(\mathit{LATC}) \\ \wedge & \mathit{fdata}(ac)[\mathit{destAPT}] = \text{‘}\mathit{BRU}\text{‘} \\ \wedge & \mathit{nextATC}(AC) = \mathit{BATC} \\ \wedge & \mathit{responsibleATC}(\text{‘}\mathit{BRU}\text{‘}) = \mathit{BATC} \\ \wedge & \mathit{destAPT}(AC) = \text{‘}\mathit{FRA}\text{‘} \end{pmatrix} \Rightarrow \Diamond \mathit{Handoff}(\mathit{LATC}, \mathit{BATC}, AC)$$

PROOF:

$$\langle 7 \rangle 1. \quad \begin{pmatrix} \wedge & \mathit{det\_destAPT}(AC) = \text{‘}\mathit{BRU}\text{‘} \\ \wedge & \mathit{fdata}(ac)[\mathit{destAPT}] = \text{‘}\mathit{BRU}\text{‘} \end{pmatrix}$$
$$\Rightarrow \mathit{det\_destAPT}(AC) = \mathit{fdata}(AC)[\mathit{destAPT}]$$

PROOF:
Follows by SOP_Specs.DetermineDestinationProcedure.

⟨7⟩2. $\begin{pmatrix} \wedge & det\_destAPT(AC) = \text{`}BRU\text{`} \\ \wedge & fdata(ac)[destAPT] = \text{`}BRU\text{`} \end{pmatrix} \Rightarrow LATC \neq det\_destATC(AC)$

PROOF:

⟨8⟩1. $\begin{pmatrix} \wedge & det\_destAPT(AC) = \text{`}BRU\text{`} \\ \wedge & responsibleATC(\text{`}BRU\text{`}) = BATC \end{pmatrix} \Rightarrow (det\_destATC(AC) = BATC)$

PROOF:
Follows immediately from *SOP_SPECS.RespDestATC_Determination_Rule*.

⟨8⟩2. $BATC \neq LATC$

PROOF:
We now from the sources that this is true.

⟨8⟩3. Q.E.D.
Follows by Propositional Logic from ⟨8⟩1 and ⟨8⟩2.

⟨7⟩3. $\begin{pmatrix} \wedge & EnRouteProcessing(LATC, AC) \\ \wedge & (AC)in\_area(LATC) \\ \wedge & det\_destAPT(AC) = fdata(AC)[destAPT] \\ \wedge & LATC \neq det\_destATC(AC) \end{pmatrix}$
$\Rightarrow \Diamond Handoff(LATC, nextATC, AC)$

PROOF:
Follows by Propositional Logic. □

⟨7⟩4. $\begin{pmatrix} \wedge & \Diamond Handoff(LATC, nextATC(AC), AC)) \\ \wedge & nextATC(AC) = BATC \end{pmatrix} \Rightarrow \Diamond Handoff(LATC, BATC, AC)$

PROOF:
Follows by Propositional Logic. □

⟨7⟩5. Q.E.D.
Follows by Propositional Logic (transitivity of ⇒) from ⟨7⟩1, ⟨7⟩2, ⟨7⟩3 and ⟨7⟩4. □

⟨6⟩3. Q.E.D.
Follows by Propositional logic from ⟨6⟩1 and ⟨6⟩2. □

⟨5⟩2. $\Diamond Handoff(LATC, BATC, AC) \Rightarrow \Diamond(AC)in\_area(BATC)$

PROOF:

⟨6⟩1. $\Diamond \begin{pmatrix} \wedge & (AC)in\_area(LATC) \\ \wedge & (AC)in\_area(BATC) \\ \wedge & nextATC(AC) = BATC \\ \wedge & \Diamond \begin{pmatrix} \wedge & \neg(AC)in\_area(LATC) \\ \wedge & (AC)in\_area(BATC) \end{pmatrix} \\ \wedge & \begin{pmatrix} \vee & ATCcomm\_history.Handoff_{correct}(LATC, BATC, fid(AC)) \\ \vee & ATCcomm\_history.Handoff_{incorrect}(LATC, BATC, fid(AC)) \end{pmatrix} \end{pmatrix}$
⇒◇(AC)in_area(BATC)

PROOF:
Follows immediately by Propositional Logic.

⟨6⟩2. Q.E.D.

PROOF:
Insertion of definition of *SOP_Specs.Handoff*$(LATC, BATC, AC)$ into ⟨5⟩2.

⟨5⟩3. Q.E.D.
Follows by Propositional logic from ⟨5⟩1 and ⟨5⟩2. □

⟨4⟩2. Q.E.D.
Insertion of interpretations from ⟨1⟩1, ⟨1⟩2, and ⟨1⟩3 into ⟨2⟩3. □

⟨3⟩2. Q.E.D.
Follows by definition of strict implication (inference rule 14.21). □
⟨2⟩4. $\diamond\langle 2\rangle$
PROOF:
This is a fact explicitly given in the sources.
⟨2⟩5. $\Box\neg\langle 2\rangle \;\Box\!\!\rightarrow \neg(\mathit{Hypotheses} \wedge \mathit{Procedures})$
PROOF:

$$\langle 3\rangle 1.\ \Box\neg(AC)\mathit{in\_area}(BATC)\ \Box\!\!\rightarrow \begin{pmatrix} \vee & \neg(AC)\mathit{in\_area}(LATC) \\ \vee & \neg \mathit{SOP\_Specs.ATC\text{--}Responsibility\text{--}Rule} \\ \vee & \neg \mathit{fdata}(ac)[\mathit{destAPT}] = \text{`}BRU\text{`} \\ \vee & \neg \mathit{nextATC}(AC) = BATC \\ \vee & \neg \mathit{responsibleATC}(\text{`}BRU\text{`}) = BATC \\ \vee & \neg \mathit{destAPT}(AC) = \text{`}FRA\text{`} \end{pmatrix}$$

PROOF:
We argue, that in the nearest possible world the flight data is wrong at BATC. Under this assumption, all possible consequences $(\neg \mathit{fdata}(ac)[\mathit{destAPT}] = \text{`}BRU\text{`})$, $(\neg \mathit{nextATC}(AC) = BATC)$, $(\neg \mathit{responsibleATC}(\text{`}BRU\text{`}) = BATC)$ and $(\neg \mathit{destAPT}(AC) = \text{`}FRA\text{`})$ will lead to $\neg(AC)\mathit{in\_area}(BATC)$.
⟨3⟩2. Q.E.D.
Follows by Propositional Logic, STL2 and STL3 as well as use of definitions from ⟨2⟩1 and ⟨2⟩2.
⟨2⟩6. Q.E.D.
Directly follows by Inference Rule 15.7 from ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4. □and ⟨2⟩5. □

Remarks:

Possible to specify FDP-Procedures as a table based on *Letters of agreement* between ATCCs. (Example Nolan p.413)

22.2.8 Proof of Node 22

Nodes used in the following module:

⟨22⟩ /* LATC uses false flight data for NW052 */
[221] /* London received false data from SATC */

module *⟨22⟩_is_explained_causally_sufficient*

VARIABLES
extends *This_ATCcomm_history*

THEOREM [221] □⇒ ⟨22⟩

PROOF:

⟨1⟩1. [221] □⇒ ⟨22⟩
⟨2⟩1. [221] ⇛ ⟨22⟩
PROOF:
⟨3⟩1. [221] ∧ ⟨22⟩
PROOF:
⟨4⟩1. [221]
PROOF: This is a fact assumed in the sources.
⟨4⟩2. ⟨22⟩
PROOF: This is a fact assumed in the sources.
⟨4⟩3. Q.E.D.
(∧-introduction) from ⟨4⟩1 and ⟨4⟩2. □
⟨3⟩2. ¬[221] □→ ¬⟨22⟩
PROOF:
⟨4⟩1. PROOF:
In the nearest possible world the transfer of flight data would have occurred as specified in TLA-module *This_ATCcomm_history*. Assuming a correct transmission (¬[221]), we can derive:

$$\begin{aligned} \neg[221] &\Rightarrow StoL_{correct} \\ &\Rightarrow \text{UNCHANGED } persistent\_data \\ &\Rightarrow \neg\langle 22\rangle \end{aligned}$$

⟨3⟩3. Q.E.D.
Directly follows by Inference Rule 14.20 from ⟨3⟩1 and ⟨3⟩2. □
⟨2⟩2. ¬⟨22⟩ □→ ¬[221]
In the nearest possible world transmitting correct data is greater more probable than making several incorrect handoffs resulting in finally the same correct flightdata. According to the specification of *This_ATCcomm_history*, we can infer:

$$\neg\langle 22\rangle \Rightarrow persistent\_data[destination]' = \text{“FRA”}$$

Therefore:

$$\begin{aligned} \begin{pmatrix} \wedge & persistent\_data[destination]' = \text{“FRA”} \\ \wedge & persistent\_data[destination] = \text{“FRA”} \end{pmatrix} &\Rightarrow \text{UNCHANGED } persistent\_data \\ &\Rightarrow StoL_{correct} \\ &\Rightarrow \neg[221] \end{aligned}$$

$\langle 2 \rangle 3$. Q.E.D.
Follows by definition of "$\Box\!\!\Rightarrow$" and from steps $\langle 2 \rangle 1$ and $\langle 2 \rangle 2$. $\Box$

22.2.9 Proof of Node 3

Nodes used in the following module:

$\langle 3 \rangle$ /* AC in LATC area */
$\langle 31 \rangle$ /* SATC handoff procedures under this flightplan are to LATC */
$\langle 32 \rangle$ /* FI is correct at SATC */
$\langle 4 \rangle$ /* AC in SATC area */

module $\langle 3 \rangle$*_is_explained_causally_sufficient*

VARIABLES
extends *SOP_Specs*
CONSTANTS $AC, destAPT, APT, SATC, LATC, BATC$

$$Hypotheses \triangleq \land \langle 32 \rangle \quad \land \langle 4 \rangle$$
$$Procedures \triangleq \langle 31 \rangle$$

THEOREM $(Hypotheses \land Procedures) \square\!\!\Rightarrow \Diamond\langle 3 \rangle$

PROOF:

$$\langle 1 \rangle 1.\ \langle 32 \rangle \Leftrightarrow \begin{pmatrix} \land & fdata(ac)[destAPT] = det\_destATP(AC) \\ & = destAP(AC) = \text{'}FRA\text{'} \\ \land & nextATC(AC) = LATC \\ \land & responsibleATC(\text{'}BRU\text{'}) = BATC \end{pmatrix}$$

PROOF:
All we use from the flighdata is the information on the AC's destination airport. This piece of information usually suffices to calculate a flight route containing the start and landing ATCCs as well as all intermediate ATCCs. We do not specify this process at this point and define this information as a part of the conjunct describing $\langle 32 \rangle$ instead.

$\langle 1 \rangle 2.\ \langle 4 \rangle \Leftrightarrow (AC)in\_area(SATC)$
PROOF:
We interpret $\langle 4 \rangle$ as a state predicate.

$$\langle 1 \rangle 3.\ \langle 31 \rangle \Leftrightarrow \begin{pmatrix} \land & nextATC(AC) = LATC \\ \land & SOP\_Specs.Spec \end{pmatrix}$$

PROOF:
Our interpretation of $\langle 31 \rangle$ is that generally the procedures are followed as specified in *SOP_Specs* that therefore the next ATCC the flightdata will be sent to, is LATC.
$\langle 1 \rangle 4.\ (Hypotheses \land Procedures) \square\!\!\Rightarrow \Diamond\langle 3 \rangle$
$\langle 2 \rangle 1.$ *Hypotheses*
PROOF:
$\langle 3 \rangle 1.\ \langle 32 \rangle$
PROOF:
$\langle 32 \rangle$ under the interpretation of $\langle 1 \rangle 1$ is true from the sources.
$\langle 3 \rangle 2.\ \langle 3 \rangle$
PROOF:

⟨4⟩ under the interpretation of ⟨1⟩2 is true from the sources.
⟨3⟩3. Q.E.D.
$\wedge$-intro from ⟨3⟩1 and ⟨3⟩2. □

⟨2⟩2. *Procedures*
PROOF:
⟨3⟩1. ⟨31⟩
PROOF:
⟨31⟩ under the interpretation of ⟨1⟩3 is true from the sources.
⟨3⟩2. Q.E.D.
Follows immediately from ⟨3⟩1. □

⟨2⟩3. $(Hypotheses \wedge \Box Procedures) \succ \Diamond\langle 3\rangle$
PROOF:
⟨3⟩1. $\vdash_{TLA} (Hypotheses \wedge \Box Procedures) \Rightarrow \Diamond\langle 3\rangle$
PROOF:
We argue in the forward sense of natural deduction.
We reformulate this expression in logic. Formulation of the goal as well as use of the logical equivalents defined above results in:

$$\langle 4\rangle 1.\quad \begin{pmatrix} \wedge & fdata(ac)[destAPT] = det\_destATP(AC) \\ & = destAP(AC) = \text{‘}FRA\text{‘} \\ \wedge & nextATC(AC) = LATC \\ \wedge & responsible\_atc(\text{‘}BRU\text{‘}) = BATC \\ \wedge & (AC)in\_area(SATC) \\ \wedge & \Box nextATC(AC) = LATC \\ \wedge & \Box SOP\_Specs.Spec \end{pmatrix} \Rightarrow \Diamond(AC)in\_area(LATC)$$

PROOF:

$$\langle 5\rangle 1.\quad \begin{pmatrix} \wedge & fdata(ac)[destAPT] = det\_destATP(AC) \\ & = destAP(AC) = \text{‘}FRA\text{‘} \\ \wedge & nextATC(AC) = LATC \\ \wedge & responsible\_atc(\text{‘}BRU\text{‘}) = BATC \\ \wedge & (AC)in\_area(SATC) \\ \wedge & \Box nextATC(AC) = LATC \\ \wedge & \Box SOP\_Specs.Spec \end{pmatrix} \\ \Rightarrow \Diamond Inter\_ATC\_Handoff(SATC, LATC, AC)$$

PROOF:

$$\langle 6\rangle 1.\quad \begin{pmatrix} \wedge & (AC)in\_area(SATC) \\ \wedge & \Box SOP\_Specs.Spec \end{pmatrix} \Rightarrow EnRouteProcessing(SATC, AC)$$

PROOF:
Follows by STL2 and Propositional Logic from *SOP_Specs.ATC-Responsibility-Rule.*

$$\langle 6\rangle 2.\quad \begin{pmatrix} \wedge & EnRouteProcessing(SATC, AC) \\ \wedge & fdata(ac)[destAPT] = det\_destATP(AC) \\ & = destAP(AC) = \text{‘}FRA\text{‘} \\ \wedge & nextATC(AC) = LATC \\ \wedge & responsible\_atc(\text{‘}BRU\text{‘}) = BATC \\ \wedge & (AC)in\_area(SATC) \\ \wedge & \Box nextATC(AC) = LATC \\ \wedge & \Box SOP\_Specs.Spec \end{pmatrix} \\ \Rightarrow \Diamond Inter\_ATC\_Handoff(SATC, LATC, AC)$$

PROOF:

$\langle 7\rangle 1.$ $(fdata(ac)[destAPT] = det\_destATP(AC) = destAP(AC) = \text{`}FRA\text{`}) \Rightarrow SATC \neq det\_destATC(AC)$

PROOF:

$$\langle 8\rangle 1. \begin{pmatrix} \wedge & fdata(ac)[destAPT] = det\_destATP(AC) \\ & = destAP(AC) = \text{`}FRA\text{`} \\ \wedge & responsible\_atc(\text{`}BRU\text{`}) = BATC \end{pmatrix} \Rightarrow (det\_destATC(AC) = BATC)$$

PROOF:

Follows immediately from $SOP\_Specs.RespDestATC\_Determination\_Rule$.

$\langle 8\rangle 2.$ $BATC \neq SATC$

PROOF:

We now from the sources that this is true.

$\langle 8\rangle 3.$ Q.E.D.

PROOF:Follows by Propositional Logic from $\langle 8\rangle 1$ and $\langle 8\rangle 2$.

$$\langle 7\rangle 2. \begin{pmatrix} \wedge & EnRouteProcessing(SATC, AC) \\ \wedge & (AC)in\_area(SATC) \\ \wedge & fdata(ac)[destAPT] = det\_destATP(AC) \\ & = destAP(AC) = \text{`}FRA\text{`} \\ \wedge & SATC \neq det\_destATC(AC) \end{pmatrix} \Rightarrow \Diamond Inter\_ATC\_Handoff(SATC, nextATC, AC)$$

PROOF:

Follows by Propositional Logic. □

$$\langle 7\rangle 3. \begin{pmatrix} \wedge & \Diamond Inter\_ATC\_Handoff(SATC, nextATC(AC), AC)) \\ \wedge & \Box nextATC(AC) = LATC \end{pmatrix} \Rightarrow \Rightarrow \Diamond Inter\_ATC\_Handoff(SATC, LATC, AC)$$

PROOF:

Follows by STL2 and Propositional Logic. □

$\langle 7\rangle 4.$ Q.E.D.

Follows by Propositional Logic (transitivity of $\Rightarrow$) from $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 7\rangle 3$. □

$\langle 6\rangle 3.$ Q.E.D.

Follows by Propositional logic from $\langle 6\rangle 1$ and $\langle 6\rangle 2$. □

$\langle 5\rangle 2.$ $\Diamond Inter\_ATC\_Handoff(SATC, LATC, AC) \Rightarrow \Diamond(AC)in\_area(LATC)$

PROOF:

$$\langle 6\rangle 1. \Diamond \begin{pmatrix} \wedge & (AC)in\_area(SATC) \\ \wedge & (AC)in\_area(LATC) \\ \wedge & \Box nextATC(AC) = LATC \\ \wedge & \Diamond \begin{pmatrix} \wedge & \neg(AC)in\_area(SATC) \\ \wedge & (AC)in\_area(LATC) \end{pmatrix} \\ \wedge & \begin{pmatrix} \vee & ATCcomm\_history.Handoff_{correct}(SATC, LATC, fid(AC)) \\ \vee & ATCcomm\_history.Handoff_{incorrect}(SATC, LATC, fid(AC)) \end{pmatrix} \end{pmatrix} \Rightarrow \Diamond\text{(AC)in\_area(LATC)}$$

PROOF:

Follows immediately by Propositional Logic.

$\langle 6\rangle 2.$ Q.E.D.

PROOF:

Insertion of definition of $SOP\_Specs.Inter\_ATC\_Handoff(SATC, LATC, AC)$ into $\langle 5\rangle 2$.

$\langle 5\rangle 3.$ Q.E.D.

Follows by Propositional logic from $\langle 5\rangle 1$ and $\langle 5\rangle 2$. □

$\langle 4\rangle 2.$ Q.E.D.

Insertion of interpretations from $\langle 1\rangle 1$, $\langle 1\rangle 2$, and $\langle 1\rangle 3$ into $\langle 2\rangle 3$. □

$\langle 3\rangle 2$. Q.E.D.

Follows by definition of strict implication (inference rule 14.21). □

$\langle 2\rangle 4$. $\Diamond\langle 3\rangle$

PROOF:

This is a fact explicitly given in the sources.

$\langle 2\rangle 5$. Q.E.D.

Directly follows by Inference Rule 15.7 from $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$ and $\langle 2\rangle 4$. □

22.2.10 The Full Explanations

Finally we can summarize all *proof obligations* (assumptions we made for the proof). Given the truth of these assumptions, *it follows by logic alone* that the explanation of the incident we gave is correct and sufficient.

module *Proof-Obligations*

THEOREM
History $\langle 4\rangle \hookrightarrow \langle 3\rangle \hookrightarrow \langle 2\rangle \hookrightarrow [1]$ *is completely explained (according to our definitions),* **iff**

1. *our specifications are sufficient to explain the part of the world we needed to focus on. We defined*
   - *A Hierarchy of Communication Procedures:*
     - *ATCtrans:*
       Specification of the communication channel between ATCCs.
     - *ATCproc:*
       Specification of low level communication functions of one ATCC.
     - *ATCcomm:*
       Specification of medium level communication functions (Handoff) from one ATCC to another.
     - *ATCcomm_history:*
       Specification of higher level communication functions between ATCCs.
     - *This_ATCcomm_history:*
       Specification of higher level communication functions between ATCCs for this special history.
   - *Cognitive Procedures:*
     - *PARDIA_Axioms:*
       Specification of axioms stating the relationships between the attitudes of the PARDIA model.
     - *PARDIA_Norms:*
       Specification of certain PARDIA principles which are intended to hold.
   - *Standard Operating Procedures (SOPs):*
     - *AC_ATC_comm.spec:*
       Specification of Communication Procedures between Aircrafts and ATCCs.
     - *Landing_Axioms:*
       General specification of domain rules, which are valid at all times.

  - *Landing_Norms:*
    Specification of SOPs concerning the landing.
  - *Landing_Specs:*
    Specification of rules to be kept in the landing phase (mainly Landing_Axioms and Landing_Norms).
  - *SOP_Specs:*
    Specifiation of the part of SOPs that covers an ATCCs responsibility for evaluation and transmission of flight data.
- *TLA-Specifications of mathematical functions which describe the behaviour of physical flight parameters over a peroid of time, like altitude for example:*
  - *RealTimeTheorems*

2. *these specifications are fullfilled in every case in which no contrary information is explicitly given.*

3. *our TLA interpretions of the text correspond sufficiently to the reality. We assumed:*

   - $\Box\neg ATC\_breakoff$
   - $[11] \Leftrightarrow Decide(CRW, \Box(AC)in\_landing\_phase)$
   - $\langle 12\rangle \Rightarrow (AC)near(BRU)$
   - $[111] \Rightarrow (APT \neq destAPT)$
   - $[1111] \Leftrightarrow \Diamond visual\_contact(crw, apt)$
   - $[11111] \Leftrightarrow below\_clouds(ac)$
   - $\langle 11112\rangle \Leftrightarrow \wedge\ ILS\_approach(ac, apt)$
     $\qquad\qquad\quad \wedge\ \Box\neg CRW\_breakoff(crw, appr)$
   - $\langle 2\rangle \Leftrightarrow (ac)in\_area(atc)$
   - $\langle 21\rangle \Rightarrow SOP\_Specs.ATC{-}Responsibility{-}Rule$
     In the sources the Procedures are assumed to be implemented correctly. We claim SOP_Specs.ATC–Responsibility–Rule is sufficient to explain the ATC procedures significant for this case.
   - $\langle 22\rangle \Leftrightarrow \begin{pmatrix} \wedge & fdata(ac)[destAPT] = \text{‘}BRU\text{‘} \\ \wedge & nextATC(AC) = BATC \\ \wedge & responsibleATC(\text{‘}BRU\text{‘}) = BATC \\ \wedge & destAPT(AC) = \text{‘}FRA\text{‘} \end{pmatrix}$
     We interpret "false flightdata" as deviation of the used data - determined from the ATCs FDC - from the original data. All we use from the flightdata is the information on the AC's destination airport. This piece of information usually suffices to calculate a flight

route containing the start and landing ATCCs as well as all intermediate ATCCs. We do not specify this process at this point and define this information as a part of the conjuncts describing $\langle 22\rangle$ *and* $\langle 32\rangle$ *instead.*

- $\langle 3\rangle \Leftrightarrow (AC)in\_area(LATC)$
- $\langle 31\rangle \Leftrightarrow \begin{pmatrix} \wedge & nextATC(AC) = LATC \\ \wedge & SOP\_Specs.Spec \end{pmatrix}$
  Our interpretation of $\langle 31\rangle$ *is that generally the procedures are followed as specified in SOP_Specs that therefore the next ATCC the flightdata will be sent to, is LATC.*
- $\langle 4\rangle \Leftrightarrow (AC)in\_area(SATC)$

4. *several assumptions used in the modal part of proofs of* [111], $\langle 12\rangle$ *and* $\langle 22\rangle$ *are correct:*

   - *Instruments providing the information necessary to determine the position without visual contact were ignored. Therefore the only other way to obtain this information is visual contact. - (used in*[111]*)*
   - *The evidence of the instruments was ignored. Thus, if they hadn't recognized the layout they saw was different from the expected (flight documents contain 2D maps of the fact of the destination airport) they wouldn't have recognized their mistake at that time.- (used in*[111]*)*
   - *No use of evidence from instrumentation was made. If neither* [1111] *nor* {1112} *then no evident was available that could call their attention to the wrong airport.- (used in*[111]*)*
   - *The flight destination was Frankfurt. If the Crew had realized they were on the wrong course, they would likely have taken actions to return to the course they were supposed to be on unless other more pressing considerations intervened.- (used in*$\langle 12\rangle$*)*
   - *In this particular case we assume that an AC only enters a specific area when it has obtained an ATC clearance before. Therefore without a clearance to BATC area the AC will not be able to get into Brussels Airport area.- (used in*$\langle 12\rangle$*)*
   - *Since they are assumed to follow the SOPs in the nearest possible world, they would have realized hints about a possible wrong course.- (used in*$\langle 12\rangle$*)*

22.3 The Final WB-Graph

Given the proof we just finished, we're now able to provide the textual and pictorial form of the causally sufficient WB-Graph, in Figure 22.4 and Figure 22.5 respectively.

module *WB-Graph_is_causally_sufficient*

DECLARATION

$[1]\_suff \triangleq$ **instance** $[1]\_is\_explained\_causally\_sufficient$
$[11]\_suff \triangleq$ **instance** $[11]\_is\_explained\_causally\_sufficient$
$[111]\_suff \triangleq$ **instance** $[111]\_is\_explained\_causally\_sufficient$
$[1111]\_suff \triangleq$ **instance** $[111]\_is\_explained\_causally\_sufficient$
$\langle 12\rangle\_suff \triangleq$ **instance** $\langle 1112\rangle\_is\_explained\_causally\_sufficient$
$(121)\_suff \triangleq$ **instance** $(11121)\_is\_explained\_causally\_sufficient$
$\langle 2\rangle\_suff \triangleq$ **instance** $\langle 2\rangle\_is\_explained\_causally\_sufficient$
$\langle 22\rangle\_suff \triangleq$ **instance** $\langle 22\rangle\_is\_explained\_causally\_sufficient$
$\langle 3\rangle\_suff \triangleq$ **instance** $\langle 3\rangle\_is\_explained\_causally\_sufficient$

DEFINITION

THEOREM $\wedge$ $[1]\_suff$.THEOREM
$\wedge$ $[11]\_suff$.THEOREM
$\wedge$ $[111]\_suff$.THEOREM
$\wedge$ $[1111]\_suff$.THEOREM
$\wedge$ $\langle 12\rangle\_suff$.THEOREM
$\wedge$ $(121)\_suff$.THEOREM
$\wedge$ $\langle 2\rangle\_suff$.THEOREM
$\wedge$ $\langle 22\rangle\_suff$.THEOREM
$\wedge$ $\langle 3\rangle\_suff$.THEOREM

Figure 22.3: Top-Level Module of the Proof

```
[1] /* AC lands at Brussels RWY 25 */
  /\[-.1] /* CRW opts to continue landing */
  /\<-.2> /* AC near Brussels Airport */

  [1.1] /\[-.1] /* CRW realizes they are landing at the wrong airport */
        /\<-.2> /* CRW has safety reasons for continuing landing */
        /\[-.3] /* Standard Operating Procedures */

    [1.1.1] /\[-.1] /* CRW gets visual contact to Brussels airport */
            /\{-.2} /* CRW notices that Brussels' airport layout is different
                       from Frankfurt's */
      [1.1.1.1]  /\[-.1] /* AC breaks out under clouds */
                 /\<-.2> /* CRW procedures */
                 /\<1.2>
                 /\<2>   /* AC in BATC area */

        <2> /\<-.1> /* LATC procedures */
            /\<-.2> /* LATC uses false flight data for NW052 */
            /\<3>   /* AC in LATC area */

          <2.2> [-.1] /* London received false data from SATC */

          <3> /\<-.1> /* SATC handoff procedures under this flightplan
                         are to LATC */
              /\<-.2> /* FI is correct at SATC */
              /\<4>   /* AC in SATC area */

  <1.2> /\(-.1) /* CRW did not realize that they were on wrong course,
                   UNTIL:[111] */
        /\<-.2> /* AC cleared to BATC according to ATC procedures */

    (1.2.1) /\{-.1} /* CRW addresses BATC controller as ``Frankfurt''
                       several times */
            /\<-.2> /* ILS has different frequency for Frankfurt. */
            /\[-.3] /* CRW asks for the Bruno VOR's frequency. */
            /\(-.4) /* Brussels did not question the addressing error
                       although it happened more than once */
            /\<-.5> /* Situation remains safe during landing */
            /\<-.6> /* Current approach plates are used */
```

Figure 22.4: Textual form of the final WB-Graph

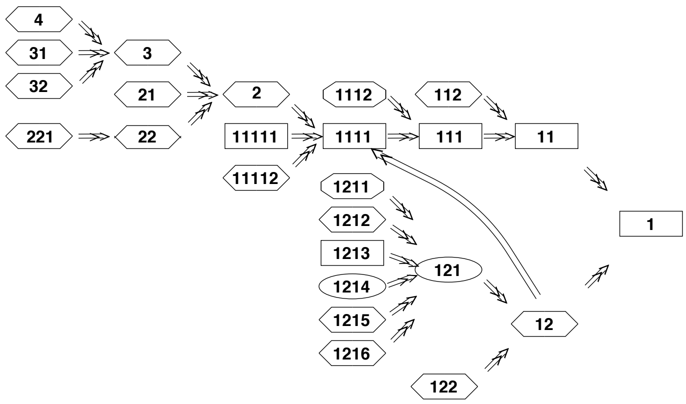

Figure 22.5: Pictorial form of the final WB-Graph