



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



UN PARE-FEU POUR LE HDMI

Pierre-Michel RICORDEL
José LOPES-ESTEVE

ANSSI/SDE/ST/LSF

LSF

La Problématique



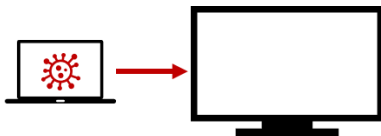
Les salles de réunion sont souvent équipées d'un système de projection fixé à demeure :

- Projecteur
- Moniteur ou Téléviseur (de plus en plus : Smart TV Android)
- Système de visio-conférence

A différents moments, le système de projection peut être utilisé par différentes personnes :

- Visiteur extérieur
- Employé interne
- V.I.P.

Le Risque



1: un ordinateur injecte un
implant logique dans l'écran



2 : l'implant reste
stocké dans l'écran



3 : l'implant déclenche une vulnérabilité
qui compromet l'ordinateur qui y est branché

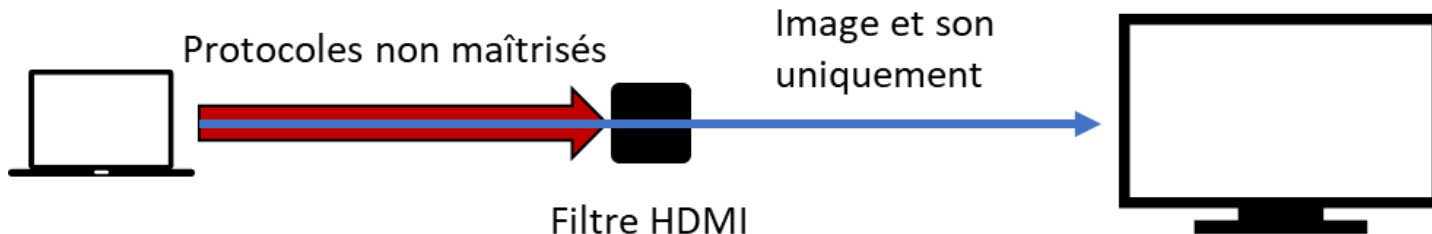
Le HDMI présente une surface d'attaque qui peut servir de rebond d'un système à un autre

La surface d'attaque

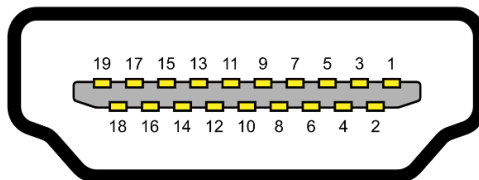
- EDID Fuzzer : <https://github.com/nccgroup/EDIDFuzzer> (Andy Davis, Blackhat EU 2012)
 - Crash du driver Nvidia nvlddmkm.sys sous Windows 7
- Fuzzing CEC : Joshua Smith DEFCON 23 (2015)
 - Crash d'un téléviseur Panasonic via CEC
- Fuzzing CEC+EDID : Hyejin Jeong, DEFCON 27 (2019) (+Changhyeon Moon, HITB 2019)
 - Vulns CEC sur Android et EDID sur le driver i915 Ubuntu Linux
- Cinq CVE en 2017 dans le noyau Linux Android (trois EDID, deux CEC)
 - CVE-2017-{9689, 9719, 9722, 11030, 11093}
- Echange de données à travers d'un KVM (l'écran sert de support de stockage)
 - C.f. Protection Profile for Peripheral Sharing Switch, NIAP 2015

Le Concept

Un « pare-feu » ou « filtre » placé en coupure qui réduit la surface d'attaque du moniteur

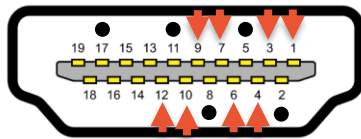


Le Connecteur HDMI



1 : TMDS Data2+	2 : Shield 2	3 : TMDS Data2-	4 : TMDS Data1+	5 : Shield 1
6 : TMDS Data1-	7 : TMDS Data0+	8 : Shield 0	9 : TMDS Data0-	10 : TMDS Clock+
11 : Shield Clock	12 : TMDS Clock-	13 : CEC	14 : HEAC+	15 : DDC (I ² C SCL)
16 : DDC (I ² C SDA)	17 : GND	18 : +5V	19 : Hot plug/HEAC-/MHL CBUS	

Le câble contient 19 fils qui véhiculent un grand nombre de protocoles que nous allons détailler



TMDS : *Transition-Minimized Differential Signaling*

Véhicule l'image et le son sous forme numérique, à travers 4 paires différentielles :

- Rouge
- Vert
- Bleu
- Horloge

Le son est transmis encodé dans les marges non visibles de l'image

Le signal est unidirectionnel

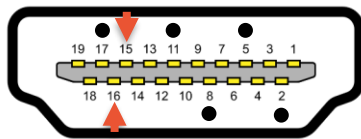
Le débit est très rapide (jusqu'à 48 Gigabit/s en HDMI 2.1)

Attention aux Signaux Parasites Compromettants !

Les signaux TMDS doivent respecter des contraintes très strictes de routage :

- Impédance conforme
- Blindage des lignes
- Symétrie, et longueur identique des lignes

Ces signaux sont unidirectionnels,
et sont essentiels au bon fonctionnement.
Ils doivent donc traverser le filtre



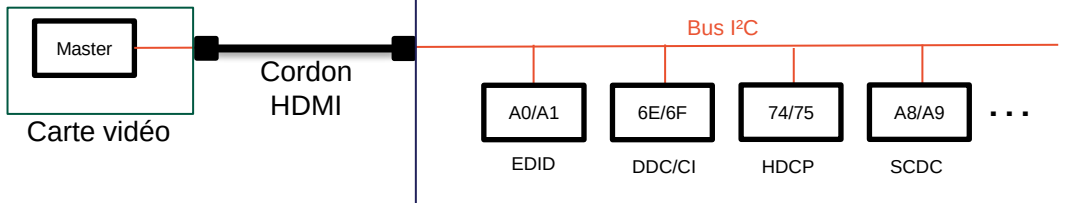
DDC : *Display Data Channel 1/2*

Bus bidirectionnel I²C

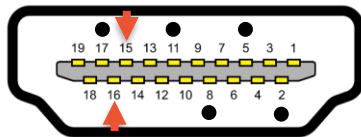
Hérité du VGA

La carte vidéo est le maître du bus

L'écran intègre un ou plusieurs esclaves :



- EDID : Extended Display Identification Data (A0/A1 & A4/A5)
 - Mémoire flash I²C contenant une structure de données qui décrit l'écran (dimensions, résolutions supportées, fonctionnalités disponibles, constructeur, etc.)
 - Normalement uniquement lu (mais parfois réinscriptible !)
- DDC/CI : Display Data Channel/Command Interface (6E/6F)
 - Permet de contrôler les fonctions du moniteur (luminosité, contraste, corrections de couleur, etc.)
- HDCP : High-bandwidth Digital Content Protection (74/75 & 76/77)
 - Interface d'échange de clefs pour le HDCP
- SCDC : Status and Control Data Channel (A8/A9) (HDMI 1.4b)
 - Nouvelle interface de contrôle et de configuration HDMI (encodage TMDS (3D, audio, etc.), détection d'erreurs, latence A/V)
- Certains écrans supportent une mise à jour de leur firmware via l'interface DDC (méthode propriétaire)
 - Reflash du firmware d'un écran Dell par DDC (encapsulé en USB à travers le Hub intégré de l'écran) : Ang Cui DEFCON 24 (2016)



DDC : *Display Data Channel 2/2*

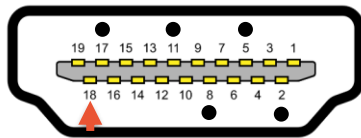
De toutes ces fonctions, seul l'EDID joue un rôle important pour la compatibilité

La structure de données peut avoir une taille comprise entre 128 octets et 32ko

La plupart du temps, l'EDID fait 256 octets

Le bus I²C portant le DDC ne traverse pas le filtre

L'EDID étant une structure statique, elle va être recopiée dans une mémoire I²C intégrée au filtre
La protection en écriture des données du filtre sera assurée par un interrupteur physique



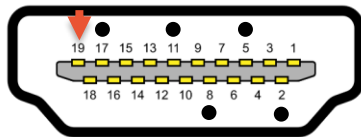
+5V DC

- La carte vidéo fournit une tension continue de +5V, avec un courant maximum de 50mA
- Permet d'alimenter la mémoire I²C de l'écran et de lire l'EDID via le DDC même lorsque l'écran n'est pas sous tension

Permet d'alimenter le filtre

Par défaut, le fil est coupé vers l'écran
Cependant, certains systèmes (systèmes de visioconférence, projecteurs) exigent la présence du +5V pour détecter la source.

Un interrupteur manuel sera utilisé pour laisser passer ou non le +5V



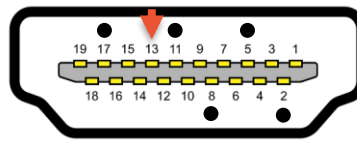
HDP : *Hot Plug Detect*

- Permet à la carte vidéo de détecter le branchement de l'écran
- L'activation du HPD déclenche la lecture de l'EDID
- Implémenté par un pull-up de 1kOhm sur le +5V dans l'écran
- Ce fil est également partagé avec d'autres fonctions (HEAC- et MHL)

Le pull-up est implanté
dans le filtre

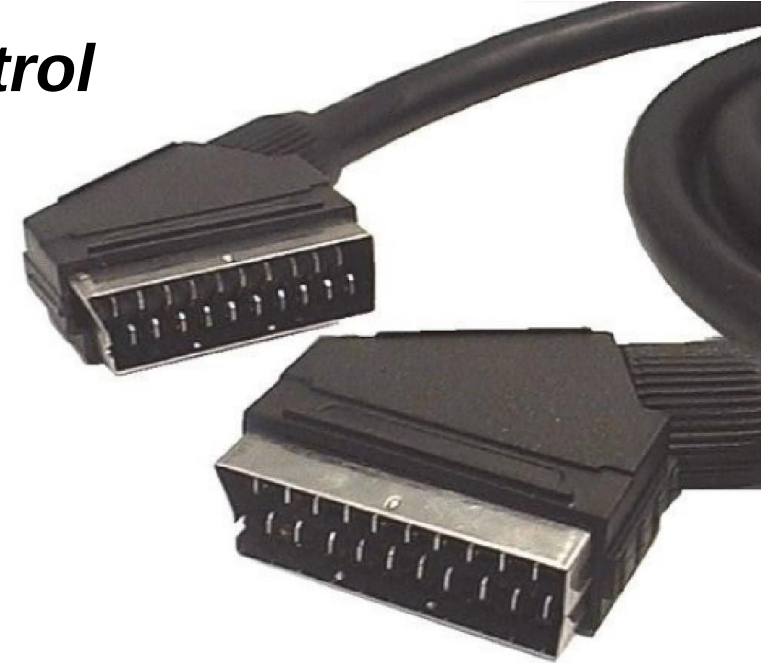
Ce signal n'est
pas relié à
l'écran



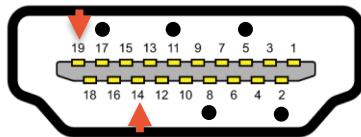


CEC : *Consumer Electronics Control*

- Bus bidirectionnel AV.link, utilisant un seul fil
- Bas débit (417 bits/s)
- Apparu originalement dans les prises PERITEL
- Permet le contrôle à distance des appareils audiovisuels (centralisation de la télécommande de tous les appareils A/V depuis l'un d'entre eux)
- Utilisé pour négocier HEAC



Ce signal ne
traverse pas le
filtre

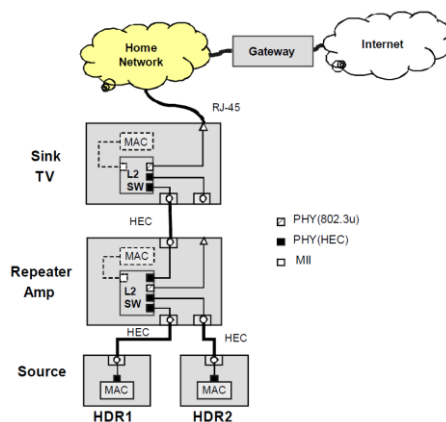
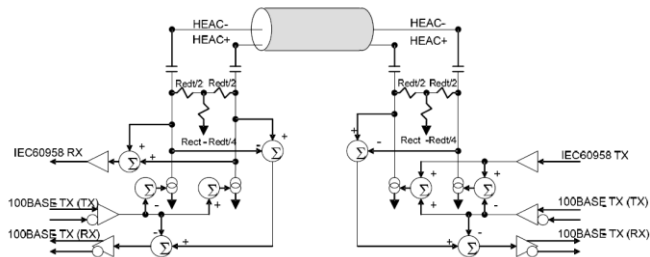


HEAC : *HDMI Ethernet and Audio return Channel*

- Deux fils, dont un des deux (HEAC-) est partagé avec Hot Plug Detect
- **ARC : Audio Return Channel**
 - Permet de faire revenir de l'audio numérique depuis l'écran vers la carte vidéo (par exemple un microphone, une app de Smart-TV, un amplificateur audio/vidéo)
 - Utilise la paire en mode commun (ou uniquement le fil HEAC+) et transmet des données au format S/PDIF
- **HEC : HDMI Ethernet Channel**
 - Ethernet 100BASE-TX (Full-Duplex)
 - Utilise la paire en mode différentiel
 - Le signal ARC peut être superposé au signal HEC
 - Utilise CEC pour négocier la capacité

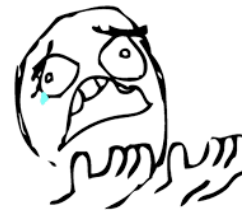
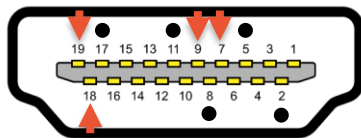
HDMI Source Device

HDMI Sink Device



- PHY(802.3u)
- PHY(HEC)
- MII

Ce signal ne traverse pas le filtre



MHL : *Mobile High-definition Link*

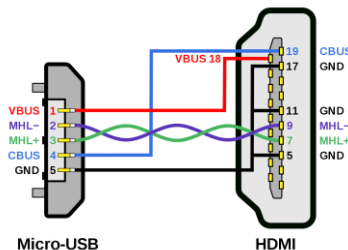
Un protocole qui n'a rien à voir avec HDMI, qui relie un micro-USB avec un HDMI

Permet d'utiliser un objet mobile compatible MHL comme source pour un écran compatible MHL

- CBUS : canal de contrôle bidirectionnel
 - Encapsule DDC et CEC, via le MSC (MHL Sideband Channel) (contrôle du téléphone par une télécommande IR)
- VBUS : permet de recharger le mobile (4,5W/900mA)
 - Alimentation dans le sens inverse de celui du HDMI
- Paire différentielle haut débit (TMDS)
 - Vidéo et audio (format multiplexé spécifique au MHL)
 - Unidirectionnel

Le signal CBUS ne traverse
pas le filtre
MHL ne pourra pas fonctionner

Existe aussi en USB-C (SuperMHL)



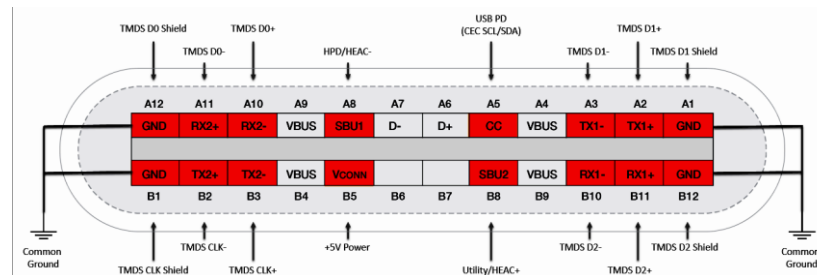
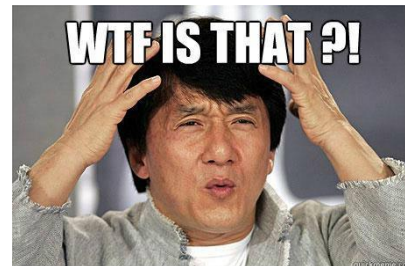
HDMI Alternate Mode

HDMI routé dans un connecteur USB-C

Signaux présents :

- TMDS (R,G,B,Clock)
- +5V, Hot Plug Detect
- HEAC (ARC et/ou HEC)
- DDC et CEC encapsulés dans USB-PD sur le fil CC
 - USB-PD : Power Delivery, CC=Configuration Channel

Le câble contient un composant (nœud USB-PD) qui décapsule DDC et CEC vers l'extrémité HDMI



Le filtre est efficace,
car l'extrémité HDMI du câble reste standard



Cas d'un câble DVI

Si l'on utilise le filtre sur un câble DVI-HDMI ou avec un adaptateur DVI-HDMI

Un câble DVI peut contenir :

- 7 paires TMDS (R1, G1, B1, R2, G2, B2, Clock)
 - Seule la première voie et l'horloge passent en HDMI (4 paires)
- Les signaux VGA analogiques (R, G, B, Vsync, Hsync)
 - N'existent pas en HDMI
- +5V et Hot Plug Detect
- DDC (EDID, HDCP et DDC/CI)

Le filtre reste efficace dans ce scénario,
mais le signal analogique (DVI-A) ne pourra pas
passer, ni la deuxième voie DVI

HDCP : *High-bandwidth Digital Content Protection*

HDCP est un DRM qui protège les contenus numériques haute définition, dont l'activation peut être un prérequis pour le visionnage de médias haute définition (Blu-ray, streaming, etc.)

Un échange de clef cryptographique est réalisé via le bus DDC

Les clefs de session sont utilisées pour chiffrer le flux TMDS

Le filtre bloque DDC, aucun échange de clef n'est possible
HDCP ne pourra pas s'activer
Certains contenus protégés ne pourront donc pas être visualisés à travers le filtre

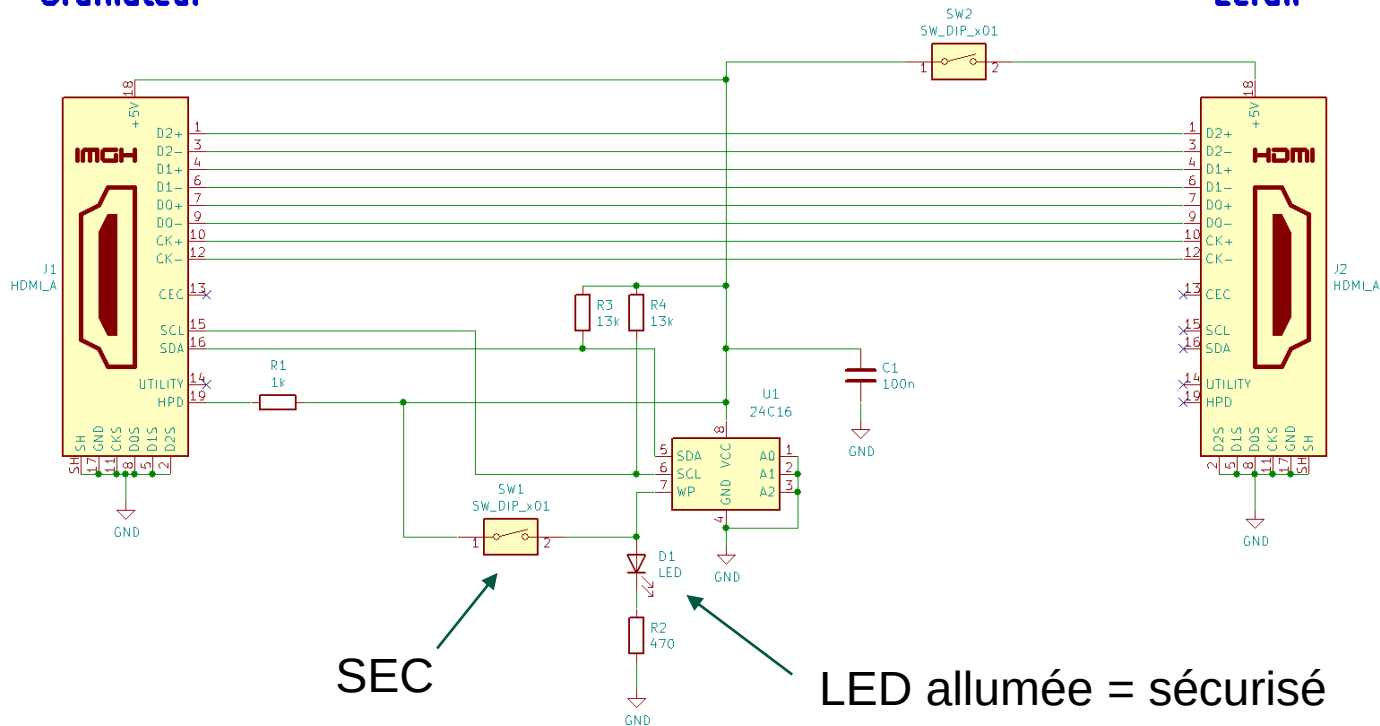


Schématique du filtre

Ordinateur

M/A

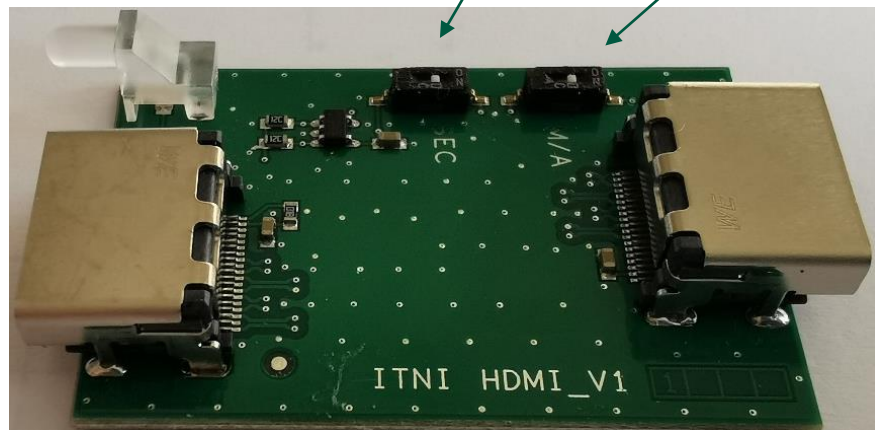
Ecran



Réalisation

SEC

M/A



Exemple de réalisation par la société ITNI

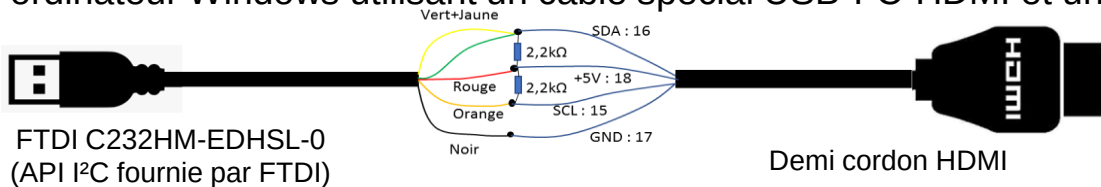
Process de programmation

Pour installer le filtre il faut :

- Lire l'EDID de l'écran qui va être équipé
- Ecrire l'EDID dans le filtre (position SEC OFF)
- Installer le filtre (SEC ON) et vérifier la compatibilité (éventuellement M/A ON)

Le programmeur permettant de lire et écrire l'EDID peut être :

- Un ordinateur Linux utilisant l'interface I²C de la carte vidéo
 - `modprobe i2c-dev`
 - `python-smbus python3-smbus i2c-tools edid-decode`
 - <https://github.com/bulletmark/edid-rw>
- Un ordinateur Windows utilisant un câble spécial USB-I²C-HDMI et un logiciel ad-hoc



Conclusion et idées

Une surface d'attaque sous estimée existe dans le standard HDMI

Une solution simple est proposée pour sécuriser un écran ou un projecteur partagé

- Le HDMI se prête très bien à l'exercice

Le concept peut s'étendre à d'autres interfaces, pour réduire leur champ fonctionnel :

- USB2 : Inspection et filtrage du flux, par exemple pour bloquer les rubber-duckies (e.g. Armadillo)
- USB-C : USB3+DisplayPort+MHL+HDMI+VirtualLink+Thunderbolt(PCIe)+Power Delivery
 - Le Configuration Channel semble être le meilleur point de contrôle, à un débit raisonnable
- DisplayPort : Inspection et filtrage du AUX CH, qui encapsule DDC, CEC, et qui peut transporter beaucoup d'autres choses (même de l'USB2 !)

La tendance de l'industrie est de multiplexer des protocoles, et d'empiler les couches protocolaires

Les signaux sont très rapides, mais les interfaces de configuration sont souvent beaucoup plus lentes et accessibles, ce qui facilite la réalisation de filtres fonctionnels