UK
Civil Aviation
Authority

Cyber Security Critical Systems Scoping Guidance

CAP 1849

Published by the Civil Aviation Authority, August 2020.

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

First published October 2019
Issue 2 – August 2020

Enquiries regarding the content of this publication should be addressed to: cyber@caa.co.uk
The latest version of this document is available at: www.caa.co.uk/CAP1849

Contents

Contents 3

Introduction 4

Supporting Documentation 4

Background 5

Aviation Essential Service and Functions 6

Critical System Scoping Method 7

Identifying Criticality 9

Completing the Critical Systems Scoping Template 10

Critical Systems Grouping 10

Critical Supplier List 10

Diagramming 11

Notification of Cyber Security Change 12

Annex A: Aviation Functions and Sub-Functions 13

Annex B: Example Critical Systems Diagrams 16

Introduction

Cyber security risk profiles are dynamic, meaning attackers are always looking to exploit vulnerabilities and can quickly develop new ways of breaching cyber security. The aviation industry's progressively interconnected systems require the industry to maintain an up to date awareness of both direct and indirect cyber security threats. The changing threat landscape therefore, encourages a proactive approach to cyber security and in response means aviation organisations need dynamic protection.

The Civil Aviation Authority's (CAA) cyber secuirty oversight strategy must be reviewed regularly in order to keep pace with these ever-changing cyber security trends.

The vision for CAA Cyber Security Oversight is:

"To have a proportionate and effective approach to cyber security oversight that enables aviation to manage their cyber security risks without compromising aviation safety, security or resilience.

To stay up-to-date and positively influence cyber security within aviation to support the UK's National Cyber Security Strategy."

Supporting Documentation

CAP1753 – Cyber Security Oversight Process for Aviation

Cyber Security Critical System Scoping Template

Cyber Assessment Framework (CAF) for Aviation

CAP1850 – Cyber Assessment Framework (CAF) for Aviation Guidance

Background

This guidance is intended to assist aviation organisations in the identification and documentation of their critical network and information systems[1].

Network and Information Systems are defined as:

a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003;

b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by elements covered under paragraph (a) or (b) for the purposes of their operation, use, protection and maintenance.

It is important to clearly identify and document your critical network and information systems to aid in applying comprehensive, appropriate and proportionate cyber security measures. This guidance document aims to provide a methodology for critical system identification that can be applied consistently to aviation organisations of varying types and scale.

When considering the scope of critical systems, the CAA expect an aviation organisation to make an informed and competent consideration of reasonable and expected impacts. The CAA does not expect an aviation organisation to consider implausible scenarios or highly complex chains of events or failures—a reasonable worst-case scenario should be used.

An aviation organisation is ultimately responsible for their own risks and the identification and validation of their critical system scope. To ensure that the scope is accurate and includes critical systems that would reasonably be considered in scope, an aviation organisation must be able to demonstrate that a logical method was followed and included all stakeholders deemed relevant by the organisation (e.g. workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc).

[1] The Network and Information Systems Regulations 2018, SI 2018/506, Schedule 2 section 4 https://www.legislation.gov.uk/uksi/2018/506/made

Aviation Essential Service and Functions

The Department for Transport (DfT) has identified the following key essential services and essential functions within aviation:

- Safe, secure and timely movement of passengers via aircraft and aerodrome[2] facilities.

Provision of this essential service[3] in the air transport sector is achieved through the ownership/management of aerodromes, provision of air traffic services (en-route as well as at an airport) and the running of an air carrier[4].

To aid in the identification of an aviation organisation's critical systems associated with the delivery of this essential service, it is recommended to break the high-level essential service into the functions which enable it. These functions can similarly be broken down further into sub-functions and so forth.

A non-exhaustive list of functions and sub-functions has been provided in **Annex A: Aviation Functions and Sub-Functions**. This should not be used as a check-list, but instead is provided to enable consistency and to assist in the initial functional decomposition of the essential service.

It is important to note that responsibility for functions and sub-functions may be shared across organisations. Aviation organisations should identify both their responsibility and their dependency on functions or sub-functions to which other organisations have responsibility. This identification may highlight previously unknown connections or interdependencies between systems.

> Organisations should ensure that where responsibility is shared, all responsible parties are aware of that responsibility and that reasonable and proportionate measures are taken to manage risk to the shared function or sub-function.

[2] "Aerodrome" has the same meaning as in the Civil Aviation Act 1982. https://www.legislation.gov.uk/ukpga/1982/16/contents

[3] Where provision of this service reaches defined thresholds an aviation organisation will be in scope of The Network and Information Systems Regulations 2018, SI 2018/506, Schedule 2 section 4. https://www.legislation.gov.uk/uksi/2018/506/made

[4] "Air carrier" has the same meaning as in Article 3(4) of Regulation (EC) No 300/2008 of the European Parliament and the Council on common rules in the field of civil aviation security and repealing Regulation EC No 2320/2202. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:PDF

Critical System Scoping Method

It is recommended to engage with diverse group of stakeholders within your organisation during this scoping exercise. This will aid an aviation organisation in better understanding not only the functions and sub-functions that are essential for your organisation, but also the possible impacts and interdependencies.

When completing the functional decomposition of the essential service, an aviation organisation should consider the journey for the passenger, the flight crew and the aircraft where applicable. It can also be helpful to distinguish locality (e.g. landside, airside) when considering the journey.

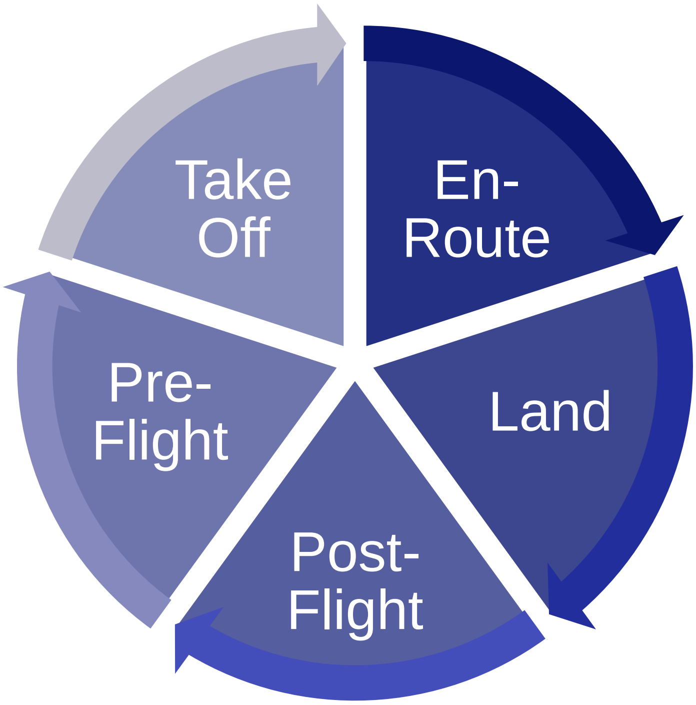

Figure 1: Aviation Journey – Passenger, Flight Crew and Aircraft[5]

As an example, considering the essential service and the start of the passenger journey:

Service: Safe, secure and timely movement of passengers and flight crew via aircraft and aerodrome facilities.

Function: Passenger Services

[5] ICAO Aircraft data definition standard:
https://www.icao.int/safety/airnavigation/AIG/Documents/ADREP%20Taxonomy/ECCAIRS%20Aviation%201.3.0.12%20(VL%20for%20AttrID%20%20391%20-%20Event%20Phases).pdf
ICAO Phase of Flight Definitions
http://www.intlaviationstandards.org/Documents/PhaseofFlightDefinitions.pdf

Sub-Function: Passenger Booking

The “Passenger Booking” sub-function can be further broken down into various network and information systems based components:

Service: Safe, secure and timely movement of passengers and flight crew via aircraft and aerodrome facilities.

Function: Passenger Services

Sub-Function: Passenger Booking

Component: Passenger Booking Application

Component: Kiosk

These components can be further broken down into the hardware, software and information assets they are comprised of:

Component: Passenger Booking Application

Asset: Online booking front end

Asset: Passenger reservation system

Asset: Mobile application

Asset: At airport check-in front end

Asset: Passenger database

Asset: Servers

Asset: Active Directory

Asset: Air Carrier LAN

Asset: API

Asset: WAN (for connectivity to Airport LAN)

Component: Kiosk

Asset: Ticket printer

Asset: Desktop

Asset: Baggage tag printer

Asset: Airport LAN

Identifying Criticality

Once an aviation organisation has identified the relevant functions, sub-functions, components and assets, it should be determined if the loss of confidentiality, integrity or availability would result in:

- Loss of life (flight safety[6]).
- Inability to deliver the essential service[7] or essential functions.

Importantly criticality must be determined without consideration for existing mitigations.

Note: Where systems are deemed mandatory by applicable aviation safety, security or cyber regulations these must be included in your critical systems scope (e.g. record keeping systems, mandatory occurrence reporting systems, CCTV where applicable).

Confidentiality

When assessing criticality complete an assessment of the safety or security impact a loss of this data would incur. Consider the level of classification for the information held within or about the system.

Integrity

While the availability of these network and information systems is necessary for safety, security or operational reasons, the systems not only need to be available but, more importantly, the information they provide must be correct.

A priority to consider when assessing the criticality of systems is therefore the safety-criticality of data elements used in the system. The assessment should distinguish between situations where data corruption is evident and situations where data corruption remains unnoticed (credible corruption).

Availability

When assessing availability, it is important to consider varying degrees of loss of availability (including a degraded but still available system).

[6] ICAO Annex 17 SARP 4.9.1 *"[.. .] critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation"* https://www.icao.int/security/sfp/pages/annex17.aspx

[7] For operators of essential services (OES) The Network and Information Systems Regulations incident reporting thresholds can be used as a guide in identifying a recovery time objective (RTO). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892104/implementation-of-the-nis-directive-dft-guidance-document.pdf

Completing the Critical Systems Scoping Template

Once critical components or assets are identified, the aviation organisation must consider the context within which they operate by identifying their security boundary. To ensure the same level of trust within the environment is maintained, the identified security boundary becomes the critical system boundary. Consistent cyber security controls must be applied to all assets within the critical system boundary. See Annex B Example Critical Systems Diagrams.

Using an appropriate method, an aviation organisation must identify and document all critical systems in scope of the relevant aviation safety, security, or resilience regulation(s). This may include systems and services operated on behalf of the aviation organisation by third party suppliers.

The aviation organisation must complete the Critical System Scoping Template and return this to the CAA as part of a provisional Statement of Assurance (see CAP1753).

Critical Systems Grouping

Critical systems can be grouped where the same cyber security controls have been applied to reduce duplication in the completion of the Cyber Assessment Framework (CAF) for Aviation's system specific Objectives (B and C). See CAF for Aviation Guidance[8] for further information. Critical systems can also be grouped where the same components or assets support multiple functions and sub-functions.

For example, an aviation organisation may group their LAN, WAN, switching, routing, messaging, network security tools, virtualisation environments and access management as “IT Infrastructure Provisioning”. This can be described in the Critical Systems Grouping section of the scoping template.

Critical Supplier List

Aviation is an interconnected, complex environment with multiple critical suppliers and service providers. It is important for aviation organisations to understand their critical supply chain for the provision of essential functions and the methods of connections into their critical system environments (where applicable). It is also important for the CAA to better understand commonality within the supply chain and where aviation organisations contract directly with the third party or rely on critical products or services which are non-contracted.

For the completion of the Critical Systems Scoping Template, the CAA require aviation organisations to document only the first layer of the critical supply chain.

[8] CAP1850
www.caa.co.uk/CAP1850

Diagramming

The following information must be detailed within the submitted diagrams:

- The critical components and/or assets (grouped if needed);
- the security boundary around the critical components and/or assets (critical system boundary);
- other, non-critical, components and assets which are within the critical system boundary, and related interconnectivity (direct wired and wireless);
- ingress and egress points within the critical system boundary.

Aviation organisations may use any existing diagrams that show these key information items. Please see Annex B: Example Critical Systems Diagrams.

Notification of Cyber Security Change

It is highly likely that there will be changes to the critical systems identified, or new critical systems will be introduced to support the essential service. An aviation organisation must notify the CAA's Cyber Security Oversight Team within 30 days of any changes to:

- Critical System scope:
  - New critical function, sub-function, component, or asset is introduced within the organisation;
  - existing critical function, sub-function, component or asset is removed from the organisation;
- critical supplier list;
- cyber security controls which would change the aviation organisation's CAF for Aviation response.

Note: This is in addition to any change notification required under existing safety or security regulations.

Notification of Cyber Security Changes must be sent to cyber@caa.co.uk. If an updated Critical Systems Scoping Template or updated diagramming is required, this must be submitted to the CAA securely.

Annex A: Aviation Functions and Sub-Functions

This is a non-exhaustive list of aviation functions and sub-functions that can be considered during critical systems scoping as part of the functional decomposition of the essential aviation service. Within your organisation these may be structured differently, and you may identify additional functions or sub-functions which are relevant to your organisation. The CAA do not expect an aviation organisation to follow the below as a prescribed list of functions and sub-functions.

Function	Sub-Functions
Landside Operations	Passenger Information Management
	Passenger Processing
	Check-In (including self service)
	Passenger Screening
	Flight Crew Screening
Airside Operations	Flight Data Management
	Airport CDM
	Stand and Gate Management
	Apron Control and Management
	Environment, Noise and Pollution
	Air Bridge Operations
Passenger Services	Passenger Booking
	Passenger Transport
Baggage Services	Baggage Loading/Unloading
	Baggage Handling (airside and landside)
	Ramp Agent
	Baggage Tracking and Reconciliation
	Baggage Screening (hold and hand)
Cargo Services	Cargo Management
	Cargo Transportation
	Cargo Screening

	Weight and Balance
Air Navigation Services	Communications
	Navigation
	Surveillance
	Meteorological
	Aeronautical Information Service
	Air Traffic Management
Aeronautical Information Management *(Aeronautical data and Information with ICAO integrity level to be published in the UK AIP)*	Data Processes (data origination, production, storage, handling, processing, exchange/transfer, distribution and publication)
	Tools and software (used to support data processes)
	Data activities contracted to a third-party
	Contingency Arrangements
Health, Safety and Security	Medical Services
	Rescue Services
	Fire Fighting Services
	Facility Management
	Security Services and Management
Aircraft Services	Aircraft Maintenance and Engineering
	Tug and Push-Back
	Aircraft De-Icing
	Fuel Management
	Waste and Water Services
Aircraft Systems and Avionics	Navigation (ground-based and space based)
	Communications
	Surveillance
	Flight Control

	Cabin Control
	Safety and Security
Flight Operations	Flight Crew Legality
	Flight Crew Information (including briefing)
	Weight and Balance
	Flight Planning

Annex B: Example Critical Systems Diagrams

These diagrams have been produced to provide examples of diagram formats that can be submitted as part of the Critical Systems Scoping Template as they include the requested information items.

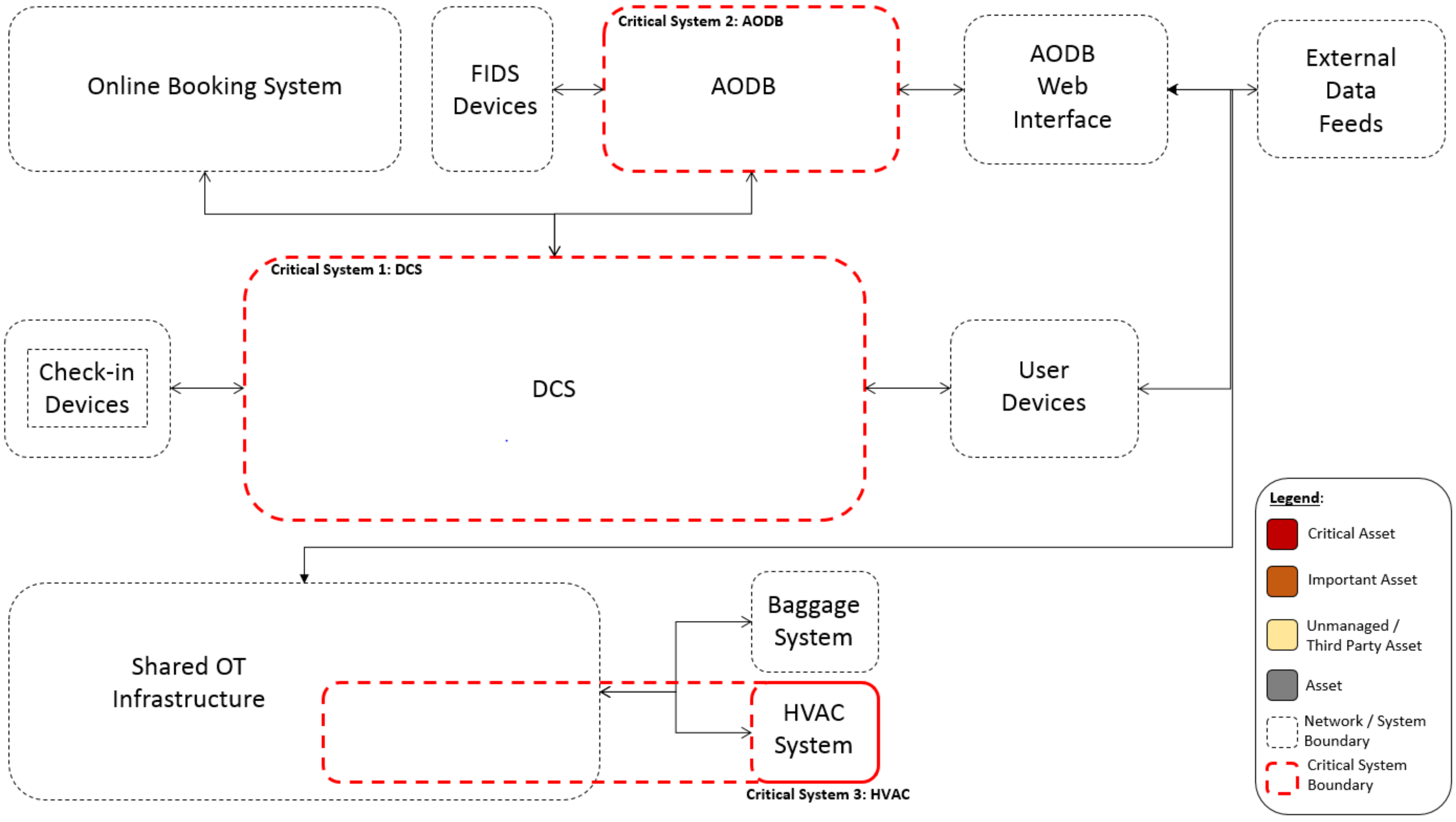

Figure 2: Example conceptual diagram

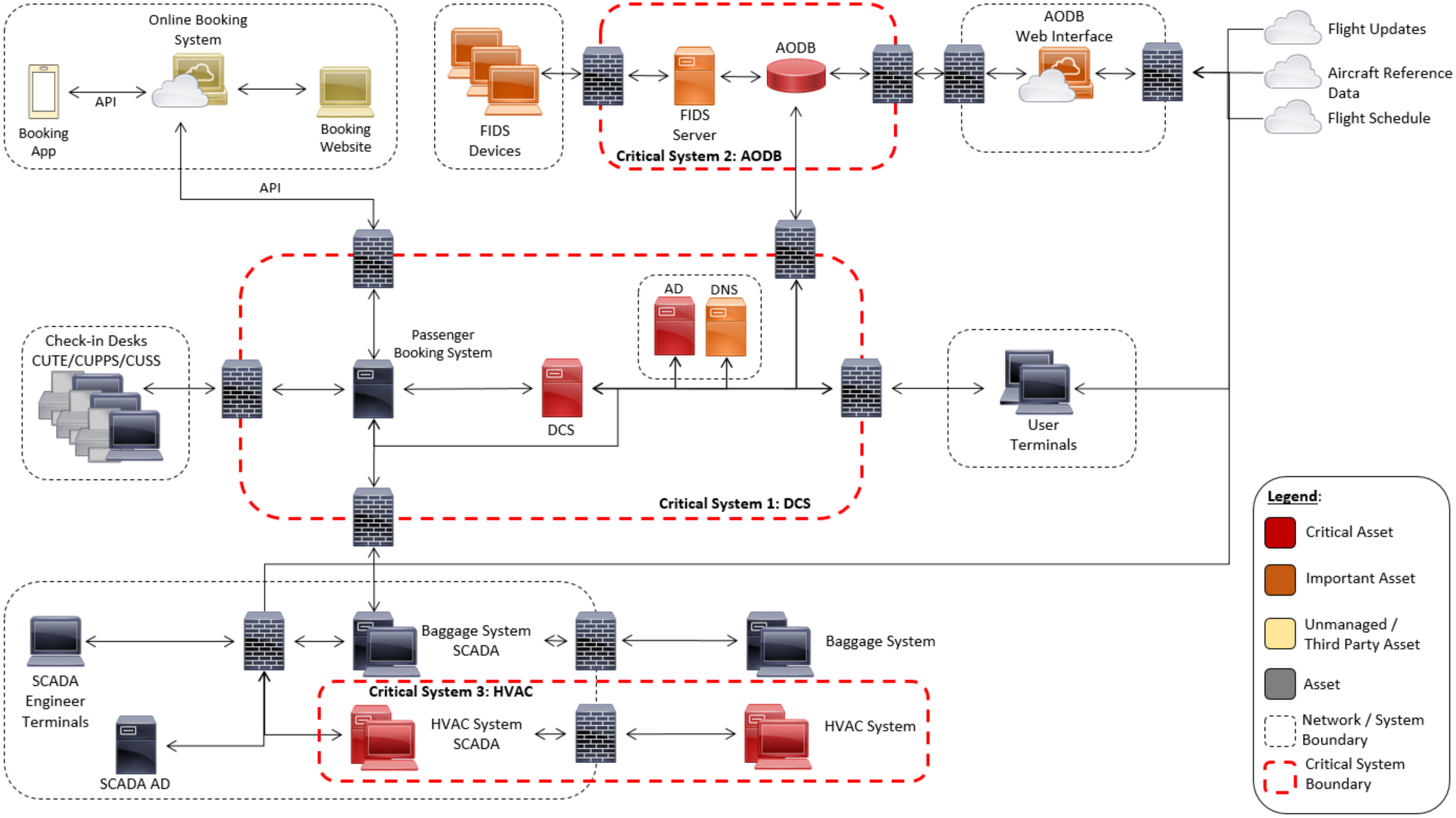

Figure 3: Example Network Diagram

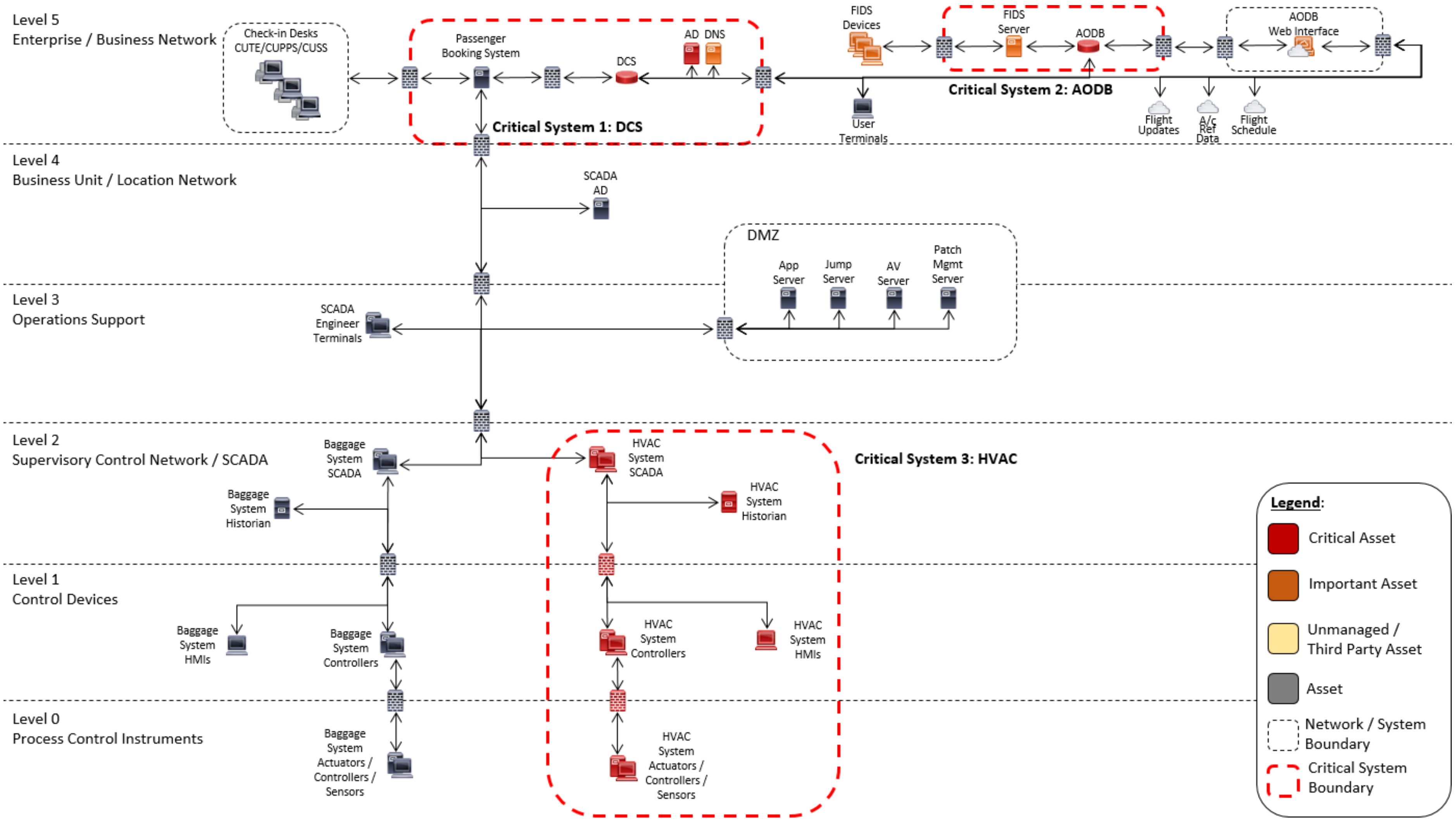

Figure 4: Example Purdue Model Diagram