RPAS Level Functional Hazard Assessment

Document Type	Deliverable
Document Number	D3.2
Primary Author(s)	Name | MICROPILOT
Document Version / Status	2.0 | Final
Distribution Level	Public

Project Acronym	HI-RISE
Project Title	High Integrity RPAS by Innovative Software Engineering
Project Coordinator	Howard W. Loewen | MicroPilot | hloewen@micropilot.com

Contributors

Name	Organization	Name	Organization
Kyle Hayes	MICROPILOT	Max Scalerandi	2B Motori Moderni s.r.l
Matias Gervai	MICROPILOT		
Diksha Randev	MICROPILOT		
Howard Loewen	MICROPILOT		
François Varigas	Aero Composites Innovations		
Jose Montero	ALTER Technology TÜV NORD		
Kenneth Revne	GRIFF Aviation AS		

Document history

Revision	Date	Author / Organization	Description
1	2020-11-24	Kyle Hayes MICROPILOT	Draft
2	2020-12-04	Kyle Hayes MICROPILOT	Final

TABLE OF CONTENTS

List of Figures

List of Tables

1. Executive Summary

This deliverable will provide an overview of the experience of using the HI-RISE framework to increase the certifiability of several members of the consortium's designs. The report will address difficulties encountered and gaps discovered.

Unfortunately, the HI-RISE consortium was unable to complete the framework prior to the end of the project. The amount of work necessary was much greater than the members of the consortium could complete prior to the end of the project. Work on the various design artifacts and related tools continues and will be completed in early 2021. Instead of the comparing designs before and after application of the HI-RISE framework, we chose to review incidents as they show a reduction in incidents resulting from application of improvements resulting from progress made on the HI-RISE framework.

Keywords: Failure Analysis, Product Development, Reliability, Regulatory Authority

2. Objectives

The use of aviation design practices within the RPAS world is relatively uncommon. One of the goals of HI-RISE is to help raise the awareness among RPAS designers about the use of tools such as functional hazard assessment, fault tree analysis, and high-level requirements. The generic block diagram of an RPAS, the generic functional hazard assessment and the generic high-level requirements will be employed to help several RPAS manufacturers improve both their processes as well as their designs and document the improvements resulting from these processes.

The original objectives for this deliverable have been achieved in measure:

Objective	Outcome
Educate several RPAS manufacturers on the use of functional hazard assessment and high-level requirements as tools to ensure reliability.	Several RPAS manufactures as part of the HI-RISE consortium have been educated through ongoing bi-weekly meetings on Failure Analysis using the techniques of Functional Hazard Assessments, Latent and Common Mode Failure Analysis, and Fault Tree Analysis using a generic RPAS model as an example.
Develop real world examples of what the certification documents might look like.	The following documents, based on a Generic RPAS model, can be used as templates for a specific RPAS Failure Analysis: • Generic RPAS Block Diagram • Generic RPAS Functional Hazard Assessment (based on the BD) • Generic RPAS Fault Tree Analysis (based on the FHA) • Generic RPAS Latent and Common Mode Failures Analysis (based on the FTA)
Find weaknesses and gaps in the generic versions of these tools.	Over the course of the bi-weekly meetings improvements, gaps, and weaknesses to the generic tools have been identified and either resolved or noted in the documentation for further analysis based on the specifics of the RPAS under consideration.

Objective	Outcome
Determine the level of difficulty RPAS manufacturers face when first presented with the HI-RISE framework.	Since the HI-RISE framework is incomplete, this measurement is unable to be taken at this time.
Measure the effectiveness of the HI-RISE framework in developing certification documentation for RPAS.	Since the HI-RISE framework is incomplete, this measurement is unable to be taken at this time. However, artifacts from HI-RISE have been used by a consortium member in their successful SORA application showing that the artifacts and documents generated by HI-RISE are effective in developing certification documentation.
Assess the level of acceptance of the HI-RISE framework to the regulatory authorities in the countries where these RPAS operate.	Since the HI-RISE framework in incomplete, this measurement is unable to be taken at this time. However, artifacts from HI-RISE have been used by a consortium member in their successful SORA application showing that regulatory authorities have accepted HI-RISE documents as acceptable proof of regulatory compliance.

3. Description of Work

3.1 Terminology

Table 3-1 - Terminology

Term	Description
Autopilot Firmware Version	Found in datalog or reported by customer.
Autopilot Hardware Fault	Includes electronic hardware failures as well as calibration faults and drift
Autopilot Model	MicroPilot Autopilot Model from serial number found in datalog or reported by customer.
Configuration	RPAS configuration type (Fixed Wing, Helicopter, Multi-rotor, etc.) found in datalog or reported by customer.
Contributing Factor(s)	Additional: actions, omissions, events, conditions, or a combination thereof, which led to the accident or incident.
Date	Date of incident or when incident was reported (if no datalog was available).
Failure Mode Mitigation	See “Unknown Failure Mode” and “Unhandled Failure Mode” for classification.
Incorrect Autopilot Configuration	Covers failures that are due to the software configuration or the physical installation of the autopilot or related systems within the airframe.
MP ground/flight testing	An autopilot that is being tested at MicroPilot. This testing is done more frequently and some failures are expected and handled by enhanced safety procedures.
Near-miss	A situation which would have resulted in a crash without the intervention of a safety pilot or ground control operator.
Poor Flight Conditions	Root Cause of incident was determined to be Environmental Conditions, i.e. poor GNSS reception or acute changes in weather; may also be intentional if takeoff occurred after the effects of the environment were known to severely degrade aircraft performance.
Potential Crash	A situation which could potentially result in a crash; e.g. A crash during a trueHWIL system simulation. Note that incidents that would normally be classified as “Potential Crash” for a customer are deemed acceptable risk for MicroPilot ground/flight testing and are not recorded in this report.
Product Development Phase	See “RPAS Manufacturer Integration”, “RPAS Operator”, and “MP ground/flight testing” for classifying Product Development Phase.
Root Cause	The most significant action, omission, event, or condition which can be said to have caused the incident, i.e. If the safety pilot stalled the aircraft after taking control from the autopilot because a software coding error caused control failure, the Root Cause would be the Software Coding Error, even though operator error was direct cause of the crash.
RPAS	Remotely Piloted Aircraft System.
Severity	See “RPAS Crash”, “Near-Miss”, and “Potential” for classifying severity.
Software Bug	Software bug causing the autopilot to becoming non-responsive, or to create an unstable flight control leading to a crash.
Software Coding Error	A software bug caused by an error in developer coding not caught by current MicroPilot processes but is covered by the policies and procedures guidelines.
Software Design Error	A software bug caused by an error in the software design process that could have missed a failure mode or where the process and procedures did not cover.
RPAS Crash	An airframe hitting the ground unexpectedly.
RPAS Manufacturer Integration	Flights Conducted by the RPAS Manufacturer as part of the product development process.

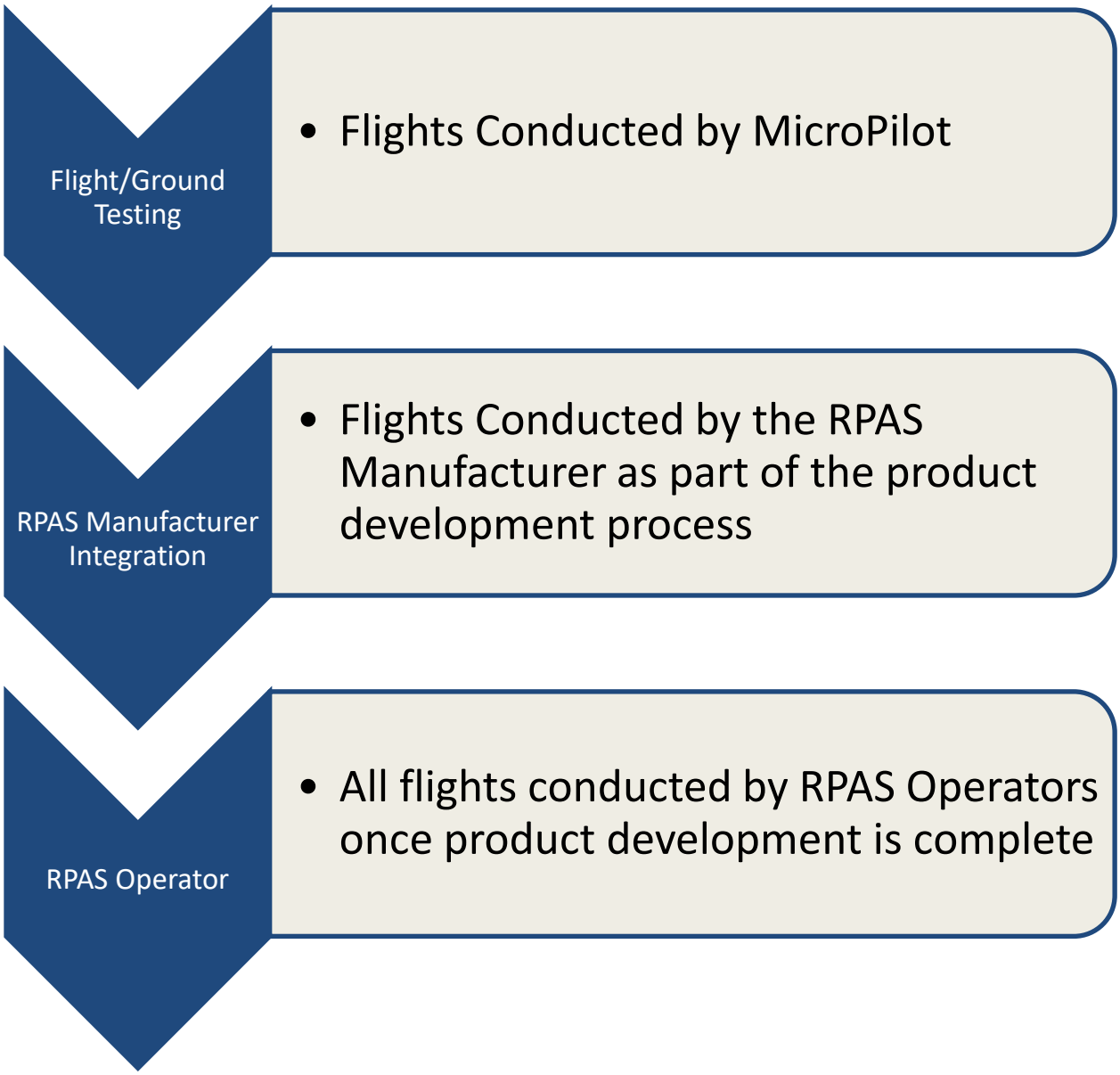
Term	Description
RPAS Operator	All flights conducted by RPAS Operators once product development is complete.[1]
Un-Communicative Customer	Root Cause of incident was not identified; customer did not respond to request for information related to the incident.
Undetermined	Root Cause of incident was undetermined after reasonable investigation by MicroPilot and Customer.
Unhandled Failure Mode	A failure mode known to MicroPilot but without any mitigation.
Unknown Failure Mode	A new failure mode that had not been identified by MicroPilot.

[1] MicroPilot may categorize a case as "RPAS Manufacturer Integration" even if the product has shipped to an RPAS Operator, if the test process does not meet MicroPilot standards. RPAS Service Provider incidents are categorized as RPAS Operator if the incident occurred on mission or in preparation for a mission.

3.2 Statistical Overview

This section of the document outlines a statistical overview of the critical incidents identified by MicroPilot for the purpose of estimating the impact of the processes and documents generated by HI-RISE.

Product Development Phases



Incident Tracking Over Time

Figure 1 contains all the incidents organized by their product development phase between November 2016 to August 2020.

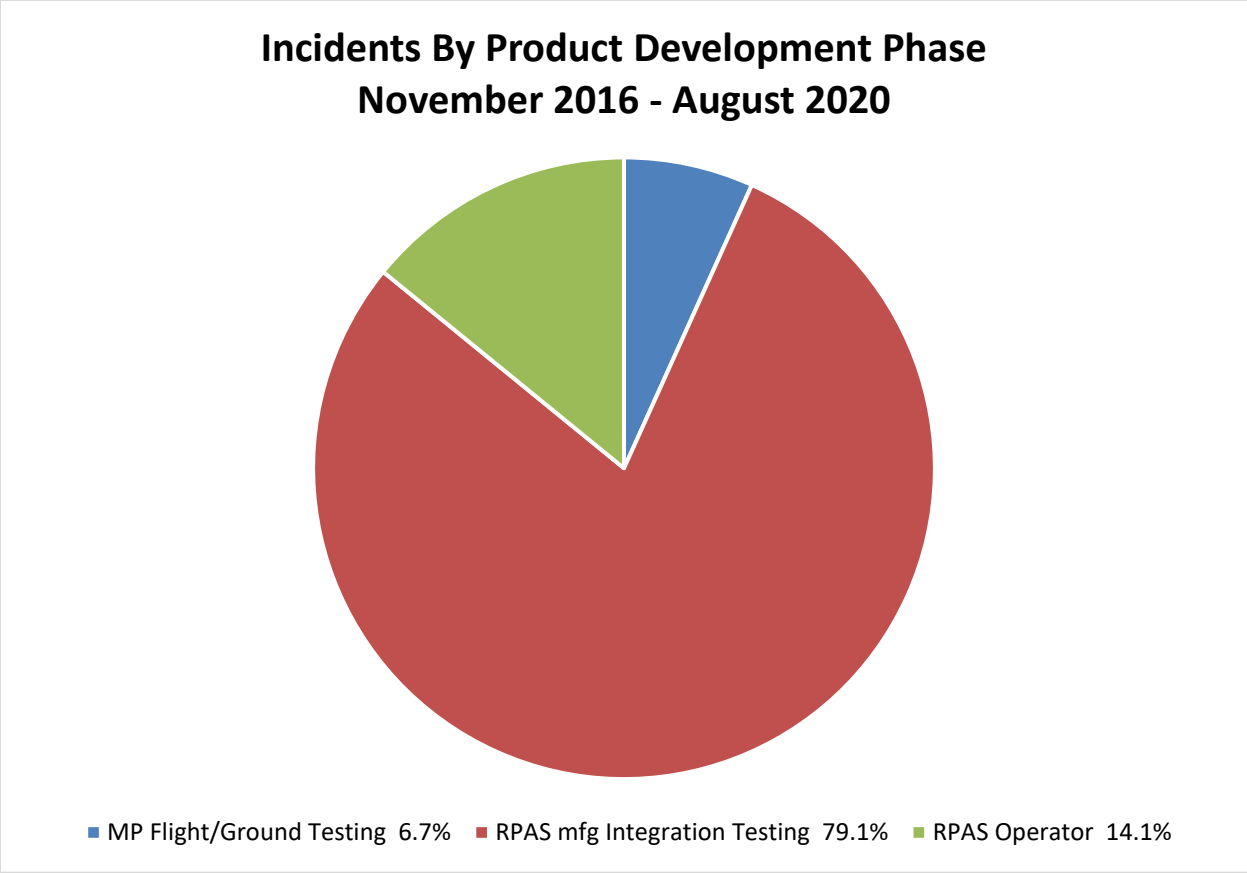


Figure 1 - Incidents by Product Development Phase

Figure 1 shows that the vast majority of incidents occur during the RPAS manufacturer integration testing phase of product development, while a significantly smaller number of incidents occur during RPAS operator use and were identified during MicroPilot flight and ground testing, a breakdown which makes sense considering RPAS manufacturers perform significantly more test flights than MicroPilot, and RPAS operators perform significantly more flight operations than RPAS manufacturer test flights. The increase in the number of incidents of RPAS manufacturer flights is due to the increase in the number of flights done compared to MicroPilot; however, the number of incidents decrease for RPAS operators because common failure modes (identified further below) are resolved by the RPAS manufacturer before the product is released to RPAS operators. If we were able to normalize the incident rates based on the number of flights performed, we would likely see incident rates decrease dramatically for RPAS operator and RPAS manufacturers and increase for MicroPilot flight and ground testing.

Figure 2 highlights the relative percent of incidents by product development phases for the years 2016 to 2020.

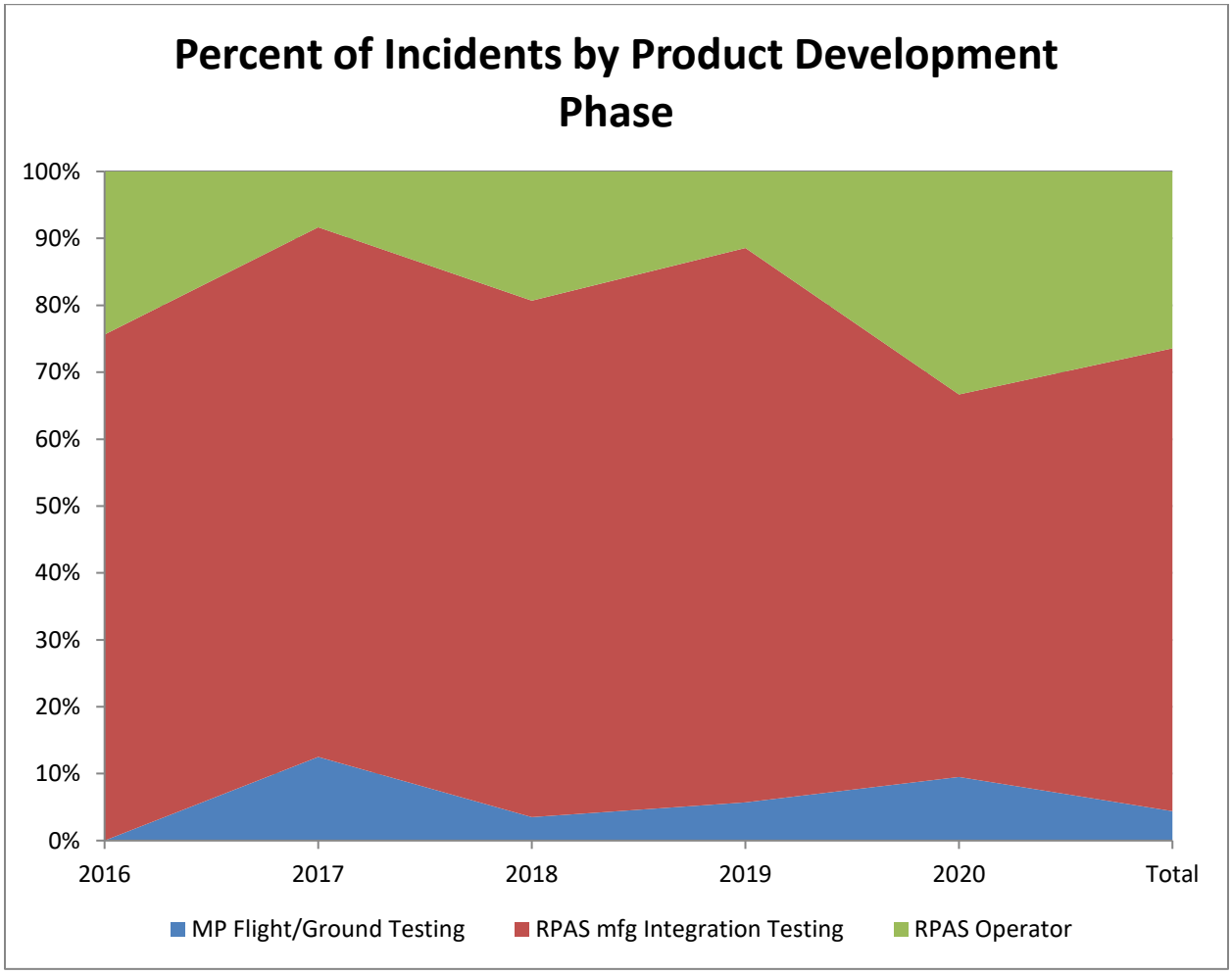


Figure 2 - Percent of Incidents by Product Development Phase

As a percent of incidents, we can see in *Figure 2* that RPAS operator incidents remain relatively stable over the years while incidents during MicroPilot flight & ground testing have shown a slight increase and incidents during RPAS manufacturer integration have decreased slightly.

Figure 3 highlights the total number of incidents (purple bars) resulting in damage to the RPA and the incidents resulting in damage during specific product development phases (coloured lines) which occurred during the entirety of years 2016 to 2020.

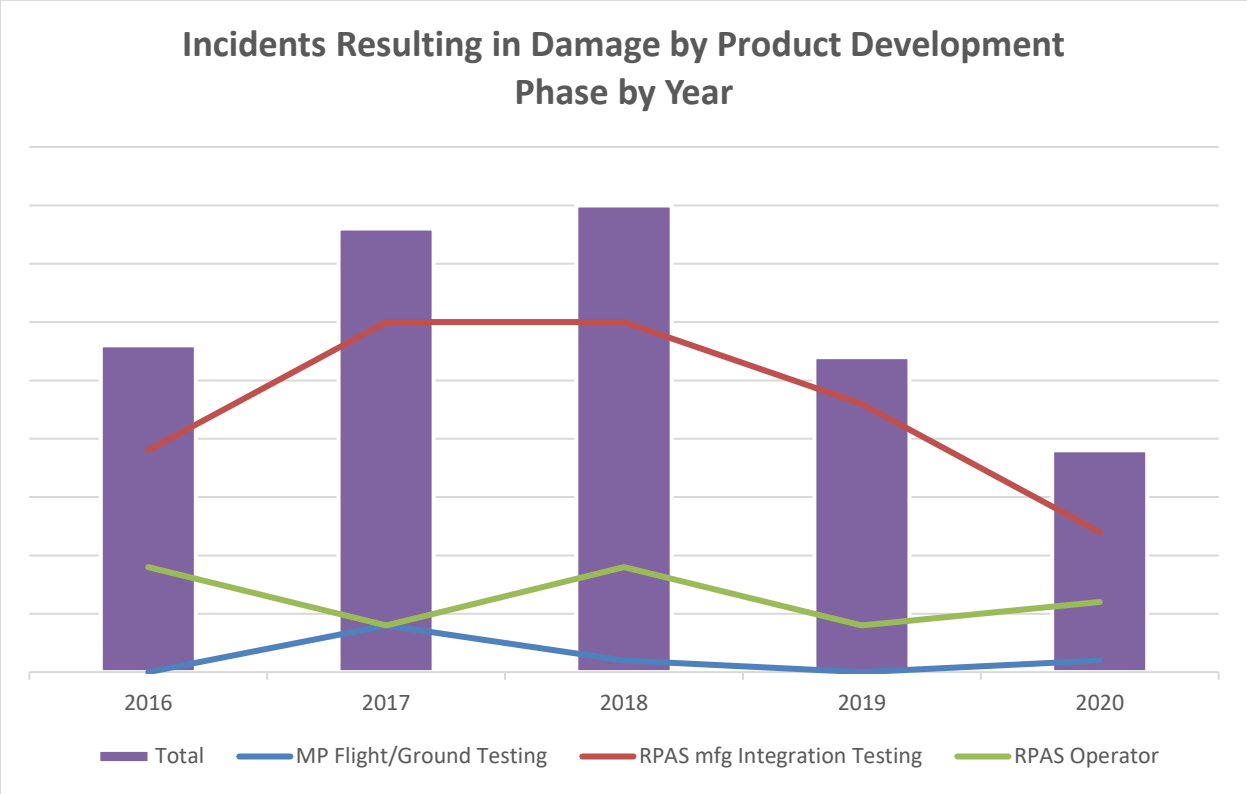


Figure 3 - Incidents Resulting in Damage by Product Development Phase by Year

This dataset shows the pre-HI-RISE incident rate resulting in damage to the RPAS. Over all phases and especially during the RPAS manufacturer integration phase, incidents resulting in damage to the RPAS were growing significantly; however, as HI-RISE processes and framework has been implemented we see a significant decrease in both the number of overall incidents resulting in damage and the number of incidents resulting in damage during the RPAS manufacturer integration phase. RPAS operator incidents resulting in damage continue an absolute decrease over the entire period. This demonstrates that the processes and framework of HI-RISE, even though only partially complete, have been able to significantly reduce risk and increase safety by reducing the number of incidents resulting in damage to the RPAS even as RPAS adoption increases through the years.

Figure 4 highlights the percent of total incidents (purple bars) that cause damage to the RPAS and the percent of incidents that cause damage to the RPAS during specific product development phases (coloured lines) for the years 2016 to 2020. The individual phases do not add up to the total as their percentage is taken just from the number of incidents resulting in damage during that respective phase.

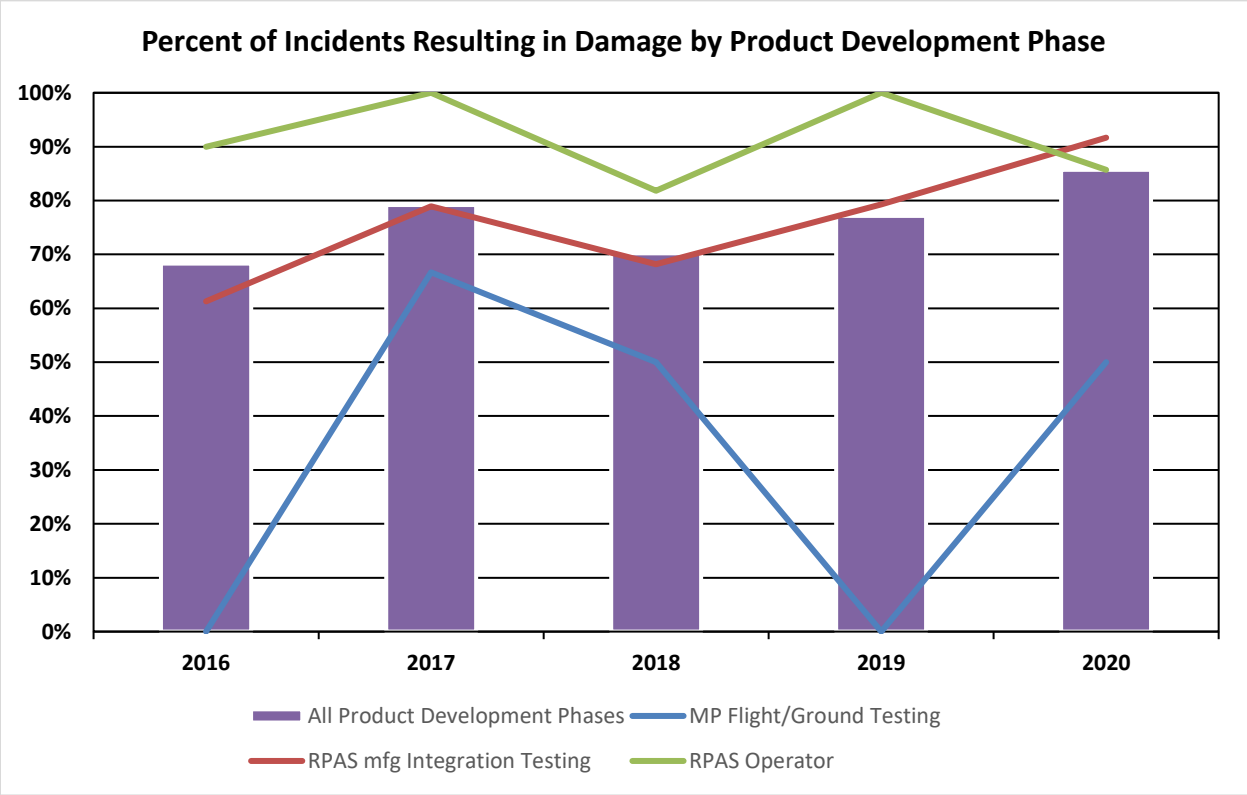


Figure 4 - Percent of Incidents Resulting in Damage by Product Development Phase

Incidents caught during earlier testing stages, such as MP Flight/Ground Testing are much less likely to cause physical damage to the RPAS than incidents that occur at later development stages such as those reported by RPAS operators. This is expected as during earlier development stages (MicroPilot flight and ground testing or RPAS manufacturer integration testing) there is an anticipation of “unexpected” results which requires more robust flight planning and operational mitigations which would be more likely to recover the RPAS before damage occurs. While the relative number of incidents resulting in damage increased for RPAS operators between 2018 and 2019 the absolute number of incidents resulting in damage decreased by more than 50%, indicating HI-RISE processes were able to reduce high-risk incidents that cause damage to the RPAS but also reduce the overall number of incidents as the number of incidents that result in damage take a larger share of the tot number of incidents. A similar explanation exists for the increase in incidents causing damage to the RPAS during the RPAS manufacturer integration testing, while the percent of incidents causing damage has increased by 20% between 2018 and 2020 the overall number of incidents resulting in damage decreased by 66%. For MicroPilot flight and ground testing the small sample size of incidents resulting in damage leads to a large variation in relative incident rates.

Incident Root Cause by Product Development Stage

Figure 5 highlights all the incidents during the MicroPilot flight and ground testing product development phase broken down by root cause for the years 2016 to 2020.

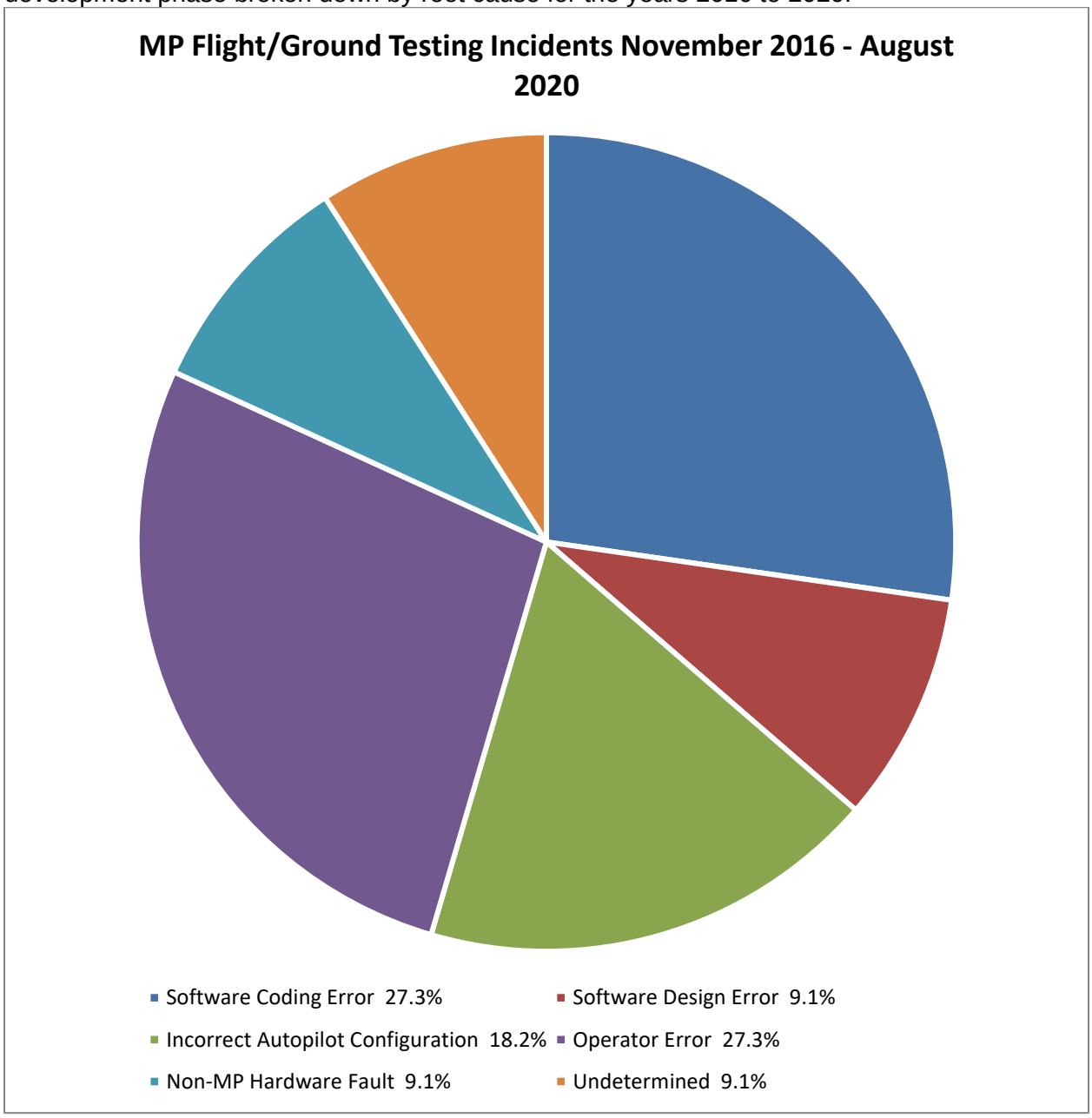


Figure 5 - MicroPilot Flight and Ground Testing Incidents

There is an even distribution of root cause failures found during MicroPilot's flight and ground testing. There is, however, a small sample size of failures over the 3-year period, but given the relatively low number of test-flights a single company is able to perform the incident rate is acceptable.

Figure 6 highlights all the incidents during the "MP Flight/Ground Testing" product development phase broken down by root cause for the years 2016 to 2020. Due to the limited number of incidents during the MicroPilot flight and ground testing phase the line graphs used for the RPAS manufacturer integration phase and RPAS operator phase have been replaced with this bar graph.

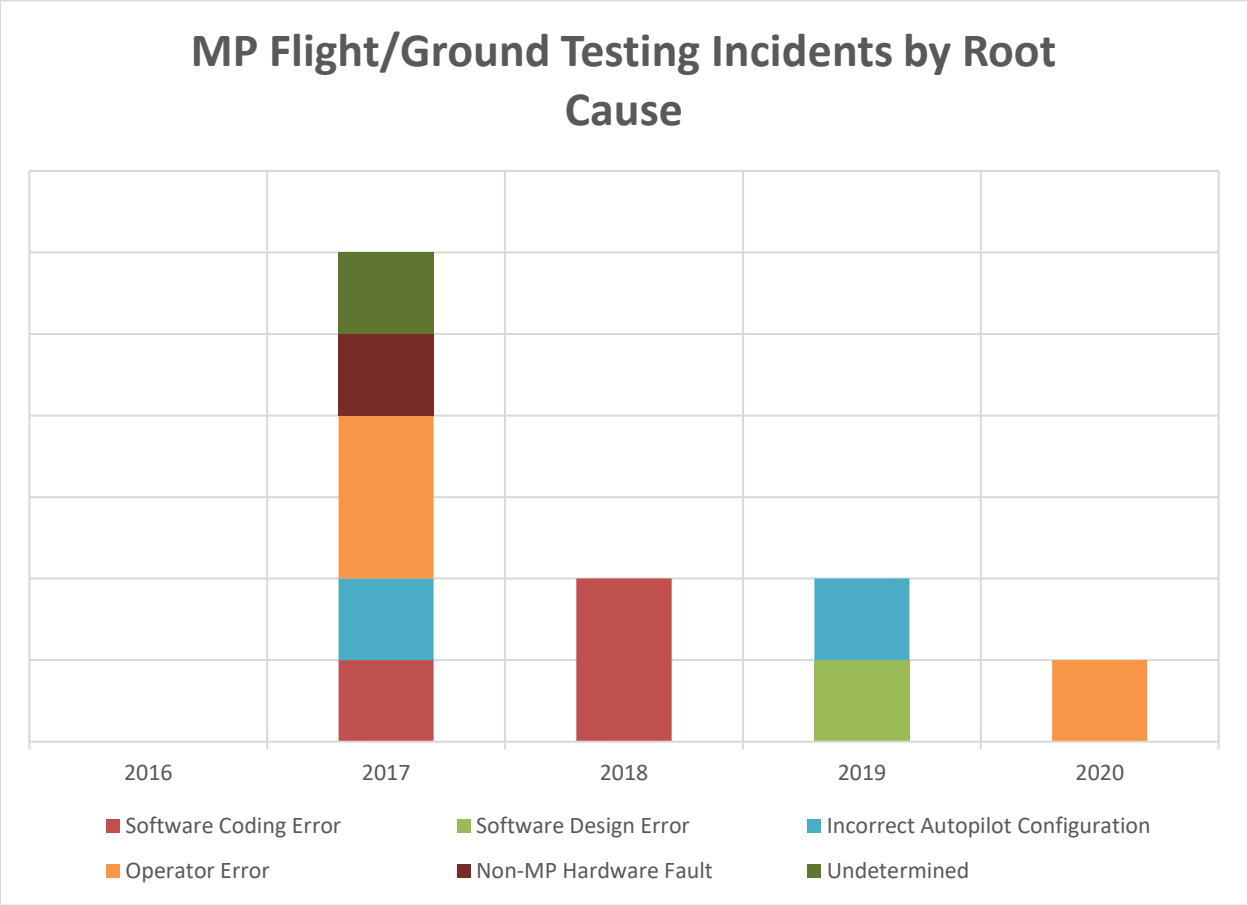


Figure 6 - MicroPilot Flight and Ground Testing Incidents by Root Cause

The limited number of incidents during the MicroPilot flight and ground testing phase do not contain a significant sample size but do show a trend of reduced risk and increased safety that can be attributed to the HI-RISE framework and processes. Note that in the year 2016 no incidents were reported during MicroPilot Flight/Ground Testing.

Figure 7 highlights all the incidents during the "RPAS Manufacturer" product development phase broken down by root cause for the years 2016 to 2020.

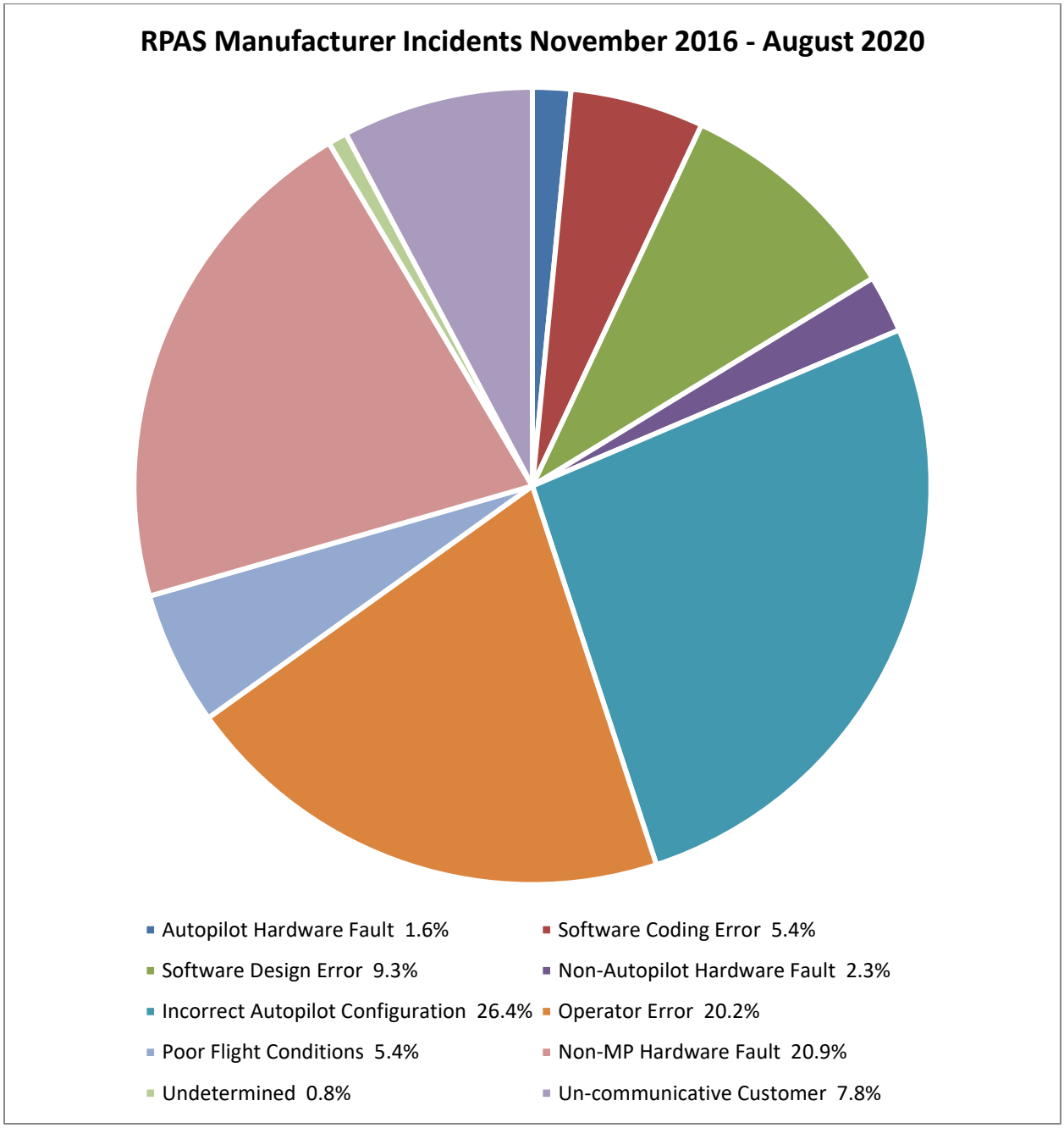


Figure 7 - RPAS Manufacturer Incidents

The most frequent root causes of incidents during RPAS manufacturer integration were due to configuration and operator error, which can be mitigated by failure analysis using the HI-RISE framework.

Figure 8 highlights the hardware-related incident root causes during the “RPAS Manufacturer” product development phase for the years 2016 to 2020:

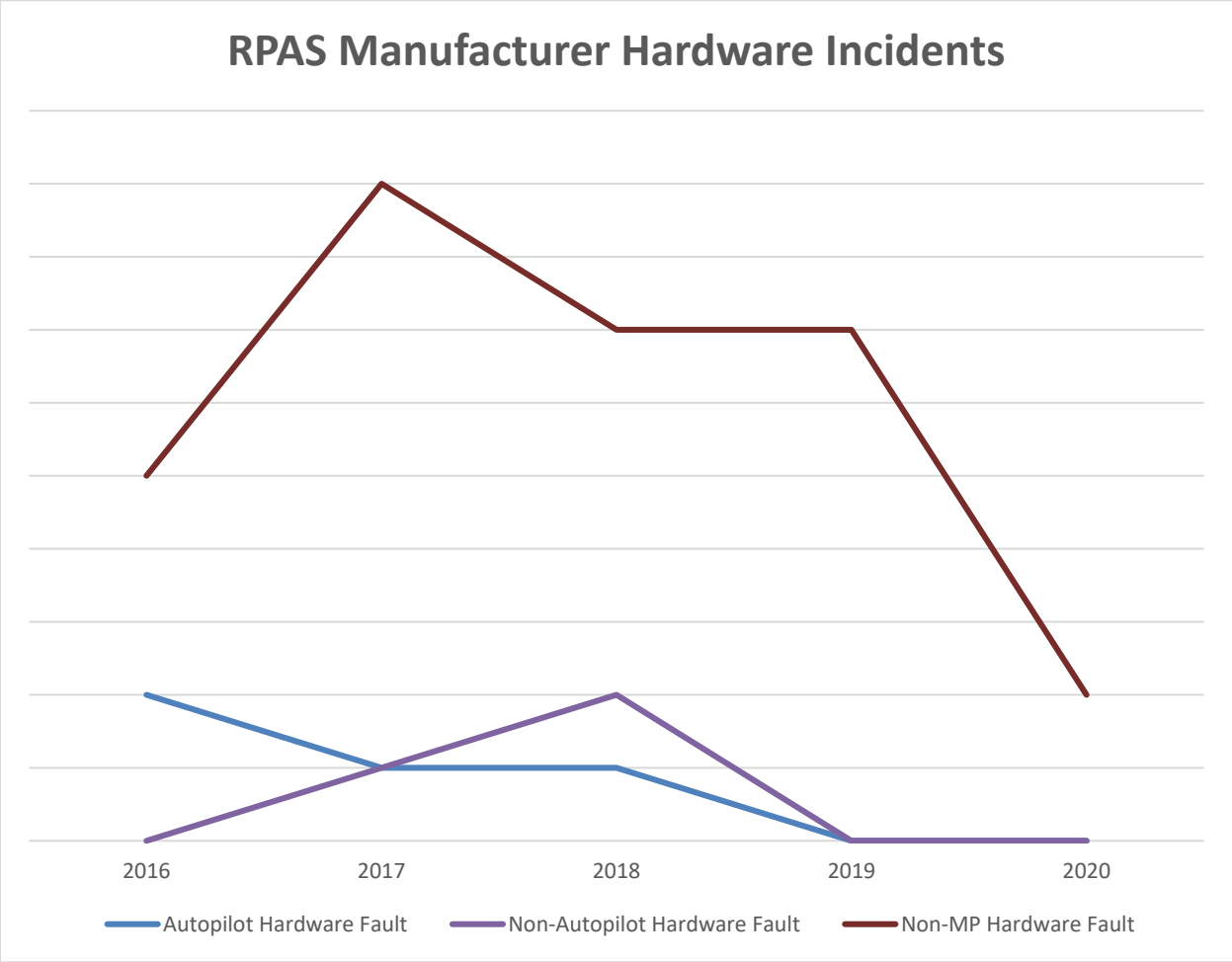


Figure 8 - RPAS Manufacturer Incidents, Hardware Incidents

As expected, incidents caused by autopilot hardware and non-autopilot hardware failure decreased over the HI-RISE project period as improved failure analysis and safety/reliability improvements were implemented. There is also a decrease in the number of non-MicroPilot hardware failures, which can be attributed to the rollout of HI-RISE artefacts and failure analysis tools.

Figure 9 highlights the software & configuration related incident root causes during the "RPAS Manufacturer" product development phase for the years 2016 to 2020:

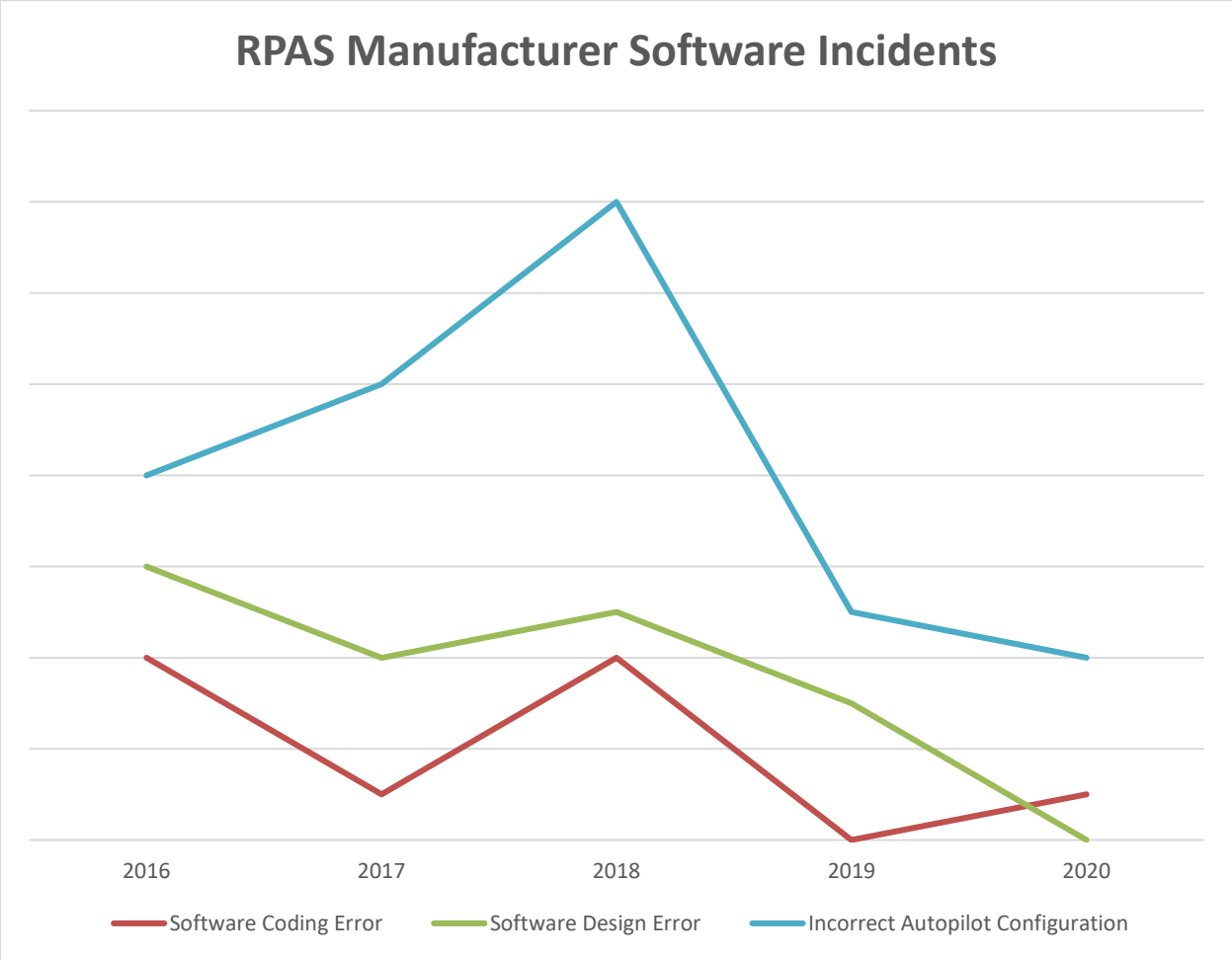


Figure 9 - RPAS Manufacturer Incidents, Software Incidents

As expected, RPAS manufacturer incidents related to software have decreased significantly during the HI-RISE period. The decline in software design errors and software coding errors can be attributed to the enhanced software development processes and testing used at MicroPilot while reductions in configuration errors can be attributed to the reliability and safety improvements developed during HI-RISE.

Figure 10 highlights the other incident root causes during the "RPAS Manufacturer" product development phase for the years 2016 to 2020:

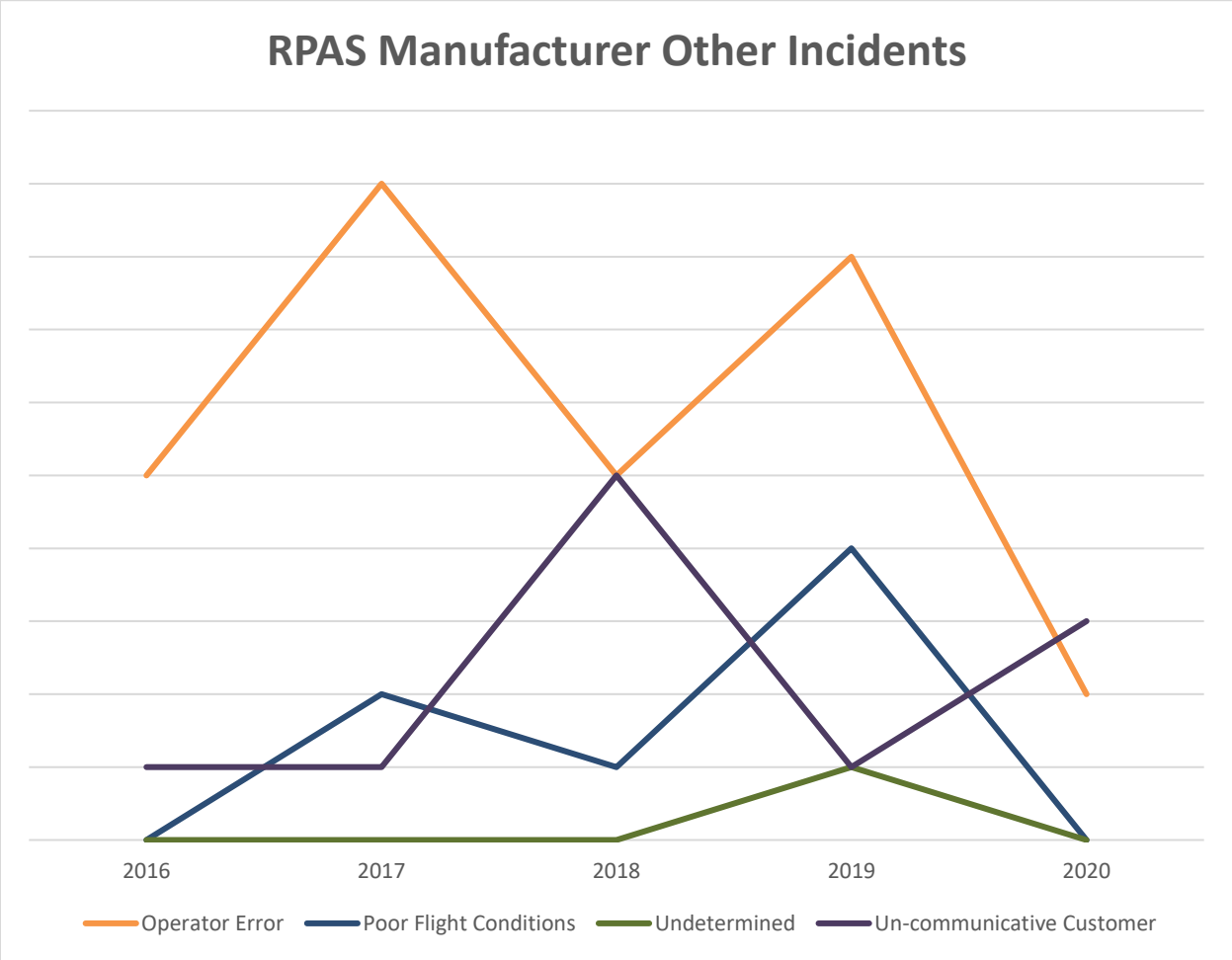


Figure 10 - RPAS Manufacturer Incidents, Other Incidents

As expected, RPAS manufacturer incidents caused by operator error have decreased during the HI-RISE project period and can be attributed to the safety and reliability improvements as well as failure analysis tools and artefacts from HI-RISE. The remaining incident classifications were not significantly affected by the HI-RISE project, given the unresolved nature of the "Undetermined" and "Un-communicative Customer" phases this is also to be expected.

Figure 11 highlights all the incidents during the "RPAS Operator" product development phase broken down by root cause for the years 2016 to 2020.

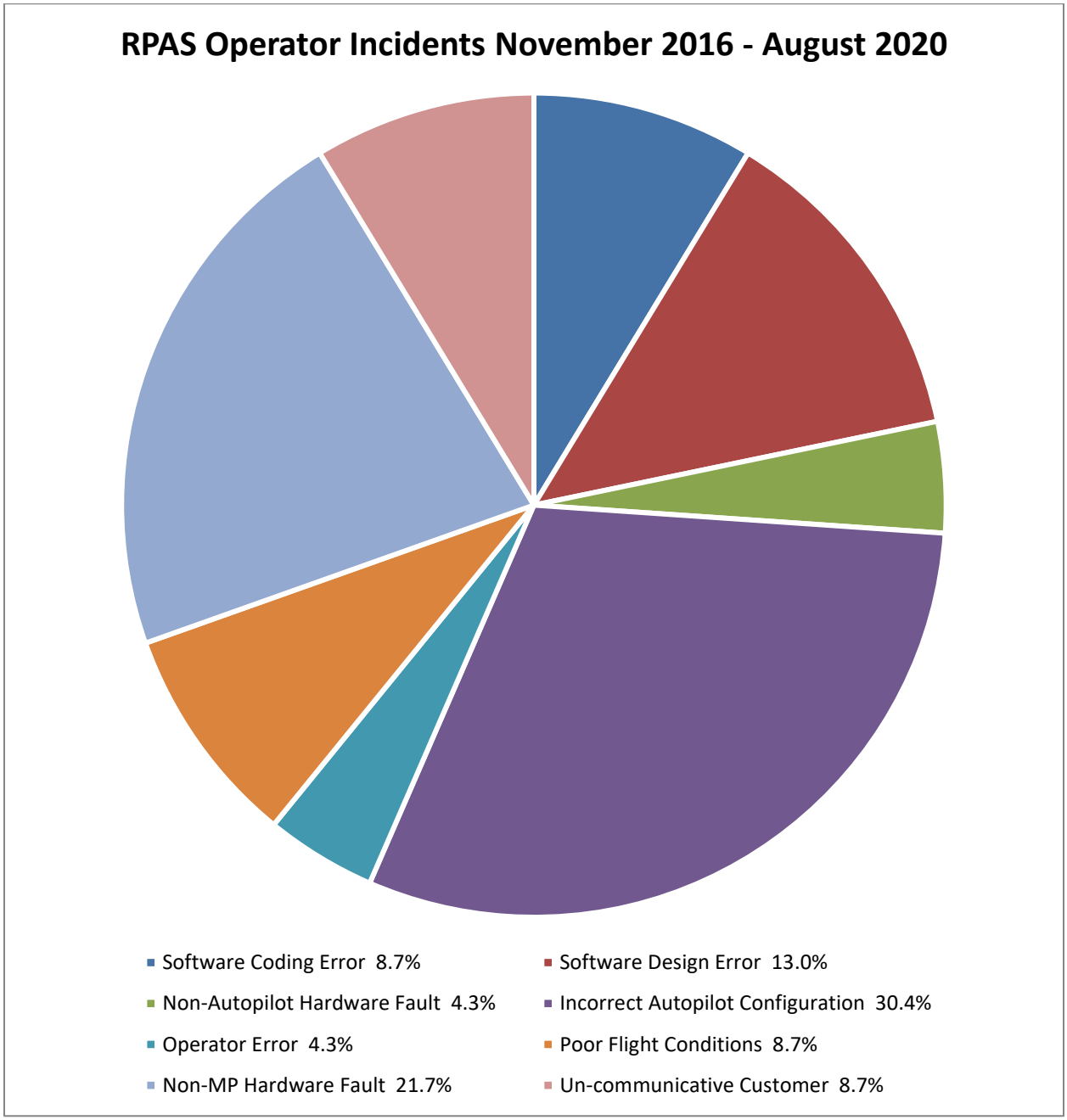


Figure 11 - RPAS Operator Incidents

There is a relatively uniform distribution of root causes for RPAS operator incidents but the two most frequent root causes are configuration errors and non-MicroPilot hardware failures. The HI-RISE failure analysis tools and artefacts will be useful at reducing the occurrence of these failures.

Figure 12 highlights the hardware related incident root causes during the “RPAS Operator” product development phase for the years 2016 to 2020:

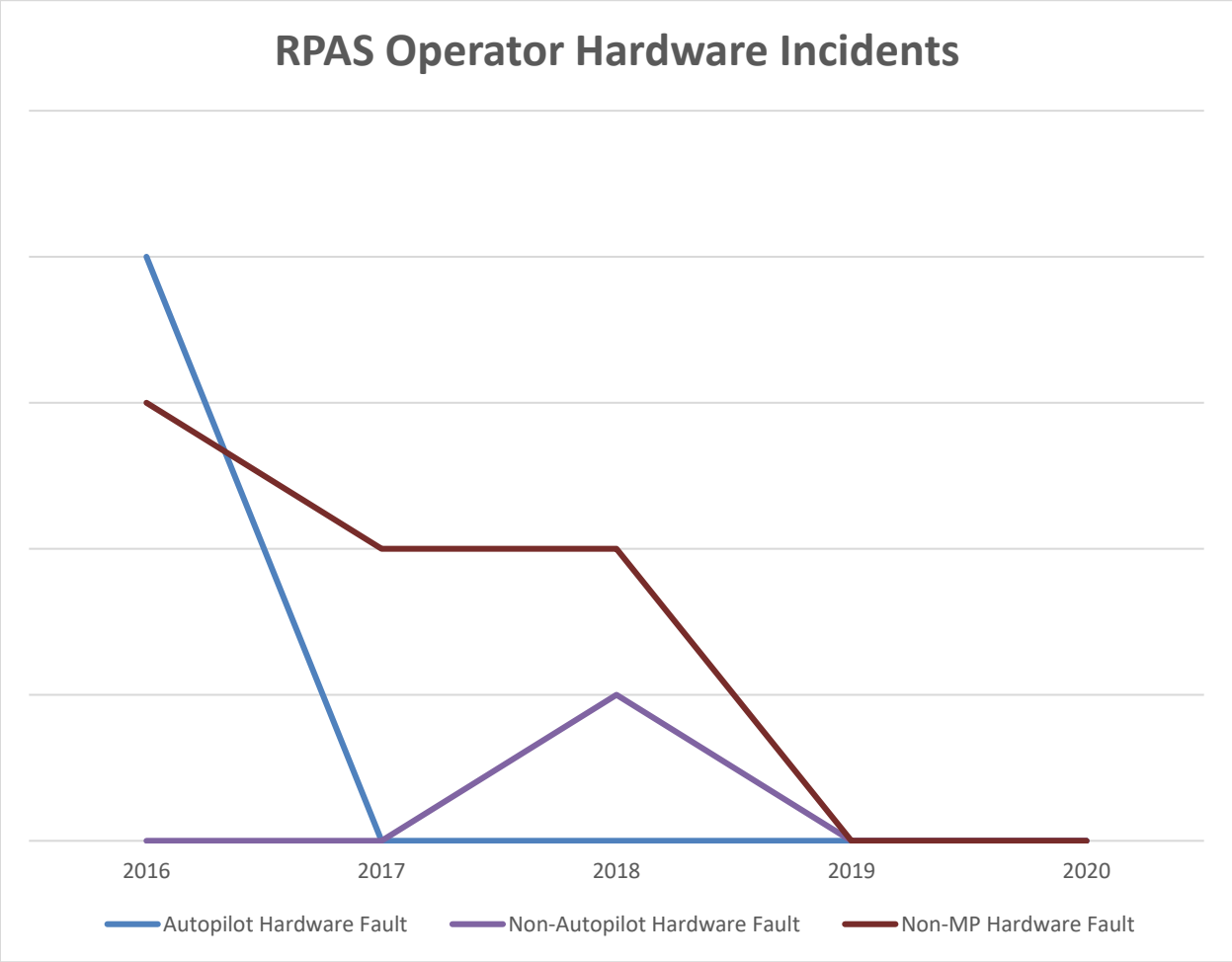


Figure 12 - RPAS Operator Incidents by Year, Hardware Incidents

The RPAS operator incidents caused by hardware failure, of any kind have decreased substantially over the period of HI-RISE.

Figure 13 highlights the software & configuration related incident root causes during the “RPAS Operator” product development phase for the years 2016 to 2020:

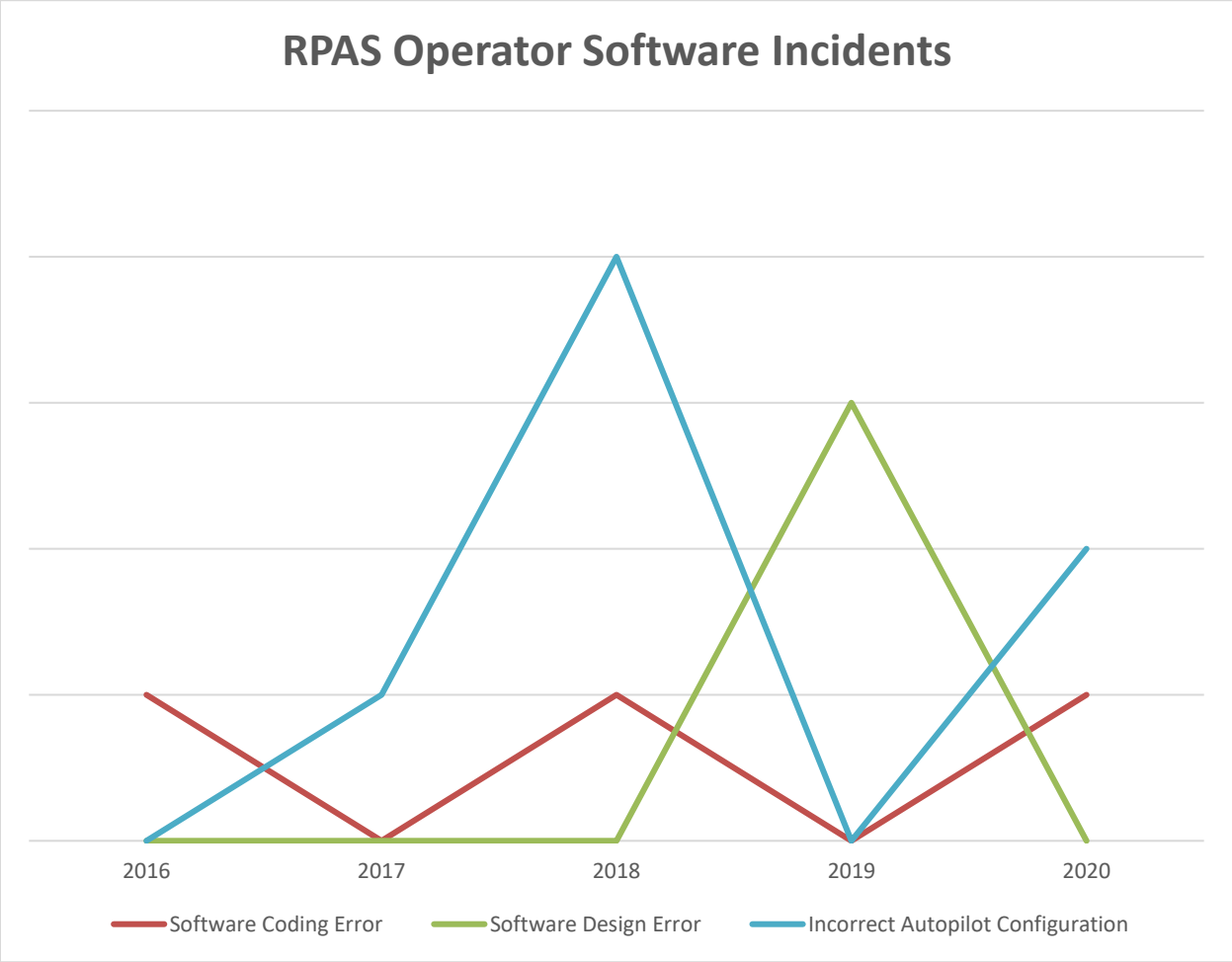


Figure 13 - RPAS Operator Incidents by Year, Software Incidents

The number of RPAS operator incidents caused by software-related failures has remained relatively constant over the HI-RISE project period, but the low number of incidents as a sample size allow for significant year-on-year variation.

Figure 14 highlights the other incident root causes during the "RPAS Operator" product development phase for the years 2016 to 2020:

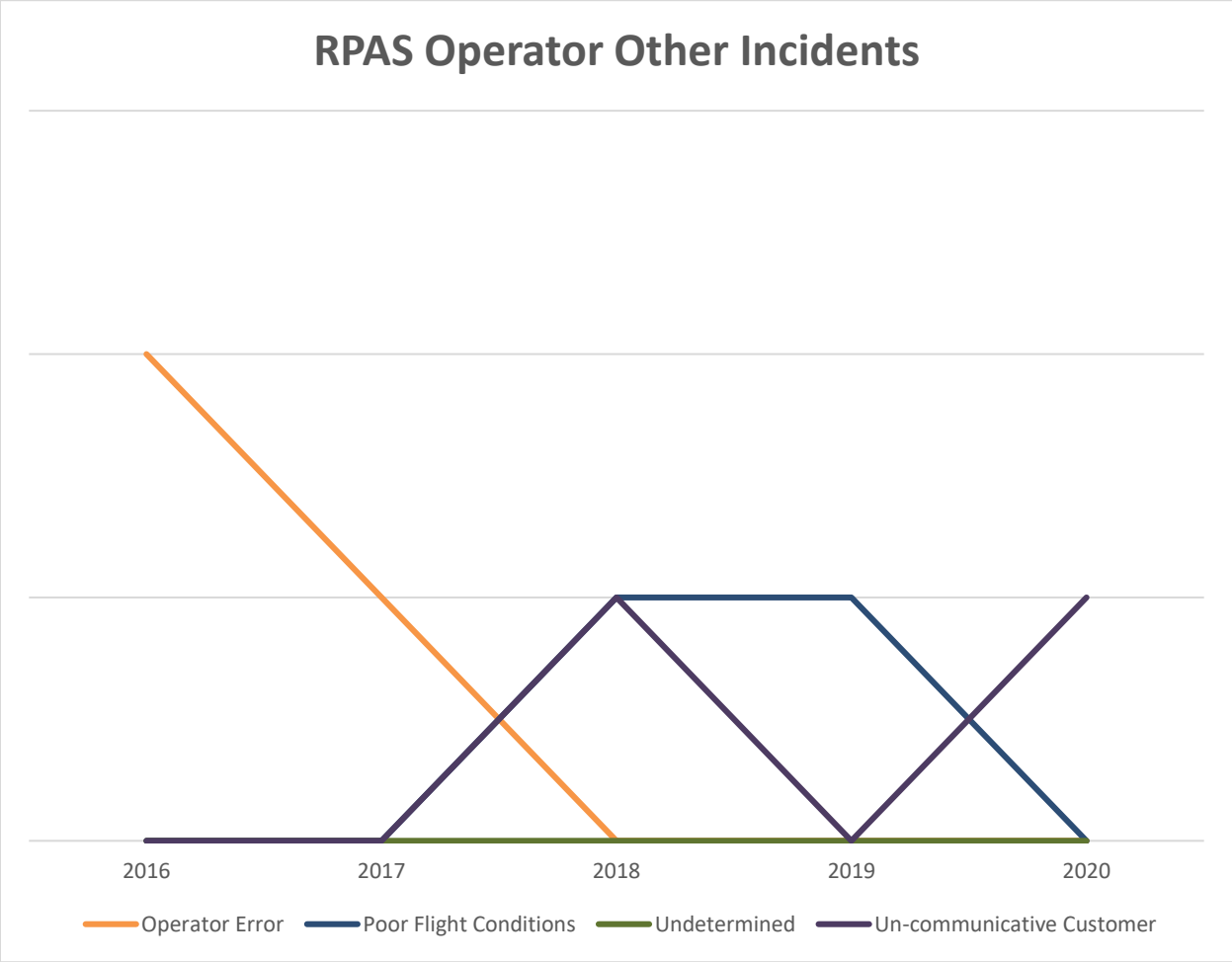


Figure 14 - RPAS Operator Incidents by Year, Other Incidents

As expected, RPAS operator incidents caused by operator error have decreased during the HI-RISE project period and can be attributed to the safety and reliability improvements as well as failure analysis tools and artefacts from HI-RISE. The remaining incident classifications were not significantly affected by the HI-RISE project, given the unresolved nature of the "Undetermined" and "Un-communicative Customer" phases this is also to be expected.

Figure 15 highlights the relative percent of grouped incident root cause during all product development phases for the years 2016 to 2020:

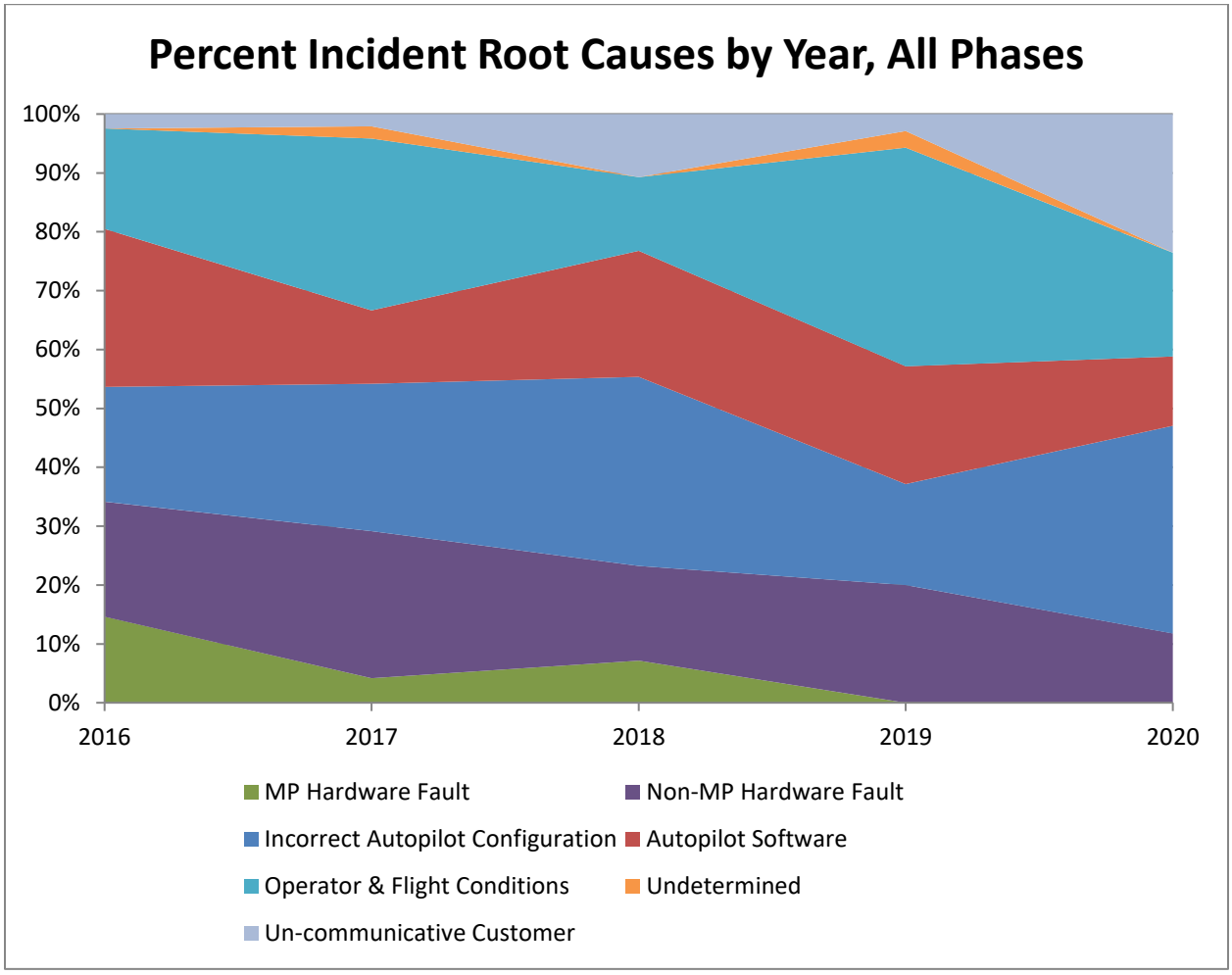


Figure 15 – Percent Incident Root Causes by Year, All Product Development Phases

During the HI-RISE project period the relative number of hardware failures has dropped significantly (combined 35% to 12%). In 2013 MicroPilot started an environmental stress screening process for their products which is seen in the decrease of MP Hardware Faults in the above graph. In 2016 there were three customer issues with the failure of the airspeed sensor. Throughout the HI-RISE project the relative number of autopilot software errors also decreased (from 27% to 12%). These decreases can be attributed to HI-RISE process and framework implementation.

Error! Reference source not found. highlights the percentage of each incident root cause by product development phase during the HI-RISE period, November 2016 to August 2020.

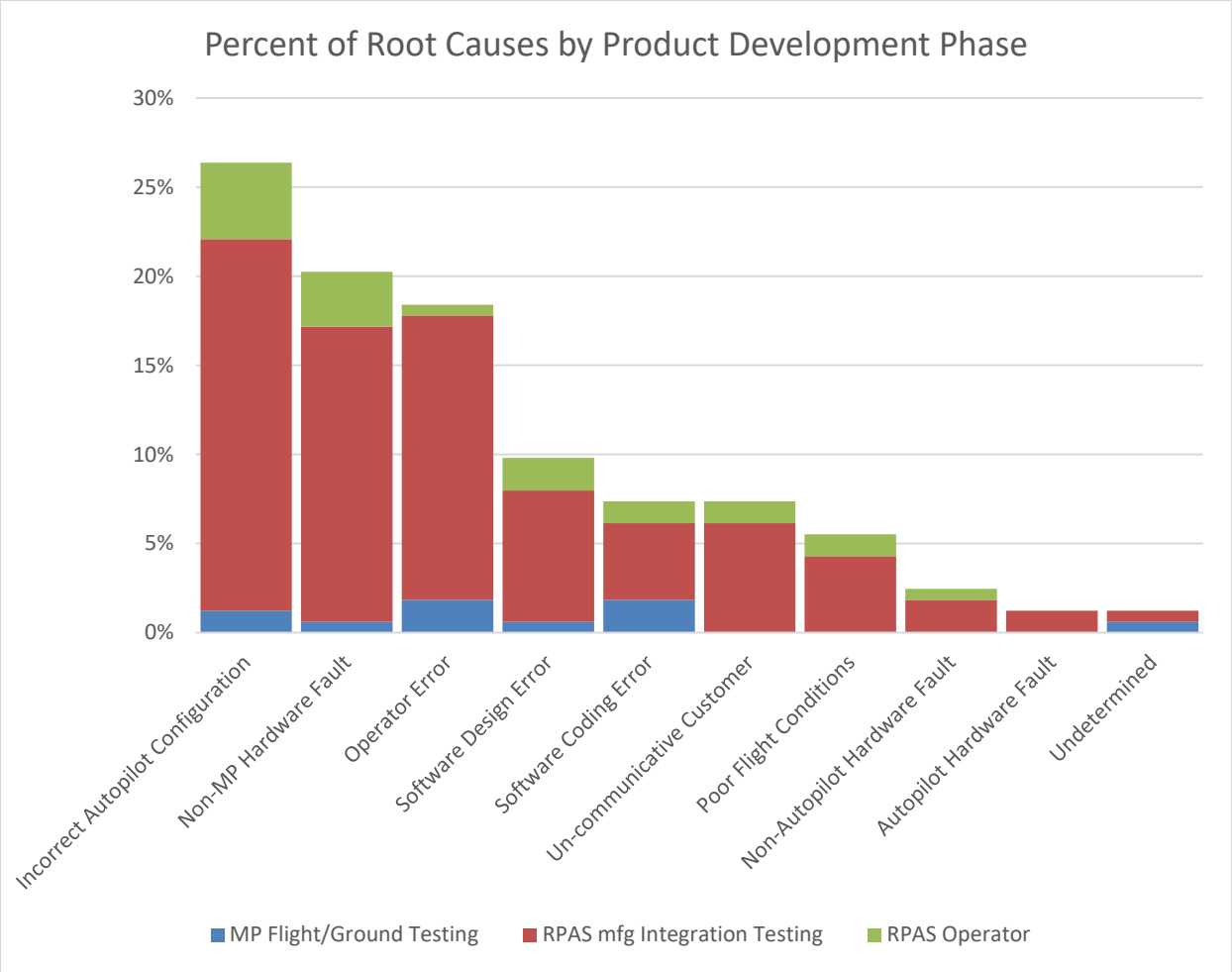


Figure 16 - Percent of Incident Root Cause by Product Development Phase

RPAS manufacturer integration incidents see a large distribution of root causes while RPAS operator incidents are localized mostly to non-autopilot hardware faults, configuration, and software design errors.