Matrice des compétences – Séquence IIoT (TP4 · TP5 · TP6)

BTS CIEL option A « Informatique et Réseaux » – Référentiel 2023 (compétences C01 à C11)

TP4	Configuration du Port IT Master IO-Link, Plan d'adressage IP, Broker MQTT Mosquitto et Analyse JSON
TP5	Stockage de séries temporelles : ingestion par Telegraf et base de données InfluxDB v2
TP6	Supervision et Alerting 4.0 : visualisation Grafana, notifications Webhook et audit IT/OT

1. Rappel : blocs de compétences de l'option A

Unité	Bloc de compétences	Compétences
U4	Bloc 1 – Étude et conception de réseaux informatiques	C04 Analyser · C05 Concevoir
U5	Bloc 2 – Exploitation et maintenance de réseaux informatiques	C02 Organiser · C06 Valider · C09 Installer · C11 Maintenir
U6	Bloc 3 – Valorisation de la donnée et cybersécurité	C01 Communiquer · C03 Gérer un projet · C08 Coder · C10 Exploiter

Activités types du référentiel principalement visées par la séquence : **R2** Installation et qualification · **R3** Exploitation et maintien en condition opérationnelle · **D4** Valorisation de la donnée · **D5** Audit de l'installation ou du système · **D3** Gestion d'incidents.

2. Matrice de synthèse compétences × TP

● **Validée**	Compétence évaluée dans la grille de notation actuelle du TP (« Valide Cxx »).
◐ **Mobilisée**	Compétence fortement sollicitée par les activités, observable mais non notée à ce jour.
○ **Partielle**	Compétence sollicitée de façon ponctuelle ou transversale.
—	Non mobilisée.

Code	Compétence (option A – IR)	Unité / Bloc	TP4 – IO-Link / IP / MQTT	TP5 – Telegraf / InfluxDB	TP6 – Grafana / Alerting / Audit	Éléments du TP qui la mobilisent
C01	**Communiquer en situation professionnelle (FR/EN)**	U6 – Bloc 3	○ Partielle	○ Partielle	◐ Mobilisée	Compte rendu + captures (TP4-5) ; conclusion argumentée et message d'alerte destiné à la maintenance (TP6) ; documentation IFM en anglais
C02	**Organiser une intervention**	U5 – Bloc 2	○ Partielle	○ Partielle	○ Partielle	Préparation du poste, respect de l'ordre des procédures (IP → Master → VM → service), sauvegarde telegraf.conf.bak
C03	**Gérer un projet**	U6 – Bloc 3	—	—	—	Non mobilisée (TP guidés)
C04	**Analyser un système informatique**	U4 – Bloc 1	● **Validée**	● **Validée**	● **Validée**	Architecture en Y, décodage JSON/pdin, persistance TSDB, analyse encrassement, conclusion Edge/Starlark
C05	**Concevoir un système informatique**	U4 – Bloc 1	● **Validée**	● **Validée**	● **Validée**	Choix d'infrastructure IoT (collecte → transmission → stockage → exploitation), sécurité des communications
C06	**Valider un système informatique**	U5 – Bloc 2	◐ Mobilisée	◐ Mobilisée	◐ Mobilisée	Tests ping/tcpdump/nc/mosquitto_sub, contrôle ingestion (journalctl, Flux), test d'alerte réel, audit de cloisonnement
C08	**Coder**	U6 – Bloc 3	○ Partielle	◐ Mobilisée	◐ Mobilisée	Netplan YAML (TP4) ; telegraf.conf TOML + parser json_v2 + requêtes Flux (TP5) ; Flux avec conversion hex → int (TP6)
C09	**Installer un réseau informatique**	U5 – Bloc 2	◐ Mobilisée	◐ Mobilisée	◐ Mobilisée	Plan d'adressage IT/OT, VM 2 cartes (pont), Mosquitto (MQTT) ; dépôts APT/GPG, InfluxDB, Telegraf ; Grafana, sysctl
C10	**Exploiter un réseau informatique**	U6 – Bloc 3	◐ Mobilisée	◐ Mobilisée	◐ Mobilisée	CLI Linux, systemctl, capture de trames ; exploitation des logs ; logiciel de supervision, alerting, audit IT/OT (D5)
C11	**Maintenir un réseau informatique**	U5 – Bloc 2	○ Partielle	◐ Mobilisée	◐ Mobilisée	Diagnostic des flux (TP4) ; détection d'encrassement / maintenance prédictive (TP5) ; alerte et qualification d'incident (TP6)

3. Détail par TP : activités, connaissances et critères

TP4 – Port IT Master IO-Link, plan d'adressage IP, Mosquitto et analyse JSON

Partie du TP	Activités élève	Comp.	Connaissances associées (niveau taxo.)	Critère d'évaluation du référentiel	Barème
VIII – Étude préalable architecture & protocoles	Rôle du Master IO-Link et intérêt de la double interface (architecture en Y) Principe MQTT : broker, publisher, subscriber, topic Risque du port 1883 en clair / apport de TLS 8883 Justifier 2 sous-réseaux, IP statiques, absence de routage OT↔IT	**C04** **C05**	Infrastructures réparties ; documents d'architecture (synoptiques, matrice de flux) – N3 Solutions de conception IoT (collecte, transmission) – N2 Niveaux de sécurité attendus (chiffrement, protection des communications) – N2	*La structure de la solution technique est critiquée* *L'organisation structurelle des sous-ensembles est conforme aux exigences fonctionnelles*	/4
IX – Configuration IP de l'architecture	Adresser le PC Étudiant (192.168.2.20/24, sans passerelle) Joindre le Port IT du Master (192.168.2.12) via Moneo Configure et navigateur VM Ubuntu : mode pont, netplan enp0s3 statique + enp0s8 DHCP, netplan apply Tests ping PC ↔ Master ↔ VM ↔ Internet	**C09** **C06** **C08**	Protocoles IPv4, TCP/IP, Ethernet, DHCP – N4 Systèmes d'exploitation, virtualisation – N3 Réseaux informatiques (protocoles, équipements industriels) – N4	*Une procédure de configuration est déterminée ainsi que les points critiques* *La ou les procédures choisies sont suivies* *Les tests sont appliqués*	/4
X – Envoi des données MQTT & capture de flux	Paramétrer l'export MQTT du Master (Event Counter/Timer[1], PDin port 2, topic usine/castelnaudary/ligne1) Capturer le flux : tcpdump -i enp0s3, écoute nc -l -p 1883 Identifier la donnée utile dans la trame JSON	**C10** **C06** **C11**	Interface ligne de commande d'équipements et d'OS – N3 Outils d'analyse, de tests et de traçabilité – N3 Caractéristiques des communications des systèmes étudiés – N3	*Le fonctionnement d'un équipement est vérifié en tenant compte du contexte opérationnel* *Les résultats de tests et d'analyse sont interprétés de manière pertinente*	/3
XI – Installation & configuration de Mosquitto	apt install mosquitto mosquitto-clients Listener 1883 sur 192.168.2.100 (default.conf) systemctl restart / status Souscription mosquitto_sub -t "…/#" -v	**C05** **C09**	Protocole MQTT – N2 (C09) Infrastructures logicielles centralisées/réparties – N2 Analyse des tests d'intégration – N3	*Les ressources permettant de réaliser le cahier des charges sont recensées et définies* *Les solutions logicielles proposées sont conformes aux spécifications*	/3 – Valide C05
XI (suite) – Analyse JSON, décodage capteur & sécurité	Expliquer les champs de la trame (code, cid, adr, eventno, srcurl, payload) Extraire la distance / réflectivité de la chaîne pdin hexadécimale Observer la variation en temps réel Analyser les limites TLS du Master et proposer une solution	**C04**	Fonctions et caractéristiques d'une chaîne de mesure – N3 Recherche et analyse de documentation y compris en anglais – N3 Méthodologies d'analyse de risque (EBIOS, ISO 27005) – N2	*Les spécifications du cahier des charges sont extraites* *La structure de la solution technique est critiquée* *Face à un ensemble de faits, des actions appropriées sont décidées*	/6 – Valide C04

TP5 – Ingestion Telegraf et base de séries temporelles InfluxDB v2

Partie du TP	Activités élève	Comp.	Connaissances associées (niveau taxo.)	Critère d'évaluation du référentiel	Barème
VIII – Étude préalable de la persistance	Comparer SQL relationnel et TSDB (InfluxDB) Justifier le middleware Telegraf plutôt qu'une écriture directe du Master Expliquer le parsing JSON, Fields vs Tags	**C04** **C05**	Infrastructures logicielles centralisées/réparties – N3 Solutions de conception IoT (exploitation des données) – N2 Bases de données et environnements de traitement de données – N4 (C08)	*La structure de la solution technique est critiquée* *Les ressources permettant de réaliser le cahier des charges sont recensées et définies*	/4
IX – Installation d'InfluxDB v2	Téléchargement et dpkg -i du paquet influxdb2 systemctl daemon-reload / enable --now / status Initialisation Web :8086 : organisation Lycee_Jules_Fil, bucket iiot_cassoulet, relevé du Token	**C09** **C10**	Systèmes d'exploitation (UNIX) – N3 Outils de mise à jour et gestion des paquets logiciels – N3 Protocole HTTP – N4	*La ou les procédures choisies sont suivies* *Les activités sont menées en respectant les règles de sécurité (gestion du Token)*	/4
X – Installation & configuration de Telegraf	Import clé GPG, déclaration du dépôt APT, installation Sauvegarde telegraf.conf.bak Rédaction du telegraf.conf : outputs.influxdb_v2 + inputs.mqtt_consumer + json_v2 (pdin_hex, compteur_event) Redémarrage et contrôle du service	**C05** **C08** **C09**	Infrastructures logicielles réparties – N2 Scripts d'automatisation et d'industrialisation – N4 Politique de sauvegarde/restauration – N3	*Les solutions logicielles proposées sont conformes aux spécifications du cahier des charges* *Les composants logiciels sont développés conformément aux spécifications et aux politiques de sécurité*	/3 – Valide C05
XI.1–2 – Ingestion MQTT, logs et requêtes Flux	Analyser les logs : journalctl -u telegraf -f Requête Flux dans le Script Editor (range, filter _field == pdin_hex) Affichage Table ; expliquer pourquoi le Graph échoue (champ string)	**C06** **C10** **C08**	Tests unitaires et d'intégration – N3 Outils de traçabilité et d'analyse – N3 Bases de données – N4	*Les tests sont appliqués* *Les résultats de tests sont synthétisés pour évaluer la conformité* *Le fonctionnement d'un logiciel est vérifié en contexte opérationnel*	/3
XI.3 – Simulation d'encrassement & maintenance prédictive	Analyser l'évolution des valeurs après pose d'un adhésif sur l'optique Mettre en évidence la chute de réflectivité Conclure sur l'intérêt de la maintenance prédictive	**C04** **C11**	Chaîne de mesure – N3 Caractérisation temporelle des signaux – N3 Outils d'analyse et de rapport d'incident – N3 (C11)	*La structure de la solution technique est critiquée* *Les causes de l'incident sont localisées* *Le client est informé des mesures de prévention possibles*	/6 – Valide C04

TP6 – Supervision Grafana, alerting Webhook et audit IT/OT

Partie du TP	Activités élève	Comp.	Connaissances associées (niveau taxo.)	Critère d'évaluation du référentiel	Barème
VIII – Étude préalable supervision & webhooks	Rôle de Grafana en IIoT et couplage avec une TSDB IHM locale vs supervision centralisée Fonctionnement d'un Webhook HTTP POST Passage du préventif au prédictif	**C04** **C05**	Logiciels de supervision et protocoles associés – N3 (C10) Infrastructures centralisées/réparties – N3 Protocoles HTTP/HTTPS – N4	*La structure de la solution technique est critiquée* *Les solutions proposées sont conformes aux spécifications*	/3
IX.1–2 – Installation & configuration de Grafana	Dépôt APT signé, installation, enable --now grafana-server Accès :3000, ajout de la source InfluxDB (Flux, URL, org, bucket, token) Test « datasource is working »	**C09** **C06**	Systèmes d'exploitation – N3 Gestion des paquets et sécurité système – N3 Environnements de déploiement logiciel – N2	*Une procédure d'installation est déterminée ainsi que les points critiques* *Les tests d'intégration sont appliqués*	/4
IX.3 – Dashboard décisionnel & mode Kiosk	Panneau Gauge réflectivité (seuils 20 / 30 %) Time-series distance + réflectivité ; Stat distance Requête Flux : substring + hex.int() (conversion pdin) Partage du tableau de bord en mode Kiosk	**C05** **C08** **C10**	Solutions de conception IoT (exploitation des données) – N2 Langages de développement / traitement de données – N4 Logiciels de supervision – N3	*Les solutions logicielles proposées sont conformes aux spécifications du cahier des charges* *Le souci constant de la qualité est recherché*	/3 – Valide C05
X – Système d'alerte & Webhook Google Chat	Création de l'espace et du Webhook entrant Point de contact + Default policy Règle « Réflectivité < 20 % » (évaluation 30 s, état Firing) Test réel par obstruction du capteur	**C06** **C10** **C11**	Fiches de recette (scénario, résultat attendu) – N3 Logiciels de supervision – N3 Procédures d'exploitation et niveaux de criticité – N2	*Les procédures de test sont établies et appliquées* *L'incident est qualifié et escaladé, le service est opérationnel*	/3
XI – Audit de cloisonnement IT/OT	Ping VM → PLC 192.168.1.10 (doit échouer) tcpdump filtre PROFINET RT Contrôle net.ipv4.ip_forward dans /etc/sysctl.conf	**C10** **C06**	Sécurisation des réseaux (ACL, pare-feu) – N3 (C06) Routage – N3 (C09) Documents réglementaires sécurité SI (ANSSI) – N2	*Le fonctionnement d'un équipement est vérifié en tenant compte du contexte opérationnel* *Face à un ensemble de faits, des actions appropriées sont décidées*	(inclus dans Conclusion)
XII – Conclusion & analyse technique	Montée en charge : 50 capteurs avec décodage Flux Archivage brut hex vs décimal Déport de la conversion (Starlark / Edge / automate) Complémentarité alerte OT (%Q0.0) / IT (Grafana)	**C04** **C01**	Infrastructures réparties – N3 Analyse de risque – N2 Communication écrite argumentée (C01)	*Les algorithmes sont critiqués* *La structure de la solution technique est critiquée*	/6 – Valide C04

4. Couverture des unités et proposition d'ajustement

Les grilles actuelles valident uniquement **C04** et **C05**, soit l'unité **U4** (Bloc 1). Or les trois TP mobilisent fortement les compétences des blocs 2 (U5) et 3 (U6). Pour alimenter aussi ces unités sans modifier le barème sur 20, il suffit d'ajouter une mention « Valide Cxx » sur les lignes existantes :

TP	Validation actuelle (grille)	Proposition complémentaire	Indicateurs de réussite
TP4	C04 (/6) + C05 (/3)	Ajouter **C09 Installer** sur « Configuration du plan d'adressage IP » (/4) et « Déploiement Mosquitto »	Critères observables : IP/masque conformes, netplan appliqué sans erreur, pings validés, service Mosquitto active (running), listener sur 192.168.2.100
TP5	C04 (/6) + C05 (/3)	Ajouter **C08 Coder** sur telegraf.conf / Flux , **C10 Exploiter** sur l'analyse des logs (/3) et **C11 Maintenir** sur la détection d'encrassement (/6)	Critères observables : fichier TOML fonctionnel avec parser json_v2, aucune erreur dans journalctl, requête Flux renvoyant la table pdin_hex
TP6	C04 (/6) + C05 (/3)	Ajouter **C06 Valider** sur le test d'alerte et **C10 Exploiter** sur l'audit IT/OT	Critères observables : notification reçue dans Google Chat après obstruction, ping OT échoue, ip_forward = 0 justifié

Avec cet ajustement, la séquence TP4 → TP6 couvre les trois unités professionnelles : U4 (C04, C05), U5 (C06, C09, C11) et U6 (C08, C10), C01 restant évaluée de façon transversale via les comptes rendus.