Business Continuity Manual

Business Continuity Plan: E3

General Building Management System (GBMS) & Supervisory Control and Data Acquisition (SCADA)

		Signature	Revision	Effective Date
Updated By	Senior Manager E&E, TSI	James Ng	32	Jun 2023
Reviewed By	Assistant General Manager BCP, SSBC	Emily Chu		
Approved By	General Manager SSBC	David Jea		

Blank Page

BCP – E3. General Building Management System (GBMS) & Supervisory Control and Data Acquisition (SCADA) Table of Contents

ITEM **SUBJECT MATTER**

Part I – General Building Management System

Part II – Supervisory Control And Data Acquisition

Blank Page

Part I – General Building Management System

A. System Description

1.0 Introduction

1.1 GBMS are installed in Terminal 1 (T1), Terminal 1 Extension (T1E), Sky Bridge, Terminal 1 Satellite Concourse (T1S), Terminal 1 Midfield Concourse (T1M), Ground Transportation Centre (GTC), Ground Transportation Lounge (GTL), Chiller Building for T1M, Midfield Tunnel Ventilation Building (MFTVB), West Hall Tunnel Ventilation Building (WHTVB), HKIA Community Building to facilitate control and monitor operation of Electrical Services.

1.2 The systems are equipped with servers, workstations, Field Control Unit (FCU) and programmable logic controllers (PLC).

1.3 All servers are located inside communication rooms and workstations are installed in Integrated Airport Centre (IAC), Backup IAC and Fault Response Team Management Office (FRTMO) for remote operations.

1.4 PLC is installed inside plant rooms directly connected to field device equipment.

B Physical System Risk

Risk	Description	Mitigation
Server Failure	Loss of communication between workstation and server due to server fail	• Servers are redundant configuration • Auto failover to backup server once the duty server is fail
Fire	Damage of servers due to fire	• Servers are located inside comms rooms protected by gas flooding system or dry pipe system
Water	Damage of server due to water ingress	• Servers are located inside comms rooms protected by water leakage detection system

C Contingency Planning for GBMS Mal-functions

1.0 Failure identified during operating GBMS

1.1 The operator should inform Fault Response Team (FRT) immediately
1.2 FRT to assess impact and report to IAC if affecting terminal operations.

1.3 If the fault could not be rectified in time and will affect terminal operations, FRT will put the associated lighting control panel and power supply equipment into manual operation.

D Contingency Procedures during the passage of Tropical Cyclones

1.0 When typhoon signal no. 1 or above is hoisted, maintenance contractor shall be alerted by TSI Typhoon Support Team or FRT Assistant Manager, Fault Response for performing the typhoon precautionary work such as server checking, workstation checking, clear alarm log and system health checking to ensure the GBMS system are under normal condition when instructed.

2.0 TSI Typhoon Support Team shall coordinate with maintenance contractor to provide sufficient manpower as stipulated in the maintenance contract, with all necessary tools and equipment to perform the typhoon precautionary work in a safe and efficient manner

3.0 After lowering of the typhoon signal and completion of the inspection of all system server, workstation and system alarm log to ensure the GBMS system are under normal condition, TSI Typhoon Support Team may official dismiss maintenance contractor’s typhoon precautionary team.

E. Cyber Security

System cyber security threat level based on the following risk rating:

Threat Level	System
Low	System uses no IT-based systems.
Medium	System uses some closed data-collection and/or alarm systems based on sensors or IoT devices.
High	System uses integrated SCADA systems, cloud-based data collections systems, or IP-based monitoring and control systems.

- General Building Management System – Threat Level: High

Rationale for threat level

General Building Management System is used IP-based for network connection.

Mitigation actions taken

Access to the locations of system workstations are restricted. Only authorized person is allowed to control the system. Further action may be taken on the results of the TS OT Systems Information System Cybersecurity Vulnerabilities survey.

In case of suspected cyber attack, Risk & Cybersecurity Team of ITD shall be informed for further investigation.

F. Interface with Other Operational Organizations during Contingency

- FRTMO
- IAC
- TOD
- LD

Part II – Supervisory Control And Data Acquisition

A. Description

1.0 Introduction

1.1 Airfield SCADA are installed in Airfield and switching station to facilitate control and monitor operation of electrical equipment.

1.2 The systems are equipped with servers, workstations, Field Control Unit (FCU) and programmable logic controllers (PLC).

1.3 All servers are located inside communication rooms and workstations are installed in IAC, Backup IAC and FRTMO for remote operations.

1.4 PLC is installed inside plant rooms directly connected to field device equipment.

B. Physical System Risk

Risk	Description	Mitigation
Server Failure	Loss of communication between workstation and server due to server fail	• Servers are redundant configuration • Auto failover to backup server once the duty server is fail
Fire	Damage of servers due to fire	• Servers are located inside comms rooms protected by gas flooding system or dry pipe system
Water	Damage of server due to water ingress	• Servers are located inside comms rooms protected by water leakage detection system

C Contingency Planning for AIRFIELD SCADA Mal-functions

1.0 Failure identified during operating Airfield SCADA

1.1 The operator should inform Fault Response Team (FRT) immediately.

1.2 FRT to assess impact and report to IAC if affecting terminal operations.

1.3 If the fault could not be rectified in time and will affect terminal operations, FRT will put the associated high mast lighting control, Airfield Tunnel Control into manual operation.

D. Contingency Procedures during the passage of Tropical Cyclones

1.0 When typhoon signal no. 1 or above is hoisted, maintenance contractor shall be alerted by TSI Typhoon Support Team or FRT Assistant Manager, Fault Response for performing the typhoon precautionary work such as Server checking, workstation checking, clear alarm log and system health checking to ensure the SCADA system are under normal condition when instructed.

2.0 TSI Typhoon Support Team shall coordinate with maintenance contractor to provide sufficient manpower as stipulated in the maintenance contract, with all necessary tools and equipment to perform the typhoon precautionary work in a safe and efficient manner.

3.0 After lowering of the typhoon signal and completion of the inspection of all system server, workstation and system alarm log to ensure the SCADA system are under normal condition, TSI Typhoon Support Team may official dismiss maintenance contractor’s typhoon precautionary team.

E. Cyber Security

System cyber security threat level based on the following risk rating:

Threat Level	System
Low	System uses no IT-based systems.
Medium	System uses some closed data-collection and/or alarm systems based on sensors or IoT devices.
High	System uses integrated SCADA systems, cloud-based data collections systems, or IP-based monitoring and control systems.

- Supervisory Control And Data Acquisition – Threat Level: High

Rationale for threat level

System is used IP-based for network connection.

Mitigation actions taken

Access to the locations of system workstations are restricted. Only authorized person is allowed to control the system. Further action may be taken on the results of the TS OT Systems Information System Cybersecurity Vulnerabilities survey.

In case of suspected cyber-attack, Risk & Cybersecurity Team of ITD shall be informed for further investigation.

F. Interface with Other Operational Organizations during Contingency

1. FRTMO
2. IAC
3. AD
4. TOD

End of BCP – E3

Blank Page