Safety Documentation

MECHTRON 3K04 Assignment 2
Group 4
Andrew De Rango, Ali Hussin, Ethan Otteson,
Marco Tan, Rafael Toameh
Friday, November 29, 2024

Table of Contents

1 Scope

This document outlines the primary safety objectives accomplished throughout the HeartFlow Pacemaker System project. The safety objectives ensure that the pacemaker system operates reliably, mitigates risk, and adheres to relevant standards. To achieve this, comprehensive safety analyses and validation activities were conducted. These include the completion of a Hazard and Operability Study (HAZOP), a Fault Tree Analysis (FTA), and an Assurance Case. These methodologies were applied to systematically identify, analyze, and address potential hazards and failure scenarios that could compromise the safety or reliability of the system.

The HAZOP facilitated the structured examination of the system's design to identify deviations from intended functionality and assess their potential impacts. The FTA further complemented this analysis by tracing potential hazards back to their root causes, providing a clear understanding of failure modes and their interrelationships. Finally, the assurance case demonstrated that the HeartFlow Pacemaker System is safe and reliable in its intended environment by integrating evidence from the HAZOP, FTA, and other safety activities into a cohesive argument.

This document serves as a summary of these efforts and highlights the mitigations implemented to address identified hazards. These include design improvements, robust testing protocols, and compliance with desired standards. Details of the mitigations are outlined in the relevant sections of the Pacemaker Firmware Documentation, Device Controller-Monitor (DCM) Documentation, and Serial Protocol Documentation. Together, these efforts ensure that the HeartFlow Pacemaker System achieves its safety and reliability objectives in line with its intended purpose.

2 Terms and Definitions

DCM - Device Controller-Monitor, see separate documentation for further details.

Pacemaker Firmware - All software that is embedded into the pacemaker microcontroller, see separate documentation for further details.

FTA - Fault Tree Analysis

HAZOP - Hazard and Operability Assessment

3 Hazard and Operability Assessment (HAZOP)

This HAZOP study systematically examines the safety and operability of the HeartFlow Pacemaker System, focusing on its interaction between the DCM software and the pacemaker firmware. The study employs structured guide words including Too Much, Not Enough, Not at All, Inaccurate, and Inconsistent to identify potential deviations in key system parameters and their associated risks. These deviations are assessed for their impact on patient safety, system performance, and clinical efficacy.

Key areas analyzed include parameter transmission, electrogram data handling, user and pacemaker verification, and pacing functionality. Each identified hazard is associated with possible failure modes, such as delays in serial communication, inaccurate telemetry, unauthorized access, and improper pacing, which could compromise patient safety and system reliability. By addressing these risks, the HAZOP ensures that the HeartFlow Pacemaker System meets stringent safety and reliability standards in its intended medical environment.

		Guidewords				
		Too Much	**Not Enough**	**Not at All**	**Inaccurate**	**Inconsistent**
Parameters	Sending parameters from DCM to pacemaker	Congestion in serial communication, slows pacemaker response time, and endangers patient's life	N/A	Unable to program endangering patient's life	Differing from doctor's orders endangering patient's life	Differing from doctor's orders endangering patient's life
	Checking bounds on parameters	N/A	N/A	Parameters may be set outside of safe operating bounds, endangering patient's life	Parameters may be set outside of safe operating bounds, endangering patient's life	Parameters may be set outside of safe operating bounds, endangering patient's life
	Toggling electrogram serial data	Some egram data dropped, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life	N/A	No egram data, no hazard	Some egram data dropped, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life	N/A
	Sending electrogram data	Too long to compute information, laggy egram, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life	Poor quality or some egram data dropped, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life	No egram data, no hazard	Some egram data dropped, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life	Some egram data dropped, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life
	Plotting electrogram data	N/A	Poor quality or some egram data dropped, inaccurate telemetry, may lead to inaccurate diagnose, endangering patient's life	No egram data, no hazard	Inaccurate plot, may lead to inaccurate diagnose, endangering patient's life	Inconsistent plot, may lead to inaccurate diagnose, endangering patient's life
	Verifying correct user	N/A	N/A	Unauthorized personnel could accidentally log into the wrong account and change behaviour, endangering patient's life	Unauthorized personnel could accidentally log into the wrong account and change behaviour, endangering patient's life	Unauthorized personnel could accidentally log into the wrong account and change behaviour, endangering patient's life
	Verifying correct pacemaker	N/A	N/A	Unintentionally modify setting on the incorrect pacemaker or with the incorrect account, endangering patient's life	Unintentionally modify setting on the incorrect pacemaker or with the incorrect account, endangering patient's life	Unintentionally modify setting on the incorrect pacemaker or with the incorrect account, endangering patient's life
	Sensing Heart Rate	N/A	Miss natural beat, over pace the heart, endangering patient's life	Miss natural beat, over pace the heart, endangering patient's life	Miss natural beat, over pace the heart, endangering patient's life	Miss natural beat, over pace the heart, endangering patient's life
	Pacing Heart	Overpace the heart, endangering patient's life	Underpace the heart, endangering patient's life	Underpace the heart, endangering patient's life	Over or underpace the heart, endangering patient's life	Over or underpace the heart, endangering patient's life
	Switching Modes	Over or underpace the heart, endangering patient's life	N/A	Potentially non-functional pacemaker, endangering patient's life	Differing from doctor's orders endangering patient's life	Differing from doctor's orders endangering patient's life

Figure 3a. HAZOP table containing all identified modes of harm based on identified system parameters and possible harm guidewords.

4 Fault Tree Analysis

The Fault Tree Analysis (FTA) was developed under the following assumptions:

- **Fair judgment:** The user has a high level of judgment, as would be expected from a professional and trained clinician.
- **Good faith:** This user is assumed to operate within the bounds of their professional capacity, with no malicious intent or deliberate actions to harm the patient.
- **Intended environment:** It is also assumed that the user will use the software in a clinical setting where access to lifesaving care is rapid should there be a situation where a patient's life is endangered.
- **Intended use:** It is assumed that the HeartFlow pacemaker system is used to reliably deliver electrical stimulation to the heart to regulate its rhythm and maintain a sufficient heart rate for the patient's needs.

The FTA focuses on identifying potential faults within the HeartFlow pacemaker system, encompassing both hardware and software components, and analyzing the sequences of events that could lead to critical failures. By examining possible system vulnerabilities and their contributing factors, the FTA provides a comprehensive understanding of risks and supports the implementation of robust mitigations to ensure patient safety and system reliability. The pacemaking system was designed to have a minimal cut set of two (2), which is shown in the FTA diagram below.

The FTA was split into multiple parts. First, a high-level FTA identifies hazards that could lead to endangerment of a patient's life. For hazards where the sub-FTA was extensive, the hazard section was split into a separate FTA. Hazards that have a sub-FTA are denoted with a dotted arrow pointing to the hazard node from the bottom.

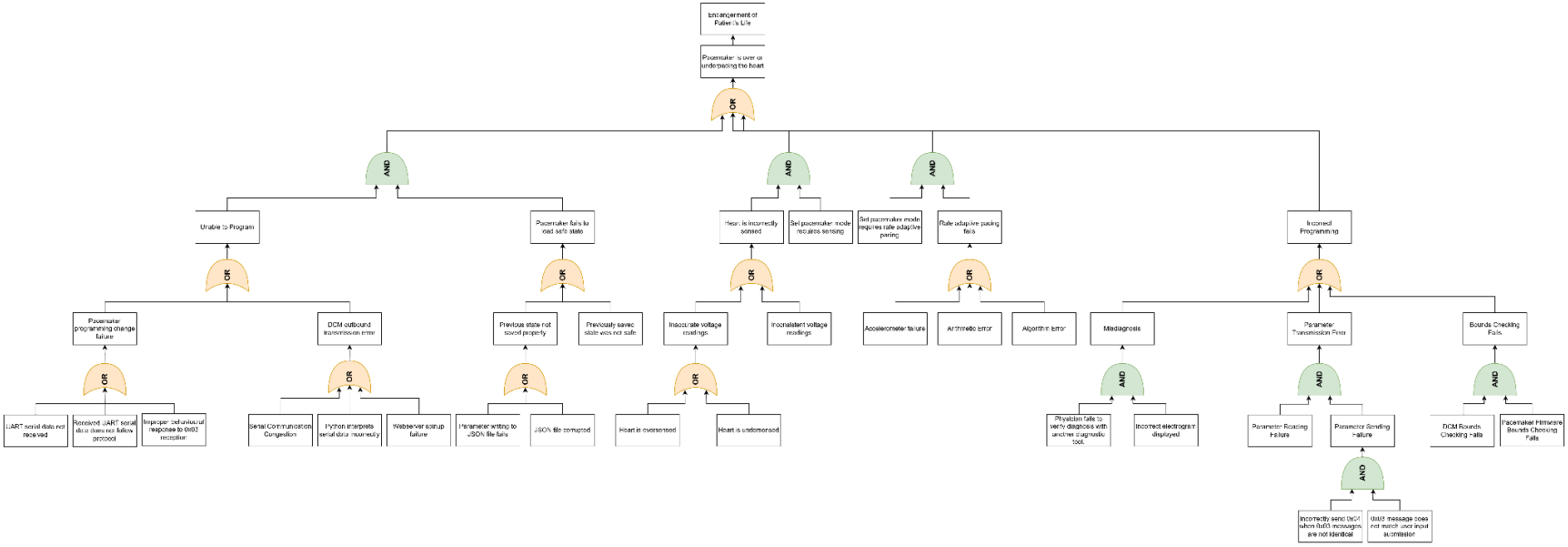

Figure 4.a. Full fault tree analysis. The truncated branches of the tree for greater visibility are documented below.

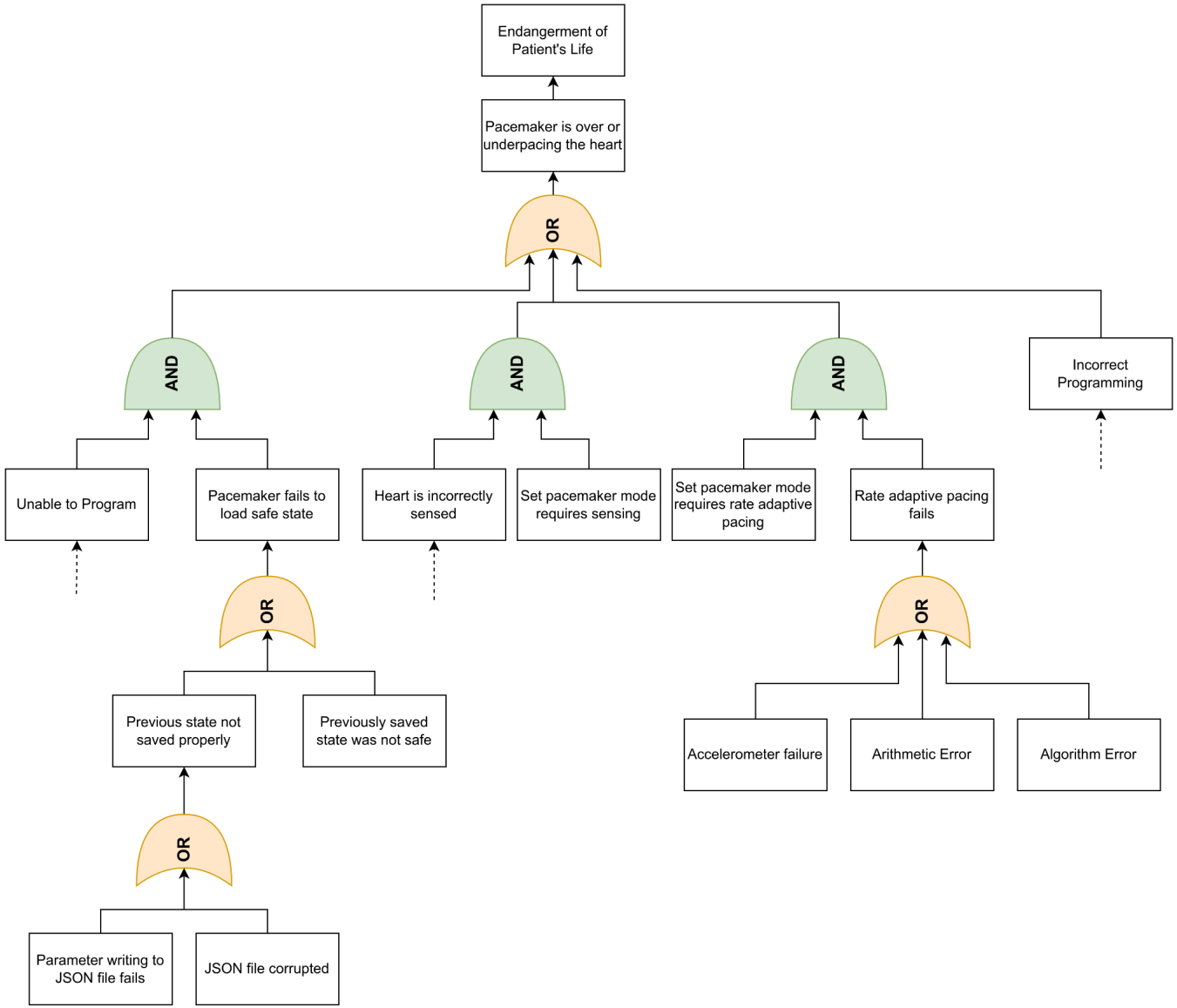

Figure 4.b. High-level FTA of hazards that may lead to endangerment of a patient's life.

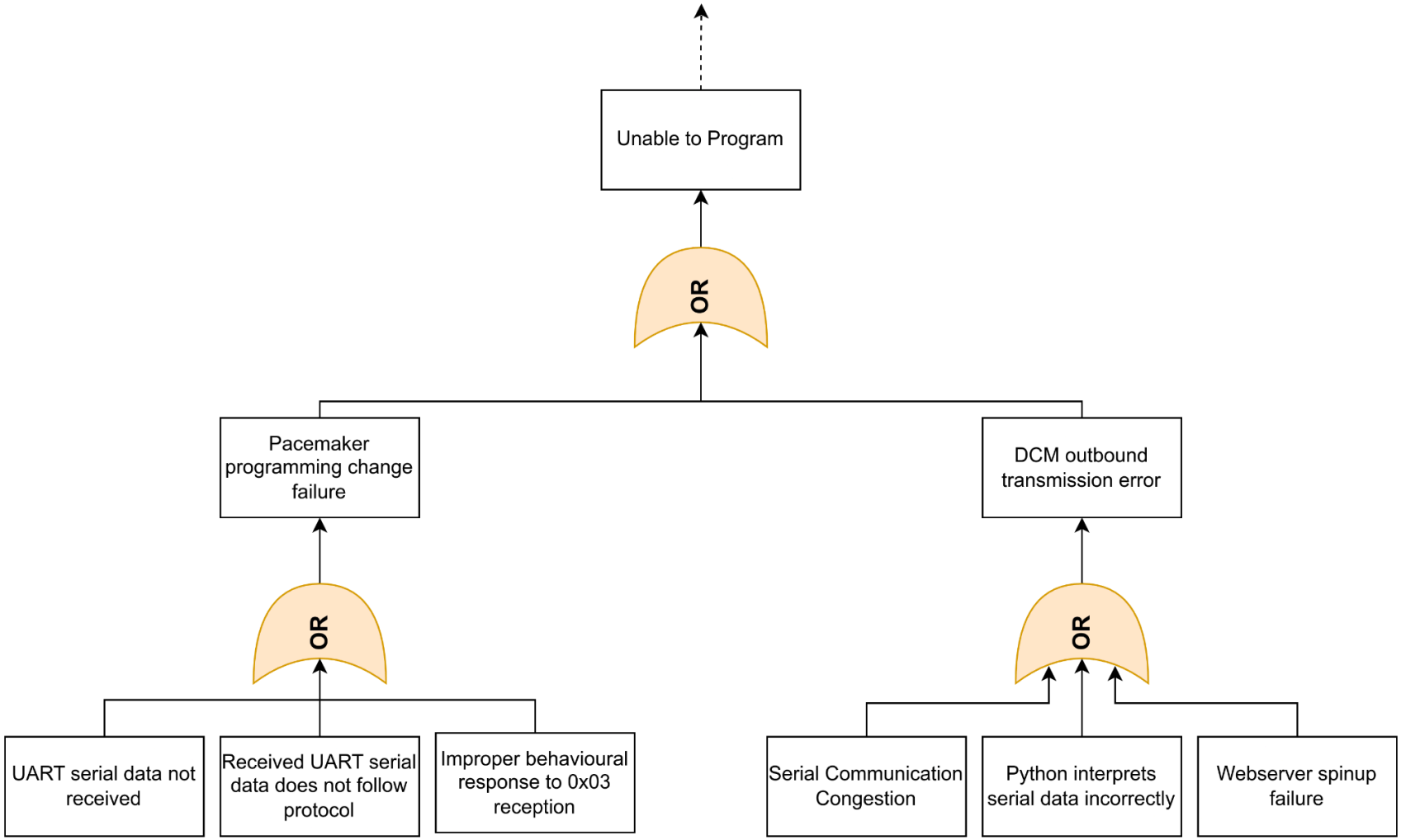

Figure 4.c. FTA of issues that may cause a failure in pacemaker mode and parameter programming.

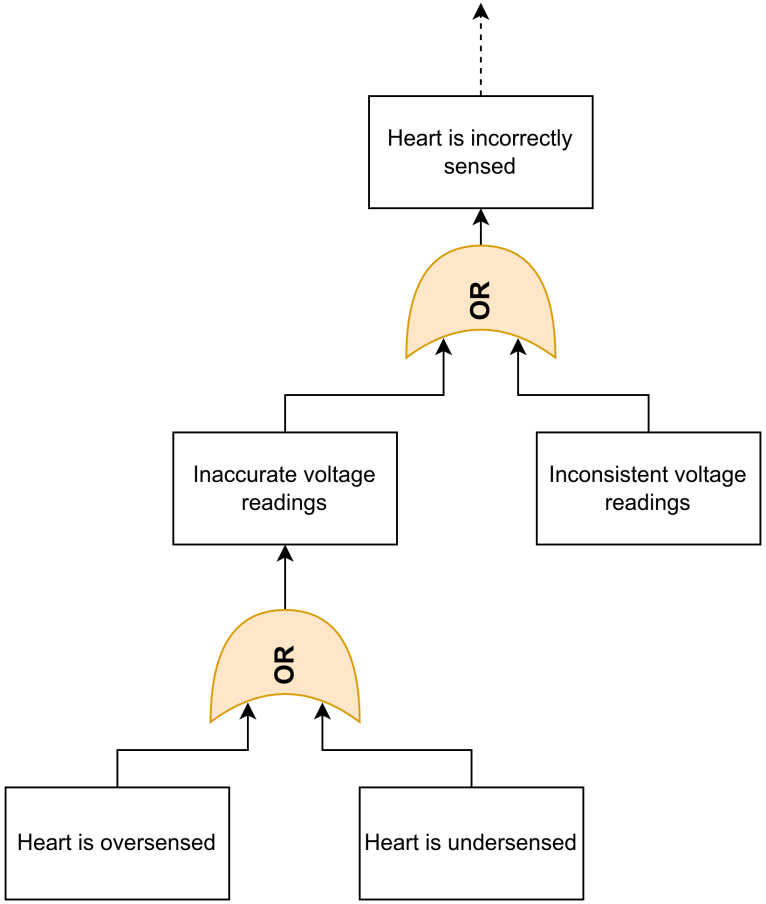

Figure 4.d. FTA of issues that may cause incorrect sensing of the heart.

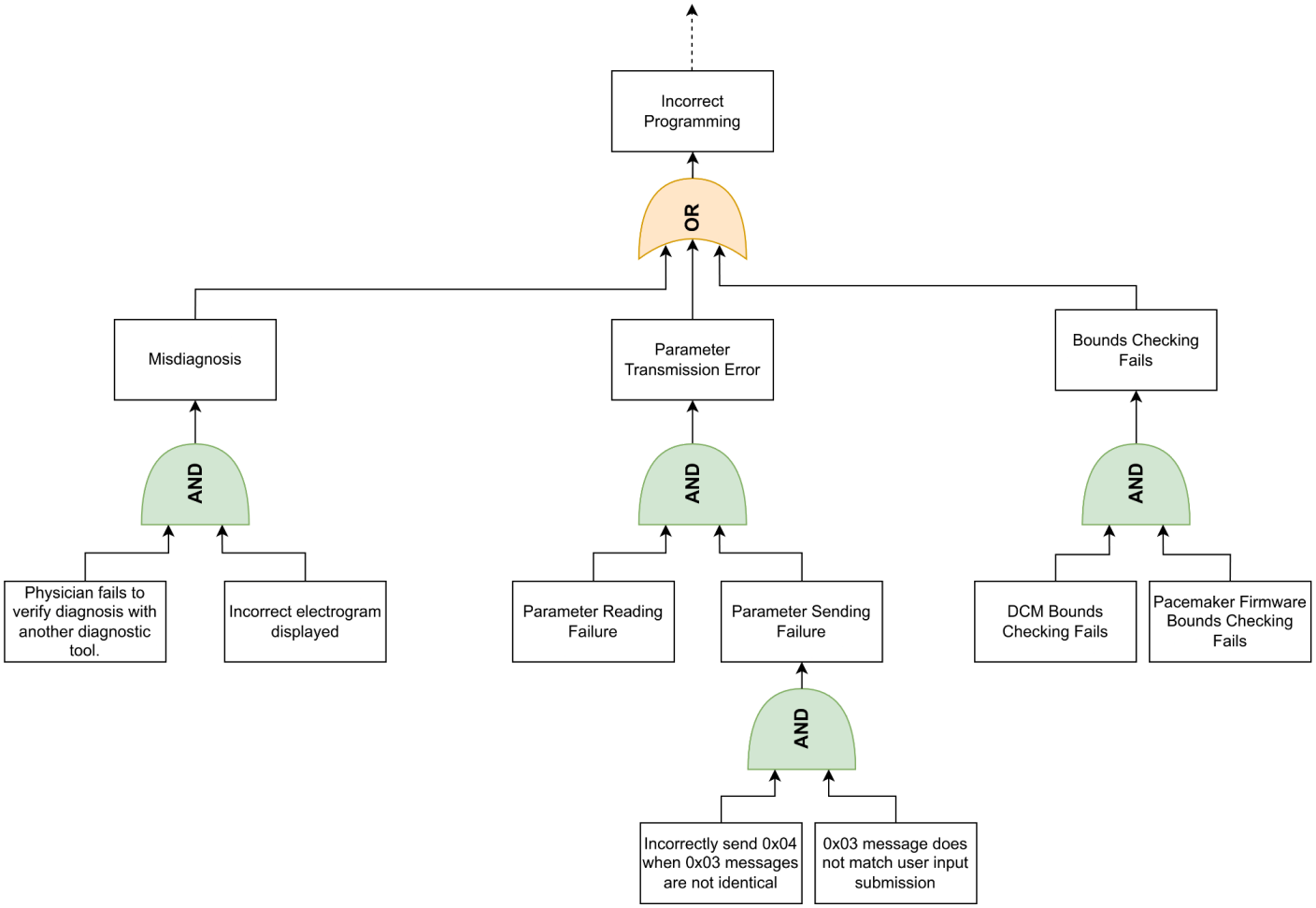

Figure 4.e. FTA of issues that may cause incorrect programming of the pacemaker.

5 Assurance Case

The Assurance Case for the HeartFlow Pacemaker System presents a structured argument, supported by evidence, that the system is safe and reliable for its intended uses in its intended environment. The objective of this Assurance Case is to demonstrate that all reasonable hazards have been identified, mitigated, and adequately controlled to ensure that the pacemaker system functions as intended without posing undue risk to patients or users. Through rigorous safety analyses, including the HAZOP, FTA, and validation of design and implementation against documented requirements, we provide a comprehensive assurance that the system meets the necessary safety standards. This Assurance Case is a critical component in confirming the integrity of the HeartFlow Pacemaker System and ensuring its compliance with relevant safety regulations and best practices for medical devices.

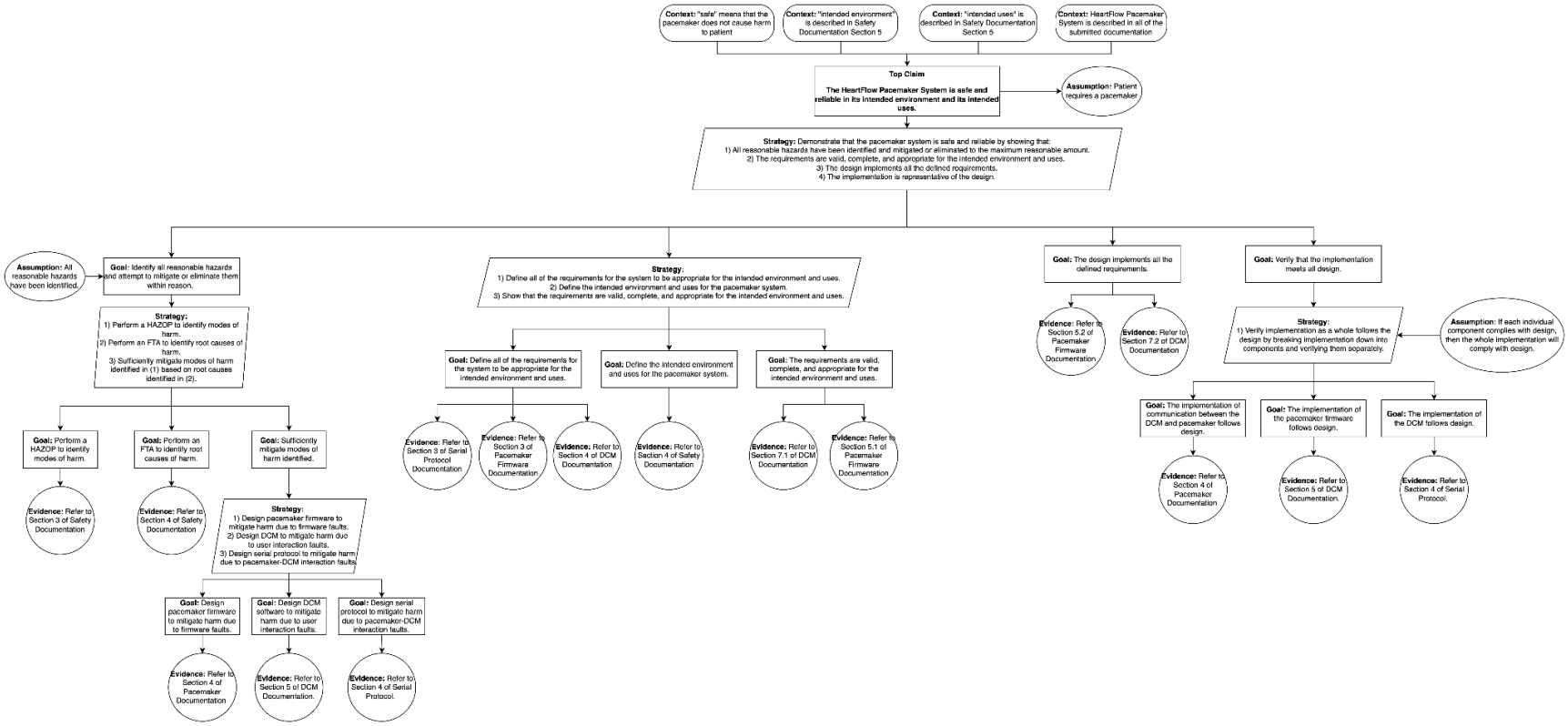

Figure 5.a. Full assurance case. The truncated branches of the tree for greater visibility are documented below.

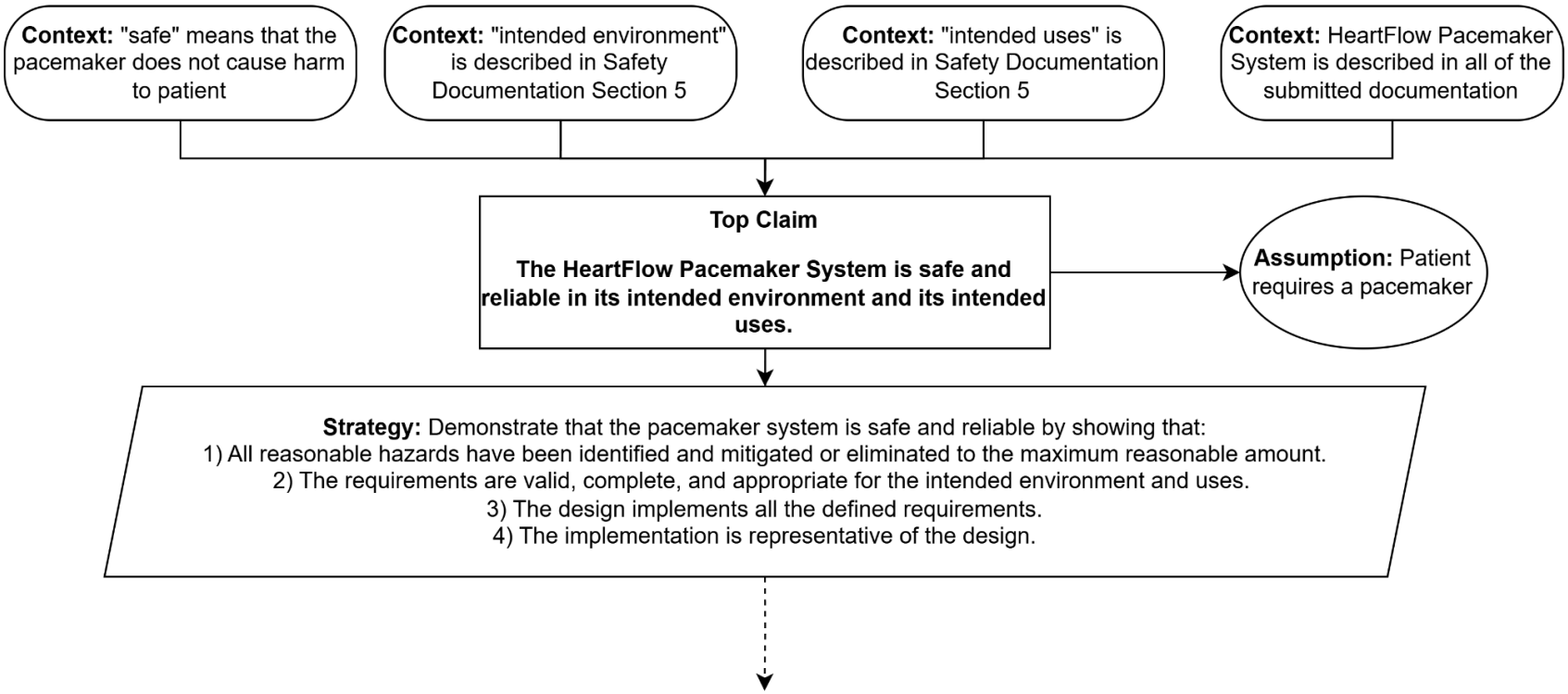

Figure 5.b. Top of the assurance case. Part 1 of 3.

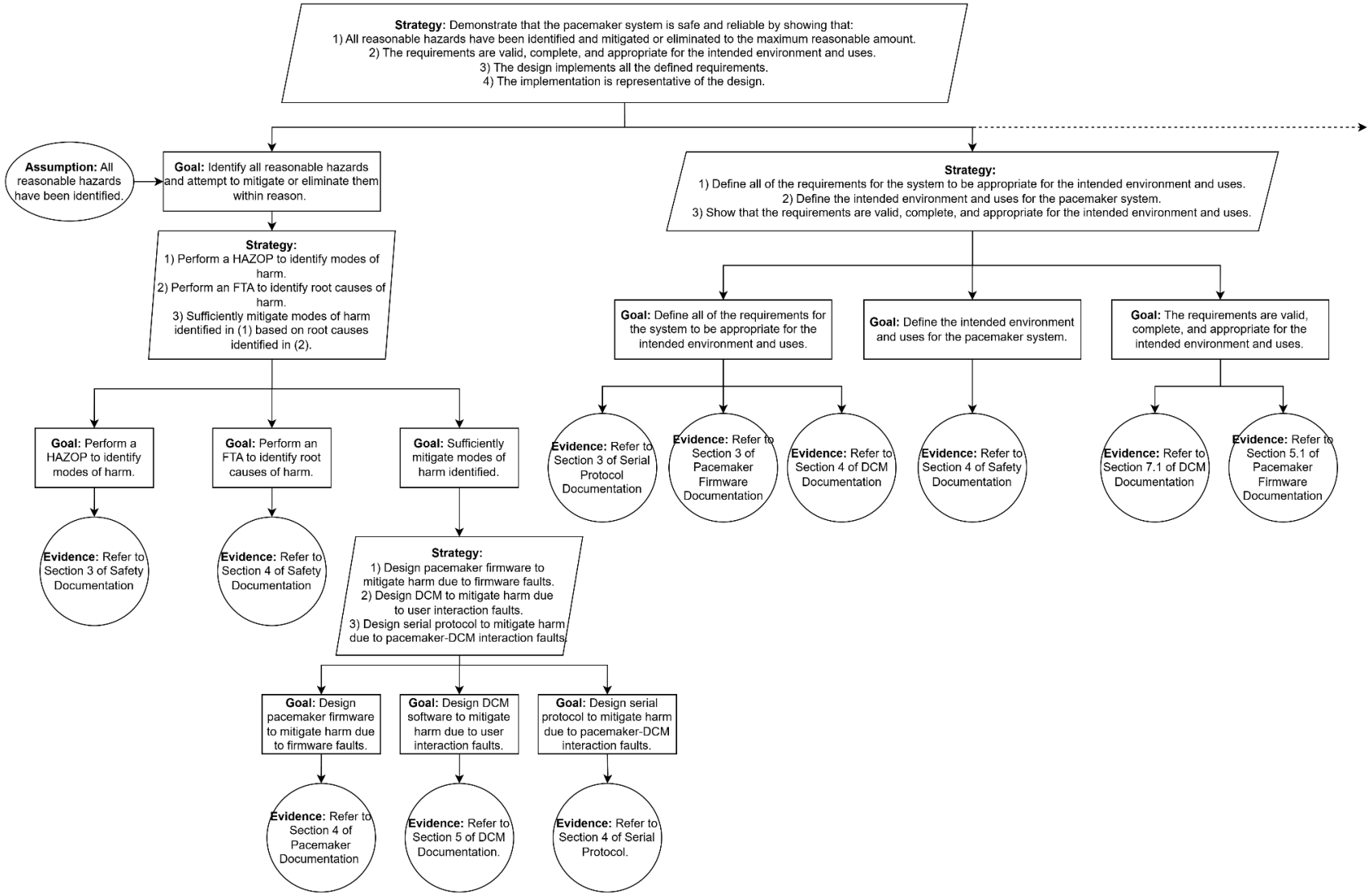

Figure 5.c. Bottom left of the assurance case. Part 2 of 3.

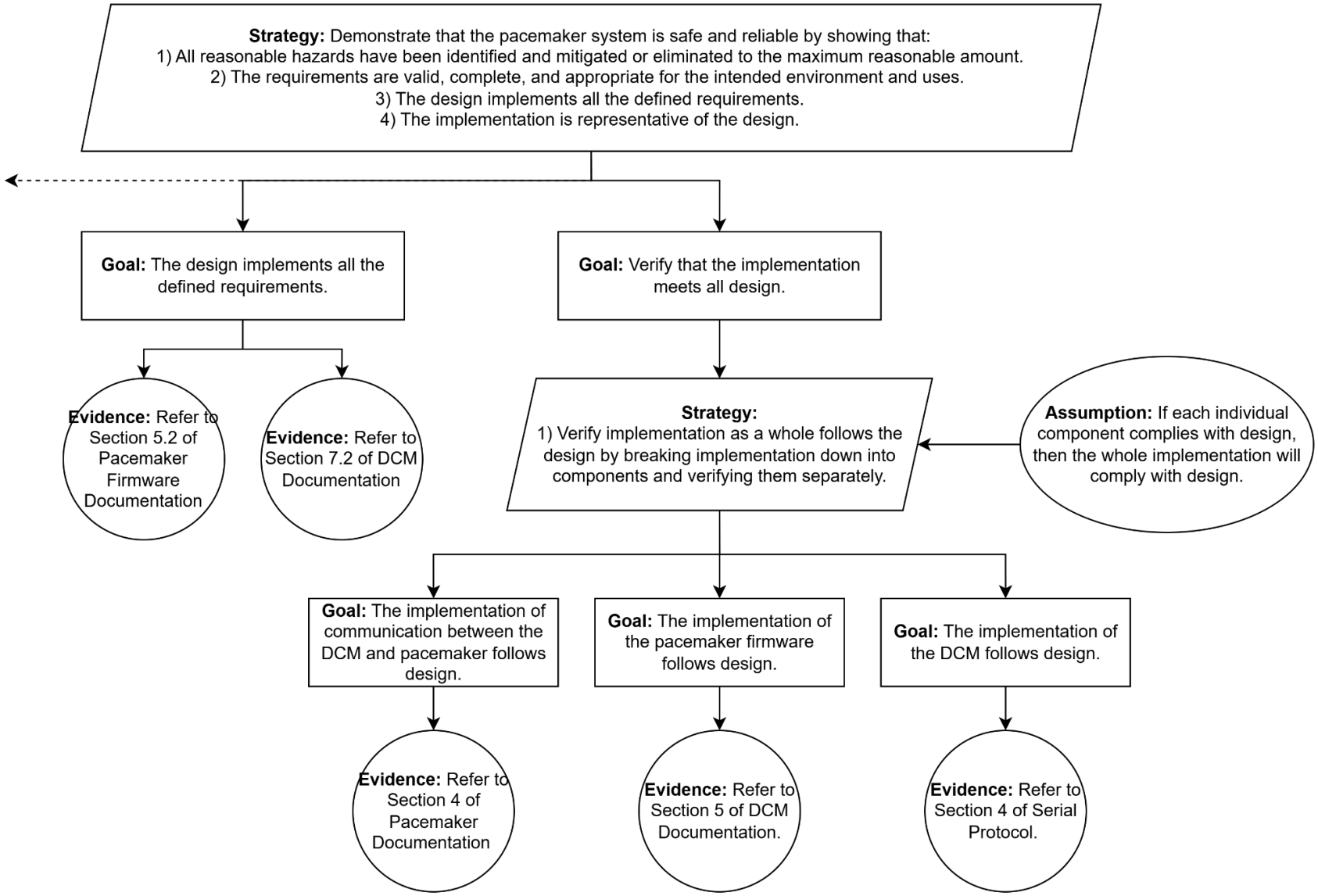

Figure 5.d. Bottom right of the assurance case. Part 3 of 3.